WTI Part No. 14023
Rev. D

TSM Series

Serial Console Server

Models Covered:

TSM-8	TSM-24	TSM-40
TSM-8DC	TSM-24DC	TSM-40DC
TSM-8-NMI	TSM-24-NMI	TSM-40-NMI
TSM-8DC-NMI	TSM-24DC-NMI	TSM-40DC-NMI
	TSM-24-DPS	TSM-40-DPS

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

1. Check nameplate ratings to assure there is no overloading of supply circuits that could have an effect on overcurrent protection and supply wiring.
2. When installing 48 VDC rated equipment, it must be installed only per the following conditions:
   A. Connect the equipment to a 48 VDC supply source that is electrically isolated from the alternating current source. The 48 VDC source is to be connected to a 48 VDC SELV source.
   B. Input wiring to terminal block must be routed and secured in such a manner that it is protected from damage and stress. Do not route wiring past sharp edges or moving parts.
   C. A readily accessible disconnect device, with a 3 mm minimum contact gap, shall be incorporated in the fixed 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.

Two Power Supply Cables

Note that TSM-24-DPS and TSM-30-DPS units feature two separate power circuits, and a separate power supply cable for each power circuit. If your TSM unit includes two power supply cables, make certain to disconnect both power supply cables from their power source before attempting to service or remove the unit.

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

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

Appendices:

List of Figures

1. Introduction

TSM Series Serial Console Servers provide in-band and out-of-band access to RS-232 console ports and maintenance ports on UNIX servers, routers and any other network element that includes a serial console port. System administrators can access the TSM via TCP/IP network, using SSH or Telnet, or out-of-band via modem or local terminal. The TSM features two separate command interfaces; a convenient, user-friendly web browser interface, and a simple, command driven text interface.

Intelligent Port Selection

Each of the TSM's RS232 serial ports can be individually accessed by number or name via SSH or Telnet. The TSM also allows direct connections using TCP port assignments. Each TSM serial port can be separately configured using simple menu driven commands to set the port password, data rate, flow control and other operating parameters.

The full matrix capability of the TSM allows you to easily connect any two serial ports, even when the ports are using different communications settings. Ports can also be connected or disconnected by a third party with Administrator or SuperUser level command rights, and system managers can swap various RS232 devices between ports at a remote location.

Security and Collocation Features

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

The TSM 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 connection/disconnection commands, status displays and configuration menus. The SuperUser level allows control of serial ports, but does not allow access to configuration functions. The User level allows access to only a select group of Administrator-defined serial ports. The ViewOnly level allows you to check unit status, but does not allow control of serial ports or access to configuration menus.

The TSM 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.

Capture Buffer

"Buffer Mode" allows individual ports to capture and store incoming data, such as error and status messages received from attached console ports. This "snapshot" of the last data received is stored in memory, and can be viewed, saved, or erased by the system operator at any time. Console messages can be stored in the TSM port buffers, and sent to a remote location via SYSLOG, or an SNMP message can be generated to alert administrators when new console messages are received.

Configuration Backup

Once you have configured the TSM to fit your application, parameters and options can be saved to an ASCII text file on your PC. This allows you to quickly restore user-selected parameters if unit configuration is accidentally altered or deleted. Saved parameters can also be uploaded to other TSM units. This allows rapid set-up when several units will be configured with identical or similar parameters.

WTI Management Utility

The TSM includes the WTI Management Utility, which allows you to manage multiple WTI units via a single menu. For more information on the Management Utility, please refer to the User's Guide that is included on the CDROM.

TSM Series Units

This User's Guide discusses several different models from our TSM product line. Throughout this User's Guide, all of these units are referred to as the "TSM." Note however that these units differ as described below:

Model No.	Input Power	Serial Ports	Internal Modem
TSM-8	100 to 240 VAC	8 ea., RJ45	Yes
TSM-8DC	-48 VDC	8 ea., RJ45	Yes
TSM-8-NMI	100 to 240 VAC	8 ea., RJ45	No
TSM-8DC-NMI	-48 VDC	8 ea., RJ45	No
TSM-24	100 to 240 VAC	24 ea., RJ45	Yes
TSM-24DC	-48 VDC	24 ea., RJ45	Yes
TSM-24-NMI	100 to 240 VAC	24 ea., RJ45	No
TSM-24DC-NMI	-48 VDC	24 ea., RJ45	No
TSM-24-DPS	2 ea., 100 to 240 VAC	24 ea., RJ45	Yes
TSM-40	100 to 240 VAC	40 ea., RJ45	Yes
TSM-40DC	-48 VDC	40 ea., RJ45	Yes
TSM-40-NMI	100 to 240 VAC	40 ea., RJ45	No
TSM-40DC-NMI	-48 VDC	40 ea., RJ45	No
TSM-40-DPS	2 ea., 100 to 240 VAC	40 ea., RJ45	Yes

Aside from the differences listed above, all other features function identically in all TSM models.

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, **/E** or **/P 02**.
[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: **/W [n]**.

2. Unit Description

2.1. Front Panel

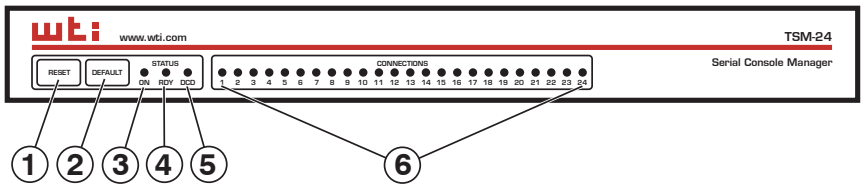

Figure 2.1: Instrument Front Panel (Model TSM-24 Shown)

① **RESET:** Can be used to restart the TSM operating system as described in Section 2.3.

② **DEFAULT:** Can be used to initialize the TSM to default parameters as described in Section 2.3.

③ **ON:** Lights when AC Power is applied.

④ **RDY:** (Ready) Flashes to indicate that the unit is operational.

⑤ **DCD:** (Data Carrier Detect) Lights when the DCD signal is present.

⑤ **CONNECTIONS LEDs:** A series of LEDs, which light to indicate data activity at the corresponding port.

- TSM-8, TSM-8DC, TSM-8-NMI and TSM-8DC-NMI units include 8 Activity LEDs
- TSM-24, TSM-24DC, TSM-24-NMI and TSM-24DC-NMI units include 24 Activity LEDs
- TSM-40, TSM-40DC, TSM-40-NMI and TSM-40DC-NMI units include 40 Activity LEDs.

2.2. Back Panel

As shown in Figures 2.2, 2.3 and 2.4, the TSM Back Panel includes the following components:

① **Power Inlet:** An IEC-320-C14 inlet, for connection to your 100 to 240 VAC power supply.

Notes:

- *48 VDC powered models include a terminal block assembly (see Figure 4.1) in place of the power inlet. For more information, please refer to Section 4.1.*
- *TSM-24-DPS and TSM-40-DPS units include two IEC-320-C14 power inlets.*

② **Power On/Off Switch** Master Power Switch.

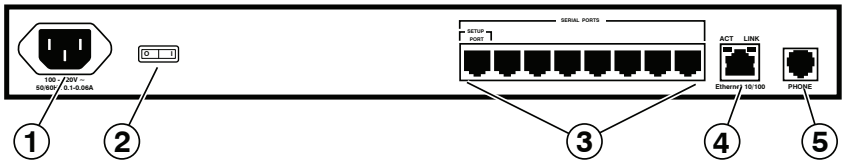

Figure 2.2: Instrument Back Panel (Model TSM-8 Shown)

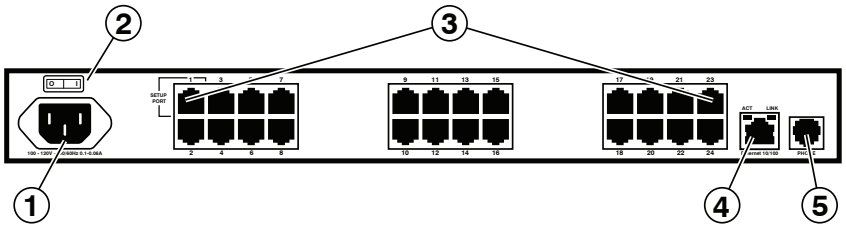

Figure 2.3: Instrument Back Panel (Model TSM-24 Shown)

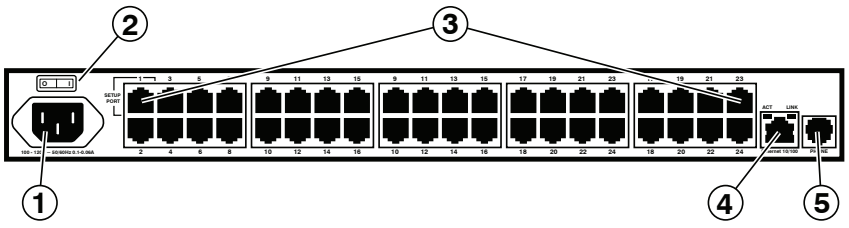

Figure 2.4: Instrument Back Panel (Model TSM-40 Shown)

③ **RS232 Serial Ports:** For connection to console ports on target devices. Standard RJ45 connectors configured as DTE ports. The RS232 ports are similar to a serial port on a PC. When connecting a modem, use a standard serial cable. When connecting a PC or other DTE device, please refer to Appendix C.

- TSM-8 series units include 8 Serial Ports.
- TSM-24 series units include 24 Serial Ports.
- TSM-40 series units include 40 Serial Ports.

④ **Network Port:** An RJ45 Ethernet port for connection to your 10/100Base-T, TCP/IP network. Note that the TSM 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 5.7.

⑤ **Phone Line Port (Internal Modem Port):** For connection to your phone line. Note that the Internal Modem Port is not present on TSM models that include the "NMI" model number suffix.

2.3. Front Panel Button Functions

The Reset and Default buttons can be used to perform several functions described below:

Notes:

- *Front Panel Button functions can also be disabled via the System Parameters menu, as described in Section 5.3.*
- *When the TSM is reset to factory defaults, all user-defined configuration parameters will be cleared, and the default "super" user account will also be restored.*
- *When the TSM is reinitialized, all ports will be disconnected.*
- *During the reboot procedure, All port activity LEDs will flash once.*

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

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

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

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

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

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

Note: *The RDY Indicator will continue to blink for about 45 seconds while parameters are being erased and keys are rebuilt. The RDY Indicator will then stop blinking during the reboot.*

3. Getting Started

This section describes a simplified installation procedure for all TSM models, which will allow you to communicate with the unit in order to demonstrate basic features and check for proper operation.

Note that this section does not provide a detailed description of unit configuration, or discuss advanced operating features in detail. In order to take full advantage of the features provided by this unit, it is recommended to complete the entire Installation and Configuration sections after completing this "Quick Start" procedure.

3.1. Quick Hardware Installation

3.1.1. Apply Power to the TSM

Refer to the safety precautions listed at the beginning of this manual and the power rating nameplate on the TSM unit, and then connect the unit to an appropriate power source. Refer to Section 4.1 and the table below for more information concerning power requirements and unit features. Note that TSM-24-DPS and TSM-40-DPS units include two power inlets for connection to two separate power supplies; a primary power supply and a fallback power supply.

Model No.	Input Power	Serial Ports	Internal Modem
TSM-8	100 to 240 VAC	8 ea., RJ45	Yes
TSM-8DC	-48 VDC	8 ea., RJ45	Yes
TSM-8-NMI	100 to 240 VAC	8 ea., RJ45	No
TSM-8DC-NMI	-48 VDC	8 ea., RJ45	No
TSM-24	100 to 240 VAC	24 ea., RJ45	Yes
TSM-24DC	-48 VDC	24 ea., RJ45	Yes
TSM-24-NMI	100 to 240 VAC	24 ea., RJ45	No
TSM-24DC-NMI	-48 VDC	24 ea., RJ45	No
TSM-24-DPS	2 ea., 100 to 240 VAC	24 ea., RJ45	Yes
TSM-40	100 to 240 VAC	40 ea., RJ45	Yes
TSM-40DC	-48 VDC	40 ea., RJ45	Yes
TSM-40-NMI	100 to 240 VAC	40 ea., RJ45	No
TSM-40DC-NMI	-48 VDC	40 ea., RJ45	No
TSM-40-DPS	2 ea., 100 to 240 VAC	40 ea., RJ45	Yes

When power is applied to the TSM, the ON LED should light, and the RDY LED should begin to flash. Note however, that the boot up procedure may take up to two minutes; this delay is due to the time required to generate SSH keys.

3.1.2. Connect your Control Device to the TSM

The TSM can either be controlled via local PC Serial Port, modem, or TCP/IP network. In order to connect ports or select parameters, commands are issued to the TSM via either the Network Port, Modem or RS232 Setup Port. Note that it is not necessary to connect to both the Network and Setup Ports, and that the Setup Port can be connected to either a local PC or an external modem.

- **Network Port:** Connect your 10Base-T or 100Base-T network interface to the TSM 10/100Base-T Network port.
- **Serial SetUp Port:** Use the supplied DX9F-DTE-RJ adapter and RJ45 Ethernet cable to connect your PC COM port to the TSM's SetUp Port (Serial Port 1).
- **Modem:** Connect your phone line to the TSM's Phone Line (Modem) port. Note that TSM model numbers that end in the "NMI" suffix do not include an internal modem.

3.2. Communicating with the TSM

When properly installed and configured, the TSM 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 Section 5.7.2.

Notes:

- *Default TSM 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 TSM 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 TSM from a node on the same subnet. When attempting to access the TSM from a node that is not on the same subnet, please refer to Section 5.7 for further configuration instructions.*

1. **Access Command Mode:** The TSM 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 TSM 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 port connections.

   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 TSM and invoke the connect command.

   c) **Via Web Browser:** Make certain that Web Browser access is enabled as described in Section 5.7.2. Start your JavaScript enabled Web Browser, enter the default TSM 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 Section 5.7.2. Start your Telnet client, and enter the TSM'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 TSM's Phone Line port. Note that TSM model numbers that end in the "NMI" suffix do not include an internal modem.

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 TSM will display either the Home Screen (Web Browser Interface) or the Port Status Screen (SSH, Telnet, or Modem.)

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

4. **Creating Connections Between Ports:** The TSM can perform two types of connections; Resident Connections and Third Party Connections. Note that Port Connection commands are only available via the Text Interface, and cannot be invoked by the Web Browser Interface.

   a) **Resident Connection:** Your local port (e.g. Port 1) issues a /C command to connect to a second port.

      i. To connect your local port to Serial Port 2, type **/C 2 [Enter]**. While the two ports are connected, the TSM will not recognize commands issued at your local 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 (e.g. Port 1) issues a /C command to create a connection between two other ports.

      i. To connect Port 2 to Port 3, type **/C 2 3 [Enter]**.

      ii. While Ports 2 and 3 are connected, the other serial ports and the Network Port will still recognize TSM commands. Type **/S [Enter]** to display the Port Status Screen. The "STATUS" column should now list Ports 2 and 3 as connected, and your local port as "Free".

      iii. Issue a Third Party Disconnect command to disconnect Ports 2 and 3; type **/D 2 [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 Port Status Screen. The Status screen should now list Ports 2 and 3 as "Free".

5. **Exit Command Mode:** When you finish communicating with the unit via the text interface, it is important to always log off using the appropriate TSM command, rather than by simply closing your Telnet program. When you log off using the proper command, this ensures that the unit has completely exited from command mode, and is not waiting for the inactivity timeout to elapse before allowing additional connections. To exit command mode, type **/x** and press **[Enter]**.

This completes the TSM Quick Start procedure. 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. If you have further questions regarding the TSM unit, please contact WTI Customer Support as described in Appendix D.

4. Hardware Installation

4.1. Connecting Power to the TSM Unit

The TSM is available in both AC and DC powered versions. Refer to the Power Rating Nameplate on your TSM unit to determine power requirements and then proceed as follows:

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.**

4.1.1. AC Powered Units

Plug the power cable (supplied with the unit) into the receptacle on the TSM back panel and then connect the power cable to an appropriate, grounded outlet. The TSM features a self adjusting power supply that automatically adapts to power supplies between 100 and 240 VAC. Set the TSM's master Power Switch in the ON position; the ON LED should light and the RDY LED should begin to flash.

> **Note:** *TSM-24-DPS and TSM-40-DPS units include two power inlets in order to allow connection to two separate power supplies; a primary power supply and a fallback power supply.*

4.1.2. DC Powered Units

When connecting a DC Powered TSM unit to your DC Power source, note that the DC terminal block is designed for connection to two separate power sources. First remove the protective cover from the terminal block, attach the wires from the -48 VDC power sources to the screw terminals, connect the ground line to the labeled ground screw, tighten the screw terminals, making certain that the wires are securely fastened, and then replace the protective cover.

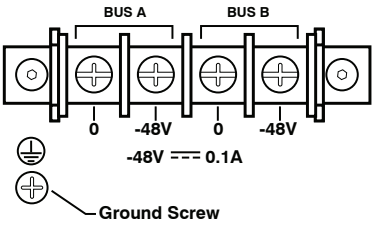

Figure 4.1: Terminal Block Assembly (DC Units Only)

4.2. Connecting the Network Cable

The Network Port is an RJ45, 10/100BaseT Ethernet Jack, for connection to a TCP/IP network. Note that the TSM features a default IP Address (192.168.168.168.) If you are communicating with the unit from a node on the same subnet, this allows you to contact the TSM without first accessing command mode to assign an IP address.

When installing the TSM in a working network environment, it is recommended to assign the IP Address, Gateway Address, and Subnet Mask as described in Section 5.7.

4.3. Connecting Devices to the TSM

1. Determine which TSM port will be used for connection to the new device (e.g. Port 3).
2. Refer to Appendix C and then use an appropriate cable and adapter to connect the RS232 serial port on the device to an RJ45 serial port on the TSM.
3. Access the TSM command mode and select communication parameters for each TSM port as described in Section 5.6.

5. Basic Configuration

This section describes the basic configuration procedure for all TSM units. For information on Invalid Access Alarm Configuration, generating SSH Keys and configuration via SNMP, please refer to Sections 6, 9 and 12.

5.1. Communicating with the TSM Unit

In order to configure the TSM, you must first connect to the unit, and access command mode. Note that the TSM offers two separate configuration interfaces; the Web Browser Interface and the Text Interface.

In addition, the TSM 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 enabled those options.

Once Telnet Access is enabled, you will then be able to use the Text Interface to communicate with the TSM via local PC, Telnet or SSH connection. If necessary, you can also use the Text Interface to access command mode via an external modem installed at an TSM Serial Port.

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

- **Access via Network:** The TSM 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 TSM's internal modem port (if present) and your PC must include a communications program.
- **Access via Local PC:** Your PC must be connected to an TSM Serial Port as described in Section 4.3, 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 SetUp Port, and by default, is configured for communication with a local control device.

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 5.7.2.*

1. Contact the TSM 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 TSM 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 5.7.

      i. **Via SSH Client:** Start your SSH client, and enter the TSM'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 TSM'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 phone line that you have connected to the TSM's internal modem.

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 TSM will display the Port 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 view unit status, by clicking on buttons or check boxes 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 TSM 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 TSM'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 TSM Home Screen will appear.

5.1.3. Access Via PDA

In addition to the Web Browser Interface and Text Interface, the TSM command mode can also be accessed by PDA devices. Note however, that only a limited selection of TSM status display functions are available to users who communicate with the unit via PDA.

When the TSM is operated via a PDA device, only the following functions are available:

- Product Status Screen (Section 7.1)
- Port Status Screen (Section 7.2)

These screens will allow PDA users to review unit status and display the Site I.D. and firmware version. Note however, that PDA users are not allowed to change or review TSM configuration parameters.

To configure the TSM for access via PDA, first consult your IT department for appropriate settings. Access the TSM command mode via the Text Interface or Web Browser interface as described in this section, then configure the TSM's Network Port accordingly, as described in Section 5.7.

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 TSM, 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 TSM 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 TSM 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 generally 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:** Use the links and fly-out menus on the left hand of the screen 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.*
- *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.*

5.3. Defining System Parameters

The System Parameters menus are used to define the Site ID Message, set the system clock and calendar, calibrate the temperature function, set up log functions and configure and enable other general TSM operating features.

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 via a separate submenu, that is accessed by clicking on the "Users" link on the left hand side of the menu.

To access the System Parameters menu via the Text Interface, type **`/F`** and press **[Enter]**. To access the System Parameters menu via the Web Browser Interface, place the cursor over the "General Parameters" link, wait for the flyout menu to appear, then click on the "System Parameters" link. The System Parameters Menus are used to define the following:

- **User Directory:** This function can be 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 ports each account will be allowed to control.

  Note: *In the Web Browser Interface, the "User Directory" option does not appear in the 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 TSM unit. (Default = undefined.)

  Note: *The Site ID will be cleared if the TSM is reset to default settings.*

- **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: *In the Web Browser Interface, the "Real Time Clock" option does not appear in the 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 TSM Serial Port or Network Port 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: *In the Web Browser Interface, the "Invalid Access Lockout" item does not appear in the System Parameters menu, and is instead, accessed via the "Invalid Access Lockout" link on the left hand side of the screen.*

- **Temperature Format:** Determines whether the temperature is displayed and read 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, which is accessed via the Temperature Calibration item. (Default = undefined.)

- **Log Configuration:** Configures the Audit Log, Alarm Log and Temperature Log. For more information on the TSM's event logging functions, please refer to Section 5.3.3. (Default = Audit Log = On without Syslog, Alarm Log = On without Syslog, Temperature Log = On.)

  Notes:

  - *The Audit Log will create a record of all port connection/disconnection and login/logout activity at the TSM unit.*
  - *The Alarm Log will create a record of each instance where the Invalid Access Alarm is triggered or cleared at the TSM unit.*
  - *The Temperature Log will create a record of ambient rack temperature over time.*

- **Callback Security:** Enables and configures the Callback Security Function as described in Section 5.3.4. 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 all front panel button functions. (Default = On.)

- **Modem Phone Number:** When a phone line is connected to the TSM's Internal Modem Port, this parameter can be used to denote the phone number for the modem. (Default = undefined.)

- **Management Utility:** Enables/Disables the Management Utility. When enabled, the Management Utility allows you to manage multiple WTI units via a single menu. For more information on the Management Utility, please refer to the Management Utility User's Guide on the CDROM included with the unit. (Default = Off.)

  Note: *Although the Management Utility can be enabled/disabled via either the Web Browser Interface and Text Interface, the Management Utility can only be accessed and operated via the Web Browser Interface.*

- **Scripting Options:** Provides access to parameters that are used to set up the TSM unit for running various scripts.

Notes:

- *To access Scripting Options parameters via the Text Interface, first type* **/F** *and press* **[Enter]** *to display the System Parameters Menu, then key in the number for the Scripting Options item and press [Enter].*
- *To access the Scripting Options parameters via the Web Browser Interface, place the cursor over the "General Parameters" link, wait for the flyout menu to appear, then click on the "Scripting Options" link.*

The Scripting Options menu allows the following parameters to be defined:

- **Command Prompt:** This item can be used to redefine the command prompt that will be displayed when the unit is accessed via the Text Interface. The command prompt can be set to either "TSM" or "RSM". (Default = TSM.)

5.3.1. The Real Time Clock and Calendar

The Real Time Clock menu is used to set the TSM's internal clock and calendar. 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 TSM's real-time clock/calendar.
- **Time:** Sets the Hour, Minute and Second for the TSM'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 TSM 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 TSM 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 TSM will also contact the NTP server and update the time whenever you change NTP parameters.*
- *To cause the TSM 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 TSM 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 5.7.5.*

- **Secondary NTP Address:** Defines the IP address or domain name (up to 64 characters long) for the secondary, fallback NTP Server. (Default = undefined.)
- **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 TSM will retry the connection four times. If neither the primary nor secondary NTP server responds, the TSM will wait 24 hours before attempting to contact the NTP server again. (Default = 3 Seconds.)
- **Test NTP Servers:** (Text Interface Only) Allows you to send a time request to the IP address or domain names defined via the Primary and Secondary NTP Address prompts, or to a new address or domain defined via the Test NTP Servers submenu. The TSM will not store the response from the IP address or domain, but will verify whether or not the target address or domain is an NTP Server.

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, Internal Modem 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 and Internal Modem Port. 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 TSM 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 TSM's Serial Ports and logical network ports.

Notes:

- *In the Web Browser Interface, the "Invalid Access Lockout" item does not appear in the System Parameters menu, and is instead, accessed via the "Invalid Access Lockout" link on the left hand side of the screen.*
- *When the Invalid Access Lockout Alarm has been enabled as described in Section 6, the TSM can also provide notification via email, Syslog Message, and/or SNMP trap whenever an Invalid Access Lockout occurs.*
- *Invalid Access Lockout parameters, will apply to the Serial Ports, Internal Modem Port 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 TSM's logical network ports is locked, all other network connections to the unit will also be locked.*
- *All invalid access attempts at the TSM 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 TSM 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.)*

To access the configuration menu for the Invalid Access Lockout feature, proceed as follows:

- **Text Interface:** Type **`/F`** and press **[Enter]**. The System Parameters menu will appear. At the System Parameters menu, type **`4`** and press **[Enter]** to display the Invalid Access Lockout configuration menu.
- **Web Browser Interface:** Place the cursor over the "General Parameters" link on the left hand side of the screen. When the fly-out menu appears, Click on the "Invalid Access Lockout" link to display the configuration menu for the Invalid Access Lockout feature.

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. Log Configuration

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

The TSM 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 and disconnection activity at the TSM unit. In addition, the Audit Log also includes login/logout records for all users. Each Log record includes a description of the activity that caused the event, 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 Invalid Access Alarm Activity at the TSM unit. Each time an Invalid Access Alarm is triggered or cleared, the TSM will generate a record that lists the time and date of the alarm, a description of the activity and the time and date that the Alarm was triggered or cleared.
- **Temperature Log:** The Temperature Log provides a record of temperature levels over time at the TSM unit. Each Log record will include the time and date, and the temperature reading.

5.3.3.1. Log Configuration Options

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

The Audit Log and Alarm Log both offer the following parameters:

- **Off:** The Log is disabled, and command activity and/or alarm events will not be logged.
- **On - With Syslog:** The Log is enabled, and port connection, port disconnection, login/logout activity and/or alarm events will be logged. The TSM will generate a Syslog Message every time a Log record is created.
- **On - Without Syslog:** The Log is enabled, and port connection, port disconnection, login/logout activity and/or alarm events will be logged, but the TSM will not generate a Syslog Message every time a Log record is created. (Default Setting.)

Notes:

- *In order for the Audit Log or Alarm Log to generate Syslog Messages, Syslog Parameters must first be defined as described in Section 10.*
- *The Audit Log will truncate usernames that are longer than 22 characters, and display two dots (..) in place of the remaining characters.*

5.3.3.2. Reading and Erasing Logs

To read the Audit Log, Alarm Log or Temperature Log, access the command mode using an account that permits Administrator or SuperUser level commands, and then proceed as follows:

- **Text Interface:** Type `/L` and press **[Enter]** to access the Display Log menu. Key in the number for the desired option and press **[Enter]**, and then follow the instructions in the resulting submenus.
- **Web Browser Interface:**
  - **Audit Log:** Move the cursor over the "Logs" link on the left hand side of the screen. When the fly-out menu appears, click on the "Audit Log (Display)" or the "Audit Log (Download)" link and then follow the instructions in the resulting submenu.
  - **Alarm Log:** Move the cursor over the "Logs" link on the left hand side of the screen. When the fly-out menu appears, click on the "Alarm Log (Display" or "Alarm Log (Download)" link and then follow the instructions in the resulting submenu.
  - **Temperature Log:** Move the cursor over the "Logs" link on the left hand side of the screen. When the fly-out menu appears, click on the "Temperature Log (Display)" or "Temperature Log (Download)" link and then follow the instructions in the resulting submenu.

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 and then proceed as follows:

- **Audit Log:** At the Display Logs menu, type `1` and then press **[Enter]**. When the Audit Log appears, type `E` and press **[Enter]** to erases the Audit Log.
- **Alarm Log:** At the Display Logs menu, type `2` and then press **[Enter]**. When the Alarm Log appears, type `E` and press **[Enter]** to erase the Alarm Log.
- **Temperature Log:** At the Display Logs menu, type `3` and press **[Enter]**. When the Temperature Log menu appears, type `E` and press **[Enter]** to erase the Temperature Log.

Notes:

- *The TSM 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.*
- *Note that once records have been erased, they cannot be recovered.*

5.3.4. 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 TSM 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 **`9`** and press **[Enter]** to display the Callback Security Menu.
- **Web Browser Interface:** Move the cursor over the General Parameters link on the left hand side of the screen. When the fly-out menu appears, click on the "Callback Security" link 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 TSM will attempt to contact the Callback number. (Default = 3 attempts.)
- **Callback Delay:** The amount of time that the TSM 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 and password. The username and password entered at login determine which Serial Port(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 TSM allows up to 128 user accounts; each account includes a username, password, security level, port 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 TSM allows you to set the command access level for each user account. The TSM offers four different access levels: Administrator, SuperUser, User and View Only. Command privileges for each user account can be set using 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 all TSM Serial Ports.
- **SuperUser:** SuperUsers are allowed to invoke all Serial Port connection 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 TSM Serial Ports.
- **User:** Users are allowed to invoke port connection commands and view all status screens, but can only apply commands to the Serial Ports 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 commands, and cannot view configuration menus or change configuration parameters. ViewOnly accounts can display the Port Status screen, but can only view the status of the Serial Ports that are specifically allowed by the account.

Section 16.2 summarizes command access for all four access levels.

In the default state, the TSM includes one predefined account that provides access to Administrator commands and allows control of all of the TSM's Serial Ports. 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 TSM 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 Serial 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 grant or deny access to each Serial Port by that account.

- **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.

5.5. 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 TSM 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 rights, 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 TSM 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 Serial Ports that the account is allowed to control and the command access level. The View User option will not display actual passwords, and instead, the password field will read "defined". Note that the View User function is only available when you 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 TSM 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 TSM 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."

5.5.2. Adding User Accounts

The "Add Username" option allows you to create new accounts and assign usernames, passwords, and Serial Port 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, access the command mode using an account that permits 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 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 TSM will display the Add User menu.

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

- **Username:** From one to 32 characters long. Duplicate usernames are not allowed. (Default = undefined.)
- **Password:** Five to 16 characters long. Note that passwords are case sensitive. (Default = undefined.)
- **Access Level:** Determines which commands this account will be allowed to invoke. 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 TSM Serial Ports this account will be allowed to access. (Defaults; Administrator & SuperUser = All Ports On, User & ViewOnly = All Ports Off.)

Notes:

- *In the Text Interface, Serial Port Access is configured by selecting item 4 and then choosing 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.*
- *When configuring a TSM unit that includes an internal modem, the Port Access parameter is also used to grant or deny user access to the internal modem port. On 8-port TSM units, port 9 is the internal modem port; on 24-port TSM units, port 25 is the internal modem port; on 40-port TSM units, port 41 is the internal modem port. Note that the internal modem is not included on model numbers that end with the "NMI" suffix.*

- **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 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 5.3.4. (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 TSM 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 access rights or Command Access Level. 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 TSM 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 TSM 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 described 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 TSM 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 TSM 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 TSM will delete the specified account without further prompting.
- **Web Browser Interface:** From the User Configuration menu, click the "View/Modify Users" link. The TSM 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 TSM 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 TSM 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. Serial Port Configuration

The Serial Port Configuration menus allow you to select parameters for the TSM's Serial Ports and Internal Modem Port.

The Serial Ports can be configured for connection to a local PC or external 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. 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 TSM via modem, modem parameters will not be changed until after you exit command mode and disconnect from the unit.
- On TSM-8 and TSM-8DC units, Port 9 is the Internal Modem Port.
- On TSM-24 and TSM-24DC units, Port 25 is the Internal Modem Port.
- On TSM-40 and TSM-40DC units, Port 41 is the Internal Modem Port.
- The Modem Port is not present on TSM models that end with the "NMI" suffix.

5.6.1. Serial Port Modes

The TSM 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 Serial Port 1.
- **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 Serial Port 1, the Network Port or the Internal Modem Port, and is the default mode at Serial Ports 2 and above.
- **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. Buffer Mode ports can be configured to support the Syslog and SNMP Trap features, discussed in Sections 10 and 11. In addition, the Buffer Threshold Alarm can also be enabled at Buffer Mode ports as described in Section 6.6. The Buffer Mode is not available at Serial 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.

For more information on Port Modes, please refer to Section 8.

5.6.2. The Serial Port Configuration Menu

To configure the TSM'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). The Serial Port Parameters menu will be displayed.
- **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.

The Serial Port Configuration menus allow 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 = 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.)

Notes:

- *When the Inactivity Timeout is disabled, this allows ports to automatically reconnect after a power interruption. When power is restored to the unit, pairs of ports that were previously connected will be automatically reconnected, providing that the Inactivity Timeout is disabled at both ports, and the two ports have been connected for at least ten minutes prior to the power interruption.*
- *The only exception to this rule is Serial Port 1, which will remain disconnected after power is restored in order to provide a free serial port for local access to command mode.*

- **Command Echo:** Enables or Disables command echo at the 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; DB9 Serial Ports = undefined; Internal Modem Port = MODEM.)
- **Port Mode:** The operation mode for this port. (Defaults: Serial Port 1 = Any-to-Any Mode; Serial Ports 2 and above = Passive Mode; Internal Modem Port = Modem Mode)

Notes:

- *The Port Mode for the Internal Modem Port cannot be changed, and will always be set to Modem Mode.*
- *Buffer Mode and Passive Mode are not available at Serial Port 1, which is reserved as a SetUp Port.*

Depending on the Port Mode selected, the TSM 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 TSM 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 TSM 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 TSM will add a time/date stamp whenever five seconds elapse between data items received. (Default = On.)
  - **Buffer Connect:** When enabled, the TSM will continue to Buffer captured data while you are connected to this Buffer Mode port. (Default = Off.)

- **Heartbeat:** The Heartbeat parameter can be used in conjunction with the Lost Communication alarm to provide notification when a WTI device that has been attached to one of the TSM's serial ports ceases to function. Normally, the TSM will send the Heartbeat message to an attached WTI device at regular intervals; if the attached device fails to respond to the Heartbeat message, the TSM can then notify you via email, Syslog Message or SNMP Trap as described in Section 6.2. Note that the Heartbeat feature is only available when the TSM serial port has been configured for "Any-to-Any" mode. (Default = Off.)

Notes:

- *The Heartbeat function will only work if the port is configured for Any-to-Any mode. In order to employ the Lost Communication Alarm, all target ports must be configured for Any-to-Any mode.*
- *In order for the Lost Communication Alarm to function, it may be necessary to update the firmware on your remote WTI equipment.*

Network Services:

- **Direct Connect:** Direct Connect allows users to access the TSM 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 9.3. 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.
  - **Break on Raw Disconnect:** The port will send a break character when a Raw Socket connection with the port is terminated. Note that this feature will work with both the "No Password" and "Password" options as described in Section 9.3.2. In the default state this feature is disabled; no break character is sent when a Raw Socket connection is terminated.

Note: *If "On - Password" is selected, and Administrator level commands are disabled at the Network Port, then only accounts that do not permit Administrator commands will be allowed to establish a direct connection via the Network Port. If Administrator level commands are disabled at any port, then that port will not allow access by accounts that permit Administrator 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 9.3.
- **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 at the Network Parameters menu. For more information, please refer to Section 10. 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 is reserved as a SetUp port and 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.)

- **Buffer Threshold:** Enables/disables the Buffer Threshold function for Buffer Mode ports and sets the level that will generate traps and/or Buffer Threshold Alarms 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 Buffer Threshold function is enabled, and traps will be sent to the SNMP Managers whenever the buffer for this port reaches the specified threshold level. For more information , please refer to Section 11. When a Buffer Threshold value is defined, this also allows the Buffer Threshold Alarm to be employed as described in Section 6.6. (Default = Off.)

  Note:

  - *The Buffer Threshold 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 SetUp Port, and cannot be configured as a Buffer Mode Port.*

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

If you are configuring the TSM via the Text Interface, the /CP (Copy Port Parameters) command can be used to select identical parameters for one or more TSM 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 TSM 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 TSM 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 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 TSM will return to the command prompt.
6. **Copy Parameters:** When you have finished selecting parameters, press **[Esc]** to copy the selected parameters.
7. The TSM will display a confirmation prompt before executing the copy command. Type **Y** to proceed or **N** to cancel the command, and then press **[Enter]**.

5.7. 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 will be displayed.
- **Web Browser Interface:** Click on the "Network Configuration" link on the left hand side of the screen. The TSM will display the Network Configuration menu, which allows you to access the various submenus used to configure the network port. Alternately, you can also access a specific Network Configuration submenu by placing the cursor over the "Network Configuration" link. When the fly-out menu appears, click on the link for the desired submenu.

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.*
- *The IP Address, Subnet Address and Gateway Address cannot be changed via the Web Browser Interface. In order to change these parameters, you must access the unit via the Text Interface.*
- *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 in this User's Guide, 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.

5.7.1. Network Port Parameters

In the Text Interface, these parameters are found in the main Network Configuration menu. 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:** This item is used to allow or deny Administrator level accounts to access the command mode at the Network Port. 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 the Network 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 timeout 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 TSM 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" parameter is only available via the Text Interface.*

5.7.2. Network Parameters

In the Text Interface, these parameters are accessed via the Network Configuration menu. 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.

Note: *The IP Address, Subnet Mask, Gateway Address and DHCP status cannot be changed via the Web Browser Interface. In order to change these parameters, you must access the TSM via the Text Interface.*

- **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 TSM will perform a DHCP request. Note that in the Text Interface, the MAC address for the TSM 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 TSM 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 option is defined via a submenu that 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 option is defined via a submenu that 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 Web Access. (Default = 80.)
- **HTTPS Access:** Enables/disables HTTPS communication. For instructions on setting up SSL encryption, please refer to Section 13. (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 5.7, then type* **23***, press* ***[Enter]*** *and use the resulting submenu (Figure 13.1) to select parameters as described in Section 13.*
- *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 13.*

- **Harden Web Security:** When the Harden Web Security feature is On (default,) only the high and medium cypher suites for SSLv3 and TLSv1 will be enabled. When the Harden Web Security feature is Off, all SSL protocols will be enabled, allowing compatibility with older browsers. Note that in the Text Interface, this function is enabled/disabled via the Web Access submenu. (Default = On.)
- **SYSLOG Address:** The IP Address or domain name (up to 64 characters) for the Syslog Daemon that will receive log records generated by the TSM. For more information, please refer to Section 10. (Default = undefined.)
- **Ping Access:** Enables/Disables response to the ping command. When Disabled, the TSM 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/or SSH connections via the TSM's Network Port. When enabled, users who are connected to the TSM command mode via one of the Serial Ports will be able to connect to the network port, and then invoke the /Telnet and/or /SSH commands to create an outbound connection. For example, to create an outbound Telnet connection, first make certain that this option is enabled for both the serial port and the password/account, then access command mode via the Text Interface at a free serial port. At the TSM> prompt, invoke the /Telnet or /SSH command as described in Section 9.4 or Section 9.5. (Default = Off.)
- **Raw Socket Access:** Enables/Disables Raw Socket Protocol access to the Network Port via Direct Connect. (Default = Off.)
- **Modem Hunt Telnet:** This option enables the TSM to support modem pooling in conjunction with third party Serial Port Redirector software as described in Section 5.7.2.1. (Default = Off.)
- **Modem Hunt Raw:** Same as Modem Hunt Telnet, except this function uses a raw socket connection. For more information, please refer to Section 5.7.2.1. (Default = Off.)

Note: *The "Modem Hunt Telnet" option is recommended for transmitting ASCII data and the "Modem Hunt Raw" option is recommended for transmitting binary data.*

5.7.2.1. Modem Pooling

The "Modem Hunt Telnet" and "Modem Hunt Raw" parameters allow the TSM to support modem pooling in conjunction with third party Serial Port Redirector software. This allows you to connect external modems to several TSM serial ports, and then use the TSM to automatically find a free modem when you need to create an outbound connection.

The Modem Hunt Telnet and Modem Hunt Raw options function as follows:

Modem Hunt Telnet: Offers three different configuration options: "Off" (Disabled), "On - No Password" and "On - Password." Each of the "On" options selects a default port number for modem pooling:

- On - No Password: Uses port number 2300.
- On - Password: Uses port number 2100. Note that when the password is enabled, you will be prompted to enter a valid TSM username and password.

Modem Hunt Raw: Offers three different configuration options: "Off" (Disabled), "On - No Password" and "On - Password." Each of the "On" options selects a default port number for modem pooling:

- On - No Password: Uses port number 3300.
- On - Password: Uses port number 3100. Note that when the password is enabled, you will be prompted to enter a valid TSM username and password.

In order to use TSM Modem Pooling functions, the TSM must be configured as follows:

- Telnet Access and/or Raw Socket Access must be enabled (Network Parameters Menu.)
- Modem Hunt Telnet and/or Modem Hunt Raw must be enabled (Network Parameters Menu.)
- The Port Mode (Port Parameters Menu) for each TSM serial port attached to an external modem must be set to "Modem Mode."
- Direct Connect must be enabled (Port Parameters Menu) for each TSM serial port attached to an external modem.

In addition, you must also acquire the following information from the TSM and enter it into your Serial Port Redirector software:

- The Port Number (shown above) for the desired TSM Modem Hunt Telnet or Modem Hunt Raw option.
- The IP address for the TSM unit.

To create an outbound modem connection, start your communications program (e.g., Hyperterminal, TeraTerm, etc.), select the virtual COM port that was defined via your Serial Port Redirector software and then place a call as you normally would.

5.7.3. IP Security

The IP Security feature allows the TSM to restrict unauthorized IP addresses and domain names from establishing inbound Telnet, web or SSH connections to the unit. This allows you to grant access to only a specific group of IP addresses, or block a particular IP address completely. In the default state, the TSM accepts incoming IP connections from all hosts.

In the Text Interface, IP Security parameters are defined via item 5 in the Network Configuration menu. 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 TSM will perform the following checks:

1. If the client's IP address or domain name is found in the "hosts.allow" list, the client will be granted immediate access. Once an IP address or domain name is found in the Allow list, the TSM will not check the Deny list, and will assume you wish to allow that address to connect.

2. If the client's IP address or domain name is not found in the Allow list, the TSM will then proceed to check the Deny list.

3. If the client's IP Address or domain name *is* found in the Deny list, the client *will not* be allowed to connect.

4. If the client's IP Address or domain name *is not* found in the Deny list, the client *will* be allowed to connect, even if the address or domain name was not found in the Allow list.

Notes:

- *If the TSM finds an IP Address or domain name 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 and domains 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.*

5.7.3.1. 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.*
- *In order to use domain names in the Allow List and/or Deny List, you must first define IP address(es) for the desired Domain Name Server(s) as described in Section 5.7.5.*

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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "IP Security" Link to display the IP Security Menu.

2. **Allow List:** Enter the IP Address(es) or domain name(s) for the clients that you wish to allow. Note that if an IP Address or domain name is found in the Allow list, the client will be allowed to connect, and the TSM 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) or domain name(s) for the clients that you wish to deny. Note that if the client's IP Address or domain name 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.

5.7.3.2. 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."

5.7.3.3. 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.*

5.7.4. Static Route

The Static Route menu allows you to type in Linux routing commands that will be automatically executed each time that the unit is powered up or reinitialized. 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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "Static Route" link to display the Static Route Menu.

5.7.5. 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.companyname111.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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "DNS Server" link to display the Domain Name Server menu.

5.7.6. 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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "SNMP Parameters" link to display the SNMP Access Parameters Menu.

  Note: *After you have configured SNMP Access Parameters, you will then be able to manage the TSM's User Directory, perform basic configuration functions and display unit status via SNMP, as described in Section 12.*

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 TSM; it does not effect the ability of the TSM to send SNMP traps.*

- **Version:** This parameter determines which SNMP Version the TSM will respond to. For example, if this item is set to V3, then clients who attempt to contact the TSM 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. When Enabled ("Yes"), you will not be able to change configuration parameters when you contact the TSM via SNMP. (Default = No.)

  Note: *In order to define user names for the TSM 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 TSM supports DES encryption, but does not currently support the AES protocol.*
  - *The TSM 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 TSM supports both MD5 and SHA1 authentication. (Default = MD5.)

Notes:

- *The Authentication Protocol that is selected for the TSM must match the protocol that your SNMP client will use when querying the TSM 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.)
- **Read Only Community:** Note that this parameter is not available when the SNMP Version is set to V3. (Default = Public.)
- **Read/Write Community:** Note that this parameter is not available when the SNMP Version is set to V3. (Default = Public.)

5.7.7. 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 11. 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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "SNMP Traps" link to display the SNMP Trap Parameters 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 11. (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.)

5.7.8. LDAP Parameters

The TSM supports LDAP (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 TSM unit, and existing users can also be removed without the need to delete the account from each TSM unit.

This type of authentication also allows administrators to assign users to LDAP groups, and then specify which ports the members of each group will be allowed to control at each TSM 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 TSM 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 TSM 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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "LDAP Parameters" link to display the LDAP Parameters Menu.

Notes:

- *Port access rights are not defined at the LDAP server. They are defined via the LDAP Group configuration menu on each TSM unit and are specific to that TSM unit alone.*
- *When LDAP is enabled and properly configured, LDAP authentication will supersede any passwords and access rights that have been defined via the TSM user directory.*
- *If no LDAP groups are defined on a given TSM 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 you to define the following parameters:

- **Enable:** Enables/disables LDAP authentication. (Default = Off.)
- **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.)
- **LDAP Port:** Defines the port that will be used to communicate with the LDAP server. (Default = 389.)

- **TLS/SSL:** Enables/Disables TLS/SSL encryption. Note that when TLS/SSL encryption is enabled, the LDAP Port should be set to 636. (Default = Off.)
- **Bind Type:** Sets the LDAP bind request password type. Note that in the Text Interface, when the Bind Type is set to "Kerberos," the LDAP menu will include an additional prompt (item 14) that is used to select Kerberos parameters as described in Section 5.7.8.5. In the Web Interface, the button which is used to access the LDAP Kerberos Parameters menu is located at the bottom of the LDAP Parameters Menu. (Default = Simple.)
- **Search Bind DN:** Selects the user name which 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 TSM 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.)
- **Kerberos Setup:** Kerberos is a network authentication protocol, which provides a secure means of identity verification for users who are communicating via a non-secure network. In the Text Interface, Kerberos parameters are selected via a submenu that is only available when Kerberos is selected as Bind Type. In the Web Browser Interface, Kerberos parameters are defined via the main LDAP Parameters menu. The following parameters are available:
  - **Port:** (Default = 88.)
  - **Realm:** (Default = Undefined.)
  - **Key Distribution Centers (KDC1 through KDC5):** (Default = Undefined.)
  - **Domain Realms 1 through 5:** (Default = Undefined.)
- **LDAP Group Setup:** Provides access to a submenu, which is used to define LDAP Groups as described in the Sections 5.7.8.1 through 5.7.8.4.

5.7.8.1. 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 TSM unit.

To add LDAP groups to your TSM 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 Setup menu. At the LDAP Group Setup menu, type `2` (Add LDAP Group) and press **[Enter]** to display the Add LDAP Group menu.
- **Web Browser Interface:** Access the LDAP Parameters Menu as described in Section 5.7.8. At the LDAP Parameters Menu, click on the LDAP Group Setup button to display the LDAP Group Setup 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:

- **Group Name:** 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.)

  Note: *When configuring a TSM unit that includes an internal modem, the Port Access parameter is also used to grant or deny user access to the internal modem port. On 8-port TSM units, port 9 is the internal modem port; on 24-port TSM units, port 25 is the internal modem port; on 40-port TSM units, port 41 is the internal modem port. The internal modem is not included on TSM model numbers that end with the "NMI" suffix.*

- **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, Web or any combination thereof, and also enables/disables Outbound Telnet. (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 TSM displays the "Saving Configuration" message.*

5.7.8.2 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 port access settings. To view an existing LDAP group on your TSM 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 Setup menu. From the LDAP Group Setup menu, type `1` and press **[Enter].** The TSM will prompt you to select the desired group; key in the name of the group and press **[Enter]**, the TSM will display the View LDAP Group screen.
- **Web Browser Interface:** Access the LDAP Parameters Menu as described in Section 5.7.8. At the LDAP Parameters Menu, click on the LDAP Group Setup button to display the LDAP Group Setup 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.

5.7.8.3. Modifying LDAP Groups

If you want to modify an existing LDAP Group in order to change parameters or port access rights, the "Modify LDAP Group" function can be used to reconfigure group parameters. To Modify an existing LDAP Group, access the TSM 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 Setup menu. From the LDAP Group Setup menu, type `3` and press **[Enter].** The TSM will prompt you to select the desired group; key in the name of the group and press **[Enter]**, the TSM will display the Modify LDAP Group screen.
- **Web Browser Interface:** Access the LDAP Parameters Menu as described in Section 5.7.8. At the LDAP Parameters Menu, click on the LDAP Group Setup button to display the LDAP Group Setup 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 5.7.8.1.

> **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 TSM displays the "Saving Configuration" message and the cursor returns to the command prompt.*

5.7.8.4. 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 Setup menu. From the LDAP Group Setup menu, type **4** and press **[Enter].** The TSM will prompt you to select the desired group; key in the name of the group and press **[Enter]**, the TSM will delete the specified LDAP Group immediately, without further prompting.
- **Web Browser Interface:** Access the LDAP Parameters Menu as described in Section 5.7.8. At the LDAP Parameters Menu, click on the LDAP Group Setup button to display the LDAP Group Setup 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.

5.7.9. TACACS Parameters

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 TSM 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 TSM will fallback to its own password/username directory when an authentication attempt fails. When enabled, the TSM will first attempt to authenticate the password by checking the TACACS Server; if this fails, the TSM will then attempt to authenticate the password by checking its own internal username directory. (Default = Off.)
  - **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 TACACS Server, or when a password or username does not match the TACACS 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 TACACS Server.
- **Authentication Port:** The port number for the TACACS function. (Default = 49.)
- **Default User Access:** When enabled, this parameter allows TACACS users to access the TSM command mode without first defining a TACACS user account on the TSM. When new TACACS users access the TSM command mode, they will inherit the default Access Level, Port Access and Service Access that are defined via the items listed below: (Default = On.)
  - **Access Level:** Determines the default Access Level setting for new TACACS users. This option can set the default access level for new TACACS users 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 the default Port Access setting for new TACACS users. The Port Access setting determines which serial ports each account will be allowed to control. (Defaults; Administrator and SuperUser = All Ports On, User = All Ports Disabled.)

Notes:

- *Administrator and SuperUser level accounts always have access to all ports.*
- *User level accounts will only have access to the ports that are defined via the "Port Access" parameter.*
- *ViewOnly level accounts cannot be granted access to the Serial Ports.*

➤ **Service Access:** Selects the default Service Access setting for new TACACS users. The Service Access setting determines whether each account will be able to access command mode via Serial Port, Telnet/SSH or Web. For example, if Telnet/SSH Access is disabled for an account, then the account will not be able to access command mode via Telnet or SSH. (Default = Serial Port = On, Telnet/SSH = On, Web = On.)

5.7.10. 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:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "RADIUS Parameters" link 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 long) 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 TSM will continue to try to contact the RADIUS Server during each connection attempt before executing a retry. (Default = 3 Seconds.)
- **Fallback Local:** Determines whether or not the TSM will fallback to its own password/username directory when an authentication attempt fails. When enabled, the TSM will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the TSM 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.
- **Retries:** Determines how many times the TSM will attempt to contact the RADIUS server. Note that the retries parameter applies to both the Primary RADIUS Server and the Secondary RADIUS Server. (Default = 3.)

- **Authentication Port:** The Authentication Port number for the RADIUS function. (Default = 1812.)
- **Accounting Port:** The Accounting Port number for the RADIUS function. (Default = 1813.)
- **Debug:** (Text Interface Only) When enabled, the TSM will put RADIUS debug information into Syslog. (Default = Off.)

5.7.10.1. Dictionary Support for RADIUS

The RADIUS dictionary file can allow you to define a user and assign command access rights and port access rights from a central location.

The RADIUS dictionary file, "dictionary.wti" is included on the CDROM along with this user's guide. To install the dictionary file on your RADIUS server, please refer to the documentation provided with your server; some servers will require the dictionary file to reside in a specific directory location, others will require the dictionary file to be appended to an existing RADIUS dictionary file.

The WTI RADIUS dictionary file provides the following commands:

- **`WTI-Super`** - Sets the command access level for the user. This command provides the following arguments:
  - `0` = ViewOnly
  - `1` = User
  - `2` = SuperUser
  - `3` = Administrator

  For example, in order to set command access level to "SuperUser", the command line would be:

  ```
  WTI-Super="2"
  ```

- **`WTI-Port-Access`** - Determines which port(s) the user will be allowed to access. This command provides an argument that consists of an 8, 16 or 32 character string, with one character for each TSM Serial Port. The following options are available for each port:
  - `0` = Off (Deny Access)
  - `1` = On (Allow Access)

  For example, to allow access to Serial Ports 1, 2, 3, 5 and 8 on an TSM-8 unit, the command line would be:

  ```
  WTI-Port-Access="11101001"
  ```

Example:
The following command could be used to set the command access level to "User" and allow access to Serial Ports 1, 3, 5 and 7:

```
tom  Auth-Type:=Local, User-Password=="tom1"
   Login-Service=Telnet,
   Login-TCP-Port=Telnet,
   User-Name="HARRY-tom",
   WTI-Super="1",
   WTI-Port-Access="10101010",
```

5.7.11. Email Parameters

The Email Parameters menu is used to define parameters for the email messages that the TSM can send to notify you when an alarm is triggered. To define email message parameters, access the TSM 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 Messaging Menu.
- **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "Email Messaging" link to display the Email Configuration Menu.

The Email Configuration menu offers the following options:

- **Enable:** Enables/Disables the Email Messaging feature. When disabled, the TSM 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 = undefined.)
- **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 5.7.5.*
- **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 TSM 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 TSM. (Default = undefined.)
- **From Address:** The email address that will appear in the "From" field in email sent by the TSM. (Default = undefined.)
- **To Address:** The address(es) that will receive email messages generated by the TSM. Note that up to three "To" addresses may be defined, and that when Alarm Configuration parameters are selected as described in Section 6, 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.*

5.8. Save User Selected Parameters

It is strongly recommended to save all user-defined parameters to an ASCII file as described in Section 14. 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 TSM 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 TSM 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 TSM will revert to the previously saved configuration after you exit from command mode.

5.8.1. Restore Configuration

If you make a mistake while configuring the TSM unit, and wish to return to the previously saved parameters, the Text Interface's "Reboot System" command (`/I`) offers the option to reinitialize the TSM unit using previously backed up parameters. This allows you to reset the unit to previously saved parameters, even after you have changed parameters and saved them.

Notes:

- *The TSM will automatically backup saved parameters once a day, shortly after Midnight. This configuration backup file will contain only the most recently saved TSM parameters, and will be overwritten by the next night's daily backup.*
- *When the /I command is invoked, a submenu will be displayed which offers several Reboot options. Option 4 is used to restore the configuration backup file. The date shown next to Option 4 indicates the date that you last changed and saved unit parameters.*
- *If the daily automatic configuration backup has been triggered since the configuration error was made, and the previously saved configuration has been overwritten by newer, incorrect parameters, then this function will not be able to restore the previously saved (correct) parameters.*

To restore the previously saved configuration, proceed as follows:

1. Access command move via the Text Interface, using a username/password that permits access to Administrator level commands (see Section 5.1.1.)
2. At the TSM command prompt, type `/I` and press **[Enter]**. The TSM will display a submenu that offers several different reboot options.
3. At the submenu, you may choose Item 4 (Reboot & Restore Last Known Working Configuration). Type **4**, and then press **[Enter]**.
4. The TSM will reboot and previously saved parameters will be restored.

6. Alarm Configuration

When properly configured, the TSM can meter temperature readings, and log this information for future review. In addition, the TSM can also generate alarms when temperature readings exceed user-defined trigger levels, when input voltage is lost and then restored to the unit, when communication with an attached WTI device is disrupted, when a Ping No Answer condition is detected, when the Invalid Access Lockout feature is triggered and when excessive data accumulates at a serial port buffer.

When any of these conditions are detected, the TSM can send an "Alarm" to the proper personnel via Email, Syslog Message or SNMP trap. This section describes the procedure for setting up the TSM to send alarm messages when any of these critical situations are detected. For instructions regarding configuration of the Log function, please refer to Section 5.3.3.

Notes:

- *In order to send alarm notification via email, email addresses and parameters must first be defined as described in Section 5.7.11. 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 5.7.2. 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 5.7.7. 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."*
- *When defining parameters via the Text Interface, make certain to press the **[Esc]** key 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 TSM'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]** to display the Alarm Configuration Menu.
- **Web Browser Interface:** Click the "Alarm Configuration" link, located on the left hand side of the screen to display the Alarm Configuration Menu

6.1. 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.

Notes:

- *In order for the TSM to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.7.11.*
- *In order for the TSM to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.7.2.*
- *In order for the TSM to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.7.7.*

To configure the Over Temperature Alarms, access the TSM 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) Alarm, or type `2` and press **[Enter]** to access the Over Temperature (Critical) 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) alarm and the Over Temperature (Critical) 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 Over Temperature Alarm will be triggered, and the TSM will send notification (if enabled.) (Initial: Default = 90°F or 32°C, Critical: Default = 100°F or 38°C.)

  Note: *The Alarm Set Threshold value must be greater than the Alarm Clear Threshold value. The TSM will not allow you to define an Alarm Clear Threshold value that is higher than the Alarm Set Threshold.*

- **Alarm Clear Threshold:** Determines how low the temperature must drop in order for the Alarm condition to be cancelled. (Initial: Default = 80°F or 27°C, Critical: Default = 90°F or 38°C.)

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

- **Resend Delay:** Determines how long the TSM 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 TSM will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the TSM will send a first 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 5.7.11,) 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)".)

6.2. The Lost Communication Alarm

The Lost Communication Alarm is intended to provide prompt notification when communication with an attached WTI device is disrupted. When communication is interrupted, the TSM can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for the TSM to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.7.11.*
- *In order for the TSM to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.7.2.*
- *In order for the TSM to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.7.7.*
- *In order for the Lost Communication Alarm to function, the Heartbeat parameter must be enabled at each serial port that you wish to monitor. For example, in order to monitor a WTI device that is connected to Serial Port 3, the Heartbeat function must be enabled at Serial Port 3.*

To configure the Lost Communication Alarm, access the TSM command mode using a password that permits Administrator Level commands. Enable the Heartbeat function and select the "Any-to-Any" port mode at the desired Serial Port as described in Section 5.6.2, and then proceed as follows:

Notes:

- *The Lost Communication Alarm will not function if target Serial Ports are not configured for Any-to-Any Mode, or if the Heartbeat function is not enabled at those ports.*
- *In order for the Lost Communication Alarm to function, it may be necessary to update the firmware on your remote WTI equipment.*

- **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 Lost Communication 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 Lost Communication link to access the configuration menu.

The Lost Communication 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 Off and then back On again.*

- **Resend Delay:** Determines how long the TSM 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 TSM will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the TSM will send initial notification when it detects lost communication with the a WTI device connected to one of the TSM Serial Ports, and then send a second notification when it determines that communication has been restored. (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 5.7.11) 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: Lost Comm with Unit")

6.3. The Ping No Answer Alarm

When properly configured, the Ping No Answer Alarm can provide notification when a device at a user-specified IP address fails to respond to a ping command. When one of the user-defined IP addresses fails to answer a Ping command, the TSM can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for this alarm to function, at least one target IP Address for the Ping No Answer Alarm must be defined as described in Section 6.3.1.*
- *When a Ping No Answer condition is detected, the TSM can send an email, Syslog Message and/or SNMP trap if properly configured as described in this Section.*
- *In order for the TSM to provide Email alarm notification, communication parameters must first be defined as described in Section 5.7.11.*
- *In order for the TSM to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.7.2.*
- *In order for the TSM 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 5.7.7.*

6.3.1. Defining Ping No Answer IP Addresses

In order for the Ping No Answer Alarm to function, you must first define at least one target IP address. To define target IP addresses for the Ping No Answer Alarm, access the TSM command mode using an account that permits Administrator Level commands and then proceed as follows:

- **Text Interface:** At the TSM command prompt, type **/PNA** and then press **[Enter]** to display the Ping No Answer menu. From the Ping No Answer menu, you may either add IP addresses, edit IP addresses, display previously defined IP addresses or delete IP addresses. Type **2** and press **[Enter]** to add a target IP address for the Ping No Answer Alarm.
- **Web Browser Interface:** Click the "Ping No Answer Configuration" link, located on the left hand side of the screen to display the Ping No Answer Configuration Menu. The Ping No Answer Configuration menu is used to add IP addresses, edit IP addresses, display currently defined IP addresses or delete IP addresses. Click on the "Add Ping No Answer" link to define a target IP address(es) for the Ping No Answer Alarm.

Up to 54 Ping No Answer IP Addresses can be defined. The Add Ping No Answer menu is used to define the following parameters for each new Ping No Answer IP Address:

- **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 Ping No Answer Alarm can provide user notification. (Default = undefined.)

  Note: *In order to use Domain Names, you must first define DNS parameters as described in Section 5.7.5.*

- **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 3,600 seconds. (Default = 60 Seconds.)

  Note: *If the Ping Interval is set lower than 20 seconds, it is recommended to define the "IP Address or Domain Name" parameter using an IP Address rather than a Domain Name. This ensures more reliable results in the event that the Domain Name Server is unavailable.*

- **Interval After Failed Ping:** Determines how often the Ping command will be sent after a previous Ping command receives no response. (Default = 10 Seconds.)
- **Ping Delay After PNA Action:** Determines how long the TSM will wait to send additional ping commands, after the Ping No Answer Alarm has been triggered. (Default = 15 Minutes.)
- **Consecutive Failures:** Determines how many consecutive failures of the Ping command must be detected in order to trigger the Ping No Answer Alarm. For example, if this value is set to "3", then after three consecutive Ping failures, the Ping No Answer Alarm will be triggered. (Default = 3.)

- **PNA Action:** Determines how the Ping No Answer Alarm will react when this IP address fails to respond to a ping. If "Continuous Alarm" is selected, the TSM will continue to generate new alarms until the Ping No Answer Alarm is cleared. If "Single Alarm" is generated, the TSM will generate a single alarm and will not generate additional alarms until a successful ping operation is completed and then another Ping No Answer condition is detected. (Default = Continuous Alarm.)
- **Ping Test:** (Text Interface Only) Sends a test Ping command to this IP Address.

  Note: *After you have finished defining or editing Ping No Answer IP Addresses, 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 TSM displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.3.2. Configuring the Ping No Answer Alarm

To configure the Ping No Answer Alarm, access the TSM 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 Ping No Answer Alarm.
- **Web Browser Interface:** Click the "Alarm Configuration" link on the left hand side of the screen to display the Alarm Configuration Menu. At 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 TSM 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 TSM will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the TSM 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 5.7.11) 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")

6.4. The Invalid Access Lockout Alarm

The Invalid Access Lockout Alarm is intended to provide notification when the TSM 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 TSM 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 TSM 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 TSM 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 TSM 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 TSM to provide Email alarm notification, communication parameters must first be defined as described in Section 5.7.11.*
- *In order for the TSM to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.7.2.*
- *In order for the TSM 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 5.7.7.*

To configure the Invalid Access Lockout Alarm, access the TSM 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 **5** 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 TSM 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 TSM will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the TSM 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 5.7.11) 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")

6.5. The Power Cycle Alarm

The Power Cycle Alarm can provide notification when input power to the TSM unit is lost and then restored. When the power supply is lost or interrupted, the TSM can provide notification via Email, Syslog Message or SNMP Trap after power to the unit is restored.

Notes:

- *In order for the TSM to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.7.11.*
- *In order for the TSM to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.7.2.*
- *In order for the TSM to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.7.7.*

To configure the Power Cycle Alarm, access the TSM 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 `6` and press **[Enter]** to access the configuration menu for the Power Cycle 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 "Power Cycle" link to access the configuration menu.

The Power Cycle 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.)
- **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 5.7.11) 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: Power Cycle")

6.6. Buffer Threshold Alarm

The Buffer Threshold Alarm can provide notification when the amount of data stored in the buffer for a given serial port exceeds the Buffer Threshold value that has been defined for that port as described in Section 5.6.2. When the amount of data in the buffer for a given serial port exceeds the user-defined Buffer Threshold value, the TSM can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *The Buffer Threshold Alarm can only be applied to serial ports that have been configured for Buffer Mode as described in Section 5.6.2.*
- *In order for the Buffer Threshold Alarm to function, you must first define the Buffer Threshold value for each desired serial port as described in Section 5.6.2.*
- *In order for the TSM to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.7.11.*
- *In order for the TSM to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.7.2.*
- *In order for the TSM to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.7.7.*
- *If the Buffer Threshold Alarm is not enabled, the TSM can still send SNMP Traps to notify you when the amount of accumulated data at a buffer mode port exceeds the Buffer Threshold value, providing that SNMP Trap Parameters have been defined as described in Section 5.7.7.*

To configure the Buffer Threshold Alarm, access the TSM command mode using a password that permits Administrator Level commands and then set the Port Mode for the desired Serial Port to Buffer Mode and define the Buffer Threshold value for the port as described in Section 5.6.2. After setting up the Serial Port, proceed as follows:

- **Text Interface:** Type **`/AC`** and then press **[Enter]** to display the Alarm Configuration Menu. From the Alarm Configuration Menu, type **`7`** and press **[Enter]** to access the configuration menu for the Buffer 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 the "Buffer Threshold" link to access the configuration menu.

The Buffer Threshold 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.)
- **Resend Delay:** Determines how long the TSM 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 TSM will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled for the Buffer Threshold Alarm, the TSM will send initial notification when it detects that the amount of data stored in the buffer for a given serial port has exceeded the user-defined Buffer Threshold value, and then send a second notification when it determines that the amount of data in the buffer has fallen below the Buffer Threshold 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 5.7.11) 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: Buffer Threshold")

6.7. The Voltage Loss Alarm

The Voltage Loss (Line In) Alarm can provide notification when the power supply to the TSM unit has been interrupted.

Notes:

- *The Voltage Loss (Line In) alarm is only available on TSM units that include two input power lines (models TSM-24-DPS and TSM-40-DPS.)*
- *The Voltage Loss (Line In) alarm will provide notification when one of the available power supplies is lost or disconnected. This alarm will not function if all input power to the TSM-DPS unit is lost. To provide notification when all input power is lost and restored, please use the Power Cycle Alarm as described in Section 6.5.*
- *In order for the TSM to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the TSM 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 and Section 11.*
- *In order for the TSM 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 and Section 12.*

To configure the Voltage Loss (Line In) Alarm, you must access the TSM-DPS command mode using a password that permits Administrator Level commands. The Voltage Loss 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 Off and then back On again.*

- **Resend Delay:** Determines how long the TSM 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 enabled, the TSM will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the TSM will send initial notification when it detects that one of it's power supplies has been lost or disconnected, and then send a second notification when it determines that power has been restored. (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: Lost Voltage")

7. The Status Screens

The Status Screens display connection status and communication parameters for the TSM unit, the Serial Ports, Internal Modem Port and Network Port.

In addition, the TSM can also display an Audit Log and an Alarm Log; the Audit Log records port connection/disconnection and logon/logoff activity at the TSM and the Alarm Log records instances where the Invalid Access Alarm has been triggered.

> **Note:** *The Port Diagnostics Screen and Port Parameters Screen are only available via the Text Interface. The Port Status Screen, Network Status Screen and Log Files are available via both the Text Interface and Web Interface.*

7.1. Product Status

The Product Status Screen lists the model number, power rating, input line count, input line frequency and software version for the TSM unit.

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

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

The Product Status Screen lists the following items for the TSM unit:

- **Product:** The make/model number of the TSM unit.
- **Modem Installed:** Indicates whether or not the TSM unit includes an internal modem.
- **SW Version:** The software version that is currently installed on the TSM unit.

7.2. The Port Status Screen

The Port Status screen shows the current status of the TSM's Serial Ports, including 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.

Note:

- *When Port Status is viewed by an account with "Administrator" or "SuperUser" command access, all TSM Serial Ports are listed.*
- *When Port Status is viewed by an account with "User" or "ViewOnly" command access, then the screen will list only the Serial Ports that are allowed by that account.*
- *The Port Status Screen also shows the current status of the TSM's Internal Modem Port.*

To view the Port Status Screen, access the TSM 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.

The Port Status Screen lists the following parameters for the TSM's Serial Ports:

- **Port:** The number of each Serial Port.

Notes:

- *On TSM-8 and TSM-8DC units, the internal modem port is Port 9.*
- *On TSM-24 and TSM-24DC units, the internal modem port is Port 25.*
- *On TSM-40 and TSM-40DC units, the internal modem port is Port 41.*
- *The internal modem port is not present on TSM model numbers that end with the "NMI" suffix.*

- **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:
  - No Connection: This column will read "Free" if the corresponding Serial 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 Serial Port.
  - Connection to Another Serial Port: If one of the other TSM Serial Ports is currently connected to this port, then this column will read "C-*nn*" (where *nn* is the number of the Serial Port connected to this 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..

7.3. 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]**.

Notes:

- *The Port Diagnostic Screen is not available via the Web Browser Interface and must be accessed via the Text Interface.*
- *When Port Diagnostic Screen is viewed by an account with "Administrator" or "SuperUser" command access, all TSM Serial Ports are listed.*
- *When Port Diagnostic Screen is viewed by an account with "User" or "ViewOnly" command access, then the screen will list only the Serial Ports that are 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.

7.4. The Network Status Screen

The Network Status screen shows activity at the TSM'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 using a password that permits access to Administrator Level commands and then proceed as follows:

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

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 (..).

7.5. The Port Parameters Screens

The /W (Who) command displays more detailed information about an individual TSM 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 will display parameters for all TSM Serial Ports, plus the Network Port. If the /W command is invoked by a User level or ViewOnly level account, then it will only display parameters for the port that was used to access command mode (the resident 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.

Notes:

- *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, User or ViewOnly level account which has accessed command mode via the Network Port, then only the Sequence Disconnect, Logoff Character and Accept Break option for the Network Port will be displayed.*
- *The Port Parameters Screen is not available via the Web Browser Interface, and can only be accessed via the Text Interface.*

7.6. The Event Logs

7.6.1. The Audit Log

The Audit Log provides a record of most command activity at the TSM unit, including 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:** Place the cursor over the "Logs" link on the left hand side of the screen wait for the fly-out menu to appear. To view the Audit Log, click on the "Audit Log (Display)" link; to download the Audit Log, click on the "Audit Log (download)" link.

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.*

7.6.2. 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:** Place the cursor over the "Logs" link on the left hand side of the screen wait for the fly-out menu to appear. To view the Alarm Log, click on the "Alarm Log (Display)" link; to download the Alarm Log, click on the "Alarm Log (download)" link.

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.*

7.6.3. The Temperature Log

The temperature log provides a record of TSM 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:** Place the cursor over the "Logs" link on the left hand side of the screen wait for the fly-out menu to appear. To view the Temperature Log, click on the "Temperature Log (Display)" link; to download the Temperature Log, click on the "Temperature Log (download)" link.

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. Operation

This section discusses the procedures for connecting and disconnecting ports, and describes the various port modes.

> **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 (also known as the "Command Line Interface or "CLI".).*

8.1. 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 Port 1.

8.1.1. Port Connection and Disconnection

The TSM allows communication between devices without the requirement that both ports use the same communication parameters.

8.1.1.1. Connecting Ports

Two different types of connections can be made between TSM ports; Resident Connections and Third Party Connections.

- **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 or 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 commands.*
- *The RS232 Ports cannot employ the /C command to initiate a connection to the Network Port.*
- *If your account does not permit Administrator or SuperUser commands, you will only be able to connect to ports allowed by your account. Accounts with Administrator or SuperUser access 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 TSM 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:** (Administrators 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 TSM 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 commands (using an account that also permits Administrator commands), and invoke the following command: **`/C 5 6`** **[Enter]**.

Notes:

- **Resident Connections:** *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.*

Notes:

- *When the Inactivity Timeout is disabled, this allows ports to automatically reconnect after a power interruption. When power is restored to the unit, pairs of ports that were previously connected will be automatically reconnected, providing that the Inactivity Timeout is disabled at both ports, and the two ports have been connected for at least ten minutes prior to the power interruption. This applies only to serial ports; connections between the Network Port and another port will not be re-established.*
- *The only exception to this rule is Serial Port 1, which will remain disconnected after power is restored in order to provide a free serial port for local access to command mode.*

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”.

8.1.1.2. 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 TSM offers two different disconnect command formats; the One Character Format and the Three Character Format (for more information, please refer to Section 5.6.2.):

   Note: *The Resident Disconnect methods discussed here cannot be used to terminate a Telnet Direct Connection. For more information, please refer to Section 9.3.4.*

   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 5.6.2.

2. **Third Party Disconnect:** (Administrator or 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 9.3.4.*

   a) The /D command uses the format: **`/D xx XX`** **[Enter]**, where **`xx`** and **`XX`** are the numbers of the ports you wish to disconnect.

   b) The /D (Disconnect) command can only be invoked by accounts and ports that permit Administrator commands.

c) The /D command can specify both connected ports, or either of the two ports. For example, if Port 1 is your resident port, any of the following commands can be used to disconnect Port 3 from Port 4:

`/D 3 4` [Enter]
or
`/D 3` [Enter]
or
`/D 4` [Enter]

d) 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 TSM 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 TSM'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 disconnect Resident Ports, or Third Party Ports.

Note: *The No Activity Timeout also applies to Telnet Direct Connections. For more information, please refer to Section 9.3.*

a) **RS232 Ports:** To select the timeout period for Serial Ports, access the Port Configuration Menu for the desired port as described in Section 5.6.2.

b) **Network Port:** To select the timeout period for the Network Port, access the Network Port Configuration Menu as described in Section 5.7.

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.*

8.1.2. Defining Hunt Groups

A Hunt Group creates a situation where the TSM 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 commands.
2. Access the Port Configuration Menu for the desired Port(s) as described in Section 5.6.2.
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 TSM 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 that does not permit Administrator or SuperUser level commands, the /C command will only connect to the ports allowed by that user 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]**.

8.2. 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 communicate with other ports, but cannot enter command mode, and therefore cannot redefine parameters, display status, or connect or disconnect ports. The Passive Mode is the default at Serial Ports 2 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 Connect Command as described in Section 8.1.1. Passive Mode ports will not buffer data, except during baud rate conversion.

Note: *In order to ensure Administrator access to important command functions, the Passive Mode is not available to Port 1 (the SetUp Port.)*

8.3. Buffer Mode

The Buffer Mode allows collection of data from various devices without the requirement that all devices use the same communication parameters (e.g. baud rate, parity, etc.). Buffer Mode ports can be configured to support the SYSLOG and SNMP Trap functions, as described in Sections 10 and 11. In addition, the Buffer Mode also allows you to enable the Buffer Threshold Alarm as described in Section 6.6.

Notes:

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

8.3.1. Reading Data from Buffer Mode Ports

To check port buffers for stored data, access command mode via the text interface, using an account and port that permit Administrator 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:

- *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 Buffer Threshold function will also be reset.*

If the buffer contains data, the TSM 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:** (Administrator Only) 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 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.

Note: *The /E command cannot erase data from a port buffer that is currently being read by another port.*

8.3.2. Port Buffers

The Status Screen lists the amount of Buffer Memory currently used by each port. The TSM 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.*

8.4. 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 TSM 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 TSM 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 TSM 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.*
- *When an external modem is installed at an TSM 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. This is also true for the TSM's Internal Modem Port.*
- *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.*

8.5. Manual Operation

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

8.6. Logging Out of Command Mode

When you have finished communicating with the TSM, 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 you disconnect using the LogOut link or /X command, this ensures that the TSM has completely exited from command mode, and is not waiting for the inactivity timeout period to elapse before allowing additional connections.

9. Telnet & SSH Functions

9.1. Network Port Numbers

Whenever an inbound Telnet or SSH session connects to an TSM 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.

9.2. SSH Encryption

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

Note that when the /K (Send SSH Key) command is invoked, the TSM can also provide you with a public SSH key, which can be used to streamline connection to the TSM 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 TSM, and once this key is supplied to the SSH client, the client will no longer display a warning indicating that the TSM 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 TSM does not support SSH1, the /K 1 command will still return a key for SSH1.*

9.3. The Direct Connect Feature

The Direct Connect feature allows you to initiate a Telnet, SSH or Raw Socket session with the TSM and make an immediate connection to a specific RS232 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 TSM's RS232 Serial Ports.

Direct Connect employs unique, pre-assigned TCP port numbers for each RS232 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 RS232 Port and can be used to connect to Any-to-Any, Passive, Buffer, or Modem Mode ports.

9.3.1. 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 TSM will respond to all IACs.

When configuring a 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 9.3.2.

When configuring a 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".

9.3.2. Configuration

The Direct Connect Function is configured on a per port basis using the Serial Port Configuration Menus and Network Port Configuration Menu. 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 TSM will prompt for a username and password. If a valid username/password is entered, the TSM 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.

4. **Break on Raw Disconnect:** When the Direct Connect option has been enabled as described in Steps 2 or 3 above, this option can be used to configure the TSM to send a break character whenever a Raw Socket connection to this port is terminated. As described below, the Break on Raw Disconnect option will work when the password feature is either enabled or disabled as described below:

   a) **Password Disabled:** To employ the Break on Raw Disconnect option with the Direct Connect password disabled, proceed as follows:

      i. Access the Serial Port configuration menu for the desired TSM serial port, and then use the Direct Connect option to select the "On - No Password" option. After "On - No Password" is selected, the menu will return to the Serial Port configuration screen.

      ii. Use the Direct Connect option to select the "Break on Raw Disconnect" parameter. After "Break on Disconnect" is selected, the menu will return to the Direct Connect configuration screen. Note that at this point, the prompt for the "Break on Disconnect" option will read "On - Break on Disconnect", indicating that both the Direct Connect feature and the Break on Disconnect feature are enabled.

   a) **Password Enabled:** To employ the Break on Raw Disconnect option with the Direct Connect password enabled, proceed as follows:

      i. Access the Serial Port configuration menu for the desired TSM serial port, and then use the Direct Connect option to select the "On - Password" option. After "On - Password" is selected, the menu will return to the Serial Port configuration screen.

      ii. Use the Direct Connect option to select the "Break on Raw Disconnect" parameter. After "Break on Disconnect" is selected, the menu will return to the Direct Connect configuration screen. Note that at this point, the prompt for the "Break on Disconnect" option will read "On - Break on Disconnect", indicating that both the Direct Connect feature and the Break on Disconnect feature are enabled.

Notes:

- *If you intend to create "Raw Socket" connections to TSM serial ports, then the "Raw Socket Access" feature must also be enabled at the Network Port, as described in Section 5.7.2.*
- *If you intend to use SSH to establish direct connections to the TSM, the "Direct Connect ON - PASSWORD option must be selected.*
- *If Administrator commands are disabled at the Network Port, then accounts that permit Administrator commands will not be able to initiate a Direct Connection.*
- *If Administrator commands are enabled at the Network Port, then accounts with Administrator access and accounts without Administrator 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.*

9.3.3. Connecting to an RS232 Port using Direct Connect

Direct Connect TCP port numbers are as follows:

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

   a) **Eight-Port TSM Units:**
   - Serial Ports: TCP port numbers 2101 through 2108.
   - Internal Modem Port (if present): TCP port number 2109.

   b) **24-Port TSM Units:**
   - Serial Ports: TCP port numbers 2101 through 2124.
   - Internal Modem Port (if present): TCP port number 2125.

   c) **40-Port TSM Units:**
   - Serial Ports: TCP port numbers 2101 through 2140.
   - Internal Modem Port (if present): TCP port number 2141.

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

   a) **Eight-Port TSM Units:**
   - Serial Ports: TCP port numbers 2301 through 2308.
   - Internal Modem Port (if present): TCP port number 2309.

   b) **24-Port TSM Units:**
   - Serial Ports: TCP port numbers 2301 through 2324.
   - Internal Modem Port (if present): TCP port number 2325.

   c) **40-Port TSM Units:**
   - Serial Ports: TCP port numbers 2301 through 2340.
   - Internal Modem Port (if present): TCP port number 2341.

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

   a) **Eight-Port TSM Units:**
   - Serial Ports: TCP port numbers 2201 through 2208.
   - Internal Modem Port (if present): TCP port number 2209.

   b) **24-Port TSM Units:**
   - Serial Ports: TCP port numbers 2201 through 2224.
   - Internal Modem Port (if present): TCP port number 2225.

   c) **40-Port TSM Units:**
   - Serial Ports: TCP port numbers 2201 through 2240.
   - Internal Modem Port (if present): TCP port number 2241.

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

   a) **Eight-Port TSM Units:**
   - Serial Ports: TCP port numbers 3101 through 3108.
   - Internal Modem Port (if present): TCP port number 3109.

   b) **24-Port TSM Units:**
   - Serial Ports: TCP port numbers 3101 through 3124.
   - Internal Modem Port (if present): TCP port number 3125.

   c) **40-Port TSM Units:**
   - Serial Ports: TCP port numbers 3101 through 3140.
   - Internal Modem Port (if present): TCP port number 3141.

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

   a) **Eight-Port TSM Units:**
   - Serial Ports: TCP port numbers 3301 through 3308.
   - Internal Modem Port (if present): TCP port number 3309.

   b) **24-Port TSM Units:**
   - Serial Ports: TCP port numbers 3301 through 3324.
   - Internal Modem Port (if present): TCP port number 3325.

   c) **40-Port TSM Units:**
   - Serial Ports: TCP port numbers 3301 through 3340.
   - Internal Modem Port (if present): TCP port number 3341.

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 9.3.2 If the TSM'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 TSM 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.

9.3.4. 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 RS232 Port.
2. The Network session is terminated.
3. The RS232 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 TSM port that allows Administrator commands can terminate a direct connection at another port by issuing the /D command as described in Section 8.1.1.*
- *Acknowledgment of data received by the TSM network port does not automatically indicate that the data has been completely sent out the serial port. Data may still be queued in TSM buffers. Any data queued at the time of a client initiated disconnect is discarded, and is not passed to the attached device.*

9.4. Creating an Outbound Telnet Connection

The TSM includes a /TELNET command, that can be used to create an outbound Telnet connection. In order to use the /TELNET command, you must access the TSM's Text Interface command mode using an account that permits Telnet Access and Outbound Access, via one of the TSM's Serial RS232 Ports as described below.

Notes:

- *In order for the /TELNET command to function, Telnet Access and Outbound Service Access must be enabled for your user account as described in Section 5.5.*
- *If you have logged in via the Network Port, the /TELNET command will not function.*

To create an outbound Telnet connection, access the Text Interface via a free Serial Port, using an account that permits Telnet Access and Outbound Access and then invoke the /TELNET command using the following format:

`/TELNET <ip> [port] [raw]` [Enter]

Where:

`ip`	Is the target IP address.
`port`	Is an optional argument which can be included to indicate the target port at the IP address.
`raw`	Is an optional argument which can be included to indicate a raw socket connection. In order to create a raw socket connection, the command line must end with the text "**`raw`**".

For example, to create a raw socket, outbound Telnet connection to port 2000 at IP Address 255.255.255.255, access the Text Interface command mode via a free TSM Serial Port using an account that permits Telnet Access and Outbound Access and invoke the TELNET command as follows:

`/TELNET 255.255.255.255 2000 raw` [Enter]

9.5. Creating an Outbound SSH Connection

The TSM's /SSH command can be used to create an outbound SSH connection. In order to use the /SSH command, you must access the TSM's Text Interface command mode using an account that permits SSH Access and Outbound Access, via one of the TSM's Serial RS232 Ports as described below.

Notes:

- *In order for the /SSH command to function, SSH Access and Outbound Service Access must be enabled for your user account as described in Section 5.5.*
- *If you have logged in via the Network Port, the /SSH command will not function.*

To create an outbound SSH connection, access the Text Interface via a free Serial Port, using an account that permits SSH Access and Outbound Access and then invoke the /SSH command using the following format:

`/SSH <ip> -l <username>` [Enter]

Where:

`ip`	Is the target IP address.
`-l`	(Lowercase letter "L") Indicates that the next argument will be the log on name.
`username`	Is the username that you wish to use to log in to the target device.

For example, to create an outbound SSH connection to a device at IP Address 255.255.255.255, with the username "employee", access the Text Interface command mode via a free TSM Serial Port using an account that permits SSH Access and Outbound Access and invoke the SSH command as follows:

`/SSH 255.255.255.255 -l employee` [Enter]

10. 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.

10.1. 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 5.7, 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 TSM, 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 an Invalid Access Alarm 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 10.1: The Test Menu (Text Interface, Administrator Mode Only)

10.2. Testing Syslog Configuration

After you have configured the TSM as described in Section 10.1, the /TEST command can be used to make certain that the function is properly set up. To test the Syslog function, access the TSM command mode via the Text Interface using an account that permits Administrator level commands, then type **`/TEST`** and press **[Enter]** to display the Test Menu shown in Figure 10.1.

When the Syslog Test feature is selected, the TSM 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 10.1 to make certain the TSM 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 5.7.5.

11. SNMP Traps

SNMP is an acronym for "Simple Network Management Protocol". The SNMP Trap function allows the TSM to send SNMP Traps to two different SNMP managers, each time an alarm is triggered or when the buffer for a properly configured serial port reaches the user-defined Buffer Threshold.

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 and/or when a buffer mode serial port reaches the user-defined Buffer Threshold. For more information on Alarm Configuration, please refer to Section 6.*

11.1. Configuration:

To configure the SNMP Trap function, proceed as follows:

1. Access command mode using an account that permits Administrator level commands.

2. **Serial Port Parameters:** If you wish to generate SNMP Traps that will notify you when a Buffer Mode Port buffer reaches the user-defined Buffer Threshold, access the Serial Port Parameters menu for the desired port as described in Section 5.8. Set the following:

   a) **Port Mode:** Make certain that the Port Mode is set to Buffer Mode.

   b) **Buffer Threshold:** Set the Buffer Threshold to the desired value. The Buffer Threshold determines how much data must accumulate in a given port buffer in order to generate a Buffer Threshold Alarm and/or SNMP Trap.

Notes:

- *It is only necessary to set the Buffer Threshold when you wish to generate SNMP Traps and/or use the Buffer Threshold Alarm to notify you when data has accumulated in a port buffer. For more information on the Buffer Threshold Alarm, please refer to Section 6.6.*
- *If you only wish to generate SNMP Traps to notify you when an Over Temperature Alarm, Lost Communications Alarm, Ping No Answer Alarm, Invalid Access Alarm or Power Cycle Alarm has been triggered, it is not necessary to set the Buffer Threshold parameter.*

3. **SNMP Trap Parameters:** Access the SNMP Trap Parameters Menu as described in Section 5.7.7. 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 TSM will send an SNMP Trap each time an alarm is triggered.

11.2. 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 11.1.
2. Access the Text Interface command mode using an account that permits Administrator level commands, then invoke the "/TEST" command at the TSM command prompt. Note that the /TEST Command is only available in Administrator 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 TSM 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 10.2.

12. Operation via SNMP

If SNMP Access Parameters have been defined as described in Section 5.7.6, then you will be able to manage user accounts, set some configuration parameters and display unit status via SNMP. This section describes SNMP communication with the TSM unit, and lists some common commands that can be employed to manage users, select configuration parameters and display unit status.

12.1. TSM SNMP Agent

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

12.2. 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 TSM 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 TSM supports either MD5 or SHA1.

12.3. Configuration via SNMP

TSM 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::userPasswd`** – 16 character password
- **`userTable::userAccessLevel`** – Account access level.
  `0` – ViewOnly Access
  `1` – User Access
  `2` – SuperUser Access
  `3` – Administrator Access
- **`userTable::userPortAccess`** – A string of characters, with one character for each of the serial ports on the TSM 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.

  Note: *The number of ports specified in the userPortAccess string must not exceed the number of serial ports available on your TSM unit. If the userPortAccess string specifies more serial ports than are available on the TSM unit, an error message will be generated.*

- **`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::userOutboundTelnetAccess`** – Access to Outbound Telnet
  `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.

12.3.1. Viewing Users

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

12.3.2. 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.

12.3.3. 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.

12.3.4. 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.

12.4. Configuring Serial Ports

Commands can be issued to set certain serial port configuration parameters via SNMP. Ports are arranged in a table, 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 Buffer Threshold 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), then SNMP Traps related to the Buffer Threshold will be disabled at this port.

12.5. Viewing Unit Status via SNMP

The temperature status and model number for the TSM unit can be retrieved via SNMP. The environmentUnitTable contains one row.

- **`environmentUnitTable::environmentUnitTemperature`** – The temperature of the TSM unit.
- **`environmentUnitTable::environmentUnitName`** – Returns the specific model number for the TSM unit.

12.6. Sending Traps via SNMP

Traps that report various unit conditions can be sent to an SNMP Management Station from the TSM. The following traps are currently supported.

- **WarmStart** Trap – Trap indicating a warm start
- **ColdStart** Trap – Trap indicating a cold start
- **Test** Trap – Test trap invoked by user via the Text Interface (CLI)

The TSM can send an SNMP trap to notify you when the Over Temperature Alarms, Ping No Answer Alarm, Invalid Access Lockout Alarm, Power Cycle Alarm, or Buffer Threshold Alarm has been triggered. In all cases except the Power Cycle Alarm, there will be one trap sent when the alarm is triggered, and a second trap sent when the alarm is cleared. For more information on alarm functions, please refer to Section 6.

- **Alarm** Trap – Trap indicating an alarm condition. A trap with a unique enterprise OID is defined for the Invalid Access Lockout Alarm, under which specific trap-types are defined to indicate the setting or clearing of that particular alarm condition. There are separate traps for the Invalid Access Lockout Alarm. The Alarm includes a "Set Trap," which indicates that the alarm has been triggered, and a "Clear Trap," which indicates that the alarm has been cleared.
- **overTemperatureInitialSetTrap** - Indicates that the Over Temperature (Initial) Alarm has been triggered. The trap will also include a numerical value that indicates the current unit temperature.
- **overTemperatureInitialClearTrap** - Indicates that the Over Temperature (Initial) Alarm has been cleared.
- **overTemperatureCriticalSetTrap** - Indicates that the Over Temperature (Critical) Alarm has been triggered. The trap will also include a numerical value that indicates the current unit temperature.
- **overTemperatureCriticalClearTrap** - Indicates that the Over Temperature (Critical) Alarm has been cleared.
- **pingNoAnswerSetTrap** - Indicates that the Ping No Answer Alarm has been triggered. The trap will also include a numerical value that indicates the IP address of the device that failed to respond to the ping command.
- **pingNoAnswerClearTrap** - Indicates that the Ping No Answer Alarm has been cleared.
- **lockoutSetTrap** - Indicates that the Invalid Access Lockout Alarm has been triggered. The trap will also include a numerical value that indicates the number of the serial port where the lockout occurred.
- **lockoutClearTrap** - Indicates that the Invalid Access Lockout Alarm has been cleared.

- **`powercycleSetTrap`** - Indicates that the Power Cycle Alarm has been triggered (Note that there is no corresponding Clear Trap for the Power Cycle Alarm.)
- **`bufferThresholdCrossedSetTrap`** - Indicates that the amount of data in the serial port buffer has exceeded the currently defined Buffer Threshold value. The trap will also include a the number of the port where the Buffer Threshold Alarm was generated, and a numerical value that indicates the amount of data currently stored in the port buffer.
- **`bufferThresholdCrossedClearTrap`** - Indicates that the data in the port buffer has either been read or erased and that the Buffer Threshold Alarm has been cleared.

13. Setting Up SSL Encryption

This section describes the procedure for setting up a secure connection via https web connection to the TSM.

> **Note:** *SSL parameters cannot be defined via the Web Browser Interface. In order to set up SSL encryption, you must contact the TSM 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 TSM, without the need to go to an outside service, and there is no need to set up your domain name server to recognize the TSM. The principal disadvantage of Self Signed certificates, is that when you access the TSM 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 TSM 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 TSM 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 TSM unit (e.g., service.companyname111.com.) Once a signed certificate has been created and uploaded to the TSM, 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:                      15. Export Server Private Key:
13. View CSR:                        16. Import Server Private Key:
14. Import CRT:                      17. Harden Web Security: On

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

Figure 13.1: Web Access Parameters (Text Interface Only)

13.1. 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 13.1.) 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 TSM, make certain to define all of the following parameters. Although most SSL applications require only the Common Name, in the case of the TSM all of the following parameters are mandatory.*

   - **5. Common Name:** A domain name, that will be used to identify the TSM 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.companyname.com.)
   - **6. State or Province:** The name of the state or province where the TSM unit will be located (e.g., California.)
   - **7. Locality:** The city or town where the TSM unit will be located (e.g., Irvine.)
   - **8. Country:** The two character country code for the nation where the TSM will be located (e.g., US.)
   - **9. Email Address:** An email address, that can be used to contact the person responsible for the TSM (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 TSM will prompt you to create a password. Key in the desired password (up to 16 characters) and then press **[Enter]**. When the TSM prompts you to verify the password, key it again and then press **[Enter]** once. After a brief pause, the TSM 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 TSM via the Web Interface, using an HTTPS connection.

   a) Before the connection is established, the TSM 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 TSM 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.

13.2. 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 13.1 and then proceed as follows:

1. **Capture the Newly Created Certificate:** Type `13` and press **[Enter]** (View CSR). The TSM 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 TSM:** After the "signed" certificate is returned from the security service, return to the Web Access menu.

   a) Access the TSM 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 TSM 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 TSM via the Web Browser Interface, using an HTTPS connection. For example, if the common name has been defined as "service.companyname111.com", then you would enter "**https://service.companyname111.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.

13.3. Downloading the Server Private Key

When configuring the TSM's SSL encryption feature (or setting up other security/ authentication features), it is recommended to download and save the Server Private Key. To download the Server Private Key, 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 13.1.)

   a) To download the Server Private Key from the TSM unit, make certain that SSL parameters have been defined as described in Section 13.1, then type **15** and press **[Enter]** and store the resulting key on your hard drive.

   b) To upload a previously saved Server Private Key to the TSM unit, make certain that SSL parameters have been defined as described in Section 13.1, then type **16** and press **[Enter]** and follow the instructions in the resulting submenu.

14. Saving and Restoring Configuration Parameters

Once the TSM 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 TSM 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.*

14.1. 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 TSM 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. TSM.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 TSM's Save Parameter File menu, and press **[Enter]** to proceed. TSM parameters will be saved on your hard drive in the file specified in Step 2 above.
4. The TSM 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.

14.2. Restoring Saved Parameters

This section describes the procedure for using your terminal emulation program to send saved parameters to the TSM.

1. Start your terminal emulation program and access the TSM'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 TSM parameters. If necessary, key in the file name and directory path.
4. Your terminal emulation program will send the ASCII text file to the TSM. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the TSM 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 TSM 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.

14.3. Restoring Previously Saved Parameters

If you make a mistake while configuring the TSM unit, and wish to return to the previously saved parameters, the Text Interface's "Reboot System" command (`/I`) offers the option to reinitialize the TSM unit using previously backed up parameters. This allows you to reset the unit to previously saved parameters, even after you have changed parameters and saved them.

Notes:

- *The TSM will automatically backup saved parameters once a day, shortly after Midnight. This configuration backup file will contain only the most recently saved TSM parameters, and will be overwritten by the next night's daily backup.*
- *When the /I command is invoked, a submenu will be displayed which offers several Reboot options. Option 4 is used to restore the configuration backup file. The date shown next to option 4 indicates the date that you last changed and saved unit parameters.*
- *If the daily automatic configuration backup has been triggered since the configuration error was made, and the previously saved configuration has been overwritten by newer, incorrect parameters, then this function will not be able to restore the previously saved (correct) parameters.*

To restore the previously saved configuration, proceed as follows:

1. Access command move via the Text Interface, using a username/password that permits access to Administrator level commands (see Section 5.1.1.)
2. At the TSM command prompt, type `/I` and press **[Enter]**. The TSM will display a submenu that offers several different reboot options.
3. At the submenu, select Item 4 (Reboot & Restore Last Known Working Configuration,) type **`4`**, and then press **[Enter]**.
4. The TSM will reboot and previously saved parameters will be restored.

15. Upgrading TSM Firmware

When new, improved versions of the TSM 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 commands.

3. When the command prompt appears, type `/UF` and then press **[Enter]**. The TSM 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.

   d) **Start FTP/SFTP Servers for Slip Stream Upgrade:** This option will upgrade only the WTI Management Utility, without updating the TSM's operating firmware. To update the WTI Management Utility only, type `4` and press **[Enter]**.

   Note that after any of the above options is selected, the TSM 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 TSM 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 TSM unit, using a username and password that permit access to Administrator Level commands.

6. Transfer the md5 format upgrade file to the TSM.

7. After the file transfer is complete, the TSM 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 TSM will send a message to all currently connected network sessions, indicating that the TSM is going down for a reboot.

   Note: *Do not power down the TSM 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 TSM via the Network Port, in order to start the FTP/SFTP servers, the TSM 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 TSM using your former IP address.

   - If you initially selected "Start FTP/SFTP Servers and Default Parameters", you must then login using the TSM's default IP address (Default = 192.168.168.168) or access command mode via Serial Port 1 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.

16. Command Reference Guide

16.1. 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 TSM 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]**.
- **Suppress Command Confirmation Prompt:** When the **/D** (Disconnect Port) or **/E** (Erase Port Buffer) commands are invoked, the "**,Y**" option can be included to override the Command Confirmation ("Sure?") prompt. For example, to disconnect Serial Port 4 without displaying the Sure prompt, type **/D 4,Y [Enter]**.
- **Connected Ports:** When two ports are connected, most TSM 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.

16.2. Command Summary

Function	Command Syntax	Command Access Level			
		Admin.	SuperUser	User	ViewOnly
Display					
Port Status	/S [Enter]	X❶	X❶	X❶	X❶
Port Diagnostics	/SD [Enter]	X❶	X❶	X❶	X❶
Port Parameters (Who)	/W [n] [Enter]	X❶	X❶	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]❹	X	X	X	X
Control					
Exit Command Mode	/X [Enter]	X	X	X	X
Connect - Local <Remote>	/C <n> [n] [Enter]	X	X	X❺	
Disconnect Ports	/D <n|Nn|*> [,Y] [Enter]❻	X	X		
Read Buffer	/R <n> [Enter]	X	X	X	
Erase Buffer(s)	/E <n|*> [,Y] [Enter]❻	X	X	X	
Send Parameter File	/U [Enter]	X			
Send SSH Keys	/K <n> [Enter]	X			
Unlock Invalid Access	/UL [Enter]	X			
Outbound Telnet	/TELNET <ip> [port] [raw] [Enter]	X❼	X❼	X❼	
Outbound SSH	/SSH <ip> -l <username> [Enter]	X❼	X❼	X❼	
Broadcast Mode	/broadcast <port list> [Enter]	X	X		
Configuration					
System Parameters	/F [Enter]	X	❽		
Serial Port Parameters	/P <n> [Enter]	X	❽		
Network Configuration	/N [Enter]	X	❽		
Ping No Answer Configuration	/PNA [Enter]	X	❽		
Alarm Configuration	/AC [Enter]	X	❽		
Reboot System	/I [Enter]	X	X❾		
Upgrade Firmware	/UF [Enter]	X			
Copy Port Parameters	/CP <z> [Enter]	X			
Test Network Configuration	/TEST [Enter]	X			

❶ In Administrator and SuperUser modes, all serial ports are displayed. In User and ViewOnly modes, the status screen will only include the ports allowed by the account.

❷ User level accounts and ViewOnly level accounts are only allowed to view parameters for their resident port (the port that was used to access command mode.)

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 If the optional asterisk argument is included in the /J command line, then in addition to the Site ID message, the TSM will also display the Model Number and Firmware Version.

❺ User level accounts are only allowed to create a connection to the Serial Ports that are specifically permitted by the account. User level accounts are not allowed to create Third Party (remote) port connections.

❻ The "**,Y**" argument can be included to suppress the command confirmation prompt.

❼ In order to invoke this command, Outbound Telnet/SSH and Outbound Service Access must be enabled for your account.

❽ In SuperUser mode, configuration menus can be displayed, but parameters cannot be changed.

❾ In SuperUser mode, the /I command only offers one option: Reboot Only (Do Not Default Parameters.)

16.3. Command Set

This Section provides information on all Text Interface commands, sorted by functionality

16.3.1. Display Commands

/S Display Port Status Screen

Displays the Port Status Screen, which lists user-defined Port Names, the username for the account that is currently using the port, connection status, Port Mode and Buffer Count. For more information, please refer to Section 7.2.

> **Note:** *In Administrator Mode and SuperUser Mode, all TSM Serial Ports are displayed. In User Mode and ViewOnly Mode, the Port Status Screen will only include the ports 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 a User level or View Only level account, the resulting screen will only display parameters for the ports allowed by the account. For more information, please refer to Section 7.3.

Availability: Administrator, SuperUser, User, ViewOnly

Format: `/SD` **[Enter]**

/W Display Port Parameters (Who)

Displays configuration information for an individual port, but does not allow parameters to be changed. User level and ViewOnly level accounts can only display parameters for their resident port. For more information, please refer to Section 7.5.

Availability: Administrator, SuperUser, User, ViewOnly

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.

Example: To display parameters for a port named "SERVER", access the Command Mode from a port and account that permits Administrator commands, and type **/W SERVER [Enter]**.

/SN Display Network Status

Displays the Network Status Screen, which lists current network connections to the TSM's Network Port. For more information, please refer to Section 7.4.

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 TSM 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 Mode.*

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 Sections 5.3.3 and 7.6.

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 TSM unit.

Availability: Administrator, SuperUser, User, ViewOnly

Format: **`/J [*]`** **[Enter]**

Where **`*`** is an optional argument, which can be included in the command line to display the model number and software version of the TSM unit.

16.3.2. 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 8.1.1. 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 Administrator and SuperUser level accounts.

Notes:

- *User level accounts can only connect to the ports that are specifically permitted by the account.*
- *User level accounts are not allowed to create "Third Party" connections. For example, a User level account, that is logged in via the Network Port cannot connect Serial Port 3 to Port 4.*
- *Administrator and SuperUser level accounts are allowed to connect to any TSM Serial Port.*
- *The Serial Ports are not allowed to create a Third Party connection to the Network Port. For example, Serial Port 1 cannot connect Serial 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.

/D Third Party Disconnect

Invoke the /D command at your resident port to disconnect two other ports.

Note: *The /D command cannot disconnect your resident port*

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.

Example: To disconnect Port 2 from Port 3 without the "Sure?" prompt, access the Command Mode from a third port with Administrator or SuperUser 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 8.3.1.

Notes:

- *Users are limited to the ports that are specifically allowed by their accounts*
- *When the /R command is invoked, the counter for the Buffer Threshold 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.

/E Erase Buffer

Erases data from the buffer for a specified port(s).

Notes:

- *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] <n> [n]`** **[Enter]**

Where:

`n`	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.

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]**.

/U Send Parameters to File

Sends all TSM configuration parameters to an ASCII text file as described in Section 14. This allows you to back up the configuration of your TSM unit.

Availability: Administrator

Format: **`/U`** **[Enter]**

/K Send SSH Key

Instructs the TSM 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 9.2.

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 TSM'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 TSM will immediately unlock all ports that are currently in the locked state.

Availability: Administrator

Format: **`/UL`** **[Enter]**

/TELNET Outbound Telnet

Creates an outbound Telnet connection.

Notes:

- *In order for the /TELNET command to function, Telnet/SSH and Outbound Service Access must be enabled for your user account as described in Section 5.5. In addition, Telnet Access and Outbound Access must also be enabled via the Network Parameters menu, as described in Section 5.7.2.*
- *If you have logged in via the Network Port, the /TELNET command will not function.*

Availability: Administrator, SuperUser, User

Format: **`/TELNET <ip> [port] [raw]`** **[Enter]**

Where:

`ip`	Is the target IP address.
`port`	Is an optional argument which can be included to indicate the target port at the IP address.
`raw`	Is an optional argument which can be included to indicate a raw socket connection. In order to create a raw socket connection, the command line must end with the text "**`raw`**".

/SSH Outbound SSH

Creates an outbound SSH connection.

Notes:

- *In order for the /SSH command to function, Telnet/SSH and Outbound Service Access must be enabled for your user account as described in Section 5.5. In addition, SSH Access and Outbound Access must also be enabled via the Network Parameters menu, as described in Section 5.7.2.*
- *If you have logged in via the Network Port, the /SSH command will not function.*

Availability: Administrator, SuperUser, User

Format: **`/SSH <ip> -l <username>`** **[Enter]**

Where:

`ip`	Is the target IP address.
`-l`	(Lowercase letter "L") Indicates that the next argument will be the log on name.
`username`	Is the username that you wish to use to log in to the target device.

/BROADCAST Broadcast Text or Commands to Serial Ports

Broadcasts text or commands to a user-specified selection of TSM Serial Ports.

Notes:

- *The Broadcast command will only be applied to Serial Ports that are configured for Any-to-Any Mode or Passive Mode. Text or commands will not be broadcast to Modem Mode or Buffer Mode ports.*
- *The Broadcast command will only be applied to Serial Ports that are not currently connected. Text or commands will not be broadcast to connected Serial Ports.*
- *Flow control (handshake) at target Serial Ports must be "ready" in order to receive text or commands.*
- *The Broadcast command will not send text or commands to the Serial Port that initiated the command.*
- *To exit Broadcast mode and send text or commands, press **[Esc]** or type ^X (**[Ctrl]** plus **[X]**.)*

Availability: Administrator, SuperUser

Format: **`/BROADCAST <port list>`** **[Enter]**

Where "**`port list`**" is a series of port numbers or names, separated by spaces or commas. Note that the "**`port list`**" argument can also include wild cards.

16.3.3. 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 TSM's serial ports and internal modem port. All functions provided by the /P command are also available via the Web Browser Interface. Section 5.6 describes the procedure for defining serial port parameters.

Availability: Administrator

Format: **`/P <n>`** **[Enter]**

Where **`n`** is the number or name of the Serial Port that you wish to configure.

/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 and domain names. All of the functions provided by the /N command are also available via the Web Browser Interface. For more information, please refer to Section 5.7.

Availability: Administrator

Format: **`/N`** **[Enter]**

/PNA Ping No Answer Configuration Parameters

Displays a menu that is used to define IP addresses and other associated parameters that will be used by the Ping No Answer Alarm. When Ping No Answer IP addresses have been defined and the Ping No Answer Alarm has been enabled, the TSM can ping user-defined IP addresses, and notify you when devices at those IP addresses are not responding to the ping command. For more information, please refer to Section 6.3.

Availability: Administrator

Format: **`/PNA`** **[Enter]**

/AC Alarm Configuration Parameters

Displays a menu that is used to configure and enable the Over Temperature Alarms, Lost Communication Alarm, Ping-No-Answer Alarm, Invalid Access Lockout Alarm, Power Cycle Alarm and Buffer Threshold Alarm. When properly configured, the TSM can notify you by email whenever the Invalid Access Lockout feature is triggered. For more information on please refer to Section 6.

Availability: Administrator
Format: `/AC` **[Enter]**

/I Reboot System (Default)

Reinitializes the TSM unit and offers the option to keep user-defined parameters or reset to default parameters. As described in Section 5.8.1, the /I command can also be used to restore the unit to previously saved parameters. When the /I command is invoked, the unit will offer four reboot options:

> **Note:** *When the Reboot System command is invoked in the SuperUser mode, only one reboot option is offered: Reboot Only (Do Not Default Parameters.)*

- Reboot Only (Do NOT default parameters)
- Reboot & Default (Keep IP Parameters & SSH Keys; Default all other parameters)
- Reboot & Default (Default ALL parameters)
- Reboot & Restore Last Known Working Configuration

Availability: Administrator, SuperUser
Format: `/I` **[Enter]**

/UF Upgrade Firmware

When new versions of the TSM firmware become available, this command is used to update existing firmware as described in Section 15.

> **Note:** *When a firmware upgrade is performed, the TSM 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 TSM will display a menu that can be used to copy parameters to RS232 ports. For more information, please refer to Section 5.6.3.

> **Note:** *To proceed with the Copy function after selecting new parameters, press **[Esc]**; the TSM will then display the confirmation prompt before proceeding.*

Availability: Administrator
Format: `/CP` **[Enter]**

/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 10.2 and Section 11.2.

Notes:

- *In order for the ping command to function with domain names, Domain Name Server parameters must be defined as described in Section 5.7.5.*
- *The Test Menu's Ping command is not effected by the status of the Network Parameters Menu's Ping Access function.*

Availability: Administrator

Format: **`/TEST`** **[Enter]**

Appendix A. RS232 Port Interface

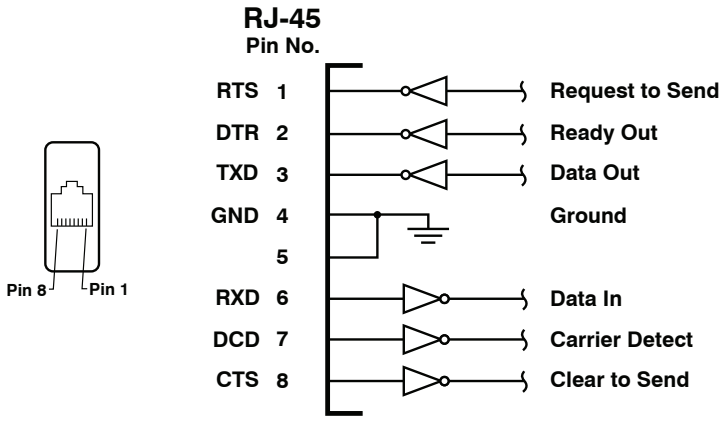

Figure A.1: RS232 Port Interface

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.

Appendix B. Specifications

Network Interface: 10/100Base-T Ethernet, RJ45, multi-session Telnet.

RS232 Port Interface:

Connectors:

- **TSM-8 Series Models:** Eight (8) RJ45 connectors (DTE pinout.)
- **TSM-24 Series Models:** Twenty Four (24) RJ45 connectors (DTE pinout.)
- **TSM-40 Series Models:** Forty (40) 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.

Memory: Stores Parameters and captured data. 256K per port.

Break: Send Break or Inhibit Break

Site ID: 32 Characters.

Port Name: 16 Characters per port.

Usernames & Passwords: 16 characters each (case sensitive.) Up to 128 pairs.

LEDs: On, Ready, DCD, plus Connection Activity for each RS232 Serial Port.

Physical / Environmental:

Power:

- **AC Models:** IEC-320-C14 Inlet, 100 to 240 VAC, 50/60 Hz, 10 Watts Max.
- **DC Models:** Terminal Strip (#6-32), -48 VDC, 0.3 Amp Max.

Size:

Height: 1.75" (4.4 cm), 1 Rack Unit.
Width: 19.00" (48.3 cm)
Depth: 6.50" (16.5 cm) Rack Mounts Included.

Shipping Weight: 7 lbs. (3.2 Kg.)

Operating Temperature: 32°F to 122°F (0°C to 50°C)

Storage Temperature: -4°F to 128°F (-20°C to 70°C)

Humidity: 10 to 90% RH, Non-Condensing

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.

Appendix C. Connecting Devices to the TSM

This section describes the cables and adapters that are used to connect common devices to the TSM's RJ-45 serial ports. For information regarding other WTI cables and adapters, please refer to the "Serial Cables and Adapters" document, which can be found on the CDROM included with the TSM.

C.1. Straight RJ-45 Cables and Rollover RJ-45 Cables

The connection examples described in this section include the use either an RJ-45 Straight cable or an RJ-45 Rollover cable. The difference between the two types of cables is the way that the pins in the connectors at each end of the cable are linked to each other.

In Straight Cables the pins on each connector are linked to the same pin number on the connector at the other end of the cable; for example, Pin 1 on the right hand connector is linked to Pin 1 on the left hand connector, as shown in Figure C.1 below.

For Rollover Cables, the order of the pins is reversed; Pin 1 on the right hand connector would be linked to Pin 8 on the left hand connector, as shown in Figure C.2.

WTI RJ-45 Straight cables are available in three different models:

- RJX-7-15: 15 Feet Long
- RJX-7-25: 25 Feet Long
- RJX-7-30: 30 Feet Long

WTI also offers an RJ-45 Rollover cable:

- RJ-ROLL

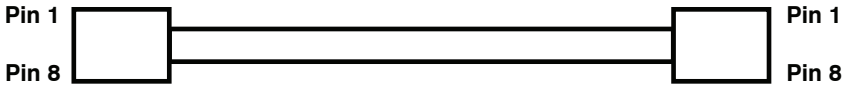

Figure C.1: Straight Cables

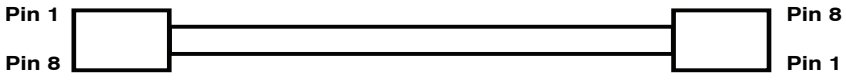

Figure C.2: Rollover Cables

C.2. Connecting DB-9M DTE Devices

The DX9F-DTE-RJ Snap Adapter can be used with a Straight RJ-45 cable to attach the following DB-9M DTE devices to the TSM's RJ-45 Serial Ports:

- PCs and Laptops
- Console Ports on WTI RSM-8, RSM-16 and RSM-32 units
- Console Ports on WTI MPC Series Units
- Other Devices with a DB-9M DTE Console Port

When connecting a DB-9M DTE device to an RJ-45 Serial Port on the TSM, please refer to Figure C.3 and Figure C.4 below:

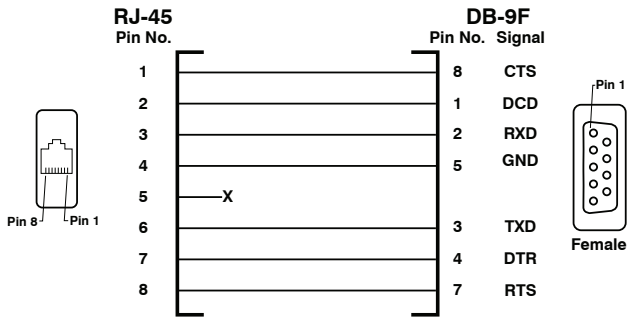

Figure C.3: DX9F-DTE-RJ Snap Adapter Interface

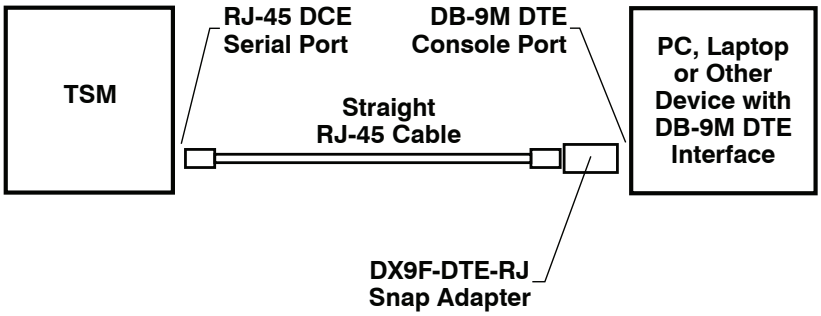

Figure C.4: Connecting DB-9M DTE Devices to an RJ-45 Serial Port on an RSM-8R4

C.3. Connecting DB-25F DTE Devices

The DX25M-DTE-RJ Snap Adapter can be used with a Straight RJ-45 cable to attach the most DB-25F DTE devices to RJ-45 Serial Ports on TSM units.

When connecting a DB-25F DTE device to an RJ-45 Serial Port on the TSM, please refer to Figure C.5 and Figure C.6 below:

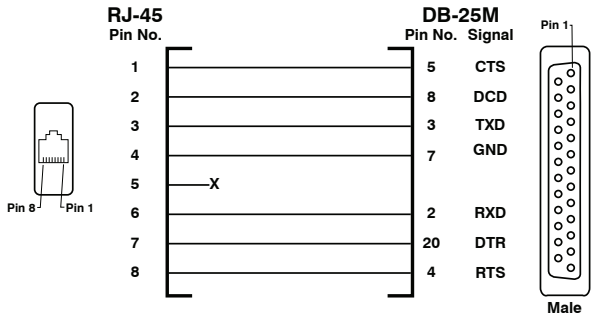

Figure C.5: DX25M-DTE-RJ Snap Adapter Interface

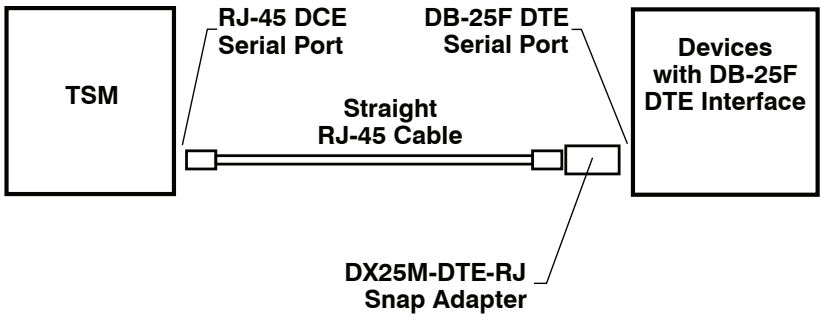

Figure C.6: Connecting DB-25F DTE Devices to an RJ-45 Serial Port on an RSM-8R4

C.4. Connecting DB-25F DCE Devices

The DX25M-DCE-RJ Snap Adapter can be used with a Straight RJ-45 cable to attach the following DB-25F DCE devices to RJ-45 serial ports on the TSM:

- External Modems with DB-25F DCE Serial Port
- Other Devices with a DB-25F DCE Console Port

When connecting a DB-35F DCE device to an RJ-45 serial port on the TSM, please refer to Figure C.7 and Figure C.8 below:

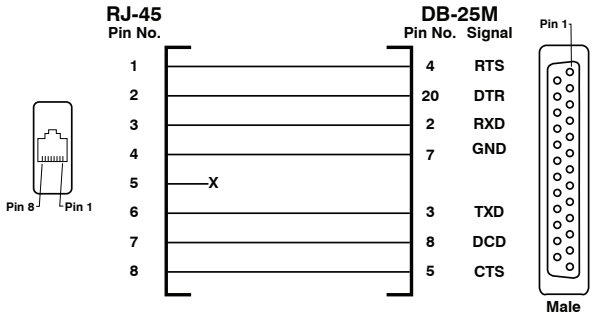

Figure C.7: DX25M-DCE-RJ Snap Adapter Interface

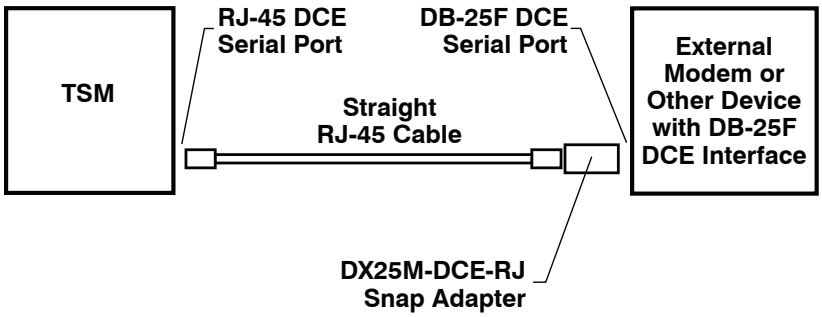

Figure C.8: Connecting DB-25F DCE Devices to an RJ-45 Serial Port on an RSM-8R4

C.5. Connecting RJ-45 DCE Devices

An RJ-ROLL Rollover cable can be used to connect the following RJ-45 DCE devices to the RJ-45 serial ports on TSM units:

- Cisco Routers with RJ-45 DCE Console Port
- Sun Routers with RJ-45 DCE Console Port
- Other Devices with RJ-45 DCE Console Port

When connecting an RJ-45 DCE device to an RJ-45 serial port on an TSM unit, please refer to Figure C.9 below:

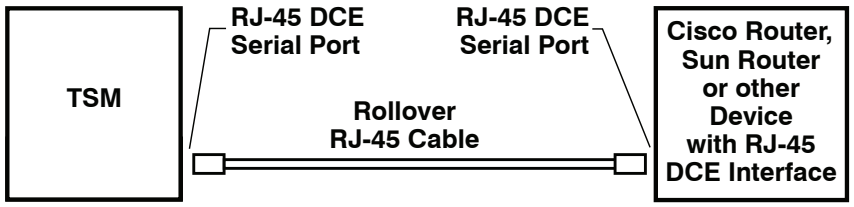

Figure C.9: Connecting RJ-45 DCE Devices to the RSM-8R4

C.6. DX9F-NULL-RJ Snap Adapter

The DX9F-NULL-RJ Snap Adapter is used for straight through cable connections (Pins 2 through 8).

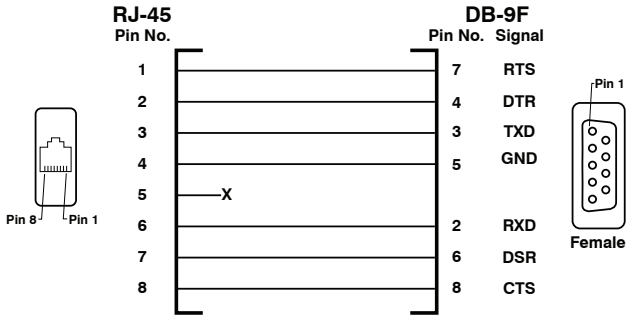

Figure C.10: DX9F-NULL-RJ Snap Adapter Interface

Appendix D. 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) 583-9514

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..

August, 2010
Part Number: 14023, Revision: D

Trademarks and Copyrights Used in this Manual

Hyperterminal is a registered trademark of the Microsoft Corporation. Portions copyright Hilgraeve, Inc.

Teraterm is a copyright of Ayera Technologies, Inc.

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