WTI Part No. 13851
Rev. B

RSM-8R4 Series

Remote Site Manager with Power Control

Models Covered:

RSM-8R4-1
RSM-8R4-2

User's Guide

Warnings and Cautions:
Installation Instructions

Secure Racking

If Secure Racked units are installed in a closed or multi-unit rack assembly, they may require further evaluation by Certification Agencies. The following items must be considered.

1. The ambient within the rack may be greater than room ambient. Installation should be such that the amount of air flow required for safe operation is not compromised. The maximum temperature for the equipment in this environment is 45°C. Consideration should be given to the maximum rated ambient.
2. Installation should be such that a hazardous stability condition is not achieved due to uneven loading.

Input Supply

Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.

Grounding

Reliable earthing of this equipment must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than direct connections to the branch circuit.

No Serviceable Parts Inside; Authorized Service Personnel Only

Do not attempt to repair or service this device yourself. Internal components must be serviced by authorized personnel only.

- **Shock Hazard - Do Not Enter**
- **Lithium Battery**
  CAUTION: Danger of explosion if battery is incorrectly replaced. Replace only with same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Disconnect Power

If any of the following events are noted, immediately disconnect the unit from the outlet and contact qualified service personnel:

1. If the power cord becomes frayed or damaged.
2. If liquid has been spilled into the device or if the device has been exposed to rain or water.

Disconnect Power Before Servicing

Before attempting to service or remove this unit, please make certain to disconnect the power supply cable from the power source.

Agency Approvals

FCC Part 15 Regulation

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation

WARNING: ***Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment***

EMC, Safety, and R&TTE Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:

- **Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility;**

  and

- **Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;**

  and

- **Council Directive 1999/5/EC of 9 March on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.**

Industry Canada - EMI Information

This Class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications

The Ringer Equivalence Number is an indication of the maximum number of devices allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices does not exceed five.

Table of Contents

List of Figures

1. Introduction

WTI's RSM-8R4 Remote Site Manager + Power Control unit allows secure, remote monitoring and management of AC powered rack mount equipment via SSL, SSH, SNMP, web browser, telnet, internal modem or local terminal. The RSM-8R4 allows you to connect to console ports on rack mounted devices, switch and reboot power, monitor equipment temperature and can automatically notify you when changes in temperature or response to ping commands exceeds user-defined threshold values.

The RSM-8R4 features eight serial ports for connection to rack mount devices, four user-switchable power outlets, an internal modem, and a convenient package of security and authentication features to provide secure, remote control and monitoring of your equipment rack.

Security and Co-Location Features:

Secure Shell (SSHv2) encryption and address-specific IP security masks help to prevent unauthorized access to command and configuration functions.

The RSM-8R4 also provides four different levels of security for user accounts: Administrator, SuperUser, User and ViewOnly. The Administrator level provides complete access to all serial port and switched plug functions, status displays and configuration menus. The SuperUser level allows control of serial ports and plugs, but does not allow access to configuration functions. The User level allows access to only a select group of Administrator-defined serial ports and plugs. The ViewOnly level allows you to check unit status, but does not allow control of serial ports or switched outlets or access to configuration menus.

The RSM-8R4 includes full Radius, LDAP and TACACS capability, DHCP and an invalid access lockout feature. An Audit Log records all user access, login and logout times and command actions, and an Alarm Log records user-defined alarm events.

Environmental Monitoring and Management:

The RSM-8R4 can constantly monitor temperature levels, ping response and other factors. If the RSM-8R4 detects that user defined thresholds for these values have been exceeded, the unit can promptly notify you via email, SNMP, or Syslog. When temperature readings exceed user-defined critical values, the RSM-8R4 can also intelligently decrease the amount of heat being generated within the rack by temporarily shutting down nonessential devices; when readings return to acceptable levels, the RSM-8R4 can restore power to those devices to return to normal operating conditions. The RSM-8R4 also records temperature readings to a convenient log file.

If you need to switch power to rack mount devices at a specific time of the day or week, the RSM-8R4 also includes a Scheduled Power Management feature, that allows you to define a daily or weekly schedule for switching each outlet off or on, or even rebooting that outlet.

The RSM-8R4 can also notify you when excessive invalid access attempts are detected, and can automatically lock ports when it determines that an unauthorized user may be attempting to gain access by "hammering" the unit with random passwords.

Model Numbers

The RSM-8R4 series includes both 120 VAC and 240 VAC models to accommodate a variety of data center applications and power distribution needs.

- **Model RSM-8R4-1:** 120 VAC, 4 ea. NEMA 5-15R Outlets, 8 ea. RJ45 Serial Ports, Internal Modem.
- **Model RSM-8R4-2:** 240 VAC, 4 ea. IEC320-C13 Outlets, 8 ea. RJ45 Serial Ports, Internal Modem.

Typographic Conventions

^ (e.g. **^X**)	Indicates a control character. For example, the text "**^X**" (Control X) indicates the **[Ctrl]** key and the **[X]** key must be pressed simultaneously.
`COURIER FONT`	Indicates characters typed on the keyboard. For example, **`/RB`** or **`/ON 2`**.
[Bold Font]	Text set in bold face and enclosed in square brackets, indicates a specific key. For example, **[Enter]** or **[Esc]**.
< >	Indicates required keyboard entries: For Example: **`/P <n>`**.
[ ]	Indicates optional keyboard entries. For Example: **`/P [n]`**.

2. Unit Description

2.1. Front Panel

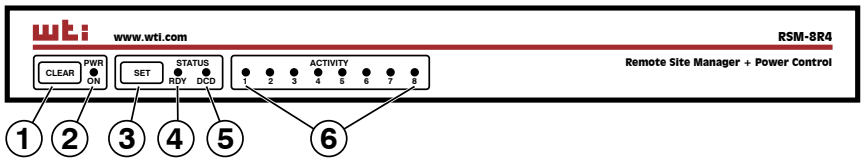

Figure 2.1: Front Panel

As shown in Figure 2.1, the RSM-8R4 Front Panel includes the following components:

① **CLEAR Button:** Restarts the RSM-8R4 as described in Section 2.3.

② **Power On Indicator:** An LED Indicator which lights when AC Power is applied to the unit.

③ **SET Button:** Switches all plugs Off or sets plugs to default values as described in Section 2.3.

④ **RDY Indicator:** (Ready) Flashes to indicate that the unit is ready to receive commands.

⑤ **DCD Indicator:** The Data Carrier Detect indicator.

⑥ **Activity Indicators:** A series of LEDs, which light to indicate data activity at the corresponding RSM-8R4 Serial Port.

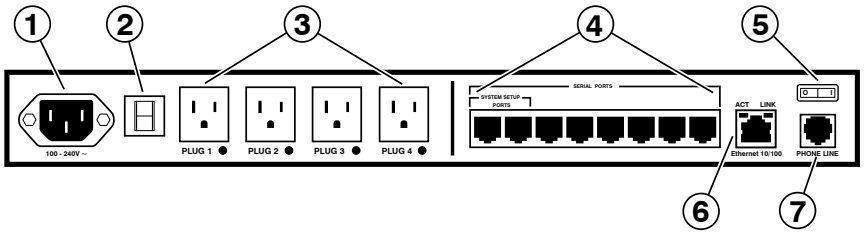

Figure 2.2: RSM-8R4-1 - Back Panel

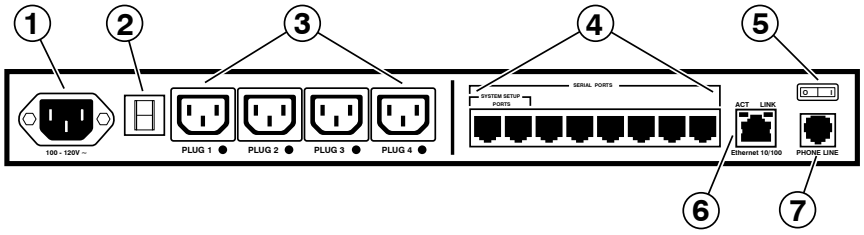

Figure 2.3: RSM-8R4-2 - Back Panel

2.2. Back Panel Components

As shown in Figures 2.2 and 2.3, the RSM-8R4 Back Panel includes the following components:

① **Power Inlet:** An IEC320-C20 AC inlet which supplies power to the RSM-8R4's control functions and switched power outlets. Also includes cable keeper (not shown.)

② **Circuit Breaker:** The circuit breaker is rated as follows:

- **RSM-8R4-1:** 15 Amp Circuit Breaker.
- **RSM-8R4-2:** 10 Amp Circuit Breaker.

③ **Switched Outlets:** Four AC Outlets that can be switched On, Off or rebooted in response to user commands:

- **RSM-8R4-1:** Four (4) each, NEMA 5-20R Outlets.
- **RSM-8R4-2:** Four (4) each, IEC320-C13 Outlets.

④ **Serial Ports:** For connection to console ports on target devices. Standard RJ45 connectors configured as DTE ports. For more information on connecting devices to the serial ports, please refer to Section 4.5. For a description of the serial port interface, please refer to Appendix A.1.

⑤ **Power On/Off Switch**

⑥ **Network Port:** An RJ45 Ethernet port for connection to your 10Base-T or 100Base-T, TCP/IP network. Note that the RSM-8R4 features a default IP address (192.168.168.168). This allows you to connect to the unit without first assigning an IP address. Note that the Network Port also includes two, small LED indicators for Link and Data Activity. For more information on Network Port configuration, please refer to Section 5.9.

⑦ **Internal Modem Port:** For connection to your external phone line. For more information on Modem Port configuration, please refer to Section 5.8.

2.3. Front Panel Button Functions

The CLEAR and SET buttons can be used to perform several functions described below:

Note: *Front Panel button functions can also be disabled via the System Parameters menu, as described in Section 5.3.*

1. **Reboot Operating System - Keep User-Defined Parameters:**

   a) Press and hold the CLEAR button for five seconds, and then release it.

   b) The RSM-8R4 operating system will reboot ; all user-defined parameters will be retained.

2. **Reboot Operating System - Reset All Parameters to Factory Defaults:**

Notes:

- *When the RSM-8R4 is reset to factory defaults, all user-defined configuration parameters will be cleared.*
- *The default "super" user account will also be restored.*

   a) Simultaneously press both the SET button and the CLEAR button, hold them for five seconds, and then release them.

   b) The RSM-8R4 operating system will reboot; all user-defined parameters will be reset to factory default settings.

3. Getting Started

This Quick Start routine describes a simplified installation procedure for the RSM-8R4 hardware, which will allow you to communicate with the unit in order to demonstrate basic features and check for proper operation.

Note that this Quick Start routine does not provide a detailed description of unit configuration, or discuss advanced operating features in detail. For more information, please refer to the remainder of this User's Guide

3.1. Apply Power to the RSM-8R4

Refer to the safety precautions listed at the beginning of this User's Guide, and then connect the unit to an appropriate power source. Connect the power supply cable to the unit's power inlet, snap the Cable Keeper into place, and then connect the cable to an appropriate power supply. Please refer to the table below for information concerning power requirements and maximum load.

Model No.	Total Outlets	Input Voltage	Input Feed	Max. Load
RSM-8R4-1	4	100 to 120 VAC	15 Amp	12 Amps*
RSM-8R4-2	4	100 to 240 VAC	10 Amp	10 Amps

* In accordance with UL requirements for branch circuits, this value has been de-rated to 80%.

When power is applied to the RSM-8R4, the ON LED on the instrument front panel should light, and the RDY LED should begin to flash within 90 seconds. This indicates that the unit is ready to receive commands.

3.2. Connect Your PC to the RSM-8R4

The RSM-8R4 can either be controlled by a local PC Serial Port, controlled via modem, or controlled via TCP/IP network. In order to select parameters, connect ports or control outlets, commands are issued to the RSM-8R4 via either the Network Port, Modem Port or Serial Setup Port.

- **Network Port:** Connect the your 10Base-T or 100Base-T network interface to the RSM-8R4 10/100Base-T Network Port.
- **Serial Port:** Use the supplied Ethernet cable and RJ45 to DB-9 adapter to connect your PC COM port to Serial Port 1 (the System SetUp Ports). For a description of the Serial Port Interface, please refer to Appendix A.1.
- **Modem:** Connect your telephone line to the RSM-8R4 Phone Line Port.

3.3. Communicating with the RSM-8R4

When properly installed and configured, the RSM-8R4 will allow command mode access via Telnet, Web Browser, SSH client, modem, or local PC. However, in order to ensure security, both Telnet and Web Browser access are disabled in the default state. To enable Telnet and/or Web Browser access, please refer to the RSM-8R4 User's Guide.

Notes:

- *Default RSM-8R4 serial port parameters are set as follows: 9600 bps, RTS/CTS Handshaking, 8 Data Bits, One Stop Bit, No Parity. Although these parameters can be easily redefined, for this Quick Start procedure, it is recommended to configure your communications program to accept the default parameters.*
- *The RSM-8R4 features a default IP Address (192.168.168.168) and a default Subnet Mask (255.255.255.0.) This allows network access to command mode, providing that you are contacting the RSM-8R4 from a node on the same subnet. When attempting to access the RSM-8R4 from a node that is not on the same subnet, please refer to the User's Guide for further configuration instructions.*

1. **Access Command Mode:** The RSM-8R4 includes two separate user interfaces; the Text Interface and the Web Browser Interface. The Text Interface is available via Local PC, SSH Client, Telnet, or Modem and can be used to both configure the RSM-8R4 and create connections between ports. The Web Browser interface is only available via TCP/IP network, and can be used to configure the unit, but cannot create connections between ports.

   a) **Via Local PC:** Start your communications program and then press **[Enter]**.

   b) **Via SSH Client:** Start your SSH client, enter the default IP address (192.168.168.168) for the RSM-8R4 and invoke the connect command.

   c) **Via Web Browser:** Make certain that Web Browser access is enabled as described in the RSM-8R4 User's Guide. Start your JavaScript enabled Web Browser, enter the default RSM-8R4 IP address (192.169.168.168) in the Web Browser address bar, and then press **[Enter]**.

   d) **Via Telnet:** Make certain that Telnet access is enabled as described in the RSM-8R4 User's Guide. Start your Telnet client, and enter the RSM-8R4's default IP address (192.168.168.168).

   e) **Via Modem:** Use your communications program to dial the number for the line connected to the RSM-8R4's Phone Line port.

2. **Username** / **Password Prompt:** A message will be displayed, which prompts you to enter your username (Login) and password.. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**". If a valid username and password are entered, the RSM-8R4 will display either the Main Menu (Web Browser Interface) or the Port Status Screen (SSH, Telnet, or Modem.)

3. **Review Help Menu:** If you are communicating with the RSM-8R4 via the text interface (SSH, Telnet or Modem), type **/H** and press **[Enter]** to display the Help Menu, which lists all available RSM-8R4 commands. Note that the Help Menu is not available via the Web Browser Interface.

3.4. Connecting Ports and Switching Outlets

Although both the Text Interface and Web Browser Interface allow you to select configuration parameters, the Text Interface is always used when invoking commands to connect ports. If you have previously accessed command mode via the Web Browser Interface, exit command mode (log out), then re-enter command mode using the Text Interface as described in Section 3.3.

Proceed as follows to connect ports and switch outlets:

1. **Review the Help Menu:** At the Text Interface command prompt, type **/H** and press **[Enter]** to display the Help Menu, which provides a basic listing of all available RSM-8R4 commands.

2. **Creating Connections Between Ports:** The RSM-8R4 can perform two different types of port connections; Resident Connections and Third Party Connections:

   a) **Resident Connection:** Your resident port issues a /C command to connect to a second port.

      i. To connect your resident port to Port 3, type **/C 3 [Enter]**. While you are connected to Port 3, the unit will not recognize additional commands issued via your resident port. However, the unit will recognize a Resident Disconnect Sequence issued at either connected port.

      ii. Issue the Resident Disconnect Sequence (Logoff Sequence); type **^X** (press **[Ctrl]** and **[X]** at the same time).

   b) **Third Party Connection:** Your resident port issues a /C command to create a connection between two other ports.

      i. To connect Port 3 to Port 4, type **/C 3 4 [Enter]**.

      ii. While Ports 3 and 4 are connected, your resident port will still recognize commands. Type **/S [Enter]** to display the Status Screen. The "STATUS" column should now list Ports 3 and 4 as connected and the other ports as "Free".

      iii. Issue a Third Party Disconnect command; type **/D 3 [Enter]**. The unit will display the "Are you Sure (y/n)?" prompt. Type **Y** and press **[Enter]** to disconnect.

      iv. Type **/S [Enter]** to display the Status Screen. The "STATUS" column should now list Ports 3 and 4 as "Free".

3. **Controlling Outlets:** You may wish to perform the following tests in order to make certain that the switched outlets are functioning properly.

   a) **Reboot Outlet:** At the command prompt, type **`/BOOT 1`** and press **[Enter]**. The status indicator for Plug 1 should go Off, pause for a moment and then go back On, indicating that the boot cycle has been successfully completed.

   b) **Switch Outlet Off:** At the command prompt, type **`/OFF 1`** and then press **[Enter]**. The status indicator for Plug 1 should go Off, indicating that the command has been successfully completed. Leave Plug 1 in the "Off" state, and then proceed to the next step.

   c) **Switch Outlet On:** At the command prompt, type **`/ON 1`** and press **[Enter]**. The status indicator for Plug 1 should then go back On, indicating that the command has been successfully completed.

4. **Exit Command Mode:** To exit command mode, type **`/X`** and press **[Enter]**.

This completes the Quick Start instructions for the RSM-8R4. Prior to placing the unit into operation, it is recommended to refer to the remainder of this user's guide for important information regarding advanced configuration capabilities and more detailed operation instructions.

4. Hardware Installation

4.1. Connecting the Power Supply Cables

4.1.1. Installing the Power Supply Cable Keeper

The RSM-8R4 includes a cable keeper, which is designed to prevent the power supply cable from being accidentally disconnected from the unit.

When attaching the power supply cable to the unit, first swing the cable keeper out of the way, then plug the power cable securely into the power input. When the cable is in place, snap the cable keeper over the plug to secure the cable to the unit.

4.1.2. Connect the RSM-8R4 to Your Power Supply

Refer to the cautions listed below and at the beginning of this User's Guide, and then connect the RSM-8R4 unit to an appropriate power supply.

 **CAUTIONS:** 

- ***Before attempting to install this unit, please review the warnings and cautions listed at the front of the user's guide.***
- ***This device should only be operated with the type of power source indicated on the instrument nameplate. If you are not sure of the type of power service available, please contact your local power company.***
- ***Reliable earthing (grounding) of this unit must be maintained. Particular attention should be given to supply connections when connecting to power strips, rather than directly to the branch circuit.***

4.2. Connecting the Network Cable

The Network Port is an RJ45 Ethernet jack, for connection to a TCP/IP network. Connect your 100Base-T cable to the Network Port. Note that the RSM-8R4 includes a default IP address (192.168.168.168) and a default subnet mask (255.255.255.0.) When installing the RSM-8R4 in a working network environment, it is recommended to define network parameters as described in Section 5.9.

4.3. The Internal Modem Port

If you wish to use the RSM-8R4's internal modem in your application, connect an RJ11 phone line to the Internal Modem port, located on the RSM-8R4 back panel. For information on Modem Port configuration, please refer to Section 5.8. Note that an external modem can also be connected to the RSM-8R4 serial ports as described in Section 4.5.

4.4. Connection to Switched Outlets

Connect the power cord from your switched device to one of the AC Outlets located on the RSM-8R4 back panel. Note that when power is applied to the RSM-8R4, the AC Outlets will be switched "ON" by default.

Maximum power ratings are summarized in the table below:

Model No.	Total Outlets	Input Voltage	Input Feed	Maximum Load
RSM-8R4-1	4	100 to 120 VAC	15 Amp	12 Amps*
RSM-8R4-2	4	100 to 240 VAC	10 Amp	10 Amps

* In accordance with UL requirements for branch circuits, this value has been derated to 80%.

4.5. Connecting Devices to the RSM-8R4 Serial Ports

The RSM-8R4 serial ports are female RS232 format RJ45 connectors, wired in a DTE configuration. In the default state, the serial ports are configured for 9600 bps, no parity, 8 data bits, 1 stop bit. For a description of the serial port interface, please refer to Appendix A.

When properly configured, the serial ports can be connected to almost any device that includes an RS232 console port. In addition, the serial ports can also be used to allow local users to configure and control the RSM-8R4 unit; Ports 1 is designated as a "Set Up Port", and accordingly cannot be reconfigured as a buffer mode or passive mode port in order to ensure the port's availability for local communication with the RSM-8R4.

1. Determine which RSM-8R4 serial port will be used for connection to the new device (e.g. Port 3).
2. Use the supplied Ethernet Cable and RJ45 to DB9 Adapter to connect the COM port on your PC to Serial Port 1 on the RSM-8R4 unit.
    a) To connect external modems, router switches, or other DTE and DCE devices to the RSM-8R4 serial ports, please refer to the interface descriptions in Appendices A.1 through A.5.
3. Access the RSM-8R4 command mode and select communication parameters for each serial port as described in Section 5.8.

This completes the RSM-8R4 installation instructions. Please proceed to the next Section for instructions regarding basic unit configuration.

5. Basic Configuration

This section describes the basic configuration procedure for all RSM-8R4 units. For more information on Reboot Options and Alarm Configuration, please refer to Section 6 and Section 7.

5.1. Communicating with the RSM-8R4 Unit

In order to configure the RSM-8R4, you must first connect to the unit, and access command mode. Note that, the RSM-8R4 offers two separate configuration interfaces; the Web Browser Interface and the Text Interface. In addition, the RSM-8R4 also offers three different methods for accessing command mode; via network, via modem, or via local console. The Web Browser interface is only available via network, and the Text Interface is available via network (SSH or Telnet), modem or local PC.

5.1.1. The Text Interface

The Text Interface (also known as the "Command Line Interface" or "CLI") consists of a series of simple ASCII text menus, which allow you to set options and define parameters by entering the number for the desired option using your keyboard, and then typing in the value for that option.

Since the Web Browser Interface and Telnet accessibility are both disabled in the default state, you will need to use the Text Interface to contact the unit via Local PC or SSH connection when setting up the unit for the first time. After you have accessed command mode using the Text Interface, you can then enable Web Access and Telnet Access, if desired, in order to allow future communication with the unit via Web Browser or Telnet. You will not be able to contact the unit via Web Browser or Telnet until you have specifically enabled those options.

Once Telnet Access is enabled, you will then be able to use the Text Interface to communicate with the RSM-8R4 via local PC, Telnet or SSH connection. You can also use the Text Interface to access command mode via an external modem installed at one of the RSM-8R4's serial ports.

In order to use the Text Interface, your installation must include:

- **Access via Network:** The RSM-8R4 must be connected to your TCP/IP Network, and your PC must include a communications program (such as HyperTerminal.)
- **Access via Modem:** A phone line must be connected to the RSM-8R4's internal modem. In addition, your PC must include a communications program.
- **Access via Local PC:** Your PC must be connected to an RSM-8R4 Serial Port, the Serial Port must be configured for Any-to-Any Mode, and your PC must include a communications program. Serial Port 1 is designated as a Set Up Port, and by default, is configured for communication with a local control device. Note that Serial Port 2 can also function as a Set Up Port, providing that you have not reconfigured Port Mode or Administrator Access at that port.

To access command mode via the Text Interface, proceed as follows:

> **Note:** *When communicating with the unit for the first time, you will not be able to contact the unit via Telnet, until you have accessed command mode, via Local PC or SSH Client, and used the Network Parameters Menu to enable Telnet as described in Section 5.9.*

1. Contact the RSM-8R4 Unit:

   a) **Via Local PC:** Start your communications program and press **[Enter]**. Wait for the connect message, then proceed to Step 2.

   b) **Via Network:** The RSM-8R4 includes a default IP address (192.168.168.168) and a default subnet mask (255.255.255.0.) This allows you to contact the unit from any network node on the same subnet, without first assigning an IP Address to the unit. For more information, please refer to Section 5.9.

      i. **Via SSH Client:** Start your SSH client, and enter the RSM-8R4's IP Address. Invoke the connect command, wait for the connect message, then proceed to Step 2.

      ii. **Via Telnet:** Start your Telnet Client, and then Telnet to the RSM-8R4's IP Address. Wait for the connect message, then proceed to Step 2.

   c) **Via Modem:** Use your communications program to dial the number for the phone line that you have connected to the RSM-8R4's internal modem port.

2. **Login** / **Password Prompt:** A message will be displayed, which prompts you to enter a username (login name) and password. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**".

3. If a valid username and password are entered, the RSM-8R4 will display the Port and Plug Status Screen, shown in Figure 5.1.

```
Remote Site Manager + Power Control  Site ID: (undefined)

PORT |       NAME       |    USERNAME      | STATUS |  MODE  | BUFFER COUNT
-----+------------------+------------------+--------+--------+--------------
 01  | (undefined)       |                  |  Free  |  Any   |            0|
 02  | (undefined)       |                  |  Free  |  Any   |            0|
 03  | (undefined)       |                  |  Free  |  Pass  |            0|
 04  | (undefined)       |                  |  Free  |  Pass  |            0|
 05  | (undefined)       |                  |  Free  |  Pass  |            0|
 06  | (undefined)       |                  |  Free  |  Pass  |            0|
 07  | (undefined)       |                  |  Free  |  Pass  |            0|
 08  | (undefined)       |                  |  Free  |  Pass  |            0|
 09  | MODEM             |                  |  Free  |  Modem |            0|

PLUG |           NAME            | STATUS | BOOT DELAY | DEFAULT | PRIORITY
-----+---------------------------+--------+------------+---------+----------
 1   | Outlet1                   |  ON    |  0.5 Secs  |   OFF   |    1     |
 2   | Outlet2                   |  ON    |  0.5 Secs  |   OFF   |    2     |
 3   | Outlet3                   |  ON    |  0.5 Secs  |   OFF   |    3     |
 4   | Outlet4                   |  ON    |  0.5 Secs  |   OFF   |    4     |
* = Plug in BUSY state           System Temperature: 59F

Enter /H for command menu.
RSM>
```

Figure 5.1: The Port and Plug Status Screen

5.1.2. The Web Browser Interface

The Web Browser Interface consists of a series of web forms, which can be used to select configuration parameters and perform reboot operations, by clicking on radio buttons and/or entering text into designated fields.

> **Note:** *In order to use the Web Browser Interface, Web Access must first be enabled via the Text Interface Network Parameters Menu (/N), the RSM-8R4 must be connected to a TCP/IP network, and your PC must be equipped with a JavaScript enabled web browser.*

1. Start your JavaScript enabled Web Browser, key the RSM-8R4's IP address (default = 192.168.168.168) into the web browser's address bar, and press **[Enter]**.
2. **Username** / **Password Prompt:** A message box will prompt you to enter your username and password. The default username is "**`super`**" (all lower case, no quotes), and the default password is also "**`super`**".
3. If a valid username and password are entered, the RSM-8R4 Home Screen will appear as shown in Figure 5.2.

Figure 5.2: The Home Screen (Web Browser Interface)

5.1.3. Access Via PDA

In addition to the Web Browser Interface and Text Interface, the RSM-8R4 command mode can also be accessed by PDA devices. Note however, that due to nature of most PDAs, only a limited selection of RSM-8R4 operating and status display functions are available to users who communicate with the unit via PDA.

When the RSM-8R4 is operated via a PDA, only the following functions are available:

- Plug Status Screen (Section 8.2)
- Plug Group Status Screen (Section 8.3)
- Plug Control Screen (Section 9.1.1)
- Plug Group Control Screen (Section 9.1.2)
- Unit Info (Shows Site I.D. message and firmware version.)

For more information on these functions, please refer to the appropriate section listed next to each function in the list above.

These screens will allow PDA users to review Plug Status and Plug Group Status, invoke power switching and reboot commands and display the Site I.D. and firmware version. Note however, that PDA users are not allowed to change or review RSM-8R4 configuration parameters.

To configure the RSM-8R4 for access via PDA, first consult your IT department for appropriate settings. Access the RSM-8R4 command mode via the Text Interface or Web Browser interface as described in this section, then configure the RSM-8R4's Network Port accordingly, as described in Section 5.9.

In most cases, this configuration will be adequate to allow communication with most PDAs. Note however, that if you wish to use a BlackBerry® to contact the RSM-8R4, you must first make certain to configure the BlackBerry to support HTML tables, as described below:

1. Power on the BlackBerry, and then click on the BlackBerry Internet Browser Icon.
2. Press the Menu button, and then choose "Options."
3. From the Options menu, choose "Browser Configuration," then verify to make certain that "Support HTML Tables" is checked (enabled.)
4. Press the Menu button, and select "Save Options."

When you have finished communicating with the RSM-8R4 via PDA, it is important to always close the session using the PDA's menu functions, rather than by simply closing the browser window, in order to ensure that the RSM-8R4 has completely exited from command mode, and is not waiting for the inactivity timeout period to elapse. For example, to close a session on a BlackBerry, press the Menu button and then choose "Close."

5.2. Configuration Menus

Although the Web Browser Interface and Text Interface provide two separate means for selecting parameters, both interfaces allow access to the same set of basic parameters, and parameters selected via one interface will also be applied to the other. To access the configuration menus, proceed as follows:

- **Text Interface:** Refer to the Help Screen (/H) and then enter the appropriate command to access the desired menu. When the configuration menu appears, key in the number for the parameter you wish to define, and follow the instructions in the resulting submenu.
- **Web Browser Interface:** Click the appropriate link on the left hand side of the screen (see Figure 5.2) to access the desired configuration menu. To change parameters, click in the desired field and key in the new value or select a value from the pull-down menu. To apply newly selected parameters, click on the "Change Parameters" button at the bottom of the menu or the "Set" button next to the field.

The following sections describe options and parameters that can be accessed via each of the configuration menus. Please note that essentially the same set of parameters and options are available to both the Web Browser Interface and Text Interface.

Notes:

- *Configuration menus are only available when you have logged into command mode using a password that permits Administrator Level commands. SuperUser accounts are able to view configuration menus, but are not allowed to change parameters.*
- *Configuration menus are not available when you are communicating with the RSM-8R4 via PDA*
- *When defining parameters via the Text Interface, make certain to press the **[Esc]** key several times to completely exit from the configuration menu and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message has been displayed and the cursor returns to the command prompt.*

```
SYSTEM PARAMETERS:

  1. User Directory
  2. Site-ID:                    (undefined)
  3. Real Time Clock:            02/12/2008 11:58:17
  4. Invalid Access Lockout:     On
  5. Command Confirmation:      On
  6. Automated Mode:             Off
  7. Temperature Format:         Fahrenheit
  8. Temperature Calibration     (undefined)
  9. Log Configuration
     21. Audit Log               On - Without Syslog
     22. Alarm Log               On - Without Syslog
     23. Temperature Log         On - Monthly
 10. Callback Security:          On - Callback (Without Password Prompt)
 11. Front Panel Buttons         On


Enter: #<CR> to change,
       <ESC> to exit and save configuration ...
```

Figure 5.3: The System Parameters Menu (Text Interface)

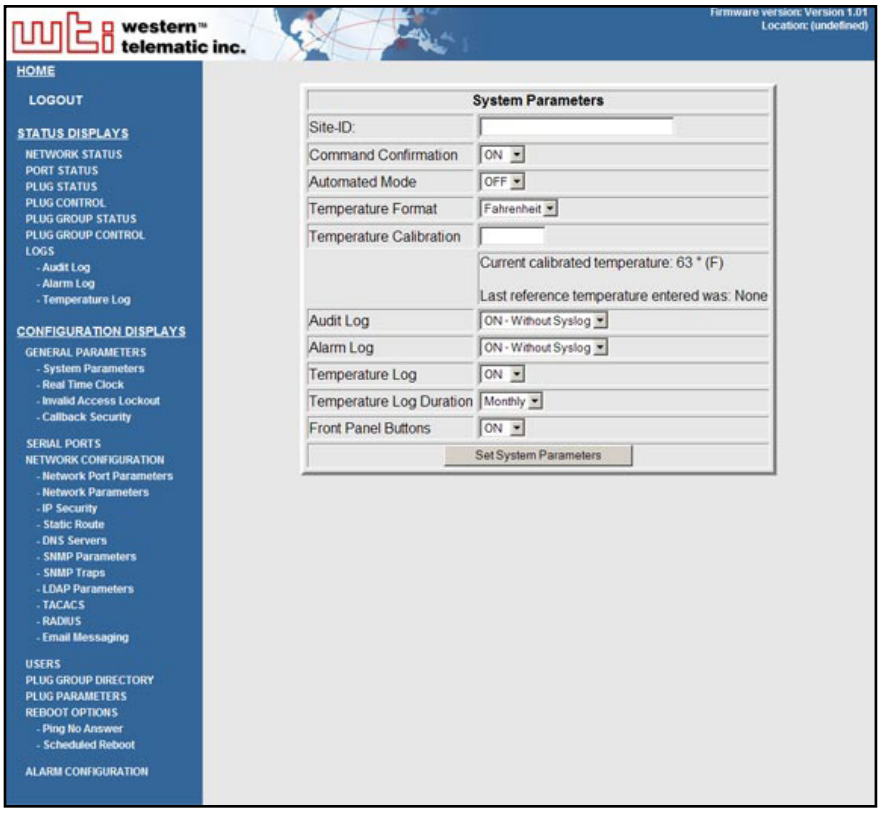

Figure 5.4: The System Parameters Menu (Web Browser Interface)

5.3. Defining System Parameters

The System Parameters menus are used to define the Site ID Message, set the system clock and calendar, set up log functions and calibrate temperature readings.

In the Text Interface, the System Parameters menu is also used to create and manage user accounts and passwords. Note however, that when you are communicating with the unit via the Web Browser Interface, accounts and passwords are managed and created using a separate menu that is accessed by clicking on the "Users" link on the left hand side of the menu.

- **Text Interface:** Type **`/F`** and press **[Enter]**. The System Parameters Menu will appear as shown in Figure 5.3.
- **Web Browser Interface:** Click the "System Parameters" link on the left hand side of the screen. The System Parameters menu will be displayed as shown in Figure 5.4.

The System Parameters Menus are used to define the following:

- **User Directory:** This function is used to view, add, modify and delete user accounts and passwords. As discussed in Section 5.4 and Section 5.5, the User Directory allows you to set the security level for each account as well as determine which plugs each account will be allowed to control.

  Note: *The "User Directory" option does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the "Users" link on the left hand side of the menu.*

- **Site ID:** A text field, generally used to note the installation site or name for the RSM-8R4 unit. (Up to 32 chars.; Default = undefined.)
- **Real Time Clock:** This prompt provides access to the Real Time Clock menu, which is used to set the clock and calendar, and to enable and configure the NTP (Network Time Protocol) feature as described in Section 5.3.1.

  Note: *The "Real Time Clock" option does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the "Real Time Clock" link on the left hand side of the screen.*

- **Invalid Access Lockout:** If desired, this feature can be used to automatically disable the Network Port, Modem Port or Serial Ports after a user specified number of unsuccessful login attempts are made. For more information, please refer to Section 5.3.2. (Default = On, 9 Attempts, 30 Minute Duration.)

  Note: *The "Invalid Access Lockout" item does not appear in the Web Browser Interface's System Parameters menu, and is instead, accessed via the link on the left hand side of the screen.*

- **Command Confirmation:** Enables/Disables the Command Confirmation feature. When enabled, a "Sure" prompt will be displayed before power switching and reboot commands are executed. When disabled, commands will be executed without further prompting. (Default = On.)

- **Automated Mode:** When enabled, the RSM-8R4 will execute switching and reboot commands without displaying a confirmation prompt, status screen or confirmation messages. For more information, please refer to Section 9.4. (Default = Off.)

  Note: *When this option is enabled, security functions are suppressed, and users are able to access configuration menus and control plugs without entering a password. If security is a concern and the Automated Mode is required, it is recommended to use the IP Security feature (Section 5.9.3) to restrict access.*

- **Temperature Format:** Determines whether the temperature is displayed as Fahrenheit or Celsius. (Default = Fahrenheit.)

- **Temperature Calibration:** Used to calibrate the unit's internal temperature sensing abilities. To calibrate the temperature, place a thermometer inside your equipment rack, in a location that usually experiences the highest temperature. After a few minutes, take a reading from the thermometer, and then key the reading into the configuration menu. In the Web Browser Interface, the temperature is entered at the System Parameters menu, in the Temperature Calibration field; in the Text Interface, the temperature is entered in a submenu of the System Parameters menu, accessed via the Temperature Calibration item. (Default = undefined.)

- **Log Configuration:** Enables and configures the Audit Log, Alarm Log and Temperature Log. For more information on the RSM-8R4's event logging functions, please refer to Section 5.3.4. (Default = Audit Log = On without Syslog, Alarm Log = On without Syslog, Temperature Log = On - Monthly.)

  Notes:

  - *The Audit Log will create a record of all power switching and reboot activity at the RSM-8R4 unit, including reboots and switching caused by Load Shedding, Load Shedding Recovery, Ping No Answer Reboots and Scheduled Reboots.*
  - *The Alarm Log will create a record of each instance where an Alarm is triggered or cleared at the RSM-8R4 unit.*

- **Callback Security:** Enables and configures the Callback Security Function as described in Section 5.3.5. In order for this feature to function, a Callback number must also be defined for each desired user account as described in Section 5.5. (Default = On - Callback without Password Prompt, 3 attempts, 30 Minute Delay.)

  Notes:

  - *In the Text Interface, Callback Security Parameters are defined via a submenu of the Systems Parameters Menu, which is accessed via the Callback Security item.*
  - *In the Web Browser Interface, Callback Security Parameters are defined via a separate menu, which is accessed by clicking the "Callback Security" link on the left hand side of the screen.*

- **Front Panel Buttons:** This item can be used to disable the reinitialization/default functions that are normally available via the Clear and Set buttons as described in Section 2.3. (Default = On.)

5.3.1. The Real Time Clock and Calendar

The Real Time Clock menu is used to set the RSM-8R4's internal clock and calendar. To access the Real Time Clock Menu, proceed as follows:

- **Text Interface:** Type **/F** and press **[Enter]**. The System Parameters menu will appear as shown in Figure 5.3. At the System Parameters menu, type **3** and press **[Enter]** to display the Real Time Clock menu.
- **Web Browser Interface:** Click on the "Real Time Clock" link on the left hand side of the screen to access the Real Time Clock menu.

The configuration menu for the Real Time Clock offers the following options:

- **Date:** Sets the Month, Date, Year and day of the week for the RSM-8R4's real-time clock/calendar.
- **Time:** Sets the Hour, Minute and Second for the RSM-8R4's real time clock/calendar. Key in the time using the 24-hour (military) format.
- **Time Zone:** Sets the time zone, relative to Greenwich Mean Time. Note that the Time Zone setting will function differently, depending upon whether or not the NTP feature is enabled and properly configured. (Default = GMT (No DST).)
  - **NTP Enabled:** The Time Zone setting is used to adjust the Greenwich Mean Time value (received from the NTP server) in order to determine the precise local time for the selected time zone.
  - **NTP Disabled:** If NTP is disabled, or if the RSM-8R4 is not able to access the NTP server, then status screens and activity logs will list the selected Time Zone and current Real Time Clock value, but will not apply the correction factor to the displayed Real Time Clock value.
- **NTP Enable:** When enabled, the RSM-8R4 will contact an NTP server (defined via the NTP Address prompts) once a day, and update its clock based on the NTP server time and selected Time Zone. (Default = Off.)

Notes:

- *The RSM-8R4 will also contact the NTP server and update the time whenever you change NTP parameters.*
- *To cause RSM-8R4 to immediately contact the NTP server at any time, make certain that the NTP feature is enabled and configured, then type* **/F** *and press* **[Enter]**. *When the System Parameters menu appears, press* **[Esc]**. *The RSM-8R4 will save parameters and then attempt to contact the server, as specified by currently defined NTP parameters.*

- **Primary NTP Address:** Defines the IP address or domain name (up to 64 characters long) for the primary NTP server. (Default = undefined.)

  Note: *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 5.9.5.*

- **Secondary NTP Address:** Defines the IP address or domain name (up to 64 characters long) for the secondary, fallback NTP Server. (Default = undefined.)

  Note: *In order to use domain names for web addresses, DNS Server parameters must be defined as described in Section 5.9.5.*

- **NTP Timeout:** The amount of time in seconds, that will elapse between each attempt to contact the NTP server. When the initial attempt is unsuccessful, the RSM-8R4 will retry the connection four times. If neither the primary nor secondary NTP server responds, the RSM-8R4 will wait 24 hours before attempting to contact the NTP server again. (Default = 3 Seconds.)

5.3.2. The Invalid Access Lockout Feature

When properly configured and enabled, the Invalid Access Lockout feature will watch all login attempts made at the Network Port and Serial Ports. If any port exceeds the selected number of invalid attempts, then that port will be automatically disabled for a user-defined length of time (Lockout Duration.) The Invalid Access Lockout feature uses two separate counters to track invalid access attempts:

- **Serial Port Counter:** Counts invalid access attempts at the Serial Ports. If the number of invalid attempts at a port exceeds the user-defined Lockout Attempts value, then the port will be locked.
- **Telnet, SSH and Web Browser Counter:** Counts all invalid attempts to access command mode via Telnet, SSH or Web Browser interface. If the number of cumulative invalid attempts exceeds the user-defined Lockout Attempts value, then the Network Port will be locked.

Note that when an Invalid Access Lockout occurs, you can either wait for the Lockout Duration period to elapse (after which, the RSM-8R4 will automatically reactivate the port), or you can issue the /UL command (type **`/UL`** and press **[Enter]**) via the Text Interface to instantly unlock all of the RSM-8R4's logical network ports.

Notes:

- *Invalid Access Lockout parameters, defined via the System Parameters menu, will apply to both the Serial Ports and the Network Port.*
- *When a Serial Port is locked, an external modem connected to that port will not answer.*
- *When either a Serial Port or the Network Port are locked, other ports will remain unlocked, unless the Invalid Access Lockout feature has also been triggered at that port.*
- *If any one of the RSM-8R4's logical network ports is locked, all other network connections to the unit will also be locked.*
- *All invalid access attempts at the RSM-8R4 Network Port are cumulative (the count for invalid access attempts is determined by the total number of all invalid attempts at all 16 logical network ports.) If a valid login name/password is entered at any of the logical network ports, then the count for all RSM-8R4 logical network ports will be restarted.*
- *If the Network Port has been locked by the Invalid Access Lockout feature, it will still respond to the ping command (providing that the ping command has not been disabled at the Network Port.)*

The Invalid Access menus allow you to select the following:

- **Lockout Enable:** Enables/Disables the Invalid Access Lockout feature. (Default = On.)
- **Lockout Attempts:** The number of invalid attempts required in order to activate the Invalid Access Lockout feature. (Default = 9.)
- **Lockout Duration:** The length of time that logical network ports will remain locked when an Invalid Access Lockout occurs. If the duration is set at "Infinite", then ports will remained locked until the /UL command is issued. (Default = 30 Minutes.)

5.3.3. Automated Mode

The Automated Mode allows the RSM-8R4 to execute power switching, reboot and port disconnection commands, without displaying menus or generating response messages. Automated Mode is designed to allow the RSM-8R4 to be controlled by a device which can generate commands to control power switching functions without human intervention.

When Automated Mode is enabled, power switching, reboot and port disconnection commands are executed without a "Sure?" confirmation prompt and without command response messages; the only reply to these commands is the "RSM>" prompt, which is re-displayed when each command is completed.

Note that although Automated Mode can be enabled using either the Web Browser Interface or Text Interface, Automated Mode is designed primarily for users who wish to send ASCII commands to the RSM-8R4 without operator intervention, and therefore does not specifically apply to the Web Browser Interface. When Automated Mode is enabled, the Web Browser Interface can still be used to invoke switching and reboot commands.

Notes:

- *When the Automated Mode is enabled, password prompts will not be displayed at login, and you will be able to access Administrator Level command functions (including the configuration menus) and control plugs without entering a password.*
- *If you need to enable the Automated Mode, but want to restrict network access to configuration menus, it is strongly recommended to enable and configure the IP Security Function as described in Section 5.9.3.*

To enable/disable the Automated Mode, go to the System Parameters menu (see Section 5.3,) and then set the "Automated Mode" option to "On". When Automated Mode is enabled, RSM-8R4 functions will change as follows:

1. **All Password Security Suppressed:** When a user attempts to access command mode via the Network Port or Serial Ports, the password prompt will not be displayed. Unless specifically restricted by the IP Security Function, all users will be allowed to access both switching and configuration functions, and all commands will be immediately accepted without the requirement to enter a password.
2. **Status Screen Suppressed:** The plug status screen will not be automatically displayed after commands are successfully executed. Note however, that the /S command can still be invoked to display the status screen as needed.
3. **"Sure?" Prompt Suppressed:** All commands are executed without prompting for user confirmation.
4. **Error Messages Suppressed:** Most error messages will be suppressed. Note however, that an error message will still be generated if commands are invoked using invalid formats or arguments.

All other status display and configuration commands will still function as normal.

5.3.4. Log Configuration

This feature allows you to create records of command activity, alarm actions and temperature readings for the RSM-8R4 unit. The Log features are enabled and configured via the System Parameters Menus.

The RSM-8R4 features three different event logs: the Audit Log, the Alarm Log and the Temperature Log:

- **Audit Log:** The Audit log creates a record of all port connection/disconnection, power switching, and reboot activity at the RSM-8R4 unit, including reboots and switching caused by Load Shedding, Load Shedding Recovery, Ping No Answer Reboots and Scheduled Reboots. In addition, the Audit Log also includes login/logout records for all users and connection/disconnection records for the serial ports. Each Log record includes a description of the activity that caused the power switching, port connection, login or reboot, the username for the account that initiated the action and the time date that each event occurred.
- **Alarm Log:** The Alarm log creates a record of all Alarm Activity at the RSM-8R4 unit. Each time that an alarm is triggered or cleared, the RSM-8R4 will generate a record that lists the time and date of the alarm, the name of the Alarm triggered, a description of the Alarm and the time and date that the Alarm was cleared.
- **Temperature Log:** The Temperature Log provides a record of temperature levels over time at the RSM-8R4 unit. Each Log record will include the time and date, and the temperature reading. The Temperature Log can be downloaded in ASCII, CSV or XML format, and when viewed via the Web Browser Interface.

5.3.4.1. The Audit Log and Alarm Log

The System Parameters menu allows you to select three different configuration parameters for the Audit Log and Alarm Log. Note that the Audit Log and Alarm Log function independently, and parameters selected for one log will not be applied to the other.

- **Off:** The Log is disabled, and command activity and/or alarm events will not be logged.
- **On - With Syslog:** The Log is enabled, and power switching, reboot activity and/or alarm events will be logged. The RSM-8R4 will generate a Syslog Message every time a Log record is created. (Default Setting.)
- **On - Without Syslog:** The Log is enabled, and power switching, reboot activity and/or alarm events will be logged, but the RSM-8R4 will not generate a Syslog Message every time a Log record is created.

Notes:

- *In order for the Audit Log or Alarm Log to generate Syslog Messages, Syslog Parameters must first be defined as described in Section 11.*
- *The Audit Log will truncate usernames that are longer than 22 characters, and display two dots (..) in place of the remaining characters.*

5.3.4.2. The Temperature Log

The System Parameters menu allows you to select two different configuration parameters for the Temperature Log:

- **Temperature Log (Enabled):** Enables/disables the Temperature Log function. When disabled, the RSM-8R4 will not log temperature readings. (Default = On.)
- **Temperature Log Duration:** The Temperature Log Duration can be set to Monthly or Weekly. This determines how often the Temperature Log will be cleared and how long Temperature data will be retained. For example, if Temperature Log Duration is set to "Monthly", then data will be kept for up to one month. (Default = Monthly.)

5.3.4.3. Reading and Erasing Logs

To read the Audit Log, Alarm Log or Temperature log, access the command mode, then proceed as follows:

- **Text Interface:** Type **`/L`** and press **[Enter]** to display the Display Log menu. Select the desired Log from the menu, key in the appropriate number and press **[Enter]**, and then follow the instructions in the resulting submenu.
- **Web Browser Interface:** To view the Audit Log, click on the "Audit Log" link on the left hand side of the screen. To view the Alarm Log, click on the "Alarm Log" link on the left hand side of the screen. To view the Temperature Log, click on the "Temperature Log" link on the left hand side of the screen.

To erase log data, access command mode via the Text Interface, using an account that permits Administrator level commands, then type **`/L`** and press **[Enter]** to access the Display Logs menu. At the Display Logs menu, key in the number for the desired log, and press **[Enter]** to display the Log, then type **`E`** and press **[Enter]** to erase all records for the selected log. Note that once records have been erased, they cannot be recovered.

Notes:

- *The RSM-8R4 dedicates a fixed amount of internal memory for Audit Log records, and if log records are allowed to accumulate until this memory is filled, memory will eventually "wrap around," and older records will be overwritten by newer records.*
- *To save the Audit Log, Alarm Log or Temperature Log as an ASCII file via the Web Browser Interface, right-click the link for the desired log, select "Save Target As", select text format, and then save the document with a ".txt" filename extension.*

5.3.5. Callback Security

The Callback function provides an additional layer of security when callers attempt to access command mode via modem. When this function is properly configured, modem users will not be granted immediate access to command mode upon entering a valid password; instead, the unit will disconnect, and dial a user-defined number before allowing access via that number. If desired, users may also be required to re-enter the password *after* the RSM-8R4 dials back.

In order for Callback Security to function properly, you must first enable and configure the feature as described in this section, and then define a callback number for each desired user account as described in Section 5.5. To configure and enable the Callback function, proceed as follows:

- **Text Interface:** Type **`/F`** and press **[Enter]** to access the System Parameters menu, then type **`10`** and press **[Enter]** to display the Callback Security Menu.
- **Web Browser Interface:** Click the "Callback Security" link on the left hand side of the screen to display the Callback Security Menu.

In both the Text Interface and Web Browser Interface, the Callback Security Menu offers the following options:

- **Callback Enable:** This prompt offers five different configuration options for the Callback Security feature: (Default = On - Callback (Without Password Prompt.)
  - **Off:** All Callback Security is disabled.
  - **On - Callback (Without Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the login prompt will *not* be displayed when the user's modem answers. If the account *does not* include a Callback Number, that user will be granted immediate access and a Callback will *not* be performed.
  - **On - Callback (With Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the login prompt *will* be displayed when the user's modem answers (accounts that include a Callback Number will be required to re-enter their username/password when their modem answers.) If the account *does not* include a Callback Number, then that user will be granted immediate access and a Callback will *not* be performed.
  - **On - Callback ONLY (Without Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the username/password prompt will *not* be displayed when the user's modem answers. Accounts that *do not* include a Callback Number will *not* be able to access command mode via modem.
  - **On - Callback ONLY (With Password Prompt):** Callbacks will be performed for user accounts that include a Callback Number, and the username/password prompt *will* be displayed when the user's modem answers (users will be required to re-enter their username/password when their modem answers.) Accounts that *do not* include a Callback Number will *not* be able to access command mode via modem.

- **Callback Attempts:** The number of times that the RSM-8R4 will attempt to contact the Callback number. (Default = 3 attempts.)
- **Callback Delay:** The amount of time that the RSM-8R4 will wait between Callback attempts. (Default = 30 seconds.)

Notes:

- *After configuring and enabling Callback Security, you must then define a callback phone number for each desired user account (as described in Section 5.5) in order for this feature to function properly.*
- *When using the "On - Callback (With Password Prompt)" option, it is important to remember that accounts that do not include a callback number will be allowed to access command mode without callback verification.*

5.4. User Accounts

Each time you attempt to access command mode, you will be prompted to enter a username (login) and password. The username and password entered at login determine which serial port(s) and plug(s) you will be allowed to control and what type of commands you will be allowed to invoke. Each username / password combination is defined within a "user account."

The RSM-8R4 allows up to 128 user accounts; each account includes a username, password, command access level, port access rights, plug access rights, service access rights and an optional callback number.

5.4.1. Command Access Levels

In order to restrict access to important command functions, the RSM-8R4 allows you to set the command access level for each user account. The RSM-8R4 offers four different access levels: Administrator, SuperUser, User and View Only. The command privileges for each user account are set using the "Access Level" parameter in the Add User or Modify User menus.

Each access level grants permission to use a different selection of commands; lower access levels are restricted from invoking configuration commands, while Administrators are granted access to all commands. The four different access levels can be summarized as follows:

- **Administrator:** Administrators are allowed to invoke all configuration and operation commands, can view all status screens, and can always connect to any RSM-8R4 serial port and direct switching and reboot commands to all of the RSM-8R4's switched outlets .
- **SuperUser:** SuperUsers are allowed to invoke all serial port connection and power switching commands and view all status screens. SuperUsers can view configuration menus, but are not allowed to change configuration parameters. SuperUsers are granted access to all RSM-8R4 serial ports and switched outlets.
- **User:** Users are allowed to invoke port connection and power switching commands and view all status screens, but can only apply commands to the serial ports and outlets that they have been specifically granted access to. In addition, Users are not allowed to view configuration menus or change configuration parameters.
- **ViewOnly:** Accounts with ViewOnly access, are allowed to view Status Menus, but are not allowed to invoke port connection and power switching commands, and cannot view configurations menus or change configuration parameters. ViewOnly accounts can display the Port/Plug Status screens, but can only view the status of ports and plugs that are specifically allowed by the account.

Section 17.2 summarizes command access for all four access levels.

In the default state, the RSM-8R4 includes one predefined account that provides access to Administrator commands and allows to control of all of the RSM-8R4's serial ports and switched power outlets. The default username for this account is "**super**" (lowercase, no quotation marks), and the password for the account is also "**super**".

Notes:

- *In order to ensure security, it is recommended that when initially setting up the unit, a new user account with Administrator access should be created, and the "super" account should then be deleted.*
- *If the RSM-8R4 is reset to default parameters, all user accounts will be cleared, and the default "super" account will be restored.*

5.4.2. Granting Serial Port Access

Each account can be granted access to a different selection of ports. Note also, that several accounts can be allowed access to the same port. When accounts are created, the Port Access parameter in the Add User or Modify User menu can be used to grant or deny access to each serial port by that account.

In addition, each command access level is also used to restricts the serial ports that the account will be allowed to access:

- **Administrator:** Accounts with Administrator access are always allowed to control all Serial Ports. Port access cannot be disabled for Administrator level accounts.
- **SuperUser:** SuperUser accounts allow access to all Serial Ports. Port access cannot be disabled for SuperUser level accounts.
- **User:** Accounts with User level access are only allowed to create connections with the Serial Ports that have been specifically permitted via the "Port Access" parameter in the Add User and Modify User menus.
- **ViewOnly:** Accounts with ViewOnly access are not allowed to create connections with Serial Ports. ViewOnly accounts can display the status of Serial Ports, but are limited to the ports specified by the account.

5.4.3. Granting Plug Access

Each account can be granted access to a different selection of switched power outlets (plugs) and plug groups. When accounts are created, the Plug Access parameter and the Plug Group Access parameter in the Add User menu or Modify User menu can be used to grant or deny access to each plug or plug group by that account.

In addition, each command access level also restricts the plugs and plug groups that the account will be allowed to access:

- **Administrator:** Accounts with Administrator access are always allowed to control all plugs and plug groups. Plug access cannot be disabled for Administrator level accounts.
- **SuperUser:** SuperUser accounts allow access to all plugs and plug groups by default. Plug access cannot be disabled for SuperUser level accounts.
- **User:** Accounts with User level access are only allowed to issue switching and reboot commands to the plugs and plug groups that have been specifically permitted via the "Plug Access" parameter in the Add User and Modify User menus.
- **ViewOnly:** Accounts with ViewOnly access are not allowed to issue switching and reboot commands to outlets or plug groups. ViewOnly accounts can display the status of plugs and plug groups, but are limited to the plugs and plug groups specified by the account.

5.5. Managing User Accounts

The User Directory function is employed to create new accounts, display parameters for existing accounts, modify accounts and delete accounts. Up to 128 different user accounts can be created. The "User Directory" function is only available when you have logged into command mode using an account that permits Administrator commands.

- **Text Interface:** Type `/F` and press **[Enter]** to access the System Parameters Menu. From the System Parameters Menu, type `1` and press **[Enter]** to access the User Directory.
- **Web Interface:** Click the "Users" link on the left hand side of the screen to access the User Directory management menus.

In both the Text Interface and the Web Browser Interface, the user configuration menu offers the following functions:

- **View User Directory:** Displays currently defined parameters for any RSM-8R4 user account as described in Section 5.5.1.
- **Add Username:** Creates new user accounts, and allows you to assign a username, password, command level, serial port access, plug access, plug group access, service access and callback number, as described in Section 5.5.2.
- **Modify User Directory:** This option is used to edit or change account information, as described in Section 5.5.3.
- **Delete User:** Clears user accounts, as described in Section 5.5.4.

  Note: *After you have finished selecting or editing user account parameters, make certain to save the new account information before proceeding. In the Web Browser Interface, click on the "Add User" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.5.1. Viewing User Accounts

The "View User Directory" option allows you to view details about each account, including the plugs and plug groups that the account is allowed to control and whether or not the account is allowed to invoke Administrator commands. The View User option will not display actual passwords, and instead, the password field will read "defined". Note that the View User Accounts function is only available to users who have accessed command mode using a password that permits Administrator Level commands. To view account details, proceed as follows:

- **Text Interface:** From the User Directory menu, type `1` and press **[Enter]**. The RSM-8R4 will display a screen which lists all defined user accounts. Key in the name of the desired account and then press **[Enter]**.
- **Web Browser Interface:** From the User menu, click the "View/Modify User" link. The RSM-8R4 will display a menu that allows you to select the desired user and directory function. Select the "View User" button, and then click on the down arrow, scroll to the desired username, select the username, and then click "Choose User."

```
ADD USERNAME TO DIRECTORY:

1. Username:              (undefined)
2. Password:              (undefined)
3. Access Level:          User
4. Port Access:           (undefined)
5. Plug Access:           (undefined)
6. Plug Group Access      (undefined)
7. Service Access         Serial Port, Telnet/SSH, Web, Outbound
8. Callback Phone #:      (undefined)


Enter: #<CR> to select,
       <ESC> to return to previous menu ...
```

Figure 5.5: The Add User Menu (Text Interface)

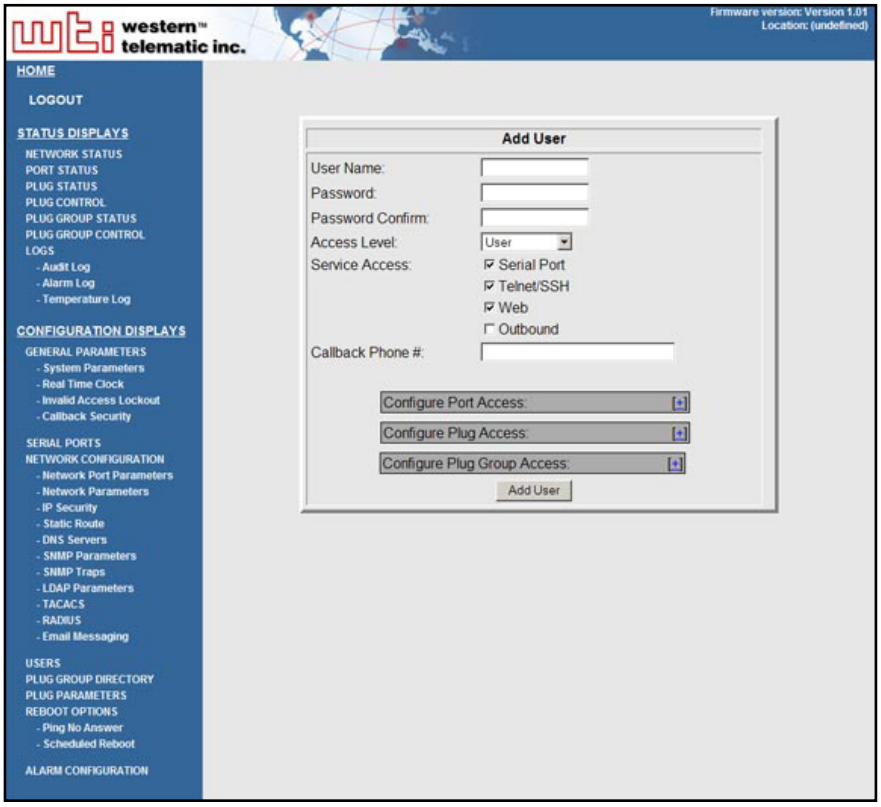

Figure 5.6: The Add User Menu (Web Browser Interface)

5.5.2. Adding User Accounts

The "Add Username" option allows you to create new accounts and assign usernames, passwords, serial port access and plug access rights to each account. Note that the Add User function is only available when you have entered command mode using a password that permits Administrator Level commands.

To create new user accounts, activate the command mode using an account that permits access to Administrator level commands and then proceed as follows:

- **Text Interface:** Type **`/F`** and press **[Enter]** to access the System Parameters menu. From the System Parameters Menu, type **`1`** and press **[Enter]** to display the User Directory Menu. From the User Directory menu, type **`2`** and press **[Enter]**. The Add User menu (Figure 5.5) will be displayed.
- **Web Browser Interface:** Click the "Users" link to display the User Configuration menu. At the User Configuration menu, click the "Add User" link. The RSM-8R4 will display the Add User menu (Figure 5.6.)

The Add User Menu can define the following parameters for each new account:

- **Username:** Up to 32 characters long, and cannot include non-printable characters. Duplicate usernames are not allowed. (Default = undefined.)
- **Password:** Five to 16 characters long, and cannot include non-printable characters. Note that passwords are case sensitive. (Default = undefined.)
- **Access Level:** Determines which commands this account will be allowed to access. This option can set the access level for this account to "Administrator", "SuperUser", "User" or "ViewOnly." For more information on Command Access Levels, please refer to Section 5.4.1 and Section 16.2. (Default = User.)
- **Port Access:** Determines which RSM-8R4 Serial Ports this account will be allowed to access. (Defaults; Administrator & SuperUser = All Ports On, User and ViewOnly = All Ports Off.)

Notes:

- *In the Text Interface, Serial Port Access is configured by selecting item 4 and then selecting the desired ports from the resulting submenu.*
- *In the Web Browser Interface, Serial Port Access is configured by clicking on the "plus" symbol to display the drop down menu, and then selecting the desired ports from the drop down menu.*
- *Administrator and SuperUser level accounts will always have access to all Serial Ports.*
- *ViewOnly accounts are allowed to display the status of Serial Ports, but are limited to the ports specified by the account. ViewOnly accounts are not allowed to create connections between ports.*

- **Plug Access:** Determines which outlet(s) this account will be allowed to control. (Defaults; Administrator and SuperUser = All Plugs On, User and ViewOnly = All Plugs Off.)

  Notes:

  - *In the Text Interface, Plug Access is configured by selecting item 5 and then selecting the desired plugs from the resulting submenu.*
  - *In the Web Browser Interface, Plug Access is configured by clicking on the "plus" symbol to display the drop down menu, and then selecting the desired plugs from the drop down menu.*
  - *Administrator and SuperUser level accounts will always have access to all plugs.*
  - *ViewOnly accounts are allowed to display the On/Off status of plugs, but are limited to the plugs specified by the account. ViewOnly accounts are not allowed to invoke switching and reboot commands.*

- **Plug Group Access:** Determines which Plug Groups this account will be allowed to control. Plug Groups allow you to define a selection of outlets, and then quickly assign those outlets to new accounts by allowing the account to access the Plug Group. For more information on Plug Groups, please refer to Section 5.6. (Default = All Plug Groups Off.)

  Notes:

  - *In order to use this feature, Plug Groups must first be defined as described in Section 5.6.*
  - *In the Text Interface, Plug Group Access is configured by selecting item 6 and then selecting the desired plug group(s) from the resulting submenu.*
  - *In the Web Browser Interface, Plug Group Access is configured by clicking on the "plus" symbol to display the drop down menu, and then selecting the desired plug group(s) from the drop down menu.*
  - *Administrator and SuperUser level accounts will always have access to all plug groups.*
  - *ViewOnly accounts are allowed to display the On/Off status of plug groups, but are limited to the plug groups specified by the account. ViewOnly accounts are not allowed to invoke switching and reboot commands.*

- **Service Access:** Determines whether this account will be able to access command mode via Serial Port, Telnet/SSH or Web and whether the account will have access to the Outbound Telnet/SSH feature. For example, if Telnet/SSH Access is disabled for this account, then this account will not be able to access command mode via Telnet or SSH. (Default = Serial Port = On, Telnet/SSH = On, Web = On, Outbound Access = Off.)

- **Callback Number:** Assigns a number that will be called when this account attempts to access command mode via modem, and the Callback Security Function has been enabled as described in Section 5.3.5. (Default = undefined.)

Notes:

- *If the Callback Number is not defined, then Callbacks will not be performed for this user.*
- *If the Callback Number is not defined for a given user, and the Callback Security feature is configured to use either of the "On - Callback" options, then this user will be granted immediate access to command mode via modem.*
- *If the Callback Number is not defined for a given user, and the Callback Security feature is configured to use the "On - Callback ONLY" option, then this user will not be able to access command mode via Modem.*
- *When using the "On - Callback (With Password Prompt)" option, it is important to remember that accounts that do not include a callback number will be allowed to access command mode without callback verification.*

Note: *After you have finished selecting or editing account parameters, make certain to save the new account information before proceeding. In the Web Browser Interface, click on the "Add User" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.5.3. Modifying User Accounts

The "Modify User Directory" function allows you to edit existing user accounts in order to change parameters, port and plug access rights or Administrator Command capability. Note that the Modify User function is only available when you have entered command mode using a password that permits Administrator Level commands. To modify a user account, proceed as follows:

- **Text Interface:** From the User Directory menu, type 3 and press **[Enter]**. The RSM-8R4 will display a screen which lists all user accounts. Key in the name of the account you wish to modify, and press **[Enter]**.
- **Web Browser Interface:** From the User Configuration menu, click the "View/Modify User" link. The RSM-8R4 will display a menu that allows you to select the user. Select the "Modify User" button, then click the down arrow, scroll to the name of the desired account, select the username, and then click "Choose User" to display the "Modify User" menu.

Once you have accessed the Modify Users menu, use the menu options to redefine parameters in the same manner that is used for the Add User menu, as discussed in Section 5.5.2.

Note: *After you have finished changing parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify User" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message.*

5.5.4. Deleting User Accounts

This function is used to delete individual user accounts. Note that the Delete User function is only available when you have accessed command mode using a password that permits Administrator Level commands. To delete an existing user account, proceed as follows:

- **Text Interface:** From the Users Directory menu, type **4** and press **[Enter]**. The RSM-8R4 will display a screen which lists all currently defined accounts. Key in the name of the account you wish to delete and press **[Enter]**. The RSM-8R4 will delete the specified account without further prompting.
- **Web Browser Interface:** From the User Configuration menu, click the "View/ Modify Users" link. The RSM-8R4 will display a menu that lists all currently defined accounts. Select the "Delete User" box, then click the down arrow, scroll to the account you wish to delete, select the account, and then click "Choose User." The RSM-8R4 will display a screen that lists details for the specified account; click "Delete User" to confirm deletion.

Notes:

- *Deleted accounts cannot be automatically restored.*
- *The RSM-8R4 allows you to delete the default "super" account, which is included to permit initial access to command mode. Before deleting the "super" account, make certain to create another account that permits Administrator Access. If you do not retain at least one account with Administrator Access, you will not be able to invoke Administrator level commands.*

5.6. The Plug Group Directory

The Plug Group Directory allows you to designate "groups" of plugs that are dedicated to a similar function, and will most likely be switched or rebooted all at the same time or controlled by the same type of user account.

For example, an individual equipment rack might include an assortment of devices that belong to different departments or clients. In order to simplify the process of granting plug access rights to the accounts that will control power to these devices, you could assign all of the plugs for the devices belonging to Department A to a Plug Group named "Dept_A", and all of the plugs for the devices belonging to Department B to a Plug Group named "Dept_B". When user accounts are defined, this would allow you to quickly grant access rights for all of the plugs for the devices belonging to Department A to the appropriate user accounts for Department A, by merely granting access to the Dept_A Plug Group, rather than by selecting the specific, individual plugs for each Department A user account.

Likewise, Plug Groups allow you to direct On/Off/Boot commands to a series of plugs, without addressing each plug individually. Given the example above, you could quickly reboot all plugs for Department A, by either including the "Dept_A" Plug Group name in a /BOOT command line via the Text Interface, or by using the Plug Group Control menu via the Web Browser Interface.

The Plug Group Directory function is only available when you have logged into command mode using an account that permits Administrator commands. To access the Plug Group Directory, proceed as follows:

- **Text Interface:** Type `/G` and press **[Enter]** to display the Plug Group Directory menu.
- **Web Interface:** Click the "Plug Group Directory" link on the left hand side of the screen to display the Plug Group Directory menu.

In both the Text Interface and the Web Browser Interface, the Plug Group Directory menu offers the following functions:

- **View Plug Group Directory:** Displays currently defined plug access rights for any RSM-8R4 Plug Group as described in Section 5.6.1.
- **Add Plug Group to Directory:** Creates new Plug Groups, and allows you to assign plug access rights to each group as described in Section 5.6.2.
- **Modify Plug Group Directory:** This option is used to edit or change plug access rights for each Plug Group, as described in Section 5.6.3.
- **Delete Plug Group from Directory:** Clears Plug Groups that are no longer needed, as described in Section 5.6.4.

5.6.1. Viewing Plug Groups

The "View Plug Group Directory" option allows you to view the configuration of each Plug Group. Note that the View Plug Group Directory function is only available when you have accessed command mode using a password that permits Administrator Level commands. To view Plug Group details, proceed as follows:

- **Text Interface:** Type `/G` and press **[Enter]** to display the Plug Group Directory menu. From the Plug Group Directory menu, type `1` and press **[Enter]**. The RSM-8R4 will display a screen which lists all defined Plug Groups. Key in the name of the Plug Group that you need to review and then press **[Enter]**.
- **Web Browser Interface:** Click the "Plug Group Directory" link on the left hand side of the screen to display the Plug Group Directory menu. From the Plug Group Directory menu, click the "View/Modify Plug Group" link. The RSM-8R4 will display a menu that allows you to select the desired Plug Group and directory function. Select the "View Plug Group" button, and then click on the down arrow, scroll to the desired Plug Group, select the Plug Group, and then click "Choose Plug Group" to view the selected Plug Group.

5.6.2. Adding Plug Groups

The "Add Plug Group to Directory" option allows you to create new Plug Groups and assign plug access rights to each group. Note that the Add Plug Group function is only available when you have accessed command mode using a password that permits Administrator Level commands. To create new Plug Groups, proceed as follows:

- **Text Interface:** Type `/G` and press **[Enter]** to display the Plug Group Directory menu. From the Plug Group Directory menu, type `2` and press **[Enter]**. The RSM-8R4 will display the Add Plug to Group.
- **Web Browser Interface:** Click the "Plug Group Directory" link on the left hand side of the screen to display the Plug Group Directory menu. From the Plug Group Directory menu, click the "Add Plug Groups" link to display the Add Plug to Group menu.

The Add Plug Group Menu can be used to define the following parameters for each new account:

- **Plug Group Name:** Assigns a name to the Plug Group. (Default = undefined.)
- **Plug Access:** Determines which plugs this Plug Group will be allowed to control. (Default = undefined.)

Notes:

- *In the Text Interface, Plug Access is configured by selecting item 2 and then selecting the desired plugs from the resulting submenu.*
- *In the Web Browser Interface, Plug Access is configured by selecting the desired plugs from a list of all plugs in the Add Plug Group menu.*
- *After you have finished defining or editing Plug Group parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Plug Group" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.6.3. Modifying Plug Groups

The "Modify Plug Group" function allows you to edit existing Plug Groups in order to change plug access rights. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands. To modify an existing Plug Group , proceed as follows:

- **Text Interface:** Type `/G` and press **[Enter]** to display the Plug Group Directory menu. From the Plug Group Directory menu, type `3` and press **[Enter]**. The RSM-8R4 will display the Modify Plug Group menu.
- **Web Browser Interface:** Click the "Plug Group Directory" link on the left hand side of the screen to display the Plug Group Directory menu. From the Plug Group Directory menu, click the "View/Modify Plug Group" link. The RSM-8R4 will display a menu that lists all currently defined Plug Groups. Select the "Modify Plug Group" button, then click the down arrow, scroll to the Plug Group that you wish to modify, select the Plug Group, and then click "Choose Plug Group." The RSM-8R4 will display the Modify Plug Group menu.

Once you have accessed the Modify Plug Group menu, use the menu options to redefine parameters in the same manner that is used for the Add Plug Group menu, as discussed in Section 5.6.2.

> **Note:** *After you have finished changing or editing parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify Plug Groups" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.6.4. Deleting Plug Groups

This function is used to delete individual Plug Groups. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands. To delete an existing user account, proceed as follows:

- **Text Interface:** Type `/G` and press **[Enter]** to display the Plug Group Directory menu. From the Plug Group Directory menu, type `4` and press **[Enter]**. The RSM-8R4 will display a screen which lists all currently defined Plug Groups. Key in the name of the Plug Group that you wish to delete and press **[Enter]**. The RSM-8R4 will delete the specified account without further prompting.
- **Web Browser Interface:** Click the "Plug Group Directory" link on the left hand side of the screen to display the Plug Group Directory menu. From the Plug Group Directory menu, click the "View/Modify Plug Group" link. The RSM-8R4 will display a menu that lists all currently defined Plug Groups. Select the "Delete Plug Group" button, then click the down arrow, scroll to the Plug Group you wish to delete, select the Plug Group, and then click "Delete Plug Group." The RSM-8R4 will display a screen that lists details for the specified Plug Group; click "Delete Plug Group" to confirm deletion.

> **Note:** *Deleted accounts cannot be automatically restored.*

```
PLUG PARAMETERS

 1. Plug 1 Name:                Outlet1
 2. Plug 1 Boot/Seq. Delay:     0.5 Secs
 3. Plug 1 Power Up Default:    On
 4. Plug 1 Boot Priority    :   1
 5. Plug 2 Name:                Outlet2
 6. Plug 2 Boot/Seq. Delay:     0.5 Secs
 7. Plug 2 Power Up Default:    On
 8. Plug 2 Boot Priority    :   2
 9. Plug 3 Name:                Outlet3
10. Plug 3 Boot/Seq. Delay:     0.5 Secs
11. Plug 3 Power Up Default:    On
12. Plug 3 Boot Priority    :   3
13. Plug 4 Name:                Outlet4
14. Plug 4 Boot/Seq. Delay:     0.5 Secs
15. Plug 4 Power Up Default:    On
16. Plug 4 Boot Priority    :   4

Enter: #<CR> to select,
       <ESC> to exit and save configuration ...
```

Figure 5.7: The Plug Parameters Menu (Text Interface)

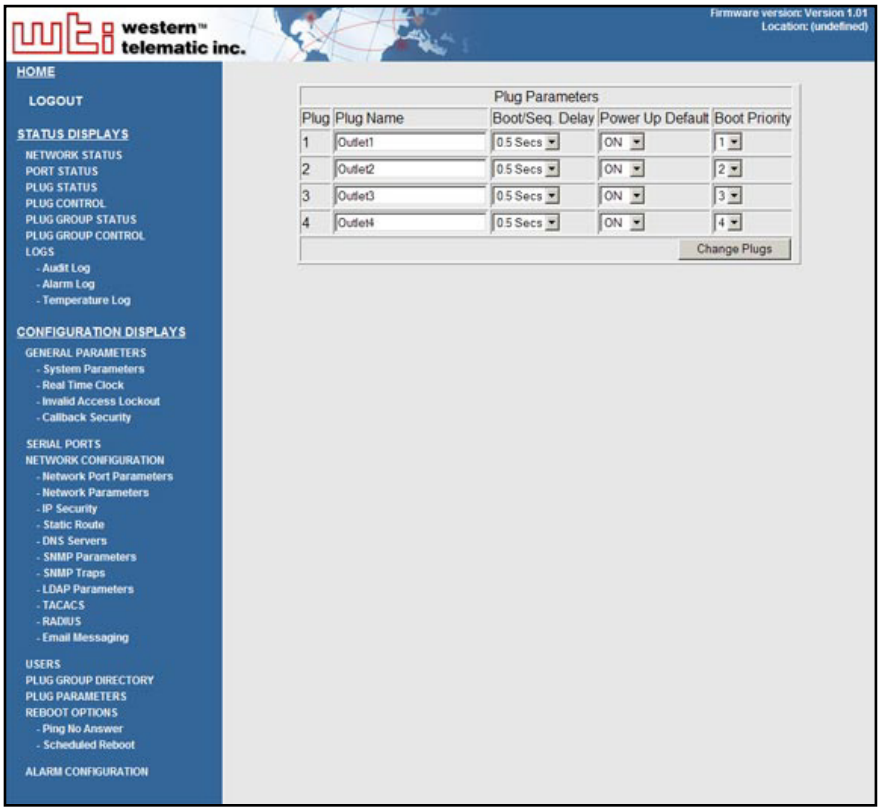

Figure 5.8: The Plug Parameters Menu (Web Browser Interface)

5.7. Defining Plug Parameters

The Plug Parameters Menu is used to define Plug Names, boot/sequence delay times and Power Up Default values for each of the RSM-8R4's Switched AC Outlets. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands. To define Plug Parameters, proceed as follows:

- **Text Interface:** Type **`/PL`** and then press **[Enter]**. The Plug Parameters Menu will be displayed as shown in Figure 5.7. To define Plug Parameters, key in the number for the desired parameter, press **[Enter]** and then follow the instructions in the resulting submenu.
- **Web Browser Interface:** Click the "Plug Parameters" link on the left hand side of the screen to display the Plug Group Directory menu (Figure 5.8.) When you are finished selecting Plug Parameters, click the "Change Plugs" button to apply the new parameters.

The Plug Parameters Menu allows you to define the following parameters:

- **Plug Name:** (Up to 16 Characters.)

  Note: *Plug Names cannot begin with a number, dash (-), underscore character (_), forward slash character (/) or backslash character (\), and cannot include non printable characters, spaces, asterisks (*), colons (:), the plus symbol (+) or quotation marks.*

- **Boot/Seq. Delay:** When more than one plug is switched On or a reboot cycle is initiated, the Boot/Sequence delay determines how much time will elapse before the next plug is switched On. When the Boot/Sequence Delay is applied, the RSM-8R4 will wait for the user-defined delay period before switching On the next plug. This allows time for the device connected to the first plug to adequately "wake up" before switching on power to the device connected to the next plug. When Reboot cycles and switching actions are initiated, the Boot/Sequence Delay will be applied as follows: (Default = 0.5 Second.)

  - Reboot Cycle Delay: During a reboot cycle, the RSM-8R4 will first switch all selected plugs "Off" (with a 0.5 second pause between each "Off" operation), and then begin to switch selected plugs back On again, pausing for the user-defined Boot/Sequence Delay before switching On the next plug. For example, if the Boot/Sequence Delay for Plug 3 is ten seconds, then the RSM-8R4 will pause for ten seconds before proceeding to the next plug.
  - "On" Sequence Delay: When two or more plugs are switched On, the RSM-8R4 will pause for the user-defined Boot/Sequence Delay before switching On the next plug.

- **Power Up Default:** Determines how this plug will react when the "Default All Plugs" command (/DPL) is invoked, or after power to the unit has been interrupted and then restored. After the default command is invoked, or power is restored, the RSM-8R4 will automatically switch each plug On or Off as specified by the Power-Up Default. (Default = On).

Notes:

- *If you have accessed command mode using an account that has Administrator or SuperUser level command access, then the Default command will be applied to all switched plugs.*
- *If you have accessed command mode using an account that has User level command access, then the Default command will only be applied to the plugs allowed by your account.*
- *The Default command is not available to ViewOnly level accounts.*

- **Boot Priority:** When commands are applied to two or more plugs, the Boot Priority parameter determines the order in which the plugs will be switched On. The Plug that has been assigned a Boot Priority of "1" will always be switched on first, followed by the plug that has been assigned the Boot Priority of "2", and so forth. When you assign a boot priority to any given plug, then all subsequent plugs will have their priority lowered by one. For more information on the Boot Priority parameter, please refer to Section 5.7.1. (Default = All plugs prioritized according to Plug Number.)

5.7.1. The Boot Priority Parameter

Normally, when an "On" or "Reboot" command is invoked, the RSM-8R4 will switch on it's plugs in their default, numeric order. Although in many cases, the default, numeric order will work fine, there are other cases where an individual device (such as a router) must be switched on first, in order to support a second device that will be switched on later.

The Boot Priority Parameter simplifies the process of setting the order in which plugs are switched On, by assigning a priority number to each plug, rather than by requiring the user to make certain that devices are always connected to the RSM-8R4 in a set order. Likewise, when new devices are added to your equipment rack, the Boot Priority Parameter eliminates the need to unplug all existing devices and then rearrange the plugs connected to the RSM-8R4 (and re-define plug parameters) to ensure that they are switched on in the desired order.

Notes:

- *No two plugs can be assigned the same Boot Priority number.*
- *When a higher Boot Priority is assigned to any given plug, all subsequent plugs will have their boot priorities lowered by a factor of 1.*
- *The Boot Priority is also displayed on the Plug Status Screen.*

5.7.1.1. Example 1: Change Plug 3 to Priority 1

In the Example shown in Figure 5.9, we start out with all Plugs set to their default Boot Priorities, with Plug 1 first, Plug 2 second and so forth.

Next, the Boot Priority for Plug 3 is changed to Priority 1. This means that Plug 3 will now be switched On first after a reboot, and that Plug 1 will now be switched On second, Plug 2 will be third, etc..

Note that when the Boot Priority for Plug 3 is set to 1, the Boot Priorities for all plugs that were previously Booted before plug A1 are now lowered by a factor of one

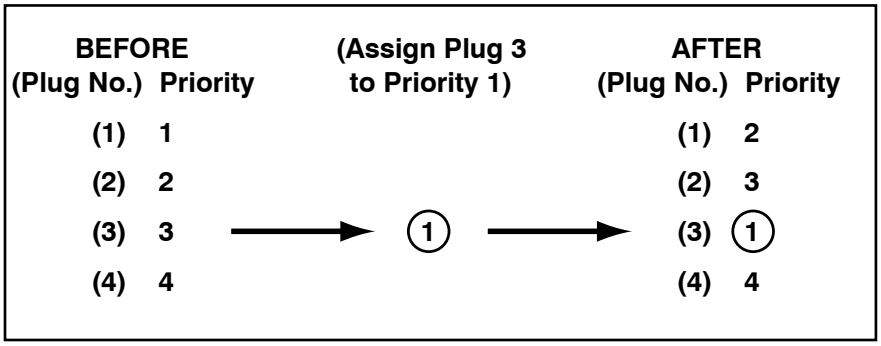

Figure 5.9: Boot Priority Example 1

5.7.1.2. Example 2: Change Plug 4 to Priority 2

In the second Example shown in Figure 5.10, we start out with Boot Priorities for the plugs set as they were at the end of Example 1; Plug 3 is first, Plug 1 is second, Plug 2 is third and Plug 4 is fourth.

Next, the Boot Priority for Plug 4 is changed to Priority 2. This means that Plug 3 will continue to be switched on first after a reboot, but now Plug 4 will be switched on second, Plug 1 will be third and Plug 2 will be fourth.

Once again, note that when the Boot Priority for Plug 4 is set to 2, the Boot Priorities for all plugs that were previously Booted before plug 4 are now lowered by a factor of one

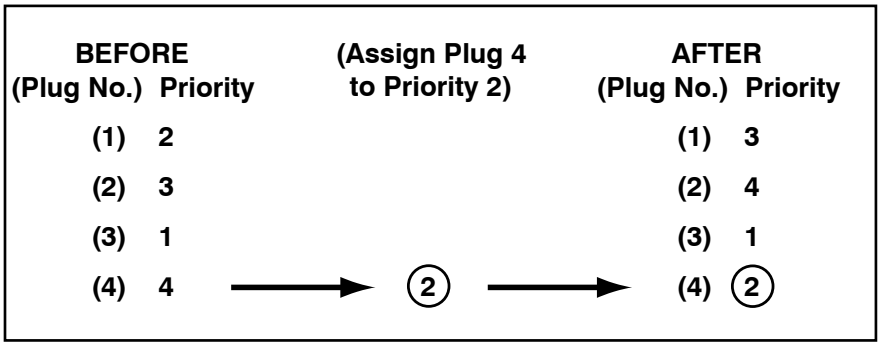

Figure 5.10: Boot Priority Example 2

5.8. Serial Port Configuration

The Serial Port Configuration menus allow you to select parameters for the RSM-8R4's eight Serial Ports as well as the Internal Modem Port.

The Serial Ports can be configured for connection to a local PC or Modem. In addition, the Serial Port Configuration menu can also be used to set communications parameters, disable Administrator level commands and also select a number of other Serial Port Parameters described in Section 5.8.2.

When responding to prompts, invoking commands, and selecting items from port configuration menus, note the following:

- Configuration menus are only available to Administrator level accounts.
- If you are configuring the RSM-8R4 via modem, modem parameters will not be changed until after you exit command mode and disconnect from the unit.
- Port 9 is the Internal Modem Port.

5.8.1. RS232 Port Modes

The RSM-8R4 offers four different serial port operation modes:

- **Any-to-Any Mode:** Allows communication between connected ports and permits access to command mode. Any-to-Any Mode Ports can be connected to other Any-to-Any, Passive, Buffer or Modem Mode Ports by invoking the /C command. The Any-to-Any Mode is available to all ports (except the Internal Modem Port) and is the default Port Mode for Ports 1 and 2.
- **Passive Mode:** Allows communication between connected ports, but does *not* allow access to command mode. Passive Mode Ports can be connected by accessing command mode from a free Any-to-Any or Modem Mode port and invoking the /C command. Passive Mode is not available at Port 1, the Network Port or the Internal Modem Port, and is the default mode at Ports 3 through 8.
- **Buffer Mode:** Allows storage of data received from connected devices. Collected data can be retrieved by accessing command mode from a free Any-to-Any or Modem Mode Port, and issuing the Read Buffer (/R) Command. Furthermore, Buffer Mode ports can also be configured to support the Syslog and SNMP Trap features, discussed in Sections 11 and 12. The Buffer Mode is not available at Port 1, the Network Port or the Internal Modem Port.
- **Modem Mode:** Allows communication between connected ports, permits access to command mode and simplifies connection to an external modem. Modem Mode ports can perform all functions normally available in Any-to-Any Mode, but Modem Mode also allows definition of a Hang-Up String, Reset String, and Initialization String. The Modem Mode is not available at the Network Port and is the default mode for the Internal Modem Port (Port 9.)

For more information on Port Modes, please refer to Section 9.

```
PORT PARAMETERS #01:

COMMUNICATION SETTING                  PORT MODE PARAMETERS
 1. Baud Rate:            9600         21. Port Name:            (undefined)
 2. Bits/Parity:          8-None       22. Port Mode:            Any-to-Any
 3. Stop Bits:            1            23. DTR Output:           Pulse
 4. Handshake:            RTS/CTS      24. Modem Params:         ---
                                       25. Buffer Params:        ---

GENERAL PARAMETERS                     NETWORK SERVICES
11. Administrator Mode:   Permit       31. Direct Connect:       Off
12. Logoff Char:          ^X               Telnet Port:          ---
13. Sequence Disc:        One Char         SSH Port:             ---
14. Inact Timeout:        5 Min            Raw Port:             ---
15. Command Echo:         On           32. Syslog:               ---
16. Accept Break:         On           33. SNMP Trap Lv:         ---


Enter #<CR> to change, "<" for previous port, ">" for next port,
      <ESC> to exit and save configuration...
```

Figure 5.11: Serial Port Configuration Menu (Text Interface)

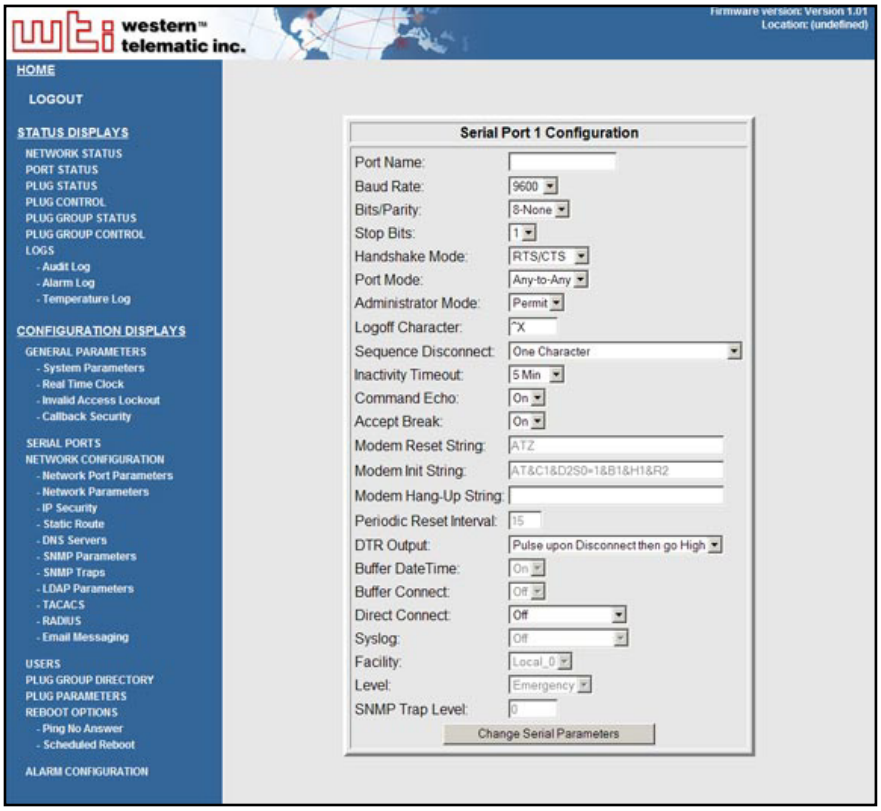

Figure 5.12: Port Configuration Menu (Web Browser Interface)

5.8.2. The Serial Port Configuration Menu

To configure the RSM-8R4's Serial Ports or Internal Modem Port, proceed as follows:

- **Text Interface:** Type **`/P n`** and then press **[Enter]** (where **`n`** is the name or number of the desired port). To configure the RSM-8R4's Internal Modem Port, type **`/p 9`** and then press **[Enter]**. The Serial Port Parameters menu will be displayed as shown in Figure 5.11.
- **Web Browser Interface:** Click the "Serial Ports" link on the left hand side of the screen to display the Serial Port Configuration Menu. From the Serial Port Configuration menu, use the dropdown menu to select the desired port and then click on the Select Port button to display the appropriate Serial Port Configuration Menu, as shown in Figure 5.12.

The Serial Port Configuration menu allows the following parameters to be defined. Note that all of these parameters are available via both the Text Interface and Web Browser Interface, and that parameters selected via one interface are also applied to the other.

Communication Settings:

- **Baud Rate:** Any standard rate from 300 bps to 115.2K bps. (Defaults; Serial Ports 1 to 8 = 9600 bps; Internal Modem Port = 57.6K bps)
- **Bits/Parity:** (Default = 8-None).
- **Stop Bits:** (Default = 1).
- **Handshake Mode:** XON/XOFF, RTS/CTS (hardware), Both, or None. (Default = RTS/CTS).

General Parameters:

- **Administrator Mode:** Permits/denies port access to Administrator level accounts. When enabled (Permit), the port will be allowed to invoke Administrator level commands, providing they are issued by an account that permits them. If disabled (Deny), then accounts that permit Administrator level commands will not be allowed to access command mode via this port. (Default = Permit).

  Note: *Administrator Mode cannot be disabled at Serial Port 1 (the SetUp port.)*

- **Logoff Character:** The Logoff Character determines the command(s) or character(s) that must be issued at this port in order to disconnect. Note that the Logoff Character does not apply to Direct Connections. (Default = **`^x.`**)
- **Sequence Disconnect:** Enables/Disables and configures the Resident Disconnect command. This offers the option to disable the Sequence Disconnect, select a one character format or a three character format. (Default = One Character.)
- **Inactivity Timeout:** Enables and selects the Timeout Period for this port. If enabled, the Serial Port will disconnect when no additional data activity is detected for the duration of the timeout period. (Default = 5 Minutes.)
- **Command Echo:** Enables or Disables command echo at this Serial Port. When disabled, commands that are sent to the Serial Port will still be invoked, but the actual keystrokes will not be displayed on your monitor. (Default = On.)

- **Accept Break:** Determines whether the port will accept breaks received from the attached device. When enabled, breaks received at the port will be passed to any port that this port is connected to. When disabled, breaks will be refused at this port. (Default = On.)

Port Mode Parameters:

- **Port Name:** Allows you to assign a name to the Serial Port. (Defaults; Serial Ports 1 to 8 = undefined; Internal Modem Port = MODEM.)
- **Port Mode:** The operation mode for this port. (Defaults; Serial Ports 1 and 2 = Any-to-Any Mode; Serial Ports 3 to 8 = Passive Mode; Internal Modem Port = Modem Mode)

Notes:

- *Passive Mode and Buffer Mode are not available at Serial Port 1 (the Setup Port.)*
- *The Port Mode for the Internal Modem Port cannot be changed, and will always be set to Modem Mode.*

Depending on the Port Mode selected, the RSM-8R4 will also display the additional prompts listed below. In the Text Interface, these parameters are accessible via a submenu, which will only be active when the appropriate port mode is selected. In the Web Browser Interface, fields will be "grayed out" unless the corresponding port mode is selected.

- **Any-to-Any Mode:** Allows communication with a local PC and permits access to command mode. When Any-to-Any Mode is selected, the following mode specific parameter can also be defined:
  - **DTR Output:** Determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed for 0.5 seconds and then held high. (Default = Pulse.)
- **Modem Mode:** Permits access to command mode and simplifies connection to an external modem. Modem Mode ports can perform all functions normally available in Any-to-Any Mode, but Modem Mode also allows definition of a Hang-Up String, Reset String, and Initialization String:
  - **Reset String:** Redefines the modem reset string. The Reset String can be sent prior to the Initialization string. (Default = **`ATZ`.**)
  - **Initialization String:** Defines a command string that can be sent to initialize a modem to settings required by your application. (Default = **`AT&C1&D2S0=1&B1&H1&R2`**)
  - **Hang-Up String:** Although the RSM-8R4 will pulse the DTR line to hang-up an attached modem, the Hang-Up string is often useful for controlling modems that do not use the DTR line. (Default = undefined.)
  - **Periodic Reset Value:** Determines how often the Reset String will be sent to the modem at this port. (15 Minutes.)

Note: *When communicating with the RSM-8R4 via modem, these parameters will not be changed until after you exit command mode and disconnect.*

- **Buffer Parameters:** When the Buffer Mode is selected, the following mode specific parameters may be defined:
  - **Date/Time Stamp:** Enables/disables the Time/Date stamp for buffered data at this port. When enabled, the RSM-8R4 will add a time/date stamp whenever five seconds elapse between data items received. (Default = On.)
  - **Buffer Connect:** When enabled, the RSM-8R4 will continue to Buffer captured data while you are connected to this Buffer Mode port. (Default = Off.)

Network Services:

- **Direct Connect:** Direct Connect allows users to access the RSM-8R4 and automatically create a connection between the Network Port and a specific serial port by including the appropriate Telnet port number in the connect command (e.g. Port 5 = 2105). For more information, please refer to Section 10. As described below, the Direct Connect feature offers three options. (Default = Off.)
  - **Off:** Telnet users will *not* be able to employ the Direct Connect feature to connect to this port.
  - **On - No Password:** Telnet users *will* be able to employ the Direct Connect feature to connect to this port without entering a password.
  - **On - Password:** Telnet and SSH users will be able to use Direct Connect to connect to this port, but will be required to enter a password before the connection is established.

  Note: *If "On - Password" is selected, and Administrator level commands are disabled at the Network Port, then only accounts that do not permit Administrator level commands will be allowed to establish a direct connection via the Network Port. If Administrator level commands are disabled at a given port, then that port will not allow access by accounts that permit Administrator level commands.*

  When the Port Parameters menu is accessed via the Text Interface and the Direct Connect feature is enabled, the menu also lists both Direct Connect port numbers for this port (port numbers are not listed in the Web Browser Interface.)

  - **Telnet Port:** The Telnet port number employed to create a Direct Connection to this port using standard Telnet protocol.
  - **SSH Port:** When Direct Connect (Item 31) is set at "On - Password", this line will display the Telnet port number used to create a Direct Connection to this port using SSH protocol. For more information, please refer to Section 10.
  - **Raw Port:** The Telnet port number that is used to create a Direct Connection to this port using Raw Socket protocol.

- **Syslog:** The Syslog feature is used to create records of each buffer event. As event records are created, they are sent to a Syslog Daemon, at an IP address defined via the Network Parameters menu. For more information, please refer to Section 11. The Syslog feature offers three possible settings. (Default = Off)

  - **Off:** Syslog disabled. (Default)
  - **On - Not Connected:** Messages will only be generated when a user is *not* connected to a buffer port (either by /C or direct connect.) This prevents information captured from the attached device from being put into Syslog messages while a user is connected to a buffer port.
  - **On - Always:** *All* captured information will be sent out via Syslog message; whether a user is connected or not.

  Notes:

  - *Syslog is only available at Buffer Mode Ports.*
  - *This option is not available to serial port 1, because port 1 cannot be configured as a Buffer Mode Port.*

  The Port Parameters menu also offers two additional items used to set the priority of Syslog messages generated by this port:

  - **Facility:** The facility under which this port will log messages. (Default = Local_0.)
  - **Level:** The severity (or priority) of messages generated by this port. (Default = Emergency.)

- **SNMP Trap Level:** Enables/disables the SNMP Trap function and sets the byte level that will generate traps at this port. If set to "0" (zero), then SNMP Traps are disabled at this port.

  If this value is set between 1 and 32,767, then the SNMP Trap function is enabled, and traps will be sent to the SNMP Managers whenever the buffer for this port reaches the specified level. For more information, please refer to Section 12. (Default = Off.)

  Note:

  - *The SNMP Trap feature only applies to Buffer Mode Ports.*
  - *This option is not available to serial port 1. This is because Port 1 is reserved as a Set Up Port, and cannot be configured as a Buffer Mode Port.*

5.8.3. Copying Parameters to Several Serial Ports (Text Interface Only)

If you are configuring the RSM-8R4 via the Text Interface, the /CP (Copy Parameters) command can be used to select identical parameters for one or more serial ports. When the /CP command (Copy Port Parameters) is invoked, the unit will display a menu which allows you to select parameters, and copy them to all or several RSM-8R4 serial ports. The Copy Port Parameters menu can set all parameters for the specified port(s), or define only a select group of parameters for a specific group of ports.

Notes:

- *The /CP command is not available via the Web Browser Interface.*
- *The /CP command will not copy parameters to the Network Port.*
- *The /CP command is only available to accounts and ports that permit Administrator level commands.*
- *The /CP command cannot be used to set Port 1 to Passive or Buffer Mode, or to disable the Administrator Mode at Port 1.*

To copy parameters to all or several RS-232 serial ports, proceed as follows:

1. Access the RSM-8R4 command mode via the Text Interface, using an account and port that permit access to Administrator level commands.
2. Invoke the **`/CP`** command at the command prompt; the Copy Parameters menu will be displayed. The following command line options are available:
   a) **Copy to All Ports:** Type **`/CP`** **[Enter]**.
   b) **Copy to a Range of Ports:** Type **`/CP m-n`** **[Enter]**. Where **`m`** and **`n`** are port numbers that specify the desired range. For example, to copy parameters to ports 3 through 7, type **`/CP 3-7`** and press **[Enter]**.
   c) **Copy to Several Ports:** Type **`/CP m,n,x`** **[Enter]**. Where **`m`**, **`n`** and **`x`** are the numbers of the desired ports. For example, to copy parameters to ports 3, 5, and 7, type **`/CP 3,5,7`** **[Enter]**.
   d) **Combination:** To invoke the /CP command in a manner where a range of ports is specified, along with several ports outside the range, type **`/CP m,n,x-z`** **[Enter]**. Where **`m`**, **`n`**, **`x`**, and **`z`** are port numbers. For example to copy parameters to ports 3 and 5 *plus* ports 7 through 9, type **`/CP 3,5,7-9`** **[Enter]**.
3. **Selecting Parameters:** To select parameters to be copied, key in the number for the desired parameter, press **[Enter]**, then follow the instructions in the submenu.
4. **Clear Menu:** After defining several parameters, if you wish to clear the /CP menu and start again, type – (dash) and press **[Enter]**, the menu will be reset.
5. **Exit Without Copy:** To exit from the Copy Parameters menu *without* copying selected parameters, type **`X`** **[Enter]**. The RSM will return to the command prompt.
6. **Copy Parameters:** When you have finished selecting parameters, press **[Esc]** to copy the selected parameters.
7. The RSM-8R4 will display a confirmation prompt before executing the copy command. Type **`Y`** to proceed or **`N`** to cancel the command, and then press **[Enter]**.

```
NETWORK PARAMETERS:

COMMUNICATION SETTING                    SERVERS AND CLIENTS
1.  IP Address:         255.255.255.0    21. Telnet Access:      On
2.  Subnet Mask:        255.255.255.0    22. SSH Access:         On
3.  Gateway Addr:       255.255.255.0    23. Web Access:         On
4.  DHCP:               Off              24. SYSLOG Addr:        Off
5.  IP Security:        Off              25. SNMP Access:        Off
6.  Static Route:       Off              26. SNMP Trap:          Off
7.  DNS Servers:        (undefined)      27. LDAP:               Off
                                         28. TACACS:             Off
GENERAL PARAMETERS                       29. RADIUS:             Off
11. Administrator Mode:Permit            30. PING Access:        On
12. Logoff Char:        ^X               31. Multiple Logins:    On
13. Sequence Disc:      One Char         32. Email Message:      Off
14. Inact Timeout:      Off              33. Outbound Access:    Off
15. Command Echo:       On               34. Raw Socket Access: Off
16. Accept Break:       On


Enter: #<CR> to change,
       <ESC> to exit and save configuration ...
```

Figure 5.13: Network Parameters Menu (Text Interface)

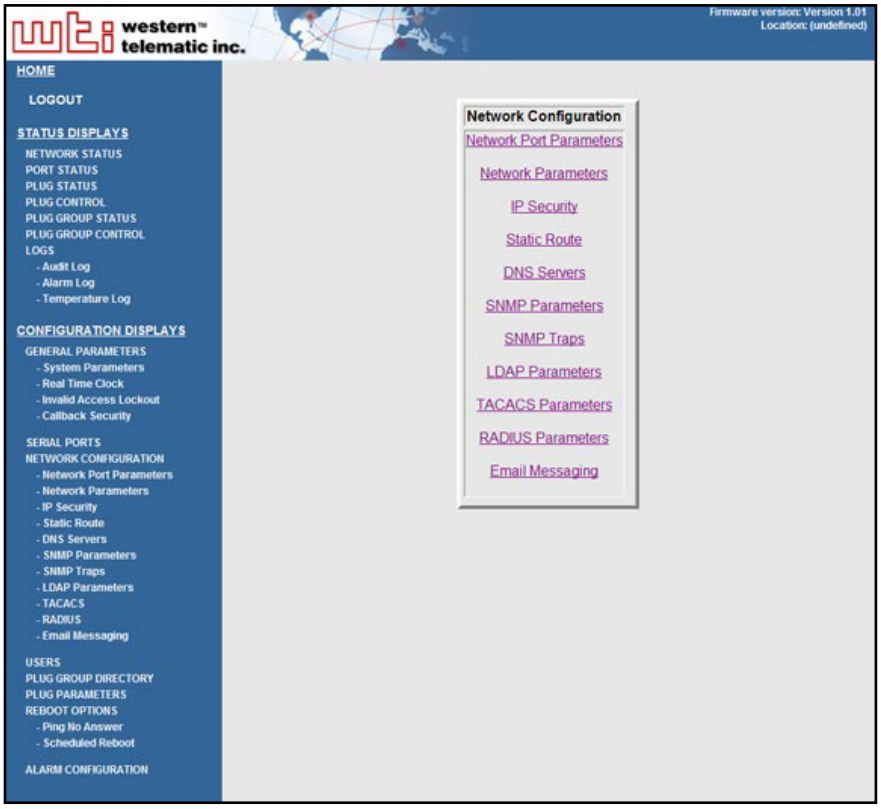

Figure 5.14: Network Configuration Menu (Web Browser Interface)

5.9. Network Configuration

The Network Parameters Menus are used to select parameters and options for the Network Port and also allow you to implement various security and authentication features.

Although the Web Browser Interface and Text Interface allow definition of essentially the same parameters, parameters are arranged differently in the two interfaces. In the Text Interface, most network parameters are defined via one menu. But in the Web Browser Interface, network parameters are divided into separate menus as described in this section.

To access the Network Parameters Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]**. The Network Parameters Menu shown in Figure 5.13 will be displayed.
- **Web Browser Interface:** Click on the "Network Configuration" link on the left hand side of the screen. The RSM-8R4 will display the Network Configuration menu shown in Figure 5.14, which allows you to access the various submenus used to configure the network port.

Notes:

- *Settings for network parameters depend on the configuration of your network. Please contact your network administrator for appropriate settings.*
- *The Network Parameters Menu selects parameters for all 16 logical Network Ports.*
- *When a new IP Address is selected, or the status of the DHCP feature is changed, the unit will disconnect and reconfigure itself with the new values when you exit the Network Parameters Menu. When configuring the unit via Web or Telnet, make certain your DHCP server is set up to assign a known, fixed IP address in order to simplify reconnection to the unit after the new address has been assigned.*
- *The Network Parameters menu is only available when you have logged into command mode using an account and port that permit Administrator level commands (Administrator Mode enabled.)*

The Network Parameters menu allows you to define the parameters discussed in the following sections. Note that although the descriptions of network parameters are arranged according to the Web Browser Interface, in the Text Interface, most parameters are included in a single menu.

5.9.1. Network Port Parameters

In the Text Interface, these parameters are accessed via the main Network Configuration menu (Figure 5.13.) In the Web Browser Interface, these parameters are found by clicking the "Network Port Parameters" link on the left hand side of the screen to display the Network Port Configuration Menu.

- **Administrator Mode:** Permits/denies port access to accounts that allow Administrator level commands. When enabled (Permit), the port will be allowed to invoke Administrator level commands, providing they are issued by an account that permits them. If disabled (Deny), then accounts that permit Administrator level commands will not be allowed to access command mode via this port. (Default = Permit)

- **Logoff Character:** Defines the Logoff Character for this port. This determines which command(s) must be issued at this port in order to disconnect from a second port. (Default = **^x** (**[Ctrl]** plus **[X]**).)

  Note: *The Sequence Disconnect parameter can be used to pick a one character or a three character logoff sequence.*

- **Sequence Disconnect:** Enables/Disables and configures the Resident Disconnect command. Offers the option to either disable the Sequence Disconnect, or select a one character, or three character command format. (Default = One Character).

  Notes:

  - *The One Character Disconnect is intended for situations where the destination port should **not** receive the disconnect command. When the Three Character format is selected, the disconnect sequence **will** pass through to the destination port prior to breaking the connection.*
  - *When Three Character format is selected, the Resident Disconnect uses the format* "**[Enter]**`LLL`**[Enter]**"*, where* `L` *is the selected Logoff Character.*

- **Inactivity Timeout:** Enables and selects the Inactivity Timeout period for the Network Port. If enabled, and the port does not receive or transmit data for the specified time period, the port will disconnect. (Default = 5 Minutes).

- **Command Echo:** Enables or Disables the command echo for the Network Port. (Default = On).

- **Accept Break:** Determines whether the port will accept breaks received from the attached device, and pass them along to a connected port. When enabled, breaks received at this port will be passed to any port this port is connected to, and sent to the device connected to the other port. When disabled, breaks will be refused at this port. (Default = On.)

- **Multiple Logins:** If the RSM-8R4 is installed in an environment that *does not* include communication via an open network (local communication only), then the Multiple Logins parameter can be used to determine whether or not multiple users will be able to communicate with the unit at the same time. If this parameter is set to "Off" then only one user will be allowed to communicate with the unit at a time. (Default = On.)

  Note: *The "Multiple Logins" prompt is not included in the Web Browser Interface.*

5.9.2. Network Parameters

In the Text Interface, these parameters are accessed via the Network Configuration menu (Figure 5.13.) In the Web Browser Interface, these parameters can be found by clicking the "Network Parameters" link on the left hand side of the screen to display the Network Parameters menu.

- **IP Address:** (Default = 192.168.168.168.)
- **Subnet Mask:** (Default = 255.255.255.0.)
- **Gateway Address:** (Default = undefined.)
- **DHCP:** Enables/Disables Dynamic Host Configuration Protocol. When this option is "On", the RSM-8R4 will perform a DHCP request. Note that in the Text Interface, the MAC address for the RSM-8R4 is listed on the Network Status Screen. (Default = Off.)

  Note: *Before configuring this feature via Telnet or Web, make certain your DHCP server is set up to assign a known, fixed IP address. You will need this new IP address in order to reestablish a network connection with the RSM-8R4 unit.*

- **Telnet Access:** Enables/disables Telnet access. When Telnet Access is "Off," users will not be allowed to establish a Telnet connection to the unit. (Default = On.)
- **Telnet Port:** Selects the TCP/IP port number that will be used for Telnet connections. Note that in the Text Interface, this item is defined via a submenu, which is displayed when the Telnet Access parameter is selected (item number 21.) (Default = 23.)
- **SSH Access:** Enables/disables SSH communication. (Default = On.)
- **SSH Port:** Selects the TCP/IP port number that will be used for SSH connections. Note that in the Text Interface, this item is defined via a submenu, which is displayed when the SSH Access parameter is selected (item number 22.) (Default = 22.)

- **HTTP Access (Web Access):** Enables/disables the Web Browser Interface. When disabled, users will not be allowed to contact the unit via the Web Browser Interface. (Default = Off.)
- **HTTP Port:** Selects the TCP/IP port number that will be used for SSH connections. (Default = 80.)
- **HTTPS Access:** Enables/disables HTTPS communication. For instructions on setting up SSL encryption, please refer to Section 14. (Default = Off.)
- **HTTPS Port:** Selects the TCP/IP port number that will be used for HTTPS connections. (Default = 443.)

Notes:

- *In the Text Interface, HTTP and HTTPS parameters reside in a separate submenu. To enable and configure HTTP and HTTPS Access via the Text Interface, access the Network Configuration Menu as described in Section 5.9, then type* **23***, press* ***[Enter]*** *and use the resulting submenu (Figure 14.1) to select parameters as described in Section 14.*
- *When the Web Access parameter is accessed via the Text Interface, the resulting submenu will also allow you to select SSL (encryption) parameters as described in Section 14.*

- **SYSLOG Address:** The IP Address or domain name (up to 64 characters) for the Syslog Daemon that will receive log records generated by the RSM-8R4. For more information, please refer to Section 12. (Default = undefined.)
- **Ping Access:** Enables/Disables response to the ping command. When Disabled, the RSM-8R4 will not respond to Ping commands. Note that disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm. (Default = On.)
- **Outbound Access:** Enables/Disables the ability to create outbound Telnet and SSH connections via the RSM-8R4's Network Port. When enabled, users who are connected to the RSM-8R4 command mode via one of the serial ports will be able to connect to the network port, and then invoke a Telnet or SSH command to create an outbound connection. For example, to create an outbound Telnet or SSH connection, first make certain that this option is enabled, then access command mode via the Text Interface at a free serial port. At the RSM> prompt, type **`/C N`** and then press **[Enter]** to connect to the network port, then invoke the Telnet command as you normally would. (Default = Off.)
- **Raw Socket Access:** Enables/Disables Raw Socket Protocol access via Direct Connect at the Network Port. If this parameter is disabled (Off), then users will not be allowed to create Raw Socket Direct Connections to RSM-8R4 serial ports. (Default = Off.)

5.9.3. IP Security

The IP Security feature allows the RSM-8R4 to restrict unauthorized IP addresses from establishing inbound Telnet connections to the unit. This allows you to grant Telnet access to only a specific group of IP addresses, or block a particular IP address completely. In the default state, the RSM-8R4 accepts incoming IP connections from all hosts.

In the Text Interface, IP Security parameters are defined via item 5 in the Network Configuration menu (Figure 5.13.) In the Web Browser Interface, these parameters are found by clicking the "IP Security" link on the left hand side of the screen. In the default state, IP Security is disabled.

The IP Security Function employs a TCP Wrapper program which allows the use of standard, Linux operators, wild cards and net/mask pairs to create a host based access control list.

The IP Security configuration menus include "hosts.allow" and "hosts.deny" client lists. Basically, when setting up IP Security, you must enter IP addresses for hosts that you wish to allow in the Allow list, and addresses for hosts that you wish to deny in the Deny list. Since Linux operators, wild cards and net/mask pairs are allowed, these lists can indicate specific addresses, or a range of addresses to be allowed or denied.

When the IP Security feature is properly enabled, and a client attempts to connect, the RSM-8R4 will perform the following checks:

1. If the client's IP address is found in the "hosts.allow" list, the client will be granted immediate access. Once an IP address is found in the Allow list, the RSM-8R4 will not check the Deny list, and will assume you wish to allow that address to connect.
2. If the client's IP address is not found in the Allow list, the RSM-8R4 will then proceed to check the Deny list.
3. If the client's IP Address *is* found in the Deny list, the client *will not* be allowed to connect.
4. If the client's IP Address *is not* found in the Deny list, the client *will* be allowed to connect, even if the address was not found in the Allow list.

Notes:

- *If the RSM-8R4 finds an IP Address in the Allow list, it will not check the Deny list, and will allow the client to connect.*
- *If both the Allow and Deny lists are left blank, then the IP Security feature will be disabled, and all IP Addresses will be allowed to connect (providing that the proper password and/or SSH key is supplied.)*
- *When the Allow and Deny lists are defined, the user is only allowed to specify the Client List; the Daemon List and Shell Command cannot be defined.*

5.9.3.1. Adding IP Addresses to the Allow and Deny Lists

To add an IP Address to the Allow or Deny list, and begin configuring the IP Security feature, proceed as follows.

Notes:

- *Both the Allow and Deny list can include Linux operators, wild cards, and net/mask pairs.*
- *In some cases, it is not necessary to enter all four "digits" of the IP Address. For example, if you wish to allow access to all IP addresses that begin with "192," then you would only need to enter "192."*
- *The IP Security Configuration menu is only available when the Administrator Mode is active.*

1. Access the IP Security Configuration Menu.

   a) **Text Interface:** Type **`/N`** **[Enter]** to display the Network Configuration Menu. From the Network Configuration Menu, type **`5`** **[Enter]** to display the IP Security Menu.

   b) **Web Browser Interface:** Click on the "IP Security" Link on the left hand side of the screen to display the IP Security Menu shown.

2. **Allow List:** Enter the IP Address(es) for the clients that you wish to allow. Note that if an IP Address is found in the Allow list, the client will be allowed to connect, and the RSM-8R4 will not check the Deny list.

   a) **Text Interface:** Note the number for the first empty field in the Allow list, then type that number at the command prompt, press **[Enter]**, and then follow the instructions in the resulting submenu.

   b) **Web Browser Interface:** Place the cursor in the first empty field in the parameters menu, then key in the desired IP Address, operators, wild cards, and/or net/mask pairs.

3. **Deny List:** Enter the IP Address(es) for the clients that you wish to deny. Note that if the client's IP Address is not found in the Deny List, that client will be allowed to connect. Use the same procedure for entering IP Addresses described in Step 2 above.

5.9.3.2. Linux Operators and Wild Cards

In addition to merely entering a specific IP address or partial IP address in the Allow or Deny list, you may also use any standard Linux operator or wild card. In most cases, the only operator used is "EXCEPT" and the only wild card used is "ALL," but more experienced Linux users may note that other operators and wild cards may also be used.

EXCEPT:
This operator creates an exception in either the "allow" list or "deny" list.

For example, if the Allow list includes a line which reads "192. EXCEPT 192.255.255.6," then all IP address that begin with "192." will be allowed; except 192.255.255.6 (providing that this address appears in the Deny list.)

ALL:
The ALL wild card indicates that all IP Addresses should be allowed or denied. When ALL is included in the Allow list, all IP addresses will be allowed to connect; conversely, if ALL is included in the Deny list, all IP Addresses will be denied (except for IP addresses listed in the Allow list.)

For example, if the Deny list includes a line which reads "ALL EXCEPT 168.255.192.192," then all IP addresses except 168.255.192.192 will be denied (except for IP addresses that are listed in the Allow list.)

Net/Mask Pairs:
An expression of the form "n.n.n.n/m.m.m.m" is interpreted as a "net/mask" pair. A host address is matched if "net" is equal to the bitwise AND of the address and the "mask."

For example, the net/mask pattern "131.155.72.0/255.255.254.0" matches every address in the range "131.155.72.0" through "131.155.73.255."

5.9.3.3. IP Security Examples

1. **Mostly Closed:** Access is denied by default and the only clients allowed, are those explicitly listed in the Allow list. To deny access to all clients except 192.255.255.192 and 168.112.112.05, the Allow and Deny lists would be defined as follows:

   - Allow List:
     1. 192.255.255.192
     2. 168.112.112.05

   - Deny List:
     1. ALL

2. **Mostly Open:** Access is granted by default, and the only clients denied access, are those explicitly listed in the Deny list, and as exceptions in the Allow list. To allow access to all clients except 192.255.255.192 and 168.112.112.05, the Allow and Deny lists would be defined as follows:

   - Allow List:
     1. ALL EXCEPT 192.255.255.192, 168.112.112.05

   - Deny List:
     1. 192.255.255.192, 168.112.112.05

Notes:

- *When defining a line in the Allow or Deny list that includes several IP addresses, each individual address is separated by either a space, a comma, or a comma and a space as shown in Example 2 above.*
- *Take care when using the "ALL" wild card. When ALL is included in the Allow list, it should always include an EXCEPT operator in order to allow the unit to proceed to the Deny list and determine any addresses you wish to deny.*

5.9.4. Static Route

The Static Route menu allows you to type in Linux routing commands that will be automatically executed each time that the unit powers up or reboots. In the Text Interface, the Static Route menu is accessed via item 6 in the Network Configuration menu. In the Web Browser Interface, the Static Route menu is accessed by clicking the Static Route link, located on the left-hand side of the screen.

To access the Static Route Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **6** and press **[Enter]** to display the Static Route Menu.
- **Web Browser Interface:** Click on the "Static Route" link on the left hand side of the screen to display the Static Route Menu.

5.9.5. Domain Name Server

The DNS menu is used to select IP addresses for Domain Name Servers. When web and network addresses are entered, the Domain Name Server interprets domain names (e.g., www.wti.com), and translates them into IP addresses. Note that if you don't define at least one DNS server, then IP addresses must be used, rather than domain names.

To access the Domain Name Server Menu, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **7** and press **[Enter]** to display the Domain Name Server menu.
- **Web Browser Interface:** Click on the "DNS Server" link to display the Domain Name Server menu.

5.9.6. SNMP Access Parameters

These menus are used to select access parameters for the SNMP feature. To define or change SNMP MIB parameters, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **25** and press **[Enter]** to display the SNMP Access (Parameters) Menu.
- **Web Browser Interface:** Click on the "SNMP Parameters" link on the left hand side of the RSM-8R4 Home screen to display the SNMP Parameters menu.

  Note: *After you have configured SNMP Access Parameters, you will then be able to manage the RSM-8R4's User Directory, control power and reboot switching and display unit status via SNMP, as described in Section 13.*

Both the Text Interface and Web Browser Interface allow the following parameters to be defined:

- **Enable:** Enables/disables SNMP Polling. (Default = Off.)

  Note: *This item only applies to external SNMP polling of the RSM-8R4; it does not effect the ability of the RSM-8R4 to send SNMP traps.*

- **Version:** This parameter determines which SNMP Version the RSM-8R4 will respond to. For example, if this item is set to V3, then clients who attempt to contact the RSM-8R4 using SNMPv2 will not be allowed to connect. (Default = V1/V2 Only.)
- **Read Only:** Enables/Disables the "Read Only Mode", which controls the ability to access configuration functions and invoke switching commands. When Enabled, you will not be able to change configuration parameters or invoke other commands when you contact the RSM-8R4 via SNMP. (Default = No.)

  Note: *In order to define user names for the RSM-8R4 via your SNMP client, the Read Only feature must be disabled. When the Read Only feature is enabled, you will not be able to issue configuration commands to the unit via SNMP.*

- **Authentication** / **Privacy:** Configures the Authentication and Privacy features for SNMPv3 communication. The Authentication / Privacy parameter offers two options, which function as follows:

  1. **Auth**/**noPriv:** An SNMPv3 username and password will be required at log in, but encryption will not be used. (Default Setting.)
  2. **Auth**/**Priv:** An SNMPv3 username and password will be required at log in, and all messages will be sent using encryption.

  Notes:

  - *The Authentication / Privacy item is not available when the Version parameter is set to V1/V2.*
  - *If the Version Parameter is set to V1/V2/V3 (all) and Authentication / Privacy parameter is set to "Auth/Priv", then only V3 data will be encrypted.*
  - *The RSM-8R4 supports DES encryption, but does not currently support the AES protocol.*
  - *The RSM-8R4 does not support "noAuth/noPriv" for SNMPv3 communication.*

- **SNMPv3 User Name:** Sets the User Name for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2. (Default = undefined.)
- **SNMPv3 Password:** Sets the password for SNMPv3. Note that this option is not available when the Version parameter is set to V1/V2. (Default = undefined.)
- **SNMPv3 Password Confirm:** This prompt is used to confirm the SNMPv3 password that was entered at the prompt above. Note that this option is not available when the Version parameter is set to V1/V2. (Default = undefined.)
- **Authentication Protocol:** This parameter determines which authentication protocol will be used. The RSM-8R4 supports both MD5 and SHA1 authentication. (Default = MD5.)

Notes:

- *The Authentication Protocol that is selected for the RSM-8R4 must match the protocol that your SNMP client will use when querying the RSM-8R4 unit.*
- *The Authentication Protocol option is not available when the Version parameter is set to V1/V2*

- **SNMP Contact:** (Default = undefined.)
- **SNMP Location:** (Default = undefined.)
- **SNMP Community:** Note that this parameter is not available when the SNMP Version is set to V3. (Default = Public.)

5.9.7. SNMP Trap Parameters

These menus are used to select parameters that will be used when SNMP traps are sent. For more information on SNMP Traps, please refer to Section 12. To define or change SNMP Trap parameters, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **26** and press **[Enter]** to display the SNMP Trap Menu.
- **Web Browser Interface:** Click on the "SNMP Traps" link on the left hand side of the RSM-8R4 Home screen to display the SNMP Traps menu.

Both the Text Interface and Web Browser Interface allow the following parameters to be defined:

- **SNMP Manager 1:** The IP Address for the first SNMP Manager. For more information, please refer to Section 12. (Default = Undefined.)

  Note: *In order to enable the SNMP Trap feature, you must define at least one SNMP Manager.*

- **SNMP Manager 2:** (Default = Undefined.)
- **Trap Community:** (Default = Public.)

5.9.8. LDAP Parameters

The RSM-8R4 supports LADP (Lightweight Directory Access Protocol,) which allows authentication via the "Active Directory" network Directory Service. When LDAP is enabled and properly configured, command access rights can be granted to new users without the need to define individual new accounts at each RSM-8R4 unit, and existing users can also be removed without the need to delete the account from each RSM-8R4 unit.

This type of authentication also allows administrators to assign users to LDAP groups, and then specify which plugs the members of each group will be allowed to control at each RSM-8R4 unit.

In order to apply the LDAP feature, you must first define User Names and associated Passwords and group membership via your LDAP server, and then access the RSM-8R4 command mode to enable and configure the LDAP settings and define port access rights and command access rights for each group that you have specified at the LDAP server.

To access the LDAP Parameters menu, login to RSM-8R4 command mode using a password that permits Administrator level commands and then proceed as follows:

- **Text Interface:** Type **`/N`** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **`27`** and press **[Enter]** to display the LDAP parameters menu.
- **Web Browser Interface:** Click on the "LDAP Parameters" link on the left hand side of the screen to display the LDAP Parameters menu.

Notes:

- *Port and Plug access rights are not defined at the LDAP server. They are defined via the LDAP Group configuration menu on each RSM-8R4 unit and are specific to that RSM-8R4 unit alone.*
- *When LDAP is enabled and properly configured, LDAP authentication will supersede any passwords and access rights that have been defined via the RSM-8R4 user directory.*
- *If no LDAP groups are defined on a given RSM-8R4 unit, then access rights will be determined as specified by the "default" LDAP group.*
- *The "default" LDAP group cannot be deleted.*

The LDAP Parameters Menu allows the following parameters to be defined:

- **Enable:** Enables/disables LDAP authentication. (Default = Off.)
- **LDAP Port:** Defines the port that will be used to communicate with the LDAP server. (Default = 389.)
- **Primary Host:** Defines the IP address or domain name (up to 64 characters) for the primary LDAP server. (Default = undefined.)
- **Secondary Host:** Defines the IP address or domain name (up to 64 characters) for the secondary (fallback) LDAP server. (Default = undefined.)

- **Bind Type:** Sets the LDAP bind request password type. Note that in the Text Interface, when the Bind Type is set to "Kerberos" LDAP, the menu will include an additional prompt (item 14) that is used to select Kerberos parameters as described in Section 5.9.8.5. In the Web Interface, the link to the Kerberos Parameters menu is located at the bottom of the LDAP Parameters Menu. (Default = Simple.)
- **Search Bind DN:** Selects the user name who is allowed to search the LDAP directory. (Default = undefined.)
- **Search Bind Password:** Sets the Password for the user who is allowed to search the LDAP directory. (Default = undefined.)
- **User Search Base DN:** Sets the directory location for user searches. (Default = undefined.)
- **User Search Filter:** Selects the attribute that lists the user name. Note that this attribute should always end with "=%s" (no quotes.) (Default = undefined.)
- **Group Membership Attribute:** Selects the attribute that list group membership(s). (Default = undefined.)
- **Group Membership Value Type:** (Default = DN.)
- **Fallback:** Enables/Disables the LDAP fallback feature. When enabled, the RSM-8R4 will revert to it's own internal user directory (see Section 5.5) if no defined users are found via the LDAP server. In this case, port access rights will then be granted as specified in the default LDAP group. (Default = Off.)
- **LDAP Group Setup:** Provides access to a submenu, which is used to define LDAP Groups as described in the Sections 5.9.8.1 through 5.9.8.4.
- **Kerberos Setup:** Provides access to the Kerberos Setup menu as described in Section 5.9.8.5. When the Bind Type parameter is set to "Kerberos", the Kerberos Setup is used to select Kerberos parameters. Note that in the Text Interface, the link to the Kerberos Setup menu will not be displayed unless the Bind Type has been set to Kerberos.

5.9.8.1. Adding LDAP Groups

Once you have defined several users and passwords via your LDAP server, and assigned those users to LDAP Groups, you must then grant command and port access rights to each LDAP Group at each individual RSM-8R4 unit.

To add LDAP groups to your RSM-8R4 unit, log in to the command mode using a password that permits access to Administrator level commands, and then proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **27** and press **[Enter]** to display the LDAP parameters menu, then type **13** and press **[Enter]** to display the LDAP Group Menu. At the LDAP Group Menu, type **2** and press **[Enter]** to display the Add LDAP Group menu.
- **Web Browser Interface:** Click on the LDAP Parameters link to display the LDAP Parameters menu. At the LDAP Parameters menu, click on the LDAP Group Configuration link to display the LDAP Group Configuration menu, then click the Add LDAP Group link to display the Add LDAP Group menu.

The Add LDAP Group menu allows the following parameters to be defined:

- **LDAP Group:** Note that this name must match the LDAP Group names that you have assigned to users at your LDAP server. (Default = undefined.)
- **Access Level:** Sets the command access level to either Administrator, SuperUser, User or ViewOnly. For more information on Access Levels, please refer to Section 5.4.1. (Default = User.)
- **Port Access:** This item is used to select the serial ports that members of this LDAP group will be allowed to connect. (Default = All Ports Off.)
- **Plug Access:** This item is used to determine which plugs members of this group will be allowed to control. (Default = All Plugs Off.)
- **Plug Group Access:** This item is used to determine which plug groups the members of this LDAP Group will be allowed to control. (Default = undefined.)
- **Service Access:** This item determines how members of this LDAP Group will be allowed to access command mode and whether or not they will be able to create outbound Telnet/SSH connections. The Service Access parameter is used to allow members of this LDAP group to access command mode via Serial Port, Telnet/SSH or any combination thereof, and also enables/disables Outbound Telnet/SSH. (Default; Serial Port = On, Telnet/SSH = On, Outbound Access = Off.)

  Note: *After you have finished defining LDAP Group parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add LDAP Group" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message.*

5.9.8.2 Viewing LDAP Groups

If you want to examine an existing LDAP group definition, the "View LDAP Groups" function can be used to review the group's parameters and Plug Access Settings. To view an existing LDAP group on your RSM-8R4 unit, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **27** and press **[Enter]** to display the LDAP parameters menu, then type **13** and press **[Enter]** to display the LDAP Group Menu, then type **1** and press **[Enter].** The RSM-8R4 will prompt you to select the desired group; key in the name of the group and press **[Enter]**, the RSM-8R4 will display the View LDAP Group screen.
- **Web Browser Interface:** At the RSM-8R4 Home Screen, click on the "LDAP Parameters" link on the left hand side of the screen to display the LDAP Parameters menu. At the LDAP Parameters menu, click on the "LDAP Group Configuration" link to display the LDAP Group Configuration menu, then click the "View/Modify LDAP Group" link to display the Choose LDAP Group menu; use the drop down menu to select the desired group, select "View LDAP Group" and then click the "Choose LDAP Group" button.

5.9.8.3. Modifying LDAP Groups

If you want to modify an existing LDAP Group in order to change parameters or plug access rights, the "Modify LDAP Group" function can be used to reconfigure group parameters. To Modify an existing LDAP Group, access the RSM-8R4 command mode using a password that permits access to Administrator Level commands, and then proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **27** and press **[Enter]** to display the LDAP parameters menu, then type **13** and press **[Enter]** to display the LDAP Group Menu, then type **3** and press **[Enter].** The RSM-8R4 will prompt you to select the desired group; key in the name of the group and press **[Enter]**, the RSM-8R4 will display the Modify LDAP Group screen.
- **Web Browser Interface:** Click on the "LDAP Parameters" link on the left hand side of the screen to display the LDAP Parameters menu. At the LDAP Parameters menu, click on the "LDAP Group Configuration" link to display the LDAP Group Configuration menu, then click the "View/Modify LDAP Group" link to display the Choose LDAP Group menu; use the drop down menu to select the desired group, select "Modify LDAP Group" and then click the "Choose LDAP Group" button.

Once you have accessed the Modify LDAP Group menu, use the menu options to redefine parameters in the same manner that is used for the Add LDAP Group menu, as discussed in Section 5.9.8.1.

> **Note:** *After you have finished modifying LDAP Group parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify LDAP Group" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.9.8.4. Deleting LDAP Groups

The Delete LDAP Group function is used to delete LDAP Groups that are no longer in use. To delete an existing LDAP Group, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **27** and press **[Enter]** to display the LDAP parameters menu, then type **13** and press **[Enter]** to display the LDAP Group Menu, then type **4** and press **[Enter].** The RSM-8R4 will prompt you to select the desired group; key in the name of the group and press **[Enter]**, the RSM-8R4 will delete the specified LDAP Group immediately, without further prompting.
- **Web Browser Interface:** Click on the "LDAP Parameters" link on the left hand side of the screen to display the LDAP Parameters menu. At the LDAP Parameters menu, click on the "LDAP Group Configuration" link to display the LDAP Group Configuration menu, then click the "View/Modify LDAP Group" link to display the Choose LDAP Group menu; use the drop down menu to select the desired group, select "Delete LDAP Group" and then click the "Choose LDAP Group" button to display the Delete LDAP Group menu. If the Delete LDAP Group menu shows the desired group, then click the "Delete LDAP Group" button to immediately delete the group.

5.9.8.5. LDAP Kerberos Set Up

Kerberos is a network authentication protocol, which provides a secure means of identity verification for users who are communicating via a non-secure network.

To access the LDAP Kerberos Set Up menu, access the command mode using a password that permits access to Administrator Level commands and then proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to display the Network Parameters Menu. At the Network Parameters Menu, type **27** and press **[Enter]** to display the LDAP Parameters menu. At the LDAP Parameters Menu, type **5** and press **[Enter]** and then use the resulting submenu to set the Bind Type to Kerberos. Next, return to the LDAP Parameters menu. Note that the LDAP Parameters Menu now includes a prompt which is used to select Kerberos parameters. Type **14** and press **[Enter]** to display the Kerberos Set Up menu.
- **Web Browser Interface:** Click on the LDAP Parameters link on the left hand side of the screen to display the LDAP Parameters menu. At the LDAP Parameters menu, click on the LDAP Kerberos Setup link to display the LDAP Kerberos Setup menu.

The LDAP Kerberos Setup menu allows you to define the following parameters:

- **Port:** (Default = 88.)
- **Realm:** (Default = Undefined.)
- **Key Distribution Centers (KDC1 through KDC5):** (Default = Undefined.)
- **Domain Realms 1 through 5:** (Default = Undefined.)

5.9.9. TACACS Parameters

To access the TACACS Configuration Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to access the Network Configuration Menu. From the Network Configuration Menu, type **28** and press **[Enter]** to display the TACACS Configuration Menu.
- **Web Browser Interface:** Click on the "TACACS Parameters" link, located on the left hand side of the screen, to display the TACACS Configuration Menu.

The TACACS Configuration Menus offer the following options:

- **Enable:** Enables/disables the TACACS feature at the Network Port. (Default = Off.)
- **Primary Address:** Defines the IP address or domain name (up to 64 characters) for your primary TACACS server. (Default = undefined.)
- **Secondary Address:** Defines the IP address or domain name (up to 64 characters) for your secondary, fallback TACACS server (if present.) (Default = undefined.)
- **Secret Word:** Defines the shared TACACS Secret Word for both TACACS servers. (Default = undefined.)
- **Fallback Timer:** Determines how long the RSM-8R4 will continue to attempt to contact the primary TACACS Server before falling back to the secondary TACACS Server. (Default = 15 Seconds.)
- **Fallback Local:** Determines whether or not the RSM-8R4 will fallback to its own password/username directory when an authentication attempt fails. When enabled, the RSM-8R4 will first attempt to authenticate the password by checking the TACACS Server; if this fails, the RSM-8R4 will then attempt to authenticate the password by checking its own internal username directory. (Default = Off.)
- **Authentication Port:** The port number for the TACACS function. (Default = 49.)

5.9.10. RADIUS Parameters

To access the RADIUS Configuration Menus, proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to access the Network Configuration Menu. From the Network Configuration Menu, type **29** and press **[Enter]** to display the RADIUS Configuration Menu.
- **Web Browser Interface:** Click on the "RADIUS Parameters" link on the left hand side of the screen to display the RADIUS Configuration Menu.

The RADIUS Configuration Menus offer the following options:

- **Enable:** Enables/disables the RADIUS feature at the Network Port. (Default = Off.)
- **Primary Address** Defines the IP address or domain name (up to 64 characters long) for your primary RADIUS server. (Default = undefined.)
- **Primary Secret Word:** Defines the RADIUS Secret Word for the primary RADIUS server. (Default = undefined.)
- **Secondary Address:** Defines the IP address or domain name (up to 64 characters) for your secondary, fallback RADIUS server (if present.) (Default = undefined.)
- **Secondary Secret Word:** Defines the RADIUS Secret Word for the secondary RADIUS server. (Default = undefined.)
- **Fallback Timer:** Determines how long the RSM-8R4 will continue to attempt to contact the primary RADIUS Server before falling back to the secondary RADIUS Server. (Default = 3 Seconds.)
- **Fallback Local:** Determines whether or not the RSM-8R4 will fallback to its own password/username directory when an authentication attempt fails. When enabled, the RSM-8R4 will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the RSM-8R4 will then attempt to authenticate the password by checking its own internal username directory. This parameter offers three options:
  - **Off:** Fallback Local is disabled (Default.)
  - **On (All Failures):** Fallback Local is enabled, and the unit will fallback to it's own internal user directory when it cannot contact the Radius Server, or when a password or username does not match the Radius Server.
  - **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to it's own internal user directory when it cannot contact the Radius Server.
- **Authentication Port:** The Authentication Port number for the RADIUS function. (Default = 1812.)
- **Accounting Port:** The Accounting Port number for the RADIUS function. (Default = 1813.)

5.9.11. Email Message Parameters

The Email Parameters menu is used to define parameters for email messages that the RSM-8R4 can send to notify you when an alarm is triggered. To define email message parameters, access the RSM-8R4 Command Mode using a password that permits access to Administrator Level commands and then proceed as follows:

- **Text Interface:** Type **/N** and press **[Enter]** to access the Network Configuration Menu. From the Network Configuration Menu, type **32** and press **[Enter]** to display the Email Configuration Menu.
- **Web Browser Interface:** Click on the "Email Messages" link on the left hand side of the screen to display the Email Configuration Menu.

The Email Configuration menu offers the following options:

- **Enable:** Enables/Disables the Email Messaging feature. When disabled, the RSM-8R4 will not be able to send email messages when an alarm is generated. (Default = On.)
- **SMTP Server:** This prompt is used to define the address of your SMTP Email server. (Default = 192.168.100.43.)
- **Port Number:** Selects the TCP/IP port number that will be used for email connections. (Default = 25.)
- **Domain:** The domain name for your email server. (Default = undefined.)

  Note: *In order to use domain names, you must first define Domain Name Server parameters as described in Section 5.9.5.*
- **User Name:** The User Name that will be entered when logging into your email server. (Default = undefined.)
- **Password:** The password that will be used when logging into your email server. (Default = undefined.)
- **Auth Type:** The Authentication type; the RSM-8R4 allows you to select None, Plain, Login, or CRAM-MD5 Authentication. (Default = Plain.)
- **From Name:** The name that will appear in the "From" field in email sent by the RSM-8R4. (Default = undefined.)
- **From Address:** The email address that will appear in the "From" field in email sent by the RSM-8R4. (Default = undefined.)
- **To Address:** The address(es) that will receive email messages generated by the RSM-8R4. Note that up to three "To" addresses may be defined, and that when Alarm Configuration parameters are selected as described in Section 7, you may then designate one, two or all three of these addresses as recipients for email messages that are generated by the alarms. (Default = undefined.)
- **Send Test Email:** Sends a test email, using the parameters that are currently defined for the Email configuration menu.

  Note: *The "Send Test Email" function is only available via the Text Interface.*

5.10. Save User Selected Parameters

It is strongly recommended to save all user-defined parameters to an ASCII file as described in Section 15. This will allow quick recovery in the event of accidental deletion or reconfiguration of port parameters.

When changing configuration parameters via the Text Interface, make certain that the RSM-8R4 has saved the newly defined parameters before exiting from command mode. To save parameters, press the **[Esc**] key several times until you have exited from all configuration menus and the RSM-8R4 displays the "Saving Configuration" menu and the cursor returns to the command prompt. If newly defined configuration parameters are not saved prior to exiting from command mode, then the RSM-8R4 will revert to the previously saved configuration after you exit from command mode.

6. Reboot Options

In addition to performing reboot cycles in response to commands, the RSM-8R4 can also be configured to automatically reboot outlets when an attached device does not respond to a Ping command (Ping-No-Answer Reboot) or according to a user defined schedule (Scheduled Reboot.)

- **Ping-No-Answer Reboot:** When the Ping-No-Answer feature is enabled, the RSM-8R4 will Ping a user selected IP address at regular intervals. If the IP address does not respond to the Ping command, the RSM-8R4 will reboot one or more user selected outlet(s). Typically, this feature is used to reboot devices when they cease to respond to the Ping command.
- **Scheduled Reboot:** A scheduled reboot is used to initiate a reboot cycle at a user selected time and day of the week. When properly configured and enabled, the RSM-8R4 will reboot one or more outlets on a daily or weekly basis. The Scheduled Reboot feature can also be used to switch outlet(s) Off at a user selected time, and then switch them back On again at a later, user selected time.

This section describes the procedure for configuring and enabling Ping-No-Answer Reboots and Scheduled Reboots.

> **Note:** *When defining parameters via the Text Interface, make certain to press the **[Esc]** key several times to completely exit from the configuration menus and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message is displayed.*

6.1. Ping-No-Answer Reboot

A Ping-No-Answer Reboot can be used to reboot one or more outlets when an attached device does not respond to a Ping Command. In addition, the Ping-No-Answer Reboot feature can also be configured to send an email, Syslog Message or SNMP Trap to notify you whenever a Ping-No-Answer Reboot occurs. Please refer to Section 7.2 for instructions on setting up email alarm notification for Ping-No-Answer reboots.

To set up a Ping-No-Answer Reboot, access command mode using a password that permits access to Administrator level commands and then proceed as follows:

- **Text Interface:** Type **/RB** and press **[Enter]**. The Reboot Options Menu will be displayed. At the Reboot Options menu, type **1** and press **[Enter]** to display the Ping-No-Answer Reboot Directory menu. From the Ping-No-Answer Reboot Directory Menu, you can Add, Modify, View or Delete Ping-No-Answer Reboots as described in the Sections that follow.
- **Web Browser Interface:** Click the "Ping-No-Answer Reboot" link on the left hand side of the screen. The Ping-No-Answer Reboot Configuration menu will be displayed. From the Ping-No-Answer Reboot Configuration menu, you can Add, Modify, View or Delete Ping-No-Answer Reboots as described in the Sections that follow.

6.1.1. Adding Ping-No-Answer Reboots

To add a Ping-No-Answer Reboot, access command mode using a password that permits Administrator Level commands and then proceed as follows:

- **Text Interface:** Access the Ping-No-Answer Reboot Directory menu as described in Section 6.1, then type **2** and press **[Enter]** to display the Add Ping-No-Answer Reboot menu.
- **Web Browser Interface:** Access the Ping-No-Answer Reboot Configuration menu as described in Section 6.1, then click on the Add Ping-No-Answer Reboot link to display the configuration menu.

Up to 54 Ping-No-Answer Reboots can be defined. The Add Ping-No-Answer menu is used to define the following parameters for each new Ping-No-Answer Reboot:

- **IP Address or Domain Name:** The IP address or Domain Name for the device that you wish to Ping. When the device at this address fails to respond to the Ping command, the RSM-8R4 will reboot the selected outlets. (Default = undefined.)

  Note: *In order to use domain names, DNS Server parameters must first be defined as described in Section 5.9.5.*

- **Ping Interval:** Determines how often the Ping command will be sent to the selected IP Address. The Ping Interval can be any whole number, from 1 to 2,800 minutes. (Default = 15 Minutes.)
- **Interval After Failed Ping:** Determines how often the Ping command will be sent after a previous Ping command receives no response. (Default = 1 Minute.)

- **Ping Delay After Reboot:** Determines how long the RSM-8R4 will wait to send additional Ping commands, after a Ping-No-Answer Reboot has been initiated. Typically, this option is used to allow time for a device to fully "wake up" after a Ping-No-Answer Reboot before attempting to Ping the device again. (Default = 15 Minutes.)

- **Consecutive Failures:** Determines how many consecutive failures of the Ping command must be detected in order to initiate a Ping-No-Answer Reboot. For example, if this value is set to "3", then after three consecutive Ping failures, a Ping-No-Answer Reboot will be performed. (Default = 3.)

- **Reboot:** Enables/Disables the Ping-No-Answer Reboot function for the specified IP address. When this item is disabled, the RSM-8R4 will not reboot the specified outlet(s) when a Ping-No-Answer is detected. However, the RSM-8R4 will continue to notify you via Email, Syslog Message and/or SNMP Trap, providing that parameters for these functions have been defined as described in Section 5.9 and email notification for the Ping-No-Answer function has been enabled as described in Section 7.2. (Default = No.)

  Notes:

  - *In order for Email/Text Message Notification to function, you must first define Email/Text Message parameters as described in Section 5.9.11.*
  - *In order for Syslog Message Notification to function, you must first define a Syslog Address as described in Section 5.9.2.*
  - *In order for SNMP Trap Notification to function, you must first define SNMP parameters as described in Section 5.9.7.*

- **Plug Access:** Determines which outlet(s) will be rebooted when this IP address for this Ping-No-Answer operation does not respond to a Ping command. Note that in the Text Interface, Plug Access is defined via a separate submenu; in the Web Browser Interface, Plug Access is defined via a drop down menu, which may be accessed by clicking on the "plus" sign in the "Configure Plug Access" field. (Default = undefined.)

- **Plug Group Access:** Determines which Plug Group(s) the Ping-No-Answer Reboot for this IP Address will be applied to. Note that in the Text Interface, Plug Group Access is defined via a separate submenu; in the Web Browser Interface, Plug Group Access is defined via a drop down menu, which may be accessed by clicking on the "plus" sign. (Default = undefined.)

- **Ping Test:** Sends a test Ping command to the IP Address or domain name that has been defined for this Ping-No-Answer Reboot.

  Note: *After you have finished defining or editing Ping-No-Answer Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Ping No Answer" button to save parameters; in the Text Interface, press the* ***[Esc]*** *key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.1.2. Viewing Ping-No-Answer Reboot Profiles

After you have defined one or more Ping-No-Answer Reboot profiles, you can review the parameters selected for each profile using the View Ping-No-Answer feature. To view the configuration of an existing Ping-No-Answer profile, access command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Access the Ping-No-Answer Reboot Directory menu as described in Section 6.1, then type `1` and press **[Enter]**. The RSM-8R4 will display a menu which shows all defined Ping-No-Answer Profiles, listed by their IP Addresses. Key in the IP Address for the desired profile, and then press **[Enter]** to display the View Ping-No-Answer Profile menu.
- **Web Interface:** Access the Ping-No-Answer Reboot Configuration menu as described in Section 6.1, then click on the View/Modify Ping-No-Answer Reboot link. The RSM-8R4 will display a menu that allows you to select the desired Ping-No-Answer Reboot and directory function. Select the "View Profile" button, and then click on the down arrow, scroll to the desired Ping-No-Answer Reboot Profile, select the profile, and then click "Choose Ping-No-Answer Profile."

The RSM-8R4 will display a screen which lists all defined parameters for the selected Ping-No-Answer Reboot Profile.

6.1.3. Modifying Ping-No-Answer Reboot Profiles

After you have defined a Ping-No-Answer profile, you can modify the configuration of the profile using the Modify Ping-No-Answer feature. To modify the configuration of an existing Ping-No-Answer profile, access the command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Access the Ping-No-Answer Reboot Directory menu as described in Section 6.1, then type `3` and press **[Enter]**. The RSM-8R4 will display a menu which shows all defined Ping-No-Answer Profiles, listed by their IP Addresses. Key in the IP Address for the desired profile, and then press **[Enter]** to display the Modify Ping-No-Answer Profile menu.
- **Web Interface:** Access the Ping-No-Answer Reboot Configuration menu as described in Section 6.1, then click on the View/Modify Ping-No-Answer Reboot link. The RSM-8R4 will display a menu that allows you to select the desired Ping-No-Answer Reboot and directory function. Select the "Modify Profile" button, and then click on the down arrow, scroll to the desired Ping-No-Answer Reboot Profile, select the profile, and then click "Choose Ping-No-Answer Profile."

The RSM-8R4 will display a screen which allows you to modify parameters for the selected Ping-No-Answer Reboot Profile. Note that this screen functions identically to the Add Ping-No-Answer Reboot menu, as discussed in Section 6.1.1.

> **Note:** *After you have finished defining or editing Ping-No-Answer Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Change Ping No Answer" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.1.4. Deleting Ping-No-Answer Reboot Profiles

After you have defined one or more Ping-No-Answer profiles, you can delete profiles that are no longer needed using the Delete Ping-No-Answer feature. To delete an existing Ping-No-Answer profile, access the command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Access the Ping-No-Answer Reboot Directory menu as described in Section 6.1, then type **4** and press **[Enter]**. The RSM-8R4 will display a menu which shows all defined Ping-No-Answer Profiles, listed by their IP Addresses. Key in the IP Address for the desired profile, and then press **[Enter]** to delete the selected profile. The selected profile will be deleted immediately, with no further prompting.
- **Web Interface:** Access the Ping-No-Answer Reboot Configuration menu as described in Section 6.1, then click on the View/Modify Ping-No-Answer Reboot link. The RSM-8R4 will display a menu that allows you to select the desired Ping-No-Answer profile and directory function. Select the "Delete Profile" button, and then click on the down arrow, scroll to the desired Ping-No-Answer Reboot Profile, select the profile, and then click "Choose Ping-No-Answer Profile." The RSM-8R4 will display a screen which lists all defined parameters for the selected profile. To confirm deletion, Click on the "Delete Profile" button.

6.2. Scheduled Reboot

The Scheduled Reboot feature can be used to reboot one or more outlets according to a user-defined schedule, or to automatically turn outlets Off and then On according to a user defined schedule.

To configure a Scheduled Reboot, access command mode using a password that permits access to Administrator level commands and then proceed as follows:

- **Text Interface:** Type **/RB** and press **[Enter]**. The Reboot Options Menu will be displayed. At the Reboot Options menu, type **2** and press **[Enter]** to display the Scheduled Reboot Directory menu. From the Scheduled Reboot Directory Menu, you can Add, Modify, View or Delete Scheduled Reboots as described in the Sections that follow.
- **Web Browser Interface:** Click the "Scheduled Reboot" link on the left hand side of the screen. The Scheduled Reboot Configuration menu will be displayed. From the Scheduled Reboot Configuration menu, you can Add, Modify, View or Delete Scheduled Reboots as described in the Sections that follow.

  Note: *After you have finished defining or editing Scheduled Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Scheduled Reboot" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R4 displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.2.1. Adding Scheduled Reboots

To add a Scheduled Reboot, access command mode using a password that permits Administrator Level commands and then proceed as follows:

- **Text Interface:** Access the Scheduled Reboot Directory menu as described in Section 6.2, then type **2** and press **[Enter]** to display the Add Scheduled Reboot menu.
- **Web Browser Interface:** Access the Scheduled Reboot Configuration menu as described in Section 6.2, then click on the Add Scheduled Reboot link to display the configuration menu.

The RSM-8R4 allows up to 54 Scheduled Reboots to be defined.

The Add Scheduled Reboot menu allows you to define the following parameters for each new Scheduled Reboot:

- **Scheduled Reboot Name:** Assigns a name to this Scheduled Reboot. (Default = undefined.)
- **Plug Action:** Determines whether the Scheduled Reboot will result in the outlet(s) being switched Off, or cycled Off and then On again (Reboot.) Note that when "Off" is selected, the "Day On" option and the "Time On" option can be used to select a time and day when the outlet(s) will be switched back On again. (Default = Off.)
- **Recurrence:** Determines whether the Scheduled Reboot will be performed on a Daily basis or a Weekly basis. (Default = Daily.)
- **Day:** Determines the day of the week that this Scheduled Reboot will occur on. (Default = undefined.)
- **Time:** Determines the time of the day that this Scheduled Reboot will occur on. (Default = 12:00.)
- **Turn ON Day:** When the "Action" parameter is set to "Off", this parameter can be used to determine the day that the outlet(s) will be switched back On again. (Default = undefined.)
- **Turn ON Time:** When the "Action" parameter has been set to "Off", this parameter can be used to determine the time when the outlet(s) will be switched back On again. (Default = 12:01.)
- **Plug Access:** Determines which outlet(s) this Scheduled Reboot action will be applied to. In the Text Interface, outlets are selected by typing 9, pressing [Enter] and then following the instructions in the resulting submenu. In the Web Browser Interface, outlets are designated by clicking on the "plus" sign in the Plug Access field, and then selecting the desired outlets from the drop down menu. (Default = undefined.)
- **Plug Group Access:** Determines which Plug Group(s) this Scheduled Reboot action will be applied to. Note that in the Text Interface, Plug Group Access is defined via a separate submenu; in the Web Browser Interface, Plug Group Access is defined via a drop down menu, which may be accessed by clicking on the "plus" sign in the Plug Group Access field. (Default = undefined.)

6.2.2. Viewing Scheduled Reboot Actions

After you have defined one or more Scheduled Reboots, you can review the parameters selected for each Reboot using the View Scheduled Reboot feature. To view the configuration of an existing Scheduled Reboot, access the command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Access the Scheduled Reboot Directory menu as described in Section 6.2, then type `1` and press **[Enter]**. The RSM-8R4 will display a menu which lists all defined Scheduled Reboots. Key in the name of the desired Scheduled Reboot, and then press **[Enter]** to display the View Scheduled Reboot menu.
- **Web Interface:** Access the Scheduled Reboot Configuration menu as described in Section 6.2, then click on the View/Modify Scheduled Reboot link. The RSM-8R4 will display a menu that allows you to select the desired Scheduled Reboot and directory function. Select the "View Scheduled Reboot" button, and then click on the down arrow, scroll to the desired Scheduled Reboot, select the reboot, and then click the "Choose Scheduled Reboot" button.

The RSM-8R4 will display a screen which lists all defined parameters for the selected Scheduled Reboot action.

6.2.3. Modifying Scheduled Reboots

After you have defined a Scheduled Reboot, you can edit the configuration of the Reboot action using the Modify Scheduled Reboot feature. To modify the configuration of an existing Scheduled Reboot action, access the command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Access the Scheduled Reboot Directory menu as described in Section 6.2, then type `3` and press **[Enter]**. The RSM-8R4 will display a menu which lists all defined Scheduled Reboot actions. Key in the name of the desired Scheduled Reboot action, and then press **[Enter]** to display the Modify Scheduled Reboot menu.
- **Web Interface:** Access the Scheduled Reboot Configuration menu as described in Section 6.2, then click on the View/Modify Scheduled Reboot link. The RSM-8R4 will display a menu that allows you to select the desired Scheduled Reboot action and directory function. Select the "Modify Scheduled Reboot" button, and then click on the down arrow, scroll to the desired Scheduled Reboot action, select the Scheduled Reboot, and then click the "Choose Scheduled Reboot" button.

The RSM-8R4 will display a screen which allows you to modify parameters for the selected Scheduled Reboot action. Note that this screen functions identically to the Add Scheduled Reboot menu, as discussed in Section 6.2.1.

6.2.4. Deleting Scheduled Reboots

After you have defined one or more Scheduled Reboot actions, you can delete Reboot actions that are no longer needed using the Delete Scheduled Reboot feature. To delete an existing Scheduled Reboot, access the command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Access the Scheduled Reboot Directory menu as described in Section 6.2, then type **4** and press **[Enter]**. The RSM-8R4 will display a menu which lists all defined Scheduled Reboot actions. Key in the name of the desired reboot action, and then press **[Enter]** to delete the selected Scheduled Reboot. The selected Scheduled Reboot action will be deleted immediately, with no further prompting.
- **Web Interface:** Access the Scheduled Reboot Configuration menu as described in Section 6.2, then click on the View/Modify Scheduled Reboot link. The RSM-8R4 will display a menu that allows you to select the desired Scheduled Reboot action and directory function. Select the "Delete Scheduled Reboot" button, and then click on the down arrow, scroll to the desired Scheduled Reboot, select the Reboot, and then click the "Choose Scheduled Reboot" button. The RSM-8R4 will display a screen which lists all defined parameters for the selected Scheduled Reboot. To confirm deletion, Click on the "Delete Scheduled Reboot" button.

7. Alarm Configuration

When properly configured, the RSM-8R4 can monitor temperature readings and user activity, and log this information for future review. In addition, the RSM-8R4 can also generate alarms when temperature readings exceed user-defined trigger levels, when a Ping-No-Answer condition is detected, and when the Invalid Access Lockout feature is triggered.

When any of these conditions are detected, the RSM-8R4 can also send an "Alarm" to the proper personnel via Email, Syslog Message or SNMP trap. If the user-defined trigger levels for temperature are exceeded, the RSM-8R4 can also automatically shut off power to non-essential devices ("Load Shedding") in order to decrease the amount of heat generated within the rack. After Load Shedding has taken place, the RSM-8R4 can also restore power to the non-essential devices when the temperature drops to user-defined acceptable levels.

This section describes the procedure for setting up the RSM-8R4 to send alarm messages when any of these critical situations are detected. For instructions regarding configuration of the Log function, please refer to Section 5.3.4.

Notes:

- *In order to send alarm notification via email, email addresses and parameters must first be defined as described in Section 5.9.11. Email alarm notification will then be sent for all alarms that are enabled as described in this Section.*
- *In order to send alarm notification via Syslog Message, a Syslog address must first be defined as described in Section 5.9.2. Once the Syslog address has been defined, Syslog Messages will be sent for every alarm that is discussed in this Section, providing that the Trigger Enable parameter for the alarm has been set to "On."*
- *In order to send alarm notification via SNMP Trap, SNMP Trap parameters must first be defined as described in Section 5.9.7. Once SNMP Trap Parameters have been defined, SNMP Traps will be sent for every alarm that is discussed in this Section, providing that the Trigger Enable parameter for the alarm has been set to "On."*
- *After defining parameters via the Text Interface, make certain to press the **[Esc]** key several times to completely exit from the configuration menu and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message is displayed.*

To configure the RSM-8R4's Alarm functions, access the command mode using a password that allows Administrator level commands and then proceed as follows:

- **Text Interface:** Type **/AC** and then press **[Enter]**. The Alarm Configuration menu will be displayed.
- **Web Browser Interface:** Click the "Alarm Configuration" link, located on the left hand side of the screen. The Alarm Configuration menu will be displayed.

7.1. The Over Temperature Alarms

The Over Temperature Alarms are designed to inform you when the temperature level inside your equipment rack reaches or exceeds certain user-defined levels. There are two separate Over Temperature Alarms; the Initial Threshold alarm and the Critical Threshold Alarm.

Typically, the Initial Threshold alarm is used to notify you when the temperature within your equipment rack reaches a point where you *might* want to investigate it, whereas the Critical Threshold alarm is used to notify you when the temperature approaches a level that may harm equipment or inhibit performance. The trigger for the Initial Threshold alarm is generally set lower than the Critical Threshold alarm.

If the user-defined trigger levels for temperature are exceeded, the RSM-8R4 can automatically shut off power to non-essential devices ("Load Shedding") in order to reduce the amount of temperature generated within the rack. In addition, the Load Shedding feature can also be used to switch On additional components, such as fans or cooling systems in order to dissipate the excess heat. After Load Shedding has taken place, the Load Shedding Recovery feature can be used to return plugs to their previous state after the temperature drops to an acceptable level.

Notes:

- *In order for the RSM-8R4 to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RSM-8R4 to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2.*
- *In order for the RSM-8R4 to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7.*

To configure the Over Temperature Alarms, access the RSM-8R4 command mode using a password that permits Administrator Level commands, and then proceed as follows:

- **Text Interface:** Type **`/AC`** and then press **[Enter]** to display the Alarm Configuration menu. From the Alarm Configuration menu, either type **`1`** and press **[Enter]** to access the Over Temperature (Initial Threshold) alarm, or type **`2`** and press **[Enter]** to access the Over Temperature (Critical Threshold) alarm.
- **Web Browser Interface:** Click the "Alarm Configuration" link, located on the left hand side of the screen to display the Alarm Configuration menu. From the Alarm Configuration menu, click on either the "Over Temperature (Initial Threshold)" link or the "Over Temperature (Critical Threshold)" link to access the desired menu.

Note that both the Initial Threshold menus and Critical Threshold menus offer essentially the same set of parameters, but the parameters defined for each alarm are separate and unique. Therefore, parameters defined for the Critical Threshold Alarm will not be applied to the Initial Threshold Alarm and vice versa.

Both the Over Temperature (Initial Threshold) alarm and the Over Temperature (Critical Threshold) alarm offer the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

  Note: *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*

- **Alarm Set Threshold:** The trigger level for this alarm. When temperature exceeds the Alarm Set Threshold, the RSM-8R4 can send an alarm (if enabled) and/or begin Load Shedding (if enabled.) For more information on Load Shedding for the Over Temperature Alarm, please refer to Section 7.1.1. (Initial Threshold: Default = 90°F or 32°C, Critical Threshold: Default = 100°F or 38°C.)

- **Alarm Clear Threshold:** Determines how low the temperature must drop in order for the Alarm condition to be cancelled and for Auto Recovery (if enabled) to occur. For more information on Load Shedding and Auto Recovery for the Over Temperature Alarm, please refer to Section 7.1.1. (Initial Threshold: Default = 80°F or 27°C, Critical Threshold: Default = 90°F or 38°C.)

  Note: *The System Parameters menu is used to set the temperature format for the RSM-8R4 unit to either Fahrenheit or Celsius as described in Section 5.3.*

- **Resend Delay:** Determines how long the RSM-8R4 will wait to resend an email message generated by this alarm, when the initial attempt to send notification was unsuccessful. (Default = 60 Minutes.)

- **Notify Upon Clear:** When this item is enabled, the RSM-8R4 will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RSM-8R4 will send initial notification when it detects that the temperature has exceeded the trigger value, and then send a second notification when it determines that the temperature has fallen below the trigger value. (Default = On.)

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)

  Note: *The Email Message parameter offers four different options: On, Off, On (Copy to All Triggers) or Off (Copy to All Triggers). If either of the "Copy to All Triggers" options is selected, then email notification for all other alarms will be switched On or Off as indicated by this parameter. For example, If "Off (Copy to All Triggers)" is selected, then Email notification will be disabled for all other alarms too.*

- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses, defined via the "Email Messages" menu (see Section 5.9.11,) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously defined, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Over Temperature (Initial)" or "Alarm: Over Temperature (Critical)".)

- **Load Shedding:** Provides access to a submenu, which is used to configure and enable the Load Shedding feature for the Over Temperature alarms. When Load Shedding is enabled and properly configured, the RSM-8R4 will switch specific, user-selected plugs On or Off whenever the temperature exceeds the Alarm Set Threshold value. If the Auto Recovery feature is enabled, the RSM-8R4 can also return these user-selected plugs to their prior status, when the temperature falls below the Alarm Clear Threshold value. For more information on the Load Shedding Feature and Auto Recovery, please refer to Section 7.1.1.

7.1.1. Over Temperature Alarms - Load Shedding and Auto Recovery

The Load Shedding feature is used to switch specific, user-defined plugs On or Off whenever the temperature exceeds the Alarm Set Threshold value. This allows the RSM-8R4 to automatically shut Off non-essential devices in order to reduce the temperature generated within the rack, or automatically switch On devices such as fans or cooling systems in order to dissipate heat from the rack. When the Auto Recovery feature is enabled, the RSM-8R4 can also automatically "undo" the effects of the Load Shedding feature when the temperature again falls to a user-defined non-critical level.

For both the Initial Threshold and Critical Threshold Over Temperature Alarms, Load Shedding and Auto Recovery are enabled and configured via submenus of the Over Temperature Alarm configuration screens. To access the Load Shedding and Auto Recovery configuration menus, access the RSM-8R4 command mode using an account that permits access to Administrator level commands, and then proceed as follows:

- **Text Interface:** Access the Over Temperature Alarm configuration menu as described in Section 7.1, and then type `5` and press **[Enter]** to display the Load Shedding configuration.

- **Web Browser Interface:** Access the Over temperature Alarm configuration menu as described in Section 7.1, and then click on the "Load Shedding" link to display the Load Shedding configuration menu.

Note that the Load Shedding configuration menus for both the Initial Threshold Alarm and Critical Threshold Alarm offer essentially the same set of parameters, but the parameters defined for each alarm are separate and unique. Therefore, parameters defined for the Critical Threshold Load Shedding will not be applied to the Initial Threshold Alarm and vice versa.

The Load Shedding configuration menus for both the Over Temperature (Initial Threshold) alarm and the Over Temperature (Critical Threshold) alarm offer the following parameters:

- **Enable:** Enables/Disables Load Shedding for the corresponding alarm. When enabled, the RSM-8R4 will switch the user specified plugs whenever the temperature exceeds the Alarm Set Threshold value. (Default = Disable.)
- **Plug State:** Determines whether the selected plugs/plug groups will be switched On or Off when Load Shedding is enabled and the temperature exceeds the user-defined Alarm Set Threshold. For example, if the Plug State is set to "Off", then the selected plugs/plug groups will be switched Off when the Alarm Set Threshold is exceeded. (Default = Off.)
- **Auto Recovery:** Enables/Disables the Auto Recovery feature. When both Load Shedding and Auto Recovery are enabled, the RSM-8R4 will return plugs to their former On/Off state after the temperature falls below the Alarm Clear Threshold value. This allows the RSM-8R4 to "undo" the effects of the Load Shedding feature after the temperature has returned to an acceptable level. (Default = Disabled.)
- **Plug Access:** Determines which Plug(s) will be switched when the temperature exceeds the Alarm Set Threshold and the Load Shedding feature is triggered. For example, if plugs 1, 2 and 3 are selected, then these plugs will be switched On or Off whenever the temperature exceeds the Alarm Set Threshold. (Default = undefined.)

  Notes:

  - *In the Text Interface, Plug Access is configured by typing* **4***, pressing* ***[Enter]*** *and then selecting the desired Plug(s) from the resulting submenu.*
  - *In the Web Browser Interface, Plug Access is configured by clicking on the "plus" symbol in the "Configure Plug Access" field to display the drop down menu, and then selecting the desired Plug(s) from the drop down menu.*

- **Plug Group Access:** Determines which Plug Group(s) will be switched when the temperature exceeds the Alarm Set Threshold and the Load Shedding feature is triggered. For example, if you have defined a Plug Group named "test", which includes Plugs 2, 3 and 4, and then select the "test" Plug Group via the Plug Group Access parameter, then all of the plugs in the "test" Plug Group will be switched On or Off whenever the temperature exceeds the Alarm Set Threshold. (Default = undefined.)

  Notes:

  - *In the Text Interface, Plug Group Access is configured by typing* **5***, pressing* ***[Enter]*** *and then selecting the desired Plug Group(s) from the resulting submenu.*
  - *In the Web Browser Interface, Plug Group Access is configured by clicking on the "plus" symbol in the "Configure Plug Group Access" field to display the drop down menu, and then selecting the desired Plug Group(s) from the drop down menu.*
  - *Plug Groups must first be defined (as described in Section 5.6) before they will be displayed in the Load Shedding menu's Plug Group Access submenu.*

7.2. The Ping-No-Answer Alarm

The Ping-No-Answer Alarm is intended to provide notification when one of the IP addresses defined via the Ping-No-Answer Reboot feature (as described in Section 6.1) fails to respond to a Ping command. When one of the user-defined IP addresses fails to answer a Ping command, the RSM-8R4 can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for this alarm to function, IP Addresses for the Ping-No-Answer reboot feature must first be defined as described in Section 6.1.*
- *When a Ping-No-Answer condition is detected, the RSM-8R4 can still reboot the user-selected outlet(s) as described in Section 6.1, and can also send an email, Syslog Message and/or SNMP trap if properly configured as described in this section.*
- *In order for the RSM-8R4 to provide Email alarm notification, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RSM-8R4 to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2.*
- *In order for the RSM-8R4 to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7.*

To configure the Lost Voltage (Line In) Alarm, access the RSM-8R4 command mode using a password that permits Administrator Level commands, and then proceed as follows:

- **Text Interface:** Type `/AC` and then press **[Enter]** to display the Alarm Configuration menu. From the Alarm Configuration menu, type `3` and press **[Enter]** to access the configuration menu for the Ping-No-Answer Alarm.
- **Web Browser Interface:** Click the "Alarm Configuration" link, located on the left hand side of the screen to display the Alarm Configuration menu. From the Alarm Configuration menu, click on the "Ping-No-Answer" link to access the configuration menu.

The Ping-No-Answer alarm configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

  Note: *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.*

- **Resend Delay:** Determines how long the RSM-8R4 will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes.)

- **Notify Upon Clear:** When this item is enabled, the RSM-8R4 will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RSM-8R4 will send initial notification when it detects that a Ping command has failed, and then send a second notification when it determines that the IP address is again responding to the Ping command. (Default = On.)

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)

  Note: *The Email Message parameter offers four different options: On, Off, On (Copy to All Triggers) or Off (Copy to All Triggers). If either of the "Copy to All Triggers" options is selected, then email notification for all other alarms will be switched On or Off as indicated by this parameter. For example, If "Off (Copy to All Triggers)" is selected, then Email notification will be disabled for all other alarms too.*

- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages that are generated by this alarm. (Default = "Alarm: Ping-No-Answer.")

7.3. The Invalid Access Lockout Alarm

The Invalid Access Lockout Alarm can provide notification when the RSM-8R4 has locked the Network port due to repeated, invalid attempts to access command mode. Normally, the Invalid Access Lockout feature (discussed in Section 5.3.2) will lock the network port whenever the RSM-8R4 detects that a user-defined number of invalid passwords have been entered at the Network Port. When the Invalid Access Lockout Alarm is properly configured and enabled as described in this section, the RSM-8R4 can also provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for this alarm to function, Invalid Access Lockout parameters must first be configured and enabled as described in Section 5.3.2.*
- *When an Invalid Access Lockout occurs, the RSM-8R4 can still lock the network port as described in Section 5.3.2, and can also send an email, Syslog Message and/or SNMP trap if properly configured.*
- *If desired, the RSM-8R4 can be configured to count Invalid Access attempts and provide notification when the counter exceeds a user defined trigger level, without actually locking the port in question. To do this, enable the Invalid Access Lockout Alarm as described here, but when you configure Invalid Access Lockout parameters as described in Section 5.3.2, set the Lockout Attempts and Lockout Duration as you would normally, and then set the "Lockout Enable" parameter to "Off."*
- *In order for the RSM-8R4 to provide Email alarm notification, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the RSM-8R4 to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2.*
- *In order for the RSM-8R4 to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7.*

To configure the Invalid Access Lockout Alarm, access the RSM-8R4 command mode using a password that permits Administrator Level commands, and then proceed as follows:

- **Text Interface:** Type **/AC** and then press **[Enter]** to display the Alarm Configuration menu. From the Alarm Configuration menu, type **4** and press **[Enter]** to access the configuration menu for the Invalid Access Lockout Alarm.
- **Web Browser Interface:** Click the "Alarm Configuration" link, located on the left hand side of the screen to display the Alarm Configuration menu. From the Alarm Configuration menu, click on the "Invalid Access Lockout" link to access the configuration menu.

The Invalid Access Lockout alarm configuration menu offers the following parameters:

- **Trigger Enable:** Enables/Disables the trigger for this alarm. When Disabled, this alarm will be suppressed. (Default = On.)

  Note: *To cancel an alarm without unlocking the port, simply toggle the Trigger Enable parameter Off and then back On again.*

- **Resend Delay:** Determines how long the RSM-8R4 will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes.)

- **Notify Upon Clear:** When this item is enabled, the RSM-8R4 will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the RSM-8R4 will send initial notification when it detects that an Invalid Access Lockout has occurred, and then send a second notification when it determines that the port has been unlocked. (Default = On.)

- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)

  Note: *The Email Message parameter offers four different options: On, Off, On (Copy to All Triggers) or Off (Copy to All Triggers). If either of the "Copy to All Triggers" options is selected, then email notification for all other alarms will be switched On or Off as indicated by this parameter. For example, If "Off (Copy to All Triggers)" is selected, then Email notification will be disabled for all other alarms too.*

- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu (see Section 5.9.11) will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

  Note: *If Email addresses have been previously specified, then the text under the parameters will list the current, user defined email addresses.*

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Invalid Access Lockout.")

8. The Status Screens

The Status Screens are used to display status information about the RSM-8R4 serial ports, switched outlets, Network Port, Plug Groups, Temperature Log, Alarm Log and Audit Log. The Status Screens are available via both the Text Interface and Web Browser Interface.

8.1. The Network Status Screen

The Network Status screen shows activity at the RSM-8R4's 16 virtual network ports, and lists the TCP Port Number, Active/Free Status and current user name for each virtual network port.

To view the Network Status Screen, access command mode and then proceed as follows:

- **Text Interface:** Type **`/SN`** and press **[Enter]**.
- **Web Browser Interface:** Click on the "Network Status" link on the left hand side of the screen.

The Network Status Screen lists the following items:

- **Port:** The virtual network port for each connection.
- **TCP Port:** The number of the TCP Port for each connection.
- **Status:** This column will read "Free" if no users are currently connected to the corresponding port, or "Active" if a user has currently accessed command mode via this port.
- **User Name:** The user name for the account that has currently accessed command mode via this port. Note that when the Network Status Screen is viewed via the Text Interface, usernames that are longer than 22 characters will be truncated and the remaining characters will be displayed as two dots (..).

8.2. The Port and Plug Status Screens

The Port Status screen and Plug Status screen show the current status of the RSM-8R4's serial ports and switched plugs. The Port Status screen lists the user-defined port name and port mode for each serial port, as well as the buffer count, connection status and the names of any user's currently accessing these ports. The Plug Status screen shows the On/Off status of the switched outlets, and lists user-defined Plug Names, Boot/Sequence Delay values, and Default On/Off settings.

Note:

- *In the Text Interface, Port and Plug status is shown on a single screen. In the Web Browser Interface, Port and Plug status is shown on two separate screens.*
- *When Port Status and Plug Status is viewed by an account with Administrator or SuperUser command access, all RSM-8R4 serial ports and plugs are listed. When Port Status and Plug Status is viewed by an account with User or ViewOnly command access, then the screen will list only the serial ports and switched outlets that are allowed by that account.*
- *The Port and Plug Status screens also display the current temperature reading for the RSM-8R4 unit.*
- *The Plug Status screen also shows the current status of the RSM-8R4's Internal Modem Port.*

To view the Plug Status Screen, access the RSM-8R4 command mode and then proceed as follows:

- **Text Interface:** Type `/s` and press **[Enter]**.
- **Web Browser Interface:** Click on the "Port Status" link on the left hand side of the screen to display the Port Status Screen. Click on the "Plug Status" link on the left hand side of the screen to display the Plug Status Screen.

Serial Port Status: The Port and Plug Status Screen in the Text Interface and the Port Status Screen in the Web Interface both list the following parameters for the RSM-8R4's serial ports:

- **Port:** The number of each serial port.
- **Name:** The user-defined name for each serial port.
- **Username:** When a user is connected to a given serial port, this column will show the name of the user account that initiated the connection.
- **Status:** The connection status of each serial port is displayed as follows:
  - Network Connection: This column will read "Free" if the corresponding port is not currently connected.
  - Network Connection: If the Network port is connected to a given serial port, this column will read "C-N**nn**" (where **nn** is the number of the virtual network port that is connected to the port.
  - Connection to Another Serial Port: This column will read "C-0**n**" (where **n** is the number of the serial port that is connected to this port) if one of the other serial ports is currently connected to the port.

- **Mode:** The user-defined Port Mode for each serial port.
- **Buffer Count:** The amount of data that is currently stored in the buffer for each serial port..

Plug Status: The Port and Plug Status Screen in the Text Interface and the Plug Status Screen in the Web Interface both list the following parameters for the RSM-8R4's switched outlets:

- **Plug:** The number of each switched outlet.

  Note: *If an asterisk appears next to the plug number in this column, this indicates that the plug is "busy", and still in the process of completing a previous command. This could be a command that was invoked by the current user or another user, or a switching action that was initiated by an alarm.*

- **Name:** The user-defined name for each switched outlet.
- **Status:** The current On/Off status of each switched outlet. If the Status column includes an asterisk, this means that this outlet is busy completing another command, that was previously invoked.
- **Boot Seq. Delay:** The user-defined Boot/Sequence Delay for each switched outlet.
- **Default:** The Default On/Off value for each switched outlet.
- **Priority:** The user-defined priority setting for each switched outlet.
- **System Temperature:** The current temperature reading for the RSM-8R4 unit.

8.3. The Plug Group Status Screen

The Plug Group Status screen shows the configuration details and On/Off status for the RSM-8R4's user-defined Plug Groups.

Notes:

- *When the Plug Group Status Screen is viewed by an account with Administrator or SuperUser command access, all RSM-8R4 plugs and plug groups are listed. When the Plug Status Screen is viewed by an account with User or ViewOnly command access, then the screen will list only the plugs and plug groups that are allowed by that account.*
- *The procedure for defining parameters for individual plugs is described in Section 5.7. The procedure for defining Plug Groups is described in Section 5.6.*
- *In order to display the Plug Group Status screen, you must first define at least one Plug Group as described in Section 5.6.*

To view the Plug Group Status Screen, access the RSM-8R4 command mode and then proceed as follows:

- **Text Interface:** Type `/SG` and press **[Enter]**.
- **Web Browser Interface:** Click on the "Plug Group Status" link on the left hand side of the screen. The RSM-8R4 will display a screen that lists all currently defined Plug Groups. Click the check box(es) next to the Plug Group(s) that you want to review, and then click on the "Get Plug Group Status" button.

The Plug Group Status Screen lists the following parameters for each Plug Group:

- **Group Name:** The user-defined name for each Plug Group.
- **Unit:** This field will read "Local" if the outlet is located on your local RSM-8R4 unit, or "Remote", if the outlet is located on an optional, remote AUX RSM-8R4 unit.
- **Plug:** The alphanumeric number of each switched outlet in the Plug Group.
- **Plug Name:** The User Defined name for each switched outlet in the Plug Group.
- **Default:** The Default On/Off value for each switched outlet in the Plug Group.
- **Boot Seq. Delay:** The user-defined Boot/Sequence Delay for each switched outlet in the Plug Group.
- **Status:** The On/Off status of each switched outlet in the Plug Group. If the Status column includes an asterisk, this means that this outlet is busy completing another command, that was previously invoked, either by you or another user.

8.4. The Event Logs

8.4.1. The Audit Log

The Audit Log provides a record of most command activity at the RSM-8R4 unit, including power switching, port connections and disconnections, login and logout activity. Note however that the Audit Log does not include user information regarding access to configuration menus or status screens.

To view the Audit Log, access command mode using a password that permits Administrator or SuperUser level commands and then proceed as follows:

- **Text Interface:** Type `/L` and press **[Enter]**. The "Display Logs" menu will be shown. At the Display Logs menu, type `1` and press **[Enter]** to display the Audit Log.
- **Web Browser Interface:** Click on the "Audit Log" link on the left hand side of the screen.

The Audit Log will display the following information for each logged event:

- **Date:** The date when the logged event occurred.
- **Time:** The time that the logged event occurred.
- **Username:** The name of the user account that initiated the logged event.
- **Description:** A brief description of the nature of the logged event.

Note: *In the Text Interface, the following commands are also available:*

- *Press **[Enter]** to display the next screen full of data.*
- *Press **[Esc]** to exit from the log menu and return to the command prompt.*
- *Type `E` and press **[Enter]** to erase the Audit Log.*

8.4.2. The Alarm Log

The Alarm Log provides a record of all alarm events that were initiated by the Over Temperature Alarms, the Ping-No-Answer Alarm and the Invalid Access Lockout.

To view the Alarm Log, access command mode using a password that permits Administrator or SuperUser level commands and then proceed as follows:

- **Text Interface:** Type `/L` and press **[Enter]**. The "Display Logs" menu will be shown. At the Display Logs menu, type `2` and press **[Enter]** to display the Alarm Log.
- **Web Browser Interface:** Click on the "Alarm Log" link on the left hand side of the screen.

The Alarm Log will display the following information for each logged event:

- **Date:** The date when the alarm occurred.
- **Time:** The time that the alarm occurred.
- **Trigger:** The name of the alarm which was triggered.
- **Description:** A brief description of the event that triggered the alarm.

Note: *In the Text Interface, the following commands are also available:*

- *Press **[Enter]** to display the next screen full of data.*
- *Press **[Esc]** to exit from the log menu and return to the command prompt.*
- *Type `E` and press **[Enter]** to erase the Alarm Log.*

8.4.3. The Temperature Log

The temperature log provides a record of RSM-8R4 temperature readings, in reverse chronological order, with the most recent events appearing at the top of the list.

To view the Temperature Log, access command mode using a password that permits Administrator or SuperUser level commands and then proceed as follows:

- **Text Interface:** Type `/L` and press **[Enter]**. The "Display Logs" menu will be shown. At the Display Logs menu, type `3` and press **[Enter]** to display the Temperature Log.
- **Web Browser Interface:** Click on the "Temperature Log" link on the left hand side of the screen.

Note: *In the Text Interface, the following commands are also available:*

- *Press **[Enter]** to display the next screen full of data.*
- *Press **[Esc]** to exit from the log menu and return to the command prompt.*
- *Type `E` and press **[Enter]** to erase the Temperature Log.*

8.5. The Port Diagnostics Screen

The Port Diagnostics Screen provides more detailed information about each port. To display the Port Diagnostics Screen, access the Text Interface command mode and type **`/SD`** **[Enter]**.

When the /SD command is invoked by an Administrator or SuperUser level account, the Port Diagnostics Screen will display the status of all ports. If the /SD command is invoked by a User or ViewOnly level account, then the Port Diagnostics Screen will only display the status of the ports that are specifically allowed by that account.

The Port Diagnostics Screen lists the following items:

- **Port:** The Port Number.
- **Name:** The user-defined name for each port.
- **Status:** The connect status for each port.
  - When the port is connected, this column will list the number of the other port connected to this port. If the column contains an asterisk, this indicates the port has accessed command mode.
  - If the connected port is listed as "**`Nn`**" (where "**`n`**" is a number), this indicates that the RS232 port is connected to the Network port. The numbers indicate which of the available Telnet sessions is being used (for example, "`C-06`".)
- **Baud:** The baud rate selected for each port.
- **COM:** The Data Bits, Parity, and Stop Bits selected for each port. For example, "8N1" indicates Eight data bits, No parity, and One stop bit.
- **HS:** The handshaking (flow control) mode for each port.
- **Mode:** The user-selected Port Mode.
- **BUF:** The amount of data (in bytes) currently stored in the buffer for this port.
- **CTS:** The High/Low status of the CTS line at the RS232 interface.

8.6. The Port Parameters Screens

The /W (Who) command displays more detailed information about an individual RSM-8R4 port. Rather than listing general connection information for all ports, the Port Parameters screen lists all defined parameters for a specific port.

When the /W command is invoked by an Administrator or SuperUser level account, it can be used to display parameters for all RSM-8R4 Serial Ports, plus the Network Port. If the /W command is invoked by a User or ViewOnly level account, then it will only display parameters for the Serial Ports that are specifically allowed for that account, and will not display parameters for the Network Port.

The /W command uses the following format:

`/W xx` [Enter]

Where **`xx`** is the desired port number. If the /W command is invoked at a serial port, by a user with access to Administrator or SuperUser level commands, then the letter "**`N`**" can be entered as the command argument to display parameters for the Network Port.

Note:

- *When the /W command is invoked by an Administrator level account which has accessed command mode via the Network Port , all Network Port Parameters will be displayed..*
- *When the /W command is invoked by a SuperUser level account which has access command mode via the Network Port, only the Sequence Disconnect, Logoff Character, and Accept Break option will be displayed.*

9. Operation

As discussed in Section 5, the RSM-8R4 offers two separate command interfaces; the Web Browser Interface and the Text Interface (also known as the "Command Line Interface" or "CLI.") Both interfaces offer essentially the same command options and features, and in most cases, parameters defined via the Web Browser Interface will also apply when communicating via the Text Interface (and vice versa.)

9.1. Controlling Power - Web Browser Interface

When using the Web Browser Interface, switching commands are invoked via the Plug Control Screen and Plug Group Control Screen.

> **Note:** *The Web Browser Interface cannot be used to create or break connections with the RSM-8R4's serial ports. Serial port connections can be made or broken via the Text Interface, as described in Section 9.3.*

9.1.1. The Plug Control Screen - Web Browser Interface

The Plug Control Screen lists the current On/Off status of the RSM-8R4's Switched Outlets and is used to control switching and rebooting of the outlets.

To invoke On, Off, or Reboot commands, proceed as follows:

1. Access the RSM-8R4 Command Mode as described in Section 5.1.
2. Click on the "Plug Control" link on the left hand side of the screen to display the Plug Control Screen.

Notes:

- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*
- *If a switching or reboot command is directed to a plug that is already in the process of being switched or rebooted by a previous command, then the new command will be placed in a queue until the plug is ready to receive additional commands.*
- *If the Status column in the Plug Control Screen includes an asterisk, this means that the corresponding outlet is busy completing a previously invoked command.*
- *When the Plug Control Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched outlets will be displayed.*
- *When the Plug Control Screen is displayed by an account that permits User or ViewOnly command access, the screen will only include the switched outlets that are specifically allowed by the account.*

3. **Initiating a Reboot Cycle:** From the Plug Control Menu, click the down arrow in the "Action" column for the desired outlet(s), then select "Reboot" from the dropdown menu and click on the "Confirm Plug Actions" button.

4. **Switching Outlets Off:** From the Plug Control Menu, click the down arrow in the "Action" column for the desired outlet(s), then select "Off" from the dropdown menu and click on the "Confirm Plug Actions" button.

5. **Switching Outlets On:** From the Plug Control Menu, click the down arrow in the "Action" column for the desired outlet(s), then select "On" from the dropdown menu and click on the "Confirm Plug Actions" button.

6. **Setting Plugs to Default State:** From the Plug Control Menu, click the down arrow in the "Action" column for the desired outlet(s), then select "Default" from the dropdown menu and click on the "Confirm Plug Actions" button. All selected outlets will be set to their user-defined default state.

Notes:

- *If Command Confirmation is enabled, then the RSM-8R4 will display a confirmation screen before completing each power switching command. When the confirmation screen appears, click on the "Execute Plug Group Actions" button to complete the command.*
- *To switch, reboot or default all RSM-8R4 outlets, use the drop down menu in the "All Plugs" row to select the desired action.*
- *When each command is complete, the Plug Status Screen will be displayed. At that time, the Status Screen will list the updated On/Off status of each plug.*

9.1.2. The Plug Group Control Screen - Web Browser Interface

The Plug Group Control Screen is used to send switching and reboot commands to the user-defined Plug Groups. As described in Section 5.6, Plug Groups allow you to define a group of outlets, dedicated to a similar purpose or client, and then direct switching and reboot commands to the group, rather than switching one plug at a time.

To invoke On, Off, or Reboot commands, proceed as follows:

1. Access the RSM-8R4 Command Mode as described in Section 5.1.

2. Click on the "Plug Group Control" link on the left hand side of the screen to display the Plug Group Control Screen.

Notes:

- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*
- *If a switching or reboot command is directed to a plug that is already in the process of being switched or rebooted by a previous command, then the new command will be placed in a queue until the plug is ready to receive additional commands.*
- *When the Plug Group Control Screen is displayed by an account that permits Administrator or SuperUser command access, all user-defined Plug Groups will be displayed.*
- *When the Plug Control Screen is displayed by an account that permits User or ViewOnly level commands, the screen will only include the Plug Groups that are allowed by the account.*

3. **Initiating a Reboot Cycle:** From the Plug Group Control Screen, locate the Plug Group(s) that you wish to reboot, then click the down arrow in the task selector box next to the Plug Group name, and use the dropdown menu to select the "Reboot" option. Then click on the "Confirm Plug Group Actions" button to proceed.

4. **Switching Plug Groups Off:** From the Plug Group Control Screen, locate the Plug Group(s) that you wish to switch Off, then click the down arrow in the task selector box next to the Plug Group name, and use the dropdown menu to select the "Off" option. Then click on the "Confirm Plug Group Actions" button to proceed.

5. **Switching Plug Groups On:** From the Plug Group Control Screen, locate the Plug Group(s) that you wish to switch On, then click the down arrow in the task selector box next to the Plug Group name, and use the dropdown menu to select the "On" option. Then click on the "Confirm Plug Group Actions" button to proceed.

7. **Switching Plug Groups to Defaults:** From the Plug Group Control Screen, locate the Plug Group(s) that you wish to default, then click the down arrow in the task selector box next to the Plug Group name, and use the dropdown menu to select the "Default" option. Then click on the "Confirm Plug Group Actions" button to proceed.

Notes:

- *If Command Confirmation is enabled, then the RSM-8R4 will display a confirmation screen before completing each power switching command. When the confirmation screen appears, click on the "Confirm Plug Group Actions" button to complete the command.*
- *When each Plug Group command is completed, the Plug Status Screen will be displayed. At that time, the Status Screen will show the updated On/Off status of each plug.*

```
COMMAND MENU:                              Version 1.01
DISPLAY                                    CONFIGURATION
/S              Status                     /F              System Parameters
/SD             Port Diagnostics           /P [n]          Port Parameters
/W [n]          Port Parameters (Who)      /PL             Plug Parameters
/SG             Plug Group Status          /G              Plug Grouping Parameters
/SN             Network Status             /N              Network Configuration
/L              Log                        /RB             Reboot Options
/J [*]          Site ID                    /AC             Alarm Configuration
CONTROL                                    /I              Reboot System
/X              Exit Command Mode          /UF             Upgrade Firmware
/C <n> [n]      Connect - Local [Remote]   /CP <z>         Copy Port Parameters
/D <n|Nn|*>     Disconnect Port(s)         /TEST           Test Network Options
/R <n>          Read Buffer                     +-------------------------------+
/E <n|*>        Erase Buffer(s)                 | n   Plug# or name             |
/BOOT <n>       Boot Plug n                     | n:n = plug n through plug n   |
/ON <n>         Turn on Plug n                  | n+n = plug n and plug n       |
/OFF <n>        Turn off Plug n                 | k   Key type (1-3)            |
/DPL            Default all plugs               | *   "all"                     |
/U              Send Parameter File             | <>  Required entry            |
/K <k>          Send SSH Keys                   | []  Optional entry            |
/UL             Unlock (Invalid Access)         +-------------------------------+
Add ,Y to bypass "Sure?"
RSM>
```

Figure 9.1: The Help Menu (Administrator Mode; Text Interface)

9.2. Controlling Power - Text Interface

When using the Text Interface, all serial port connection and power switching functions are performed by invoking simple, ASCII commands. ASCII commands are also used to display status screens and to log out of command mode. The Text Interface includes a Help Menu, which summarizes all available RSM-8R4 commands. To display the Text Interface Help Menu (Figure 9.1), type **`/H`** and press **[Enter]**.

> **Note:** *When the Help Menu is displayed by an account that permits SuperUser, User or ViewOnly level commands, the screen will not include commands that are only available to Administrators.*

9.2.1. The Port and Plug Status Screen - Text Interface

When you login to the RSM-8R4 command mode via the Text Interface, the first screen displayed after login is the Port and Plug Status Screen. The Port and Plug Status Screen lists the current status of the RSM-8R4's serial ports and switched AC Outlets, displays the current temperature and displays the user-defined Site I.D. Message.

Normally, the Plug Status Screen will also be re-displayed each time a command is successfully executed. Note however, that if desired, the Automated Mode (See Section 9.4) can be enabled to suppress the display of the Plug Status Screen after each command.

9.2.2. Switching and Reboot Commands - Text Interface

These commands can be used to switch or reboot the RSM-8R4's switched plugs, and can also be used to set plugs to the user-defined Power-Up Default values. Plugs may be specified by name or number.

Notes:

- *If a switching or reboot command is directed to a plug that is already being switched or rebooted by a previous command, then the new command will be placed in a queue until the plug is ready to receive additional commands.*
- *If an asterisk appears in the "Status" column for any given plug, this indicates that the plug is currently busy, processing a previously issued command.*
- *When the Port and Plug Status Screen is displayed by an account that permits Administrator or SuperUser level commands, all serial ports and switched outlets will be displayed.*
- *When the Port and Plug Status Screen is displayed by an account that permits ViewOnly or User command access, the screen will only include the serial ports and switched outlets that are specifically allowed by the account.*
- *When you have accessed command mode using an account that permits Administrator or SuperUser level commands, switching and reboot commands can be applied to all plugs.*
- *When you have accessed command mode using an account that permits only User level commands, switching and reboot commands can only be applied to the plugs that are specifically allowed by that account.*
- *If command confirmation is enabled, the RSM-8R4 will display the Status Screen after commands are successfully completed.*
- *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*
- *Text Interface commands are **not** case sensitive. When used in On/Off/Reboot command lines, plug names and plug group names are also **not** case sensitive.*

When switching and reboot commands are executed, the RSM-8R4 will display a "Sure?" prompt, wait for user response, and then complete the command. The unit will pause for a moment while the command is executed, and then return to the Port and Plug Status Screen.

To Switch Plugs, or initiate a Reboot Cycle, proceed as follows:

1. **Switch Plug(s) On:** To power-on a plug or Plug Group, type **/ON *n*** and press **[Enter]**. Where "**n**" is the number or name of the desired plug or Plug Group. For example:

   /ON 1 [Enter] or **/ON ROUTER [Enter]**

2. **Switch Plug(s) Off:** To power-off a plug or Plug Group, type **/OFF n** and press **[Enter]**. Where "**n**" is the number or name of the desired plug or Plug Group. Note that the "**/OFF**" command can also be entered as "**/OF**". For example:

   /OFF 2 [Enter] or **/OF ROUTER [Enter]**

3. **Reboot Plug(s):** To initiate a Boot cycle, type **/BOOT n** and press **[Enter]**. Where "**n**" is the number or name of the desired plug or Plug Group. Note that the "**/BOOT**" command can also be entered as "**/BO**". For example:

   /BOOT 3 [Enter] or **/BO ATMSWTCH [Enter]**

4. **Set All Plugs to Power Up Defaults:** Type **/DPL** and press **[Enter]**. All plugs permitted by your account will be set to their default On/Off status, which is defined via the Plug Parameters Menu as described in Section 5.7.

   Notes:

   - *When you have accessed command mode using an account that permits Administrator or SuperUser level command access, the Default command will be applied to all plugs.*
   - *When you have accessed command mode using an account that only permits User level command access, the Default command will only be applied to the plugs specifically allowed by that account.*
   - *The /DPL command is not available in ViewOnly mode.*

5. **Suppress Command Confirmation Prompt:** To execute a Boot/On/Off command without displaying the "Sure?" prompt, you can either disable command confirmation via the System Parameters Menu, or include the "**,Y**" option at the end of the command line. For example:

   /ON ROUTER,Y or **/BOOT 2,Y**

9.2.2.1. Applying Commands to Several Plugs - Text Interface

As described below, switching and reboot commands can be applied to only one Switched AC Outlet, or to an assortment of outlets.

Note: *When switching and reboot operations are initiated, Boot/Sequence Delay times will be applied as described in Section 5.7.*

1. **Switch Several Plugs:** To apply a command to several plugs, enter the numbers or names for the plugs, separated by a "plus sign" (+) or a comma (,). For example to switch plugs 1, 3, and 4 Off, enter either of the following commands:

   /OFF 1+3+4 [Enter]
   or
   /OFF 1,3,4 [Enter]

   Note: *When the "+" or "," are used, do not enter spaces between the plug name or number and the plus sign or comma.*

2. **Switch a Series of Plugs:** To apply a command to a series of plugs, enter the number for the plugs that mark the beginning and end of the series, separated by a colon. For example to switch On plugs 1 through 3, enter the following:

   /ON 1:3 [Enter]

4. **All Plugs:** To apply a command to all plugs, enter an asterisk in place of the name or number. For example, to Boot all plugs, enter the following:

   /BO * [Enter]

   Note: *When this command is invoked by an account that permits only User level command access, it will be applied only to the plugs that are allowed for that account.*

9.3. Connecting and Disconnecting Serial Ports - Text Interface

The Text Interface can also be used to create connections between RSM-8R4 serial ports. This allows you to access the console port of a connected device, or allow connected devices to access the RSM-8R4's internal modem or network port.

> **Note:** *The Web Browser Interface cannot be used to connect or disconnect ports. In order to connect or disconnect ports, you must access command mode via the Text Interface.*

As discussed in Section 5, There are four available operating modes for the RSM-8R4 serial ports: the Any-to-Any Mode, the Passive Mode, the Buffer Mode and the Modem Mode.

9.3.1. Any-to-Any Mode

Any-to-Any Mode Ports can be connected to other Any-to-Any, Passive, Buffer, or Modem Mode ports by accessing command mode via the Text Interface and issuing the /C Command. All ports can be configured for Any-to-Any Mode, and it is also the default mode for Ports 1 and 2.

9.3.1.1. Connecting Ports

Two different types of connections can be made between RSM-8R4 serial ports; Resident Connections and Third Party Connections The RSM-8R4 allows communication between devices without the requirement that both ports use the same communication parameters.

- **Resident Connections:** Your resident port issues a /C command to connect to a second port. For example, Port 4 issues the /C command to connect to Port 5.
- **Third Party Connections:** (Administrator and SuperUser Mode Only) Your resident port issues a /C command to create a connection between two *other* ports. For example, Port 1 is your resident port, and Port 1 issues a command to connect Port 2 to Port 3.

Notes:

- *Third Party Connections can only be initiated by accounts and ports that permit Administrator or SuperUser level commands.*
- *The serial ports cannot employ the /C command to initiate a connection to the Network Port.*
- *User level accounts are only allowed to connect to ports that are specifically allowed by the account. Administrator and SuperUser level are allowed to connect to all serial ports.*

To Connect ports, proceed as follows:

1. Access command mode via the Text Interface.
2. Invoke the /C command to connect the desired ports.

   a) **Resident Connect:** To connect your resident port to another port, type **`/C xx`** **[Enter]**. Where **`xx`** is the number or name of the port you want to connect. The RSM-8R4 will display the numbers of the connected ports, along with the command required in order to disconnect the two ports.

   Example: To connect your resident port to Port 8, type **`/C 8`** **[Enter]**.

   b) **Third Party Connect:** (Administrator and SuperUser Mode Only) To connect any two ports (other than your resident port), type **`/C xx XX`** **[Enter]**. Where **`xx`** and **`XX`** are two port names or numbers. The RSM-8R4 will display the numbers of the two connected ports.

   Example: To connect Port 5 to Port 6, access command mode at a third port that permits Administrator level commands (using an account that also permits Administrator or SuperUser level commands), and invoke the following command: **`/C 5 6`** **[Enter]**.

Notes:

- **Resident Connections:** *RSM-8R4 serial ports are not allowed to initiate a Resident Connection to the Network Port.*
- **Third Party Connections:** *Serial ports are not allowed to connect another port to the network port. For example, Port 1 is not allowed to connect Port 3 to the Network Port.*

When the /C command specifies the port name, it is only necessary to enter enough letters to differentiate the desired port from other ports. Type an asterisk (*) to represent the remaining characters in the port name. For example, to connect your resident port to a port named “SALES”, the connect command can be invoked as **`/C S*`**, providing no other port names begin with the letter “S”.

9.3.1.2. Disconnecting Ports

There are three different methods for disconnecting ports, the Resident Disconnect, the Third Party Disconnect, and the No Activity Timeout. Providing the Timeout feature is enabled, a No Activity Timeout will disconnect resident ports or third party ports.

> **Note:** *The "DTR Output" option in the Port Parameters menu determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed and then held high.*

1. **Resident Disconnect:** Disconnects your resident port from another port. For example, if you are communicating via Port 3, and Port 3 is connected to Port 4, a Resident Disconnect is used to disassociate the two ports. The RSM-8R4 offers two different disconnect command formats; the One Character Format and the Three Character Format (for more information, please refer to Section 5.8.2.):

   > **Note:** *The Resident Disconnect methods discussed here cannot be used to terminate a Telnet Direct Connection. For more information, please refer to Section 10.3.4.*

   a) **One Character (Default):** Enter the logoff character once (Default = **[Ctrl]** plus **[X]**). It is not necessary to enter a carriage return before or after the logoff character.

   b) **Three Characters:** Uses the "**[Enter]**`LLL`**[Enter]**" format, where `L` is the logoff character. For example, if the logoff character is "**+**", then the disconnect sequence is **[Enter]+++[Enter]**.

   c) If the default disconnect command is not compatible with your application, both the command format and logoff character can be redefined via the Port Configuration menus, as described in Section 5.8.2.

2. **Third Party Disconnect:** (Administrator and SuperUser Mode Only) The /D command is issued from your resident port to disconnect two other ports. For example, if your Resident Port is Port 1, a Third Party Disconnect is used to disconnect Ports 3 and 4.

   > **Note:** *The Third Party Disconnect method can be used to terminate a Telnet Direct Connection. For more information, please refer to Section 10.3.4.*

   a) The /D command uses the format: **`/D xx`** **[Enter]**, where **`xx`** is the number of either of the connected ports that you wish to disconnect.

   b) Third Party (Remote) Disconnects can only be performed by accounts that permit Administrator or SuperUser level commands.

   c) The /D command can also disconnect a remote user from the Network Port. This is useful in cases where a user has unsuccessfully disconnected via Telnet, and you can't wait for the RSM-8R4 to timeout in order to free up the TCP port. To disconnect a TCP port, type **`/D Nn`** and then press **[Enter]**. Where **`Nn`** is one of the RSM-8R4's logical TCP ports (e.g. **`/D N2`** **[Enter]**).

3. **No Activity Timeout:** Providing the Timeout feature is enabled at either connected port, the No Activity Timeout can also disconnect ports when no command activity is detected at the ports for the user-defined timeout period.

   Note: *The No Activity Timeout also applies to Telnet Direct Connections. For more information, please refer to Section 5.8.*

   a) **RS232 Ports:** To select the timeout period for RS232 Ports, access the Port Configuration Menu for the desired port as described in Section 5.8.

   b) **Network Port:** To select the timeout period for the Network Port, access the Network Port Configuration Menu as described in Section 5.9.

   c) When the Timeout Feature is enabled, the port will automatically disconnect if no data is received during the defined Timeout Period.

Notes:

- *When two connected ports time out, both ports will exit command mode after disconnecting.*
- *The Timeout value also applies to unconnected ports that are left in command mode. When an unconnected port is left in command mode, and no additional activity is detected, the port will automatically exit command mode when its timeout value elapses.*

9.3.1.3. Defining Hunt Groups

A Hunt Group creates a situation where the RSM-8R4 will scan a group of similarly named ports and connect to the first available port in the group. Hunt Groups are created by assigning identical or similar names to two or more ports. Hunt Groups can be defined using Any-to-Any, Passive, Buffer, or Modem Mode Ports. Note that the Network Port *cannot* be included in Hunt Groups.

1. Access command mode using a port and account that permit Administrator level commands.
2. Access the Port Configuration Menu for the desired Port(s) as described in Section 5.8.
3. From the Port Configuration Menu, define the Port Name.
4. Repeat steps 2 and 3 to assign identical names to the other ports in the Hunt Group. For example, a series of ports in a group could all be named "SERVER".
5. To connect to the next available port in the hunt group, invoke the /C command using the port name to specify the desired group. For example, **`/C SERVER` [Enter]**.
6. Your port will be connected to the first available port in the group. If all ports are presently connected, the RSM-8R4 will respond with the "BUSY" message.
7. It is only necessary to enter enough letters of the port name to differentiate Hunt Group ports from other ports. Type an asterisk (*) to represent the remaining characters in the name. For example, to connect to the first available port in a group of ports named "SALES1", "SALES2", and "SALES3", the connect command can be invoked as **`/C S*` [Enter]**, providing no other port names begin with the letter "S".

Notes:

- *If the Hunt Group method is used by a port or account with User level command access, the /C command will only connect to the ports allowed by that account.*
- *Hunt Group port names must be unique. Otherwise, ports with similar names will also be included in the Hunt Group.*

Hunt Group Example 1:

1. Ports 1 and 2 are Modem Mode ports, and modems are installed at both ports. Port 1 is named "MODEM1" and Port 2 is named "MODEM2".
2. Your resident port is Port 4. To connect to the first available Modem, type **`/C MODEM*` [Enter]**.

Hunt Group Example 2:

1. Ports 3, 4, and 5 are Any-to-Any Mode ports. All three ports are named "SERVER".
2. Your resident port is Port 1. If you want to connect Port 2 to the first available server, type **`/C 2 SERVER` [Enter]**.

9.3.2. Passive Mode

Passive Mode Ports function the same as Any-to-Any Mode Ports, but do not allow access to command mode. A Passive Mode Port can be connected to other serial ports, but cannot enter command mode, and therefore cannot define parameters, display status, or invoke commands to connect ports or control power switching. The Passive Mode is the default at Serial Ports 3 and above.

Passive Mode Ports can be connected by accessing command mode from a free Any-to-Any or Modem Mode Port, and invoking the Third Party Connect or Resident Connect Command as described in Section 9.3.1.2. Passive Mode ports will not buffer data, except during baud rate conversion.

> **Note:** *In order to ensure Administrator level access to important command functions, the Passive Mode is not available at Port 1 (the Set Up Port) or the Network Port.*

9.3.3. Buffer Mode

The Buffer Mode allows collection of data from various devices without the requirement that all devices use the same communication parameters. In addition, Buffer Mode ports can also be configured to support the SYSLOG and SNMP Trap functions, as described in Sections 11 and 12.

Notes:

- *Buffer Mode Ports cannot access command mode.*
- *Buffer Mode is not available to Port 1 (the SetUp Port) or the Network Port.*

9.3.3.1. Reading Data from Buffer Mode Ports

To check port buffers for stored data, access command mode via the text interface, using an account that permits Administrator, SuperUser or User level commands, and type **`/S`** **[Enter]** to display the Port Status Screen. The "Buffer Count" column in the Port Status Screen indicates how much data is currently being stored for each port.

To retrieve data from buffer memory, go to a free Any-to-Any or Modem Mode Port, then issue the /R command using the following format: **`/R xx`** **[Enter]**. Where **`xx`** is the number of the port buffer to be read.

Notes:

- *The /R command is not available to ViewOnly level accounts.*
- *In order to read data from a given port, your account must allow access to that port.*
- *When the /R command is invoked, the counter for the SNMP Trap function will also be reset.*

If the buffer contains data, the RSM-8R4 will display a prompt that offers the following options:

- **Display One Screen:** To send data one screen at a time, press **[Enter]**. Each time **[Enter]** is pressed, the next screen is sent.
- **Display All Data:** To send all data currently stored in the buffer, type `1` and press **[Enter]**.
- **Erase Data on Screen:** To erase the data currently displayed on-screen, type `2` and press **[Enter]**.
- **Erase all Data:** To erase all data currently stored in the buffer, type `3` and press **[Enter]**.
- **Exit:** To exit from Read Buffer mode, press **[Esc]**.

  Note: *Only one user can read from a port buffer at a time. If a second user attempts to read from a port that is already being read, an error message will be sent.*

To clear data from any port buffer (with or without reading it first), access command mode via the text interface, using an account and port that permit Administrator, SuperUser or User level commands, then issue the /E (Erase Buffer) command using the following format:

`/E xx` [Enter]

Where **`xx`** is the number of the port buffer to be cleared.

Notes:

- *The /E command cannot erase data from a port buffer that is currently being read by another port.*
- *The /E command is not available to ViewOnly level accounts.*

9.3.3.2. Port Buffers

The Status Screen lists the amount of Buffer Memory currently used by each port. The RSM-8R4 uses buffer memory in two different ways, depending on the user-selected port mode.

- **Any-to-Any, Passive, and Modem Mode Ports:** When two ports are communicating at dissimilar baud rates, the buffer memory prevents data overflow at the slower port.
- **Buffer Mode Ports:** Stores data received from connected devices. The user issues a Read Buffer command (/R) from an Any-to-Any or Modem Mode port to retrieve data.

If the Status Screen indicates an accumulation of data, the /E (Erase Buffer) command can be invoked to clear the buffer.

Note: *When a Buffer Mode port is reconfigured as an Any-to-Any, Passive, or Modem Mode port, any data stored in the buffer prior to changing the port mode will be lost.*

9.3.4. Modem Mode

The Modem Mode provides features specifically related to modem communication. A Modem Mode Port can perform all functions normally available in Any-to-Any Mode. The Modem Mode is available to all RSM-8R4 ports except the Network Port, and is the default port mode at the Internal Modem port.

When Modem Mode is selected, the Port Configuration menu will display three additional prompts, which allow you to re-define the modem reset string, initialization string, and hang-up string.

When a call is received, the unit will prompt the caller to enter a username and password. The RSM-8R4 allows three attempts to enter a valid username and password. If a valid username and password is not entered within three attempts, or if the user does not respond to the login prompt within 30 seconds, the modem will disconnect.

Notes:

- *When a Modem Mode port exits command mode, or the DCD line is lost while command mode is active, the RSM-8R4 will pulse DTR to the modem. The unit will then send the user-defined modem command strings to make certain the modem is properly disconnected and reinitialized.*
- *The Internal Modem Port (Port 9) is always configured for Modem Mode; the port mode for the Internal Modem Port cannot be changed.*
- *When an external modem is installed at an RSM-8R4 port, other ports can use the modem for calling out. To call out, invoke the /C command to connect to the port, then access the modem as you normally would.*
- *If desired, the Invalid Access Lockout feature can provide additional security for Modem Mode ports. When properly configured, the Invalid Access Lockout will automatically shut down a port whenever that port exceeds the user defined number of invalid access attempts. For more information, please refer to Section 5.3.2.*

9.4. The Automated Mode

The Automated Mode allows the RSM-8R4 to execute switching and reboot commands, without displaying menus or generating response messages. Automated Mode is designed to allow the RSM-8R4 to be controlled by a device which can generate commands to control power switching functions without human intervention.

When Automated Mode is enabled, the /ON, /OFF, /BOOT, /DPL and /X commands are executed without a "Sure?" confirmation prompt and without command response messages; the only reply to these commands is the "RSM>" prompt, which is displayed when the command is complete.

Note that although Automated Mode can be enabled using either the Web Browser Interface or Text Interface, Automated Mode is designed primarily for users who wish to send ASCII commands to the RSM-8R4 without operator intervention, and therefore does not specifically apply to the Web Browser Interface. When Automated Mode is enabled, the Web Browser Interface can still be used to invoke On / Off / Boot commands.

Notes:

- *When Automated Mode is enabled, all RSM-8R4 password security functions are disabled, and users are able to access System Level command functions (including the configuration menus) and control plugs without entering a password.*
- *If you need to enable the Automated Mode, but want to restrict network access to RSM-8R4 configuration menus, it is recommended to enable and configure the IP Security Function as described in Section 5.9.3.*

To enable/disable Automated Mode, access the System Parameters menu (see Section 5.3,) then set the "Automated Mode" option to "On". When Automated Mode is enabled, RSM-8R4 functions will change as follows:

1. **All Password Security Suppressed:** When a user attempts to access command mode, the password prompt will not be displayed at either the Console Port or the Network Port. Unless specifically restricted by the IP Security Function, all users will be allowed to access both switching and configuration functions, and all commands will be immediately accepted without the requirement to enter a password.
2. **Status Screen Suppressed:** The status screens will not be automatically displayed after commands are successfully executed. Note however, that the /S command can still be invoked to display the status screen as needed.
3. **"Sure?" Prompt Suppressed:** All commands are executed without prompting for user confirmation.
4. **Error Messages Suppressed:** If the **[Enter]** key is pressed without entering a command, the RSM-8R4 will not respond with the "Invalid Command" message. Note however, that an error message will still be generated if commands are invoked using invalid formats or arguments.

All other status display and configuration commands will still function as normal.

9.5. Manual Operation

In addition to the command driven functions available via the Web Browser Interface and Text Interface, some RSM-8R4 functions can also be controlled manually. For a summary of front panel control functions, please refer to Section 2.3.

9.6. Logging Out of Command Mode

When you have finished communicating with the RSM-8R4, it is important to always disconnect using either the "LogOut" link (Web Browser Interface) or the /X command (Text Interface), rather than by simply closing your browser window or communications program. When communicating via a PDA, use the PDA's "Close" function to disconnect and logout.

When you disconnect using the LogOut link or /X command, this ensures that the RSM-8R4 has completely exited from command mode, and is not waiting for the inactivity timeout period to elapse before allowing additional connections.

10. Telnet & SSH Functions

10.1. Network Port Numbers

Whenever an inbound Telnet or SSH session connects to an RSM-8R4 serial port, the Port Status Screen and Port Diagnostics Screen will indicate that the serial port is presently connected to Port "**Nn**" (where "**N**" indicates a network connection, and "**n**" is a number that lists the logical Network Port being used; for example, "**N11**".) This "Nn" number is referred to as the logical Network Port Number.

10.2. SSH Encryption

In addition to standard Telnet protocol, the RSM-8R4 also supports SSH connections, which provide secure, encrypted access via network. In order to communicate with the RSM-8R4 using SSH protocol, your network node must include an appropriate SSH client.

Note that when the /K (Send SSH Key) command is invoked, the RSM-8R4 can also provide you with a public SSH key, which can be used to streamline connection to the RSM-8R4 when using SSH protocol.

Although you can establish an SSH connection to the unit *without* the public key, the public key provides validation for the RSM-8R4, and once this key is supplied to the SSH client, the client will no longer display a warning indicating that the RSM-8R4 is not a recognized user when the client attempts to establish a connection.

The /K command uses the following format:

/K <k> [Enter]

Where **k** is an argument that determines which type of public key will be displayed, and the **k** argument offers the following options:

1. SSH1
2. SSH2 RSA
3. SSH2 DSA

For example, to obtain the public SSH key for an SSH2 RSA client, type **/K 2** and then press **[Enter]**.

> **Note:** *Although the RSM-8R4 does not support SSH1, the /K 1 command will still return a key for SSH1.*

10.3. The Direct Connect Feature

The Direct Connect feature allows you to initiate a Telnet, SSH or Raw Socket session with the RSM-8R4 and make an immediate connection to a specific serial port of your choice, without first being presented with the command interface. This allows you to connect to a TCP port that is mapped directly to one of the RSM-8R4's serial ports.

Direct Connect employs unique, pre-assigned TCP port numbers for each serial port. The user connects to the port of choice by including the associated TCP port number in the Telnet or SSH connect command line.

The Direct Connect feature can be individually configured at each serial port and can be used to connect to Any-to-Any, Passive, Buffer, or Modem Mode ports.

10.3.1. Standard Telnet Protocol, SSH and Raw Socket

The Direct Connect feature allows you to establish port connections using either Standard Telnet Protocol, SSH encryption or Raw Socket. When Standard Telnet Protocol is used, the RSM-8R4 will respond to all IACs.

When configuring a serial port to allow Direct Connections using SSH protocol, note that the Direct Connect option (Port Configuration Menu, Item 31), must be set to "On - Password" as described in Section 10.3.2.

When configuring a serial port to allow Direct Connections using either Standard Telnet or Raw Socket Mode, note that the Direct Connect option (Port Configuration Menu, Item 31) may be set to either "On - Password" or "On - No Password".

10.3.2. Configuration

The Direct Connect Function is configured on a per port basis using the Port Configuration Menus (**`/P nn`**), item 31, "Direct Connect". The following options are available:

1. **Direct Connect OFF:** Direct Connect disabled at this port. (Default)
2. **Direct Connect ON - NO PASSWORD:** The Direct Connect feature is enabled at this port, but no password is required in order to connect to the port.
   a) When the Telnet connection is established, the user is immediately connected directly to the specified port, and the client is notified at the TCP level.
   b) This option is intended for situations where security is provided by the attached device.

   Note: *The SSH Direct Connection function is disabled when the "On - No Password" option is selected.*

3. **Direct Connect ON - PASSWORD:** The Direct Connect feature is enabled at this port, but a password must be entered before a Direct Connection is established.

   a) Upon login, the RSM-8R4 will prompt for a username and password. If a valid username/password is entered, the RSM-8R4 will return a message which confirms the connection and lists the name and number of the port (providing the user account allows access to the target port.)

   b) If a valid username / password is not entered in 30 seconds or three attempts, the port will timeout and disconnect.

Notes:

- *If you intend to create "Raw Socket" connections to RSM-8R4 serial ports, then the "Raw Socket Access" feature must also be enabled at the Network Port, as described in Section 5.9.2.*
- *If you intend to use SSH to establish direct connections to the RSM-8R4, the "Direct Connect ON - PASSWORD option must be selected.*
- *If Administrator level commands are disabled at the Network Port, then accounts that permit Administrator level commands will not be able to initiate a Direct Connection.*
- *If Administrator level commands are enabled at the Network Port, then accounts with Administrator level access and accounts without Administrator level access will both be allowed to establish Direct Connections.*
- *If your user account does not permit access to the target port, the connection will be refused.*

10.3.3. Connecting to a Serial Port using Direct Connect

Direct Connect TCP port numbers are as follows:

1. **Standard Telnet Direct Connection (with Password):**

   - Serial Ports: TCP port numbers 2101 through 2108.
   - Internal Modem Port: TCP port number 2109.

2. **Standard Telnet Direct Connection (without Password):**

   - Serial Ports: TCP port numbers 2301 through 2308.
   - Internal Modem Port: TCP port number 2309.

3. **SSH Direct Connection (with Password):**

   - Serial Ports: TCP port numbers 2201 through 2208.
   - Internal Modem Port: TCP port number 2209.

4. **Raw Socket Direct Connection (with Password):**

   - Serial Ports: TCP port numbers 3101 through 3108.
   - Internal Modem Port: TCP port number 3109.

5. **Raw Socket Direct Connection (without Password):**

   - Serial Ports: TCP port numbers 3301 through 3308.
   - Internal Modem Port: TCP port number 3309.

   Note: *In order to create a Raw Socket Direct Connection, the "Raw Socket Access" parameter for the Network Port must be enabled as described in Section 5.9.2.*

When establishing a Direct Connection, the correct TCP port number must be used. If conditions are acceptable (e.g. Target Port must be free and properly configured), an immediate connection will be made, with one possible exception; password entry may first be required depending on configuration settings.

Note: *When a Direct Connect attempt fails because the Port is busy, the call is rejected at the TCP level.*

Connection Example

1. Assume that Port 8 is configured as described in Section 10.3.2 If the RSM-8R4's IP address is "1.2.3.4", and you wish to establish a standard Telnet protocol connection with port 8 (TCP Port Number 2108), then on a UNIX system, the connect command would be invoked as follows:

   `$ telnet 1.2.3.4 2108` **[Enter]**

2. The RSM-8R4 will first send the site ID, Port Number, Port Name, and Telnet Port number, and then once a connection is established, the "Connected" message will be sent.

10.3.4. Terminating a Direct Connect Session

To terminate a Direct Connect session, use the client program's "disconnect" feature. The following will occur immediately upon a client initiated disconnect:

1. The Network port is disconnected from the serial port.
2. The Network session is terminated.
3. The serial port is put to sleep.

Notes:

- *The Sequence Disconnect Command, which is defined via the Port Configuration menus, cannot be used to terminate a Direct Connection.*
- *Any RSM-8R4 port that allows Administrator or SuperUser level commands can terminate a direct connection at another port by issuing the /D command as described in Section 9.3.1.2.*
- *Acknowledgment of data received by the RSM-8R4 network port does not automatically indicate that the data has been completely sent out the serial port. Data may still be queued in RSM-8R4 buffers. Any data queued at the time of a client initiated disconnect is discarded, and is not passed to the attached device.*

11. Syslog Messages

The Syslog feature can create log records of each Alarm Event. As these event records are created, they are sent to a Syslog Daemon, located at an IP address defined via the Network Parameters menu.

11.1. Configuration

In order to employ this feature, you must set the real-time clock and calendar via the System Parameters Menu, and define the IP address for the Syslog Daemon via the Network Port Configuration menu.

To configure the Syslog function, please proceed as follows:

1. **Access command mode:** Note that the following configuration menus are only available to accounts that permit Administrator level commands.
2. **System Parameters Menu:** Access the System Parameters Menu as described in Section 5.3, then set the following parameters:
    a) **Set Clock and Calendar:** Set the Real Time Clock and Calendar and/or configure and enable the NTP server feature.
3. **Network Parameters Menu:** Access the Network Parameters Menu as described in Section 5.9, then set the following parameters:
    a) **Syslog IP Address:** Determine the IP address for the device that will run the Syslog Daemon, then use the Network Port Configuration menu to define the IP Address for the Syslog Daemon.
5. **Syslog Daemon:** In order to capture messages sent by the RSM-8R4, a computer must be running a Syslog Daemon (set to UDP Port 514) at the IP address specified in Step 4 above.

Once the Syslog Address is defined, Syslog messages will be generated whenever one of the alarms discussed in Section 7 is triggered.

```
TEST NETWORK OPTIONS:

1. SNMP Trap Test Manager 1
2. SNMP Trap Test Manager 2
3. Syslog Test
4. Ping




Enter: #<CR> to select,
       <ESC> to exit ...
```

Figure 11.1: The Test Menu (Text Interface)

11.2. Testing Syslog Configuration

After you have configured the RSM-8R4 as described in Section 11.1, the /TEST command can be used to make certain that the function is properly set up. To test the Syslog function, access the RSM-8R4 command mode via the Text Interface using an account that permits Administrator or SuperUser level commands, then type **/TEST** and press **[Enter]** to display the Test Menu shown in Figure 11.1.

When the Syslog Test feature is selected, the RSM-8R4 will attempt to send a test Syslog message, using the current Syslog configuration. If the test message is not received by your Syslog Daemon, review the procedure outlined in Section 11.1 to make certain the RSM-8R4 and the Syslog Daemon are properly configured.

In addition to providing a means to test the Syslog and SNMP Trap features, the Test Menu also includes a Ping command option, which can be used in a manner similar to the DOS ping command to check to make certain that the unit is communicating properly. Note that in order for the Ping command to function with domain names, you must first configure Domain Name Server parameters as described in Section 5.9.5.

12. SNMP Traps

SNMP is an acronym for "Simple Network Management Protocol". The SNMP Trap function allows the RSM-8R4 to send Alarm Notification messages to two different SNMP managers, each time one of the Alarms discussed in Section 7 is triggered.

Note:

- *The SNMP feature cannot be configured via the SNMP Manager.*
- *SNMP reading ability is limited to the System Group.*
- *The SNMP feature includes the ability to be polled by an SNMP Manager.*
- *Once SNMP Trap Parameters have been defined, SNMP Traps will be sent each time an Alarm is triggered. For more information on Alarm Configuration, please refer to Section 7.*

12.1. Configuration:

To configure the SNMP Trap function, proceed as follows:

1. Access command mode using an account that permits Administrator level commands.
2. **SNMP Trap Parameters:** Access the SNMP Trap Parameters Menu as described in Section 5.9.7. Set the following:

   a) **SNMP Managers 1 and 2:** The address(es) that will receive SNMP Traps that are generated by one of the Alarms discussed in Section 7. Consult your network administrator to determine the IP address(es) for the SNMP Manager(s), then use the Network Parameters menu to set the IP address for each SNMP Manager. Note that it is not necessary to define both SNMP Managers.

   Note: *To enable the SNMP Trap feature, you must define at least one SNMP Manager. SNMP Traps are automatically enabled when at least one SNMP Manager has been defined.*

   b) **Trap Community:** Consult your network administrator, and then use the Network Parameters menus to set the Trap Community.

Once SNMP Trap Parameters have been defined, the RSM-8R4 will send an SNMP Trap each time an alarm is triggered.

12.2. Testing the SNMP Trap Function

After you have finished setting up the SNMP Trap function, it is recommended to test the configuration to ensure that it is working correctly. To test configuration of the SNMP Trap function, proceed as follows:

1. Configure the SNMP Trap function as described in Section 12.1.
2. Access the Text Interface command mode using an account that permits Administrator or SuperUser level commands, then invoke the "/TEST" command at the RSM-8R4 command prompt. Note that the /TEST Command is only available in Administrator and SuperUser Mode.
3. Select Item 1 or 2 to send an SNMP test trap to Manager 1 or 2, respectively. It is possible that the ARP table will not be properly setup. If this occurs a message to that effect is displayed and the RSM-8R4 immediately refreshes the ARP table. Repeat steps 2 and 3 to try again.

For more information on the **/TEST** command and the Test Menu, please refer to Section 11.2.

13. Operation via SNMP

If SNMP Access Parameters have been defined as described in Section 5.9.6, then you will be able to manage user accounts, control power and reboot switching and display unit status via SNMP. This section describes SNMP communication with the RSM-8R4 unit, and lists some common commands that can be employed to manage users, control switching and reboot actions and display unit status.

13.1. RSM-8R4 SNMP Agent

The RSM-8R4's SNMP Agent supports various configuration, control, status and event notification capabilities. Managed objects are described in the WTI-RSM8R4-MIB.txt document, which can be found on the CDROM included with the RSM-8R4 unit, or on the WTI web site (http://www.wti.com). The WTI-RSM8R4-MIB.txt document can be compiled for use with your SNMP client.

13.2. SNMPv3 Authentication and Encryption

The major limitations of SNMPv2 were the failure to include proper username/password login credentials (v2 only used a password type of login, i.e., community name) and the exclusion of encryption for data moving over the internet. SNMPv3 addresses both of these shortcomings.

For SNMPv3, the RSM-8R4 supports two forms of Authentication/Privacy: Auth/noPriv which requires a username/password, but does not encrypt data going over the internet and Auth/Priv which requires a username/password AND encrypts the data going over the internet using DES (AES is not supported at this time). For the Password protocol, the RSM-8R4 supports either MD5 or SHA1.

13.3. Configuration via SNMP

RSM-8R4 User accounts can be viewed, created, modified, and deleted via SNMP. User accounts are arranged in a table of 128 rows, and indexed 1-128. User account parameters, as seen through the SNMP, are summarized below.

- **`userTable::userName`** – 32 character username
- **`userTable::userPassword`** – 16 character password
- **`userTable::userAccessLevel`** – Account access level.
  `0` – View Access
  `1` – User Access
  `2` – Superuser Access
  `3` – Administrator Access
- **`userTable::userPlugAccess`** – A string of up to 4 characters, with one character for each of the 4 possible plugs on the RSM-8R4 unit. A '`0`' indicates that the account **does not** have access to the plug, and a '`1`' indicates that the user *does* have access to the plug.
- **`userTable::userPortAccess`** – A string of up to 9 characters, with one character for each of the 9 possible serial ports on the RSM-8R4 unit. A '`0`' indicates that the account **does not** have access to the port, and a '`1`' indicates that the user *does* have access to the port.
- **`userTable::userGroupAccess`** – A string of 54 characters, with one character for each of the 54 possible plug groups in the system. A '`0`' indicates that the account **does not** have access to the plug group, and a '`1`' indicates that the user *does* have access to the plug group.
- **`userTable::userSerialAccess`** – Access to the serial interface
  `0` – No access
  `1` – Access
- **`userTable::userTelnetSshAccess`** – Access to the Telnet/SSH interface
  `0` – No access
  `1` - Access
- **`userTable::userOutboundTelSshAccess`** – Access to Outbound Telnet/SSH
  `0` – No access
  `1` - Access
- **`userTable::userWebAccess`** – Access to the Web interface
  `0` – No access
  `1` - Access
- **`userTable::userCallbackNum`** – 32 character callback number for account
- **`userTable::userSubmit`** – Set to `1` to submit changes.

13.3.1. Viewing Users

To view users, issue a GET request on any of the user parameters for the index corresponding to the desired user.

13.3.2. Adding Users

For an empty index, issue a SET request on the desired parameters. Minimum requirement is a username and password to create a user, all other parameters will be set to defaults if not specified. To create the user, issue a SET request on the userSubmit object.

13.3.3. Modifying Users

For the index corresponding to the user you wish to modify, issue a SET request on the desired parameters to be modified. Once complete, issue a SET request on the userSubmit object.

13.3.4. Deleting Users

For the index corresponding to the user you wish to delete, issue a SET request on the username with a blank string. Once complete, issue a SET request on the userSubmit object.

13.4. Plug Control via SNMP

13.4.1. Controlling Plugs

ON, OFF, BOOT, and DEFAULT commands can be issued for plugs via SNMP. Plugs are arranged in a table of N rows, where N is the number of plugs in the system. Plug parameters are described below.

- **`plugTable::plugID`** – String indicating the plug's ID
- **`plugTable::plugStatus`** – Current state of the plug
  - **`0`** – Plug is OFF
  - **`1`** – Plug is ON
- **`plugTable::plugAction`** – Action to be taken on plug
  - **`1`** – Mark to turn ON (does not execute)
  - **`2`** – Mark to turn OFF (does not execute)
  - **`3`** – Mark to BOOT (does not execute)
  - 4 – Mark to DEFAULT (does not execute)
  - 5 – Mark to turn ON and execute plug actions
  - 6 - Mark to turn OFF and execute plug actions
  - 7 - Mark to BOOT and execute plug actions
  - 8 - Mark to DEFAULT and execute plug actions

Set **`plugTable::plugAction`** to desired action, as specified by values 1-4 above, for each plug index the action is to be applied to. For the last plug you wish to set before executing the commands, use values 5-8 instead, which will invoke the requested commands all at once.

13.4.2. Controlling Plug Groups

ON, OFF, BOOT, and DEFAULT commands can be issued for plug groups via SNMP. Plug groups are arranged in a table of 54 rows, one row for each plug group in the system. Plug Group parameters are described below.

- **`plugGroupTable::plugGroupName`** – String indicating the plug groups name
- **`plugGroupTable::plugGroupAction`** – Action to be taken on plug group
  - **`1`** – Mark to turn ON (does not execute)
  - **`2`** – Mark to turn OFF (does not execute)
  - **`3`** – Mark to BOOT (does not execute)
  - **`4`** – Mark to DEFAULT (does not execute)
  - **`5`** – Mark to turn ON and execute plug group actions
  - **`6`** - Mark to turn OFF and execute plug group actions
  - **`7`** - Mark to BOOT and execute plug group actions
  - **`8`** - Mark to DEFAULT and execute plug group actions

Set **`plugGroupTable::plugGroupAction`** to desired action, as specified by values 1-4 above, for each plug group index the action is to be applied to. For the last plug group you wish to set before executing the commands, use values 5-8 instead, which will invoke the requested commands all at once.

13.5. Configuring Serial Ports

Commands can be issued to set certain serial port configuration parameters via SNMP. Ports are arranged in a table of 9 rows, with one row for each serial port. Serial port parameters are described below.

- **`portTable::portID`** – String indicating the serial port's ID
- **`portTable::portThreshold`** – An integer that sets the serial port's SNMP Trap Level value. If this value is set between 1 and 32,757, then the SNMP trap function is enabled and traps will be sent to the SNMP Managers whenever the buffer for this port reaches the specified level. If set to "0" (zero), the SNMP Traps are disabled at this port.

13.6. Viewing RSM-8R4 Status via SNMP

Status of various components of the RSM-8R4 can be retrieved via SNMP. Plug Status, and Environmental Status are currently supported.

13.6.1. Plug Status

The status of each plug in the system can be retrieved using the command below.

- **`plugTable::plugStatus`** – The status of the plug.
  `0` – Plug is OFF
  `1` – Plug is ON

13.6.2. Unit Temperature Status

The temperature status can be retrieved for various variables for the RSM-8R4 unit. The environmentUnitTable contains one row.

- **`environmentUnitTable::environmentUnitTemperature`** – The temperature of the RSM-8R4 unit.

13.7. Sending Traps via SNMP

Traps that report various unit conditions can be sent to an SNMP Management Station from the RSM-8R4. The following traps are currently supported.

- **`WarmStart`** Trap – Trap indicating a warm start
- **`ColdStart`** Trap – Trap indicating a cold start
- **`Alarm`** Trap – Trap indicating an alarm condition
- **`Test`** Trap – Test trap invoked by user via the Text Interface (CLI)

14 Setting Up SSL Encryption

This section describes the procedure for setting up a secure connection via an https web connection to the RSM-8R4.

> **Note:** *SSL parameters cannot be defined via the Web Browser Interface. In order to set up SSL encryption, you must contact the RSM-8R4 via the Text Interface.*

There are two different types of https security certificates: "Self Signed" certificates and "Signed" certificates.

Self Signed certificates can be created by the RSM-8R4, without the need to go to an outside service, and there is no need to set up your domain name server to recognize the RSM-8R4. The principal disadvantage of Self Signed certificates, is that when you access the RSM-8R4 command mode via the Web Browser Interface, the browser will display a message which warns that the connection might be unsafe. Note however, that even though this message is displayed, communication will still be encrypted, and the message is merely a warning that the RSM-8R4 is not recognized and that you may not be connecting to the site that you intended.

Signed certificates must be created via an outside security service (e.g., VeriSign®, Thawte™, etc.) and then uploaded to the RSM-8R4 unit to verify the user's identity. In order to use Signed certificates, you must contact an appropriate security service and set up your domain name server to recognize the name that you will assign to the RSM-8R4 unit (e.g., service.wti.com.) Once a signed certificate has been created and uploaded to the RSM-8R4, you will then be able to access command mode without seeing the warning message that is normally displayed for Self Signed certificate access.

```
WEB ACCESS:

HTTP:
1.  Enable: On
2.  Port:   80

HTTPS:
3.  Enable: Off
4.  Port:   443

SSL Certificates:
5.  Common Name:
6.  State or Province:
7.  Locality:
8.  Country:
9.  Email Address:
10. Organization Name:
11. Organizational Unit:
12. Create CSR:
13. View CSR:
14. Import CRT:

Enter: #<CR> to change,
       <ESC> for previous menu ...
```

Figure 14.1: Web Access Parameters (Text Interface Only)

14.1. Creating a Self Signed Certificate

To create a Self Signed certificate, access the Text interface via Telnet or SSH, using a password that permits access to Administrator level commands and then proceed as follows:

1. Type **/N** and press **[Enter]** to display the Network Parameters menu.
2. At the Network Parameters menu, type **23** and press **[Enter]** to display the Web Access menu (Figure 14.1.) Type **3** and press **[Enter]** and then follow the instructions in the resulting submenu to enable HTTPS access.
3. Next, use the Web Access menu to define the following parameters.

   Note: *When configuring the RSM-8R4, make certain to define all of the following parameters. Although most SSL applications require only the Common Name, in the case of the RSM-8R4 all of the following parameters are mandatory.*

   - **5. Common Name:** A domain name, that will be used to identify the RSM-8R4 unit. If you will use a Self Signed certificate, then this name can be any name that you choose, and there is no need to set up your domain name server to recognize this name. However, if you will use a Signed certificate, then your domain name server must be set up to recognize this name (e.g., service.wti.com.)
   - **6. State or Province:** The name of the state or province where the RSM-8R4 unit will be located (e.g., California.)
   - **7. Locality:** The city or town where the RSM-8R4 unit will be located (e.g., Irvine.)
   - **8. Country:** The two character country code for the nation where the RSM-8R4 will be located (e.g., US.)
   - **9. Email Address:** An email address, that can be used to contact the person responsible for the RSM-8R4 (e.g., jsmith@yourcompany.com.)
   - **10. Organizational Name:** The name of your company or organization (e.g., Western Telematic.)
   - **11. Organizational Unit:** The name of your department or division; if necessary, any random text can be entered in this field (e.g., tech support.)

4. After you have defined parameters 5 through 11, type `12` and press **[Enter]** (Create CSR) to create a Certificate Signing Request. By default, this will overwrite any existing certificate, and create a new Self Signed certificate.

   a) The RSM-8R4 will prompt you to create a password. Key in the desired password (up to 16 characters) and then press **[Enter]**. When the RSM-8R4 prompts you to verify the password, key it again and then press **[Enter]** once. After a brief pause, the RSM-8R4 will return to the Web Access Menu, indicating that the CSR has been successfully created.

   b) When the Web Access Menu is re-displayed, press **[Esc]** several times until you exit from the Network Parameters menu and the "Saving Configuration" message is displayed.

5. After the new configuration has been saved, test the Self Signed certificate by accessing the RSM-8R4 via the Web Interface, using an HTTPS connection.

   a) Before the connection is established, the RSM-8R4 should display the warning message described previously. This indicates that the Self Signed certificate has been successfully created and saved.

   b) Click on the "Yes" button to proceed. The RSM-8R4 will prompt you to enter a user name and password. After keying in your password, the main menu should be displayed, indicating that you have successfully accessed command mode.

14.2. Creating a Signed Certificate

To create a Signed certificate, and eliminate the warning message, first set up your domain name server to recognize the Common Name (item 5) that you will assign to the unit. Next, complete steps one through five as described in Section 14.1 and then proceed as follows:

1. **Capture the Newly Created Certificate:** Type `13` and press **[Enter]** (View CSR). The RSM-8R4 will prompt you to configure your communications (Telnet) program to receive the certificate. Set up your communications program to receive a binary file, and then press **[Enter]** to capture the file and save it. This is the Code Signing Request that you will send to the outside security service (e.g., VeriSign, Thawte, etc.) in order to have them sign and activate the certificate.

2. **Obtain the Signed Certificate:** Send the captured certificate to the outside security service. Refer to the security service's web page for further instructions.

3. **Upload the Signed Certificate to the RSM-8R4:** After the "signed" certificate is returned from the security service, return to the Web Access menu.

   a) Access the RSM-8R4 command mode via the Text Interface using an account that permits Administrator level commands as described previously, then type **`/N`** and press **[Enter]** to display the Network Parameters menu, and then type **`23`** and press **[Enter]** to display the Web Access menu.

   b) From the Web Access menu, type **`14`** and press **[Enter]** (Import CRT) to begin the upload process. At the CRT Server Key submenu, type **`1`** and press **[Enter]** to choose "Upload Server Key."

   c) Use your communications program to send the binary format Signed Certificate to the RSM-8R4 unit. When the upload is complete, press **[Escape]** to exit from the CRT Server Key submenu.

   d) After you exit from the CRT Server Key submenu, press [Escape] several times until you have exited from the Network Parameters menu and the "Saving Configuration" message is displayed.

4. After the configuration has been saved, test the signed certificate by accessing the RSM-8R4 via the Web Browser Interface, using an HTTPS connection. For example, if the common name has been defined as "service.wti.com", then you would enter "**`https://service.wti.com`**" in your web browser's address field. If the Signed Certificate has been properly created and uploaded, the warning message should no longer be displayed.

15. Saving and Restoring Configuration Parameters

Once the RSM-8R4 is properly configured, parameters can be downloaded and saved as an ASCII text file. Later, if the configuration is accidentally altered, the saved parameters can be uploaded to automatically reconfigure the unit without the need to manually assign each parameter.

Saved parameters can also be uploaded to other identical RSM-8R4 units, allowing rapid set-up when several identical units will be configured with the same parameters.

The "Save Parameters" procedure can be performed from any terminal emulation program (e.g. HyperTerminal™, TeraTerm©, etc.), that allows downloading of ASCII files.

> **Note:** *The Save and Restore features described in this section are only available via the Text Interface.*

15.1. Sending Parameters to a File

1. Start your terminal emulation program and access the Text Interface command mode using an account that permits Administrator level commands.
2. When the command prompt appears, type `/u` and press **[Enter]**. The RSM-8R4 will prompt you to configure your terminal emulation program to receive an ASCII download.
   a) Set your terminal emulation program to receive an ASCII download, and the specify a name for a file that will receive the saved parameters (e.g. RSM-8R4.PAR).
   b) Disable the Line Wrap function for your terminal emulation program. This will prevent command lines from being broken in two during transmission.
3. When the terminal emulation program is ready to receive the file, return to the RSM-8R4's Save Parameter File menu, and press **[Enter]** to proceed. RSM-8R4 parameters will be saved on your hard drive in the file specified in Step 2 above.
4. The RSM-8R4 will send a series of ASCII command lines which specify currently selected parameters. When the download is complete, press **[Enter]** to return to the command prompt.

15.2. Restoring Saved Parameters

This section describes the procedure for using your terminal emulation program to send saved parameters to the RSM-8R4.

1. Start your terminal emulation program and access the RSM-8R4's Text Interface command mode using an account that permits Administrator level commands.
2. Configure your terminal emulation program to upload an ASCII text file.
3. Upload the ASCII text file with the saved RSM-8R4 parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the ASCII text file to the RSM-8R4. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the RSM-8R4 detects an error in the file, it will respond with the "Invalid Parameter" message. If an error message is received, carefully check the contents of the parameters file, correct the problem, and then repeat the Upload procedure.*

5. If the parameter upload is successful, the RSM-8R4 will send a confirmation message, and then return to the command prompt. Type `/s` and press **[Enter]**, the Status Screen will be displayed. Check the Status Screen to make certain the unit has been configured with the saved parameters.

16. Upgrading RSM-8R4 Firmware

When new, improved versions of the RSM-8R4 firmware become available, the "Upgrade Firmware" function can be used to update the unit. Updates can be uploaded via FTP or SFTP protocols.

Notes:

- *The FTP/SFTP servers can only be started via the Text Interface.*
- *All other ports will remain active during the firmware upgrade procedure.*
- *If the upgrade includes new parameters or features not included in the previous firmware version, these new parameters will be set to their default values.*
- *The upgrade procedure will require approximately 15 minutes.*

1. Obtain the update file. Firmware modifications can either be mailed to the customer, or downloaded from WTI. Place the upgrade CDR in your disk drive or copy the file to your hard drive.

2. Access Text Interface command mode via Serial Port, Telnet or SSH client session, using a username/password and port that permit Administrator level commands.

3. When the command prompt appears, type `/UF` and then press **[Enter]**. The RSM-8R4 will display a screen which offers the following options:

   a) **Start FTP/SFTP Servers Only (Do NOT default parameters):** To proceed with the upgrade, while retaining user-defined parameters, type `1` and press **[Enter]**. All existing parameter settings will be restored when the upgrade is complete.

   b) **Start FTP/SFTP Servers & Default (Keep IP parameters & SSH Keys):** To proceed with the upgrade and default al user-defined parameters except for the IP Parameters and SSH Keys, type `2` and press **[Enter]**. When the upgrade is complete, all parameter settings except the IP Parameters and SSH Keys, will be reset to factory default values.

   c) **Start FTP/SFTP Servers & Default (Default ALL parameters):** To proceed with the upgrade, and reset parameters to default settings, type `3` and press **[Enter]**. When the upgrade is complete, all parameters will be set to default values.

   Note that after any of the above options is selected, the RSM-8R4 will start the receiving servers and wait for an FTP/SFTP client to make a connection and upload a valid firmware binary image.

4. To proceed with the upgrade, select either option 1 or option 2. The RSM-8R4 will display a message that indicates that the unit is waiting for data. Leave the current Telnet/SSH client session connected at this time.

5. Open your FTP/SFTP application and (if you have not already done so,) login to the RSM-8R4 unit, using a username and password that permit access to Administrator level commands.

6. Transfer the md5 format upgrade file to the RSM-8R4.

7. After the file transfer is complete, the RSM-8R4 will install the upgrade file and then reboot itself and break all port connections. Note that it will take approximately 10 minutes to complete the installation process. The unit will remain accessible until it reboots.

   a) Some FTP/SFTP applications may not automatically close when the file transfer is complete. If this is the case, you may close your FTP/SFTP client manually after it indicates that the file has been successfully transferred.

   b) When the upgrade process is complete, the RSM-8R4 will send a message to all currently connected network sessions, indicating that the RSM-8R4 is going down for a reboot.

   Note: *Do not power down the RSM-8R4 unit while it is in the process of installing the upgrade file. This can damage the unit's operating system.*

8. If you have accessed the RSM-8R4 via the Network Port, in order to start the FTP/SFTP servers, the RSM-8R4 will break the network connection when the system is reinitialized.

   - If you initially selected "Start FTP/SFTP Servers and Save Parameters", you may then reestablish a connection with the RSM-8R4 using your former IP address.
   - If you initially selected "Start FTP/SFTP Servers and Default Parameters", you must then login using the RSM-8R4's default IP address (Default = 192.168.168.168) or access command mode via Serial Port 1 or 2 or via Modem.

When firmware upgrades are available, WTI will provide the necessary files. At that time, an updated Users Guide or addendum will also be available.

17. Command Reference Guide

17.1. Command Conventions

Most commands described in this section conform to the following conventions:

- **Text Interface:** Commands discussed in this section, can only be invoked via the Text Interface. These commands *cannot* be invoked via the Web Browser Interface.
- **Slash Character:** Most RSM-8R4 Text Interface commands begin with the Slash Character (**/**).
- **Apply Command to All Ports:** When an asterisk is entered as the argument of the **/D** (Disconnect) or **/E** commands (Erase Buffer) the command will be applied to all ports. For example, to erase all port buffers, type **/E * [Enter]**.
- **Apply Command to All Plugs:** When an asterisk is entered as the argument of the **/ON** (Switch Plugs On), **/OFF** (Switch Plugs Off) or **/BOOT** (Reboot Plugs) commands, the command will be applied to all plugs. For example, to reboot all allowed plugs, type **/BOOT * [Enter]**.
- **Command Queues:** If a switching or reboot command is directed to a plug that is already being switched by a previous command, then the new command will be placed into a queue until the plug is ready to receive additional commands.
- **"Busy" Plugs:** If the "Status" column in the Plug Status Screen includes an asterisk, this means that the plug is currently busy, and is in the process of completing a previously issued command. If a new command is issued to a busy plug, then the new command will placed into a queue to be executed later.
- **Plug Name Wild Card:** It is not always necessary to enter the entire plug name. Plug names can be abbreviated in command lines by entering the first character(s) of the name followed by an asterisk (*****). For example, a plug named "SERVER" can be specified as "**S***". Note however, that this command would also be applied to any other plug name that begins with an "S".
- **Suppress Command Confirmation Prompt:** When the **/ON** (Switch Plug On), **/OFF** (Switch Plug Off), **/BOOT** (Reboot Plug) or **/DPL** (Default All Plugs) commands are invoked, the "**,Y**" option can be included to override the Command Confirmation ("Sure?") prompt. For example, to reboot Plug A4 without displaying the Sure prompt, type **/BOOT A4,Y [Enter]**.
- **Connected Ports:** When two ports are connected, most RSM commands will not be recognized by either of the connected ports. The only exception is the Resident Disconnect Sequence (Default = **^X** (**[Ctrl]** plus **[X]**).)
- **Enter Key:** Most commands are invoked by pressing **[Enter]**.
- **Configuration Menus:** To exit from a configuration menu, press **[Esc]**. The only exception to this rule is the Copy Parameters Menu (/CP), and in that case the **[Esc]** key is used to confirm the copy operation.

17.2. Command Summary

Function	Command Syntax	Command Access Level			
		Admin.	SuperUser	User	ViewOnly
Display					
Port and Plug Status	`/S` **[Enter]**	X❶	X❶	X❶	X❶
Port Diagnostics	`/SD` **[Enter]**	X❶	X❶	X❶	X❶
Port Parameters (Who)	`/W [n]` **[Enter]**	X❶	X❶		
Plug Group Status	`/SG` **[Enter]**	X❷	X❷	X❷	X❷
Network Status	`/SN` **[Enter]**	X	X	X	X
Help Menu	`/H` **[Enter]**	X❸	X❸	X❸	X❸
Log Functions	`/L` **[Enter]**	X	X		
Site ID / Unit Information	`/J[*]` **[Enter]**	X	X	X	X
Control					
Exit Command Mode	`/X` **[Enter]**	X	X	X	X
Connect - Local <Remote>	`/C <n> [n]` **[Enter]**	X	X	X	
Disconnect Ports	`/D <n|Nn|*>` **[Enter]**	X	X		
Read Buffer	`/R <n>` **[Enter]**	X	X	X	
Erase Buffer(s)	`/E <n|*>` **[Enter]**	X	X	X	
Boot Plug *n*	`/BOOT <n>[,Y]` **[Enter]**❹	X	X	X	
Turn Plug *n* On	`/ON <n>[,Y]` **[Enter]**❹	X	X	X	
Turn Plug *n* Off	`/OFF <n>[,Y]` **[Enter]**❹	X	X	X	
Default All Plugs	`/DPL[,Y]` **[Enter]**❹	X	X	X	
Send Parameter File	`/U` **[Enter]**	X			
Send SSH Keys	`/K <n>` **[Enter]**	X			
Unlock Invalid Access	`/UL` **[Enter]**	X			
Configuration					
System Parameters	`/F` **[Enter]**	X	❺		
Serial Port Parameters	`/P` **[Enter]**	X	❺		
Plug Parameters	`/PL <n>` **[Enter]**	X	❺		
Plug Group Parameters	`/G` **[Enter]**	X	❺		
Network Configuration	`/N` **[Enter]**	X	❺		
Reboot Options	`/RB` **[Enter]**	X	❺		
Alarm Configuration	`/AC` **[Enter]**	X	❺		
Reboot System	`/I` **[Enter]**	X	X		
Upgrade Firmware	`/UF` **[Enter]**	X			
Copy Port Parameters	`/CP <z>` **[Enter]**	X			
Test Network Configuration	`/TEST` **[Enter]**	X	X		

❶ In Administrator and SuperUser modes, all ports and plugs are displayed. In User and ViewOnly modes, the status screen will only include the ports and plugs allowed by the account.

❷ In Administrator mode, all Plug Groups are displayed. In SuperUser, User and ViewOnly modes, the Plug Group Status Screen will only include the Plug Groups allowed by the account.

❸ In Administrator Mode, Help Menus will list all commands. In SuperUser, User and ViewOnly modes, Help Menus will only list the commands allowed by the access level.

❹ The "`,Y`" argument can be included to suppress the command confirmation prompt.

❺ In SuperUser mode, configuration menus can be displayed, but parameters cannot be changed.

17.3. Command Set

This Section provides information on all Text Interface commands, sorted by functionality

17.3.1. Display Commands

/S Display Port and Plug Status Screen

Displays the Port and Plug Status Screen, which lists the current status of the RSM-8R4's eight serial ports and four switched outlets. For more information, please refer to Section 9.2.

> **Note:** *In Administrator Mode and SuperUser Mode, all RSM-8R4 outlets are displayed. In User Mode and ViewOnly Mode, the Plug Status Screen will only include the plugs allowed by your account.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/S`** **[Enter]**

/SD Display Port Diagnostics

Provides detailed information regarding the status of each port. When this command is issued by an account that does not permit Administrator level commands, the resulting screen will only display parameters for the ports allowed by the account. For more information, please refer to Section 8.5.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/SD`** **[Enter]**

Response: Displays Port Diagnostics Screen.

/W Display Port Parameters (Who)

Displays configuration information for an individual port, but does not allow parameters to be changed. Accounts that do not permit Administrator level commands can only display parameters for their resident port. For more information, please refer to Section 8.6.

Availability: Administrator, SuperUser

Format: **`/W [x]`** **[Enter]**

Where **`x`** is the port number or name. To display parameters for the Network Port, enter an "**`N`**". If the "**`x`**" argument is omitted, parameters for your resident port will be displayed.

Response: Displays port parameters.

Example: To display parameters for a port named "SERVER", access the Command Mode from a port and account that permits Administrator level commands, and type **`/W SERVER`** **[Enter]**.

/SG Display Plug Group Status Screen

Displays the Plug Group Status Screen, which lists the available Plug Groups, the numbers of the plugs included in each Plug Group, the current On/Off state, the user-defined Boot/Sequence Delay value, and the Default On/Off value for each plug. For more information, please refer to Section 8.3.

> **Note:** *In Administrator Mode all user defined Plug Groups are displayed. In SuperUser Mode, User Mode and ViewOnly Mode, the Plug Group Status Screen will only include the Plug Groups allowed by your account.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/S` **[Enter]**

/SN Display Network Status

Displays the Network Status Screen, which lists current network connections to the RSM-8R4's Network Port. For more information, please refer to Section 8.1.

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/SN` **[Enter]**

/H Help

Displays a Help Screen, which lists all available Text Interface commands along with a brief description of each command.

> **Note:** *In the Administrator Mode, the Help Screen will list the entire Text Interface command set. In SuperUser Mode, User Mode and ViewOnly Mode, the Help Screen will only list the commands that are allowed for that Access Level.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/H` **[Enter]**

/L Log Functions

Provides access to a menu which allows you to display the Audit Log, Alarm Log and Temperature Log. For more information on Log Functions, please refer to Section 5.3.4.

Availability: Administrator, SuperUser

Format: `/L` **[Enter]**

/J Display Site ID / Unit Information

Displays the user-defined Site I.D. message. If the optional asterisk (*) argument is included in the command line, the command will also show the model number and software version for the RSM-8R4 unit.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/J`** **[Enter]**

17.3.2. Control Commands

/X Exit Command Mode

Exits command mode. When issued at the Network Port, also ends the Telnet session.

> **Note:** *If the /X command is invoked from within a configuration menu, recently defined parameters may not be saved. In order to make certain that parameters are saved, always press the **[Esc]** key to exit from all configuration menus and then wait until "Saving Configuration" message has been displayed and the cursor has returned to the command prompt before issuing the /X command.*

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/x`** **[Enter]**

/C Connect

Establishes a bidirectional connection between two ports. For more information, see Section 9.3. There are two types of connections:

- **Resident Connect:** If the /C command specifies only one port, your resident port will be connected to the specified port.
- **Third Party Connect:** If the /C command specifies two ports, the unit will connect the two ports indicated. Third Party Connections can only be initiated by ports and accounts that permit Administrator level commands.

Notes:

- *If your account does not permit Administrator level commands, you will only be allowed to connect to ports specifically allowed by that account.*
- *If the account permits Administrator level commands, you are allowed to connect to any port.*
- *RS232 Ports are not allowed to create a Third Party connection to the Network Port. For example, Port 1 cannot connect Port 3 to the Network Port.*

Availability: Administrator, SuperUser, User

Format: **`/C <x> [x]`** **[Enter]**

Where **`x`** is the number or name of the port(s) to be connected.

Response:

Verbose: "Connected xx." When a Resident Connection is initiated, the RSM will also display the Resident Disconnect Sequence.

Terse: 1

/D Third Party Disconnect

Invoke the /D command at your resident port to disconnect two other ports.

Notes:

- *The /D command cannot disconnect your resident port*
- *SuperUsers and Users are limited to the ports that are specifically allowed by their accounts.*

Availability: Administrator, SuperUser

Format: **`/D[/Y] <x> [x]`** **[Enter]**

Where:

`/Y`	(Optional) suppresses the "Sure?" prompt.
`x`	Is the number or name of the port(s) to be disconnected. To disconnect all allowed ports, enter an asterisk. To disconnect a Telnet session, enter the "**`Nn`**" format Network Port Number.

Response:

Verbose: "Are you Sure (y/n)?", if Y, unit will respond with "Disconnected".

Terse: 5, if Y, unit will respond with 3.

Example: To disconnect Port 2 from Port 3 without the "Sure?" prompt, access the Command Mode from a third port with Administrator level command capability and type:

`/D/Y 2` **[Enter]** or **`/D/Y 3`** **[Enter]**

/R Read Buffer

Reads from Buffer Mode ports as described in Section 9.3.3.1.

Notes:

- *SuperUsers and Users are limited to the ports that are specifically allowed by their accounts*
- *When the /R command is invoked, the counter for the SNMP Traps function will also be reset.*

Availability: Administrator, SuperUser, User

Format: **`/R <n>`** **[Enter]**

Where **`n`** is the number or name of the port buffer to be read.

Response: The Read Buffer Menu is displayed.

/E Erase Buffer

Erases data from the buffer for a specified port(s).

Notes:

- *SuperUsers and Users are limited to the ports that are specifically allowed by their accounts*
- *Erased data cannot be recovered.*

Availability: Administrator, SuperUser, User

Format: **`/E[/Y] <x> [x]`** **[Enter]**

Where:

`x`	Is the number or name of the port buffer(s) to be cleared. To erase buffers for all ports, enter an asterisk.
`/Y`	(Optional) Suppresses the "SURE? (Y/N)" prompt.

Response:

Verbose: "Are You Sure (y/n)?", if Y, unit responds with "OK".
Terse: 5, if Y, the unit will respond with 0.

Example: To clear the buffer for Port 3, access the Command Mode using an account that provides access to Port 3, and then type **`/E 3`** **[Enter]**.

/BOOT Initiate Boot Cycle

Initiates a boot cycle at the selected plug(s) or Plug Group(s). When a Boot cycle is performed, the RSM-8R4 will first switch the selected plug(s) Off, then pause for the user-defined Boot/Sequence Delay Period, then switch the plug(s) back on. The /BOOT command can also be entered as /BO.

Note: *When this command is invoked in Administrator Mode, it can be applied to all RSM-8R4 plugs and Plug Groups. When this command is invoked in SuperUser Mode or User Mode, it can only be applied to the plugs and/or Plug Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **`/BOOT <n>[,Y]`** **[Enter]** or **`/BO <n>`** **[Enter]**

Where:

`n`	The number or name of the plug(s) or Plug Group(s) that you intend to boot. To apply the command to several plugs, enter a plus sign (+) between each plug number. To apply the command to a range of plugs, enter the numbers for the first and last plugs in the range, separated by a colon character (:). To apply the command to all plugs allowed by your account, enter an asterisk character (*).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Plug 2 and Plug 3. To initiate a boot cycle at Plugs 2 and 3, without displaying the optional command confirmation prompt, invoke either of the following command lines:

`/BOOT 2+3,Y` **[Enter]** or **`/BO 2+3,Y`** **[Enter]**

/ON Switch Plug(s) ON

Switches selected plugs(s) or Plug Group(s) On, as described in Section 9.2.2. When the /ON command is used to switch more than one plug, Boot/Sequence Delay Period will be applied as described in Section 5.7.

> **Note:** *When this command is invoked in Administrator Mode, it can be applied to all RSM-8R4 plugs and Plug Groups. When this command is invoked in SuperUser Mode or User Mode, it can only be applied to the plugs and/or Plug Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: `/ON <n>[,Y]` **[Enter]**

Where:

`n`	The number or name of the plug(s) or Plug Group(s) that you intend to Switch On. To apply the command to several plugs, enter a plus sign (+) between each plug number. To apply the command to a range of plugs, enter the numbers for the first and last plugs in the range, separated by a colon character (:). To apply the command to all plugs allowed by your account, enter an asterisk character (*).
`,Y`	(Optional) Suppresses the command confirmation prompt.

Example:

Assume that your account allows access to Plug 2 and Plug 3. To switch Plugs 2 and 3 On, without displaying the optional command confirmation prompt, invoke following command line:

`/ON 2+3,Y` **[Enter]**

/OFF Switch Plug(s) OFF

Switches selected plugs(s) or Plug Group(s) Off, as described in Section 9.2.2. When the /OFF command is used to switch more than one plug, Boot/Sequence Delay Period will be applied as described in Section 5.7. The /OFF command can also be entered as /OF.

> **Note:** *When this command is invoked in Administrator Mode, it can be applied to all RSM-8R4 plugs and Plug Groups. When invoked in SuperUser Mode or User Mode, the command can only be applied to the plugs and/or Plug Groups that are enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **`/OFF <n>[,Y]`** **[Enter]** or **`/OF <n>[,Y]`** **[Enter]**

Where:

`n` The number or name of the plug(s) or Plug Group(s) that you intend to Switch Off. To apply the command to several plugs, enter a plus sign (+) between each plug number. To apply the command to a range of plugs, enter the numbers for the first and last plugs in the range, separated by a colon character (:). To apply the command to all plugs allowed by your account, enter an asterisk character (*).

`,Y` (Optional) Suppresses the command confirmation prompt.

Examples:
Assume that your account allows access to Plug 2 and Plug 3. To switch Plugs 2 and 3 on your RSM-8R4 unit Off, without displaying the optional command confirmation prompt, invoke either of the following command lines:

`/OFF 2+3,Y` **[Enter]** or **`/OF 2+3,Y`** **[Enter]**

/DPL Set All Plugs to Default States

Sets all switched outlets to their user-defined default state. For information on setting outlet defaults, please refer to Section 5.7.

> **Note:** *When this command is invoked in Administrator Mode and SuperUser Mode, it will be applied to all RSM-8R4 outlets. When invoked in User Mode, the command will only be applied to the plugs that are allowed by your account.*

Availability: Administrator, SuperUser, User

Format: **`/DPL[,Y]`** **[Enter]**

Where ,Y is an optional command argument, which can be included to suppress the command confirmation prompt.

/U Send Parameters to File

Sends all RSM-8R4 configuration parameters to an ASCII text file as described in Section 14. This allows you to back up the configuration of your RSM-8R4 unit.

Availability: Administrator

Format: **`/U`** **[Enter]**

/K Send SSH Key

Instructs the RSM-8R4 to provide you with a public SSH key for validation purposes. This public key can then be provided to your SSH client, in order to prevent the SSH client from warning you that the user is not recognized when you attempt to create an SSH connection. For more information, please refer to Section 10.2.

Availability: Administrator

Format: **`/K k`** **[Enter]**

Where k is a required argument, which indicates the key type. The k argument provides the following options: 1 (SSH1), 2 (SSH2 RSA), 3 (SSH2 DSA.)

/UL Unlock Port (Invalid Access Lockout)

Manually cancels the RSM-8R4's Invalid Access Lockout feature. Normally, when a series of failed login attempts are detected, the Invalid Access Lockout feature can shut down the effected port for a user specified time period in order to prevent further access attempts. When the /UL command is invoked, the RSM-8R4 will immediately unlock all ports that are currently in the locked state.

Availability: Administrator

Format: **`/UL`** **[Enter]**

Response: The RSM-8R4 will unlock all RSM-8R4 ports, including the Network Port.

17.3.3. Configuration Commands

/F Set System Parameters

Displays a menu which is used to define the Site ID message, create user accounts, set the system clock, and configure and enable the Invalid Access Lockout feature. All functions provided by the /F command are also available via the Web Browser Interface. For more information, please refer to Section 5.3.

Availability: Administrator

Format: **`/F`** **[Enter]**

/P Set Serial Port Parameters

Displays a menu that is used to select options and parameters for the RSM-8R4's serial ports and internal modem port. All functions provided by the /P command are also available via the Web Browser Interface. Section 5.8 describes the procedure for defining serial port parameters.

Availability: Administrator

Format: **`/P <n>`** **[Enter]**

Where **`<n>`** is the number or name of the desired serial port.

/PL Set Plug Parameters

Displays a menu that is used to select options and parameters for the RSM-8R4's switched outlets (plugs). All functions provided by the /PL command are also available via the Web Browser Interface. Section 5.7 describes the procedure for defining plug parameters.

Availability: Administrator
Format: **`/PL` [Enter]**

/G Plug Group Parameters

Displays a menu that is used to View, Add, Modify or Delete Plug Groups. For more information on Plug Groups, please refer to Section 5.6.

Availability: Administrator
Format: **`/G` [Enter]**

/N Network Port Parameters

Displays a menu which is used to select parameters for the Network Port. Also allows access to the IP Security function, which can restrict network access by unauthorized IP addresses. All of the functions provided by the /N command are also available via the Web Browser Interface. For more information, please refer to Section 5.9.

Availability: Administrator
Format: **`/N` [Enter]**

/RB Reboot Options

Displays a menu that is used to configure Scheduled Reboots and Ping-No-Answer Reboots. Scheduled Reboots allow the the devices connected to RSM-8R4's switched outlets to be rebooted on a regular basis, according to a user defined schedule. Ping-No-Answer Reboots allow the RSM-8R4 to automatically reboot specific outlets when a user-specified IP address does not respond to a Ping command. For more information on Reboot options, please refer to Section 6.

> **Note:** *If desired, the Ping-No-Answer Reboot function can also be configured to send email notification whenever a Ping-No-Answer Reboot is generated. For more information, please refer to Section 7.2.*

Availability: Administrator
Format: **`/RB` [Enter]**

/AC Alarm Configuration Parameters

Displays a menu that is used to configure and enable the Over Temperature Alarms, Ping-No-Answer Alarm, and the Invalid Access Lockout Alarm. When properly configured, the Over Temperature Alarms offer the option of "Load Shedding", which allows the unit to automatically switch Off user-defined, non-essential outlets when temperature exceeds user-defined values. For more information on Alarm Configuration, please refer to Section 7.

Availability: Administrator
Format: **`/AC`** **[Enter]**

/I Reboot System (Default)

Reinitializes the RSM-8R4 unit and offers the option to keep user-defined parameters or reset to default parameters. When the /I command is invoked, the unit will offer four reboot options:

- Unit to Reboot
- Reboot Only (Do NOT default parameters)
- Reboot & Default (Keep IP Parameters & SSH Keys; Default all other parameters)
- Reboot & Default (Default ALL parameters)

Availability: Administrator
Format: **`/I`** **[Enter]**

/UF Upgrade Firmware

When new versions of the RSM-8R4 firmware become available, this command is used to update existing firmware as described in Section 16.

> **Note:** *When a firmware upgrade is performed, the RSM-8R4 will require 15 minutes for the upgrade procedure.*

Availability: Administrator
Format: **`/UF`** **[Enter]**

/CP Copy RS232 Port Parameters

Allows quick set-up when several serial ports will be configured with similar parameters. When the /CP command is invoked, the RSM-8R4 will display a menu that can be used to copy parameters to RS232 ports. For more information, please refer to Section 5.8.3.

> **Note:** *To proceed with the Copy function after selecting new parameters, press [Esc]; the RSM-8R4 will then display the confirmation prompt before proceeding.*

Availability: Administrator
Format: **`/CP`** **[Enter]**
Response: Displays Copy Parameters Menu.

/TEST Test Network Parameters

Displays a menu which is used to test configuration of the Syslog and SNMP Trap functions and can also be used to invoke a Ping Command. For more information, please refer to Section 11.2 and Section 12.2.

Notes:

- *In order for the ping command to function with domain names, Domain Name Server parameters must be defined as described in Section 5.9.5.*
- *The Test Menu's Ping command is not effected by the status of the Network Parameters Menu's Ping Access function.*

Availability: Administrator, SuperUser

Format: **`/TEST`** **[Enter]**

Appendix A. Interface Descriptions

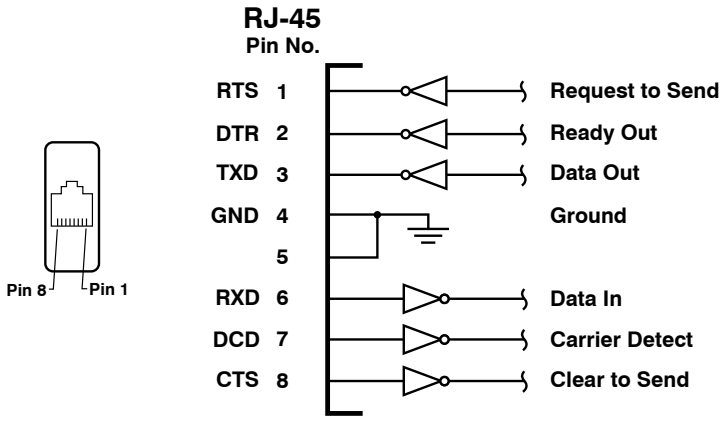

Figure A.1: Serial Port Interface

A.1. Serial Port (RS232)

DCD and DTR hardware lines function as follows:

1. **When connected:**

   a) If either port is set for Modem Mode, the DTR output at either port reflects the DCD input at the other end.

   b) If *neither* port is set for Modem Mode, DTR output is held high (active).

2. **When not connected:**

   a) If the port is set for Modem Mode, upon disconnect DTR output is pulsed for 0.5 seconds and then held high.

   b) If the port is *not* set for Modem Mode, DTR output is controlled by the DTR Output option (Serial Port Parameters Menu, Option 23). Upon disconnect, Option 23 allows DTR output to be held low, held high, or pulsed for 0.5 seconds and then held high.

A.2. DX9F-WTI-RJ Snap Adapter

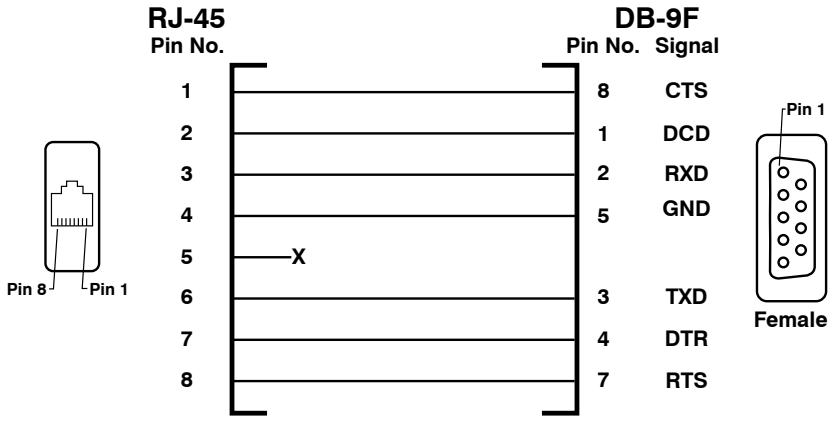

Figure A.2: DX9F-WTI-RJ Snap Adapter Interface

The DX9F-WTI-RJ Snap Adapter is used to connect the following devices to RSM-8R4 serial ports:

- Laptop, PC or other device that includes a DB9 DTE Interface: Use the DX9F-WTI-RJ snap adapter with a straight RJ45 cable.
- WTI RSM-8, RSM-16, RSM-32 or WTI MPC Series Console Port: Use the DX9F-WTI-RJ snap adapter with a straight RJ45 cable.

A.3. DX25M-DCE-RJ Snap Adapter

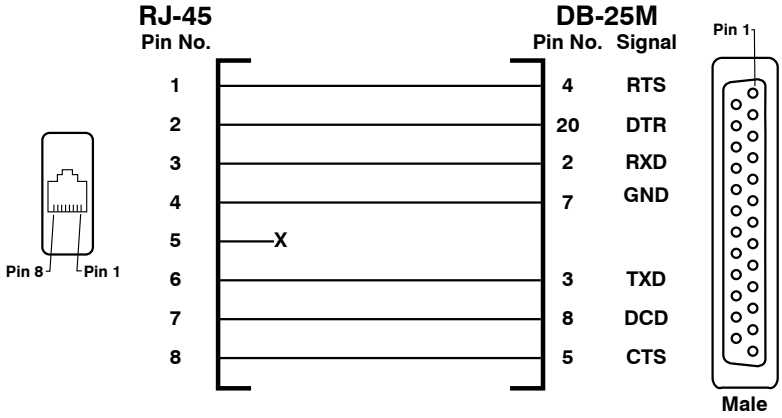

Figure A.3: DX25M-DCE-RJ Snap Adapter Interface

The DX25M-DCE-RJ Snap Adapter is used to connect the following devices to RSM-8R4 serial ports:

- External Modem or other device that includes a DB25 DCE Interface: Use the DX25M-DCE-RJ snap adapter with a straight RJ45 cable.

A.4. DX25M-DTE-RJ Snap Adapter Interface

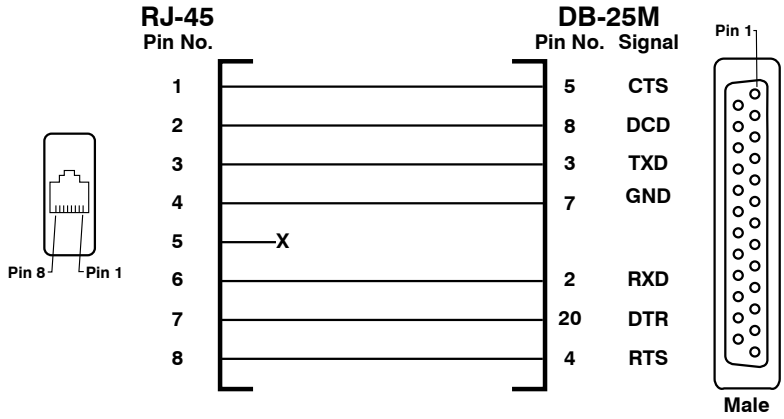

Figure A.4: DX25M-DTE-RJ Snap Adapter Interface

The DX25M-DTE-RJ Snap Adapter is used to connect the following devices to RSM-8R4 serial ports:

- Devices with DB25 DTE Interface: Use the DX25M-DTE-RJ snap adapter with a straight RJ45 cable.

A.5. DXF-NULL-RJ Snap Adapter

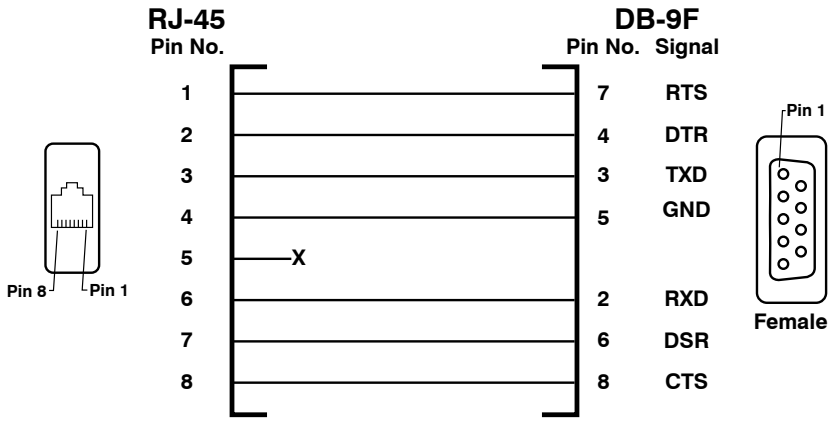

Figure A.5: DX9F-NULL_RJ Snap Adapter Interface

The DXF-NULL-RJ Snap Adapter is used for straight through cable connections (Pins 2 through 8).

Appendix B. Specifications

Power Input/Output:

Voltage: 100 - 120 VAC or 208 - 240 VAC, 50/60 Hz

AC Input Feed:

120 VAC Models: 20 Amps Max. Input Feed

240 VAC Models: 16 Amps Max. Input Feed

AC Inlets: Two (2) IEC320-C20

AC Outlets:

120 VAC Models: 4 each, NEMA 5-15R Outlets

240 VAC Models: 4 each, IEC320-C13 Outlets

RS232 Port Interface:

Connectors: Eight (8) RJ45 connectors (DTE pinout.)

Coding: 7/8 bits, Even, Odd, No Parity, 1, 2 Stop Bits.

Flow Control: XON/XOFF, RTS/CTS, Both, or None.

Data Rate: 300 to 115.2K bps (all standard rates).

Inactivity Timeout: No activity timeout disconnects port/modem sessions. Off, 5, 15, 30, 90 minutes.

Break: Send Break or Inhibit Break

Site ID: 32 Characters.

Port Name: 16 Characters per port.

Usernames & Passwords: 32 character usernames; 16 character passwords (case sensitive.) Up to 128 pairs, definable port, plug and system access.

Internal Modem: V.34

Physical/Environmental:

Dimensions:

Width: 19" (48.3 cm) (Including Rack Brackets)

Depth: 8.7" (16.5 cm)

Height: 1.75" (4.5 cm) One Rack U

Operating Temperature: 32˚F to 122˚F (0˚C to 50˚C)

Humidity: 10 - 90% RH

Agency Approvals: FCC, UL, CE (240 VAC Units)

Venting: Side vents are used to dissipate heat generated within the unit. When mounting the unit in an equipment rack, make certain to allow adequate clearance for venting.

Control Ports:

Ethernet Port: 100Base-T

Serial Console Ports: 8 each, RJ45, RS232C

Internal Modem Port (Phone Line): RJ11 connector for connection to your telco line

Appendix C. Customer Service

Customer Service hours are from 8:00 AM to 5:00 PM, PST, Monday through Friday. When calling, please be prepared to give the name and make of the unit, its serial number and a description of its symptoms. If the unit should need to be returned for factory repair it must be accompanied by a Return Authorization number from Customer Service.

WTI Customer Service
5 Sterling
Irvine, California 92618

Local Phone: (949) 586-9950
Toll Free Service Line: 1-888-280-7227
Service Fax: (949) 457-8138

Email: service@wti.com

Trademark and Copyright Information

WTI and Western Telematic are trademarks of Western Telematic Inc.. All other product names mentioned in this publication are trademarks or registered trademarks of their respective companies.

Information and descriptions contained herein are the property of Western Telematic Inc.. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Western Telematic Inc..

February, 2008
Part Number: 13851, Revision: B

Trademarks and Copyrights Used in this Manual

Hyperterminal is a registered trademark of the Microsoft Corporation. Portions copyright Hilgraeve, Inc.

ProComm is a trademark of Datastorm Technologies, Inc™.

Crosstalk is a trademark of Digital Communications Associates, Inc.

Teraterm is a copyright of Ayera Technologies, Inc.

BlackBerry is a registered trademark of Research In Motion Limited.

JavaScript is a trademark of Sun Microsystems, Inc.

Telnet is a trademark of Telnet Communications, Inc.

Thawte is a trademark of Thawte, Inc.

VeriSign is a registered trademark of VeriSign, Incorporated

All other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.

Index

T