User's Manual
Installation and Operation Guidelines

TeleBoss™ 830 Pollable Remote Access Unit

Version 2.03.050

Asentria Corporation
1200 North 96th Street
Seattle, Washington, 98103
U.S.A.
Tel: 206.344.8800
Fax: 206.344.2116
www.asentria.com

TeleBoss™ 830 Pollable Remote Access Unit
Installation and Operation Guidelines

For firmware Version 2.03.050 _STD
Manual revision A
Release Date: March 21, 2008

Changes In This Version of the User Manual

- Added the Static Route Settings menu to the Network Settings section, and a further detail Static Routes section in the Features chapter.
- Added a section describing the installation, configuration, and operation of the optional ADSL modem.
- Added the DSL Settings and VPN Settings menus to the Network Settings section.
- Added the Default Route Enable option to the Wireless Modem Settings section and a description of this option in the Wireless Modem chapter.
- Added product graphics for the back panels of both the T830-2 and T830-6 products.

Table of Contents

Quick Start

What's Included

This chapter is a brief guide to help get your TeleBoss 830 (T830) up and running quickly.

Hardware Needed
- Asentria TeleBoss 830
- 15VDC power adaptor (Included if AC power option)
- DC power source (if DC power option)
- Computer with DB9 RS-232 Serial port and terminal emulation software
- Ethernet cable
- RJ45 M-M unshielded serial cable and RJ45/DB9 straight thru adapter (Included)
- PC running AlarmManager software -- may be obtained from http://www.asentria.com/docsandsoftware/productManuals.aspx or Asentria Technical Support (for SNMP trap receiving purposes)

Information Needed
- IP address(es) to assign to the T830
- Subnet mask
- Default router IP or gateway router IP address if on a WAN (Optional)
- IP address of the PC running Asentria AlarmManager (for SNMP trap receiving purposes)

Connecting

Cables and Power
1. Connect the RJ45 serial cable and DTE adaptor together, and connect the RJ45 end to serial port I/O2 of the T830, and the DB9 end to COM1 of a computer with a terminal emulator.
2. Connect the attached ground wire securely to an appropriate earth ground (this is essential).
3. Connect an Ethernet cable, if available, into the RJ45 jack labeled ETH1.
4. Connect the power supply to the unit (see Power Requirements section).

Power Requirements

The T830 is configured with one of two types of power connectors: AC or DC.

If configured for AC, the unit uses a barrel connector for connecting to the 15VDC power adapter shipped with the unit.

If configured for DC, the unit is configured with a 4-pin Molex connector for use with a DC power source. The unit is shipped with the cables and instructions for direct connection to a DC power source. The instructions are shown below, in case they are missing from the box.

Note: This instruction sheet describes connection of the provided –48V wiring harness kit to the source power supply. This unit should be assembled and installed by a qualified technician who can ensure the power source is an isolated, SELV (Safety Extra Low Voltage) circuit. There are two versions of the harness using different wiring colors as shown below.

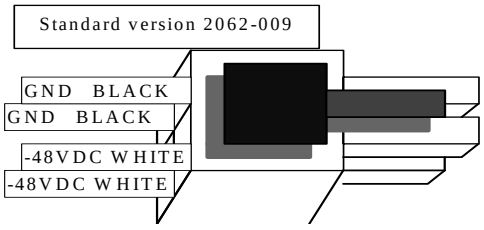
Note: Because the T830 is generally considered to be "permanently connected“, safety standards require that an appropriate disconnect device shall be provided as part of the building installation. The -48VDC input should be protected by an external 2A Slow Blow Fuse conforming to CSA/UL 248-14, IEC 60127-4/2, at the power supply or within the building circuitry as appropriate. The input DC power current limiting fuse circuit is provided for by the end user, and is required for unit operation in compliance with safety agency approvals.

One example of a compliant fuse for the -48V input is a Littelfuse 239P series, 2 amp fuse with a 250 VDC minimum voltage rating and interrupt rating 10,000 amps at 125 VAC, 0.7 to 0.8 power factor and 100 amps at 125VAC, 0.7-0.8 power factor.

CONTENTS:

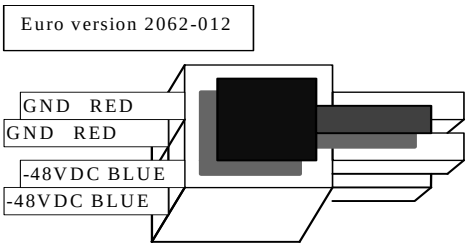
Please inventory the package contents and ensure you have the following items pertaining to the -48VDC Power Option:

1. A cable harness consisting of 2 black or red and 2 white or blue wires connected to a white nylon “molex” connector.
2. A bare white nylon housing.
3. 5 crimp-on contacts.



-48VDC CONNECTION:

The -48VDC power supply option has 4 input connections. This gives the user the ability to connect this unit to an auxiliary -48VDC power source. Note: The dark area on the diagram represents the latching mechanism on the housing.



DANGER! FIRE HAZARD!
DO NOT LEAVE AN UNCONNECTED WIRE EXPOSED!
DO NOT CONNECT THE UNIT TO ANY OTHER EQUIPMENT UNTIL YOU KNOW THE UNIT POWERS UP CORRECTLY!

Option A: Connect the supplied harness assembly to your -48VDC voltage source:

1. Ensure the unit is not connected to any peripheral equipment.
   NOTE: Peripheral Equipment connections may cause a short circuit of your -48V supply if the power connections are reversed! Do not connect peripheral equipment connections until you know the unit is operational by observing the front panel Power LED.
2. Strip the ends of the wires.
3. Using wire nuts (not supplied), connect the stripped wires to the power source. The black (red) wires connect to ground or the most Positive connection on the voltage source. The white (blue) wires connect to -48VDC or the most Negative connection on the voltage source.

Option B: Use the supplied kit to make a wire harness:

1. You will need a crimping tool that crimps standard Molex type 18-24 AWG Mini-Fit Terminals (Molex Part Number: 39-00-0060, Engineering Series 5556).
2. Crimp the supplied terminals to your cable connections.
3. Insert the crimped terminals into the supplied white nylon housing. Orient the housing so the latching mechanism is up and you are looking into the large end of the housing. See diagram above. Insert the 2 Ground or Most Positive leads into the upper and lower compartments on the left side of the connector, e.g. the same positions as the black wires on the supplied harness assembly. Insert the 2 -48VDC or Most Negative leads into the upper and lower compartments on the right side of the connector, e.g. the same positions as the white leads on the supplied harness assembly.
4. Connect the completed assembly into the power input receptacle at the rear of the unit.

Accessing the Command Line

1. Connect to I/O2 with a serial terminal emulation program at 19200 baud, 8N1.
2. Enter **STATUS** or **?** and press <Enter>. You will be presented with a status screen similar to the following.

```
TeleBoss 830 2.03.050 STD  -  Status
Site Name       : 830-830000085
Serial Number   : 830000085        Eth 1    : STATIC
Date            : TUE 03/25/2008   IP Addr  : 0.0.0.0
Time            : 12:53:03         MAC Addr : 00:10:A3:60:01:20
Memory          : 2048K            Eth 2    : STATIC
% Full Alarm    : OFF              IP Addr  : 0.0.0.0
No-Data Alarm 1 : OFF              MAC Addr : 00:10:A3:60:01:21
No-Data Alarm 2 : OFF              Modem    : Yes
Duplex          : HALF
-------------------------------------------------------------------------
Port   Baud/Etc.  Recs     Bytes    Full Wrap Name
IO1  : 19200,8N1  00000000 00000000   0% OFF  I/O 1
IO2  : 19200,8N1  00000000 00000000   0% OFF  I/O 2

COMPLETE
>
```

When the status screen appears, the unit is successfully connected and ready for use.

Network Setup

Setup

1. Access the setup menu by typing **SETUP** and pressing <ENTER>.
2. Select the Network Settings branch.
3. Select A) Ethernet Settings and select the Ethernet interface that corresponds to the one on the back panel that you plugged your network cable into (ETH1).
4. Enter an IP address, subnet mask and--if necessary--a router address.
5. Toggle NAT on/off as desired.
6. Press <ESC> to go back one level in the menu tree, or <CTRL + C> to exit the setup menu and return to the command prompt.

Testing Network Connectivity

1. Verify that the network router is available to the unit by typing the command **PING *IP_address***. A router is always a good candidate to test pings. The following screenshot is an example of a successful ping test.

```
ping 192.168.100.59
PING 192.168.100.59 (192.168.100.59): 56 data bytes
64 bytes from 192.168.100.59: icmp_seq=0 ttl=128 time=8.0 ms
64 bytes from 192.168.100.59: icmp_seq=1 ttl=128 time=0.7 ms
64 bytes from 192.168.100.59: icmp_seq=2 ttl=128 time=1.8 ms
64 bytes from 192.168.100.59: icmp_seq=3 ttl=128 time=0.8 ms
64 bytes from 192.168.100.59: icmp_seq=4 ttl=128 time=0.7 ms
64 bytes from 192.168.100.59: icmp_seq=5 ttl=128 time=0.7 ms

--- 192.168.100.59 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.7/8.0 ms
```

2. Press <CTRL + C> to stop the ping testing. If <CTRL + C> is not pressed, the unit will continue pinging attempts indefinitely.
3. If there is an error message or no response from the router, first check the network settings and connection, then consult your System Administrator or Asentria Technical Support.
4. Using a Telnet client, connect to the IP address assigned to the unit.

SNMP Trap Setup

If you will be using your T830 to send SNMP traps, this section will help you ensure it is set up correctly.

Setup

1. Configure the network settings as described in the previous section.
2. Select the Network Settings then SNMP Settings sub-menu.
3. Verify the SNMP Community name is correct for your network.
4. Switch to the Actions Definitions menu and enter the host name or IP address of the computer to receive the traps into the field, “Hostname/IP Address 1”.
5. Press <CTRL + C> to exit the Setup menu and return to the command prompt.
6. On the computer that will be receiving the SNMP traps, start AlarmManager or your preferred SNMP trap manager.

Testing SNMP Traps

1. Using a Telnet client, connect to the IP address assigned to the unit.
2. Enter the command **DOTRAP** from the T830 command prompt.
3. Verify that the trap manager receives the test trap.
4. If there is an error message or no response from the router, first check the network settings and connection, then consult your System Administrator or Asentria Technical Support.

What is a TeleBoss 830

The Basics

Fig 1: T830-2

The T830 is a powerful remote device management system which can collect and forward text records such as those used by Call Accounting and Telemangement billing applications. These records are collected by the T830 from PBX serial ports, and in some cases directly over a TCP/IP connection. The T830 can also make a passthrough connection directly to devices connected on one of its serial ports, and can also connect you via web or telnet to other devices on the same remote network as the T830. The T830 provides versatile alarm management of text-based alarms as well as interfaces with environmental monitoring equipment and contact closure alarms at your remote site. The T830 is a powerful remote network management solution for Call Accounting systems, Service Bureaus, and end users who need to collect PBX data as well as get remote access, and collect alarms from equipment at remote sites.

Communication Methods
The T830 has a diverse selection of communication methods available for different applications. The following methods can be used to either access the command processor or provide a passthrough connection to devices attached to the serial ports. All methods of connecting to the unit can be secured via password for protection of data and hardware.

- RS-232 serial
- Telnet
- Standard modem serial

Data may be retrieved from or through the T830 by any of the following methods:

- Serial or modem connection to command processor (using Line or Zmodem) or pass-through
- Inline Mode (data in I/O1, data out I/O2)
- Telnet to command processor or passthrough
- Telnet real-time sockets
- FTP push (automatic delivery to FTP server)
- FTP get (manual retrieval from FTP server)

Alarms generated or detected within the T830 can be delivered through any of the following means:

- Modem callout
- SNMP trap
- Email
- Asentria Alarms
- Relays (if configured with optional relay Expansion Card)

Data Storage

Basic data storage in the T830 is accomplished in a database of four files – FILE1, FILE2, EVENTS, and AUDIT. FILE1 and FILE2 are typically associated with Serial Port I/O1 and Serial Port I/O2 respectively, although either serial port can store to either FILE1 and FILE2, or both. Data collected via IP Record Collection (IPRC) is also typically stored to either FILE1 or FILE2. EVENTS and AUDIT are log files generated from the Event Log Settings and Audit Log Settings menus per the parameters set there. The number of records stored in each these four files can be displayed using the **DIR** command on any connection to the command processor, including FTP.

Remote Access
The T830 can provide an administrator transparent access to devices connected to the serial ports of the unit via passthrough connections or through the login menu in the web interface, Telnet and modem connections. This sort of access can be used to configure, maintain, or manipulate devices that would normally have no remote access.

Serial Monitoring (Data Events)
The T830 has the capability to monitor incoming data for user-defined strings and then report the event via several avenues. The T830 allows for up to 64 different data events. Each data event contains independent actions, counters, and other unique settings. Data events triggered within the T830 can be logged to an Event Log. This file can be viewed through the Event Log section of the setup menu, via the **TYPE EVENTS** command, or through FTP.

Event Notification
Actions generated or detected within the T830 can be delivered through any of the following means:

- Modem callout
- SNMP trap
- Email
- Asentria Alarms
- Relays (if configured with optional relay Expansion Card)

Audit Log
The T830 has the capability to log many types of administrative events, from DIP switch changes to login attempts. These Audit Log entries are stored in a file and can be viewed through the Audit Log section of the setup menu, via the **TYPE AUDIT** command, or through FTP.

Parts Identification

Features and Accessories

Standard Equipment
The base T830 comes with the following standard on-board equipment:
- AC or DC Power Input
- 1MB logging database for CDR or other text records
- 2 – RJ45 DTE serial I/O ports
- 2 – 10/100Mb Ethernet interfaces
- 1 – MMC memory I/O slot
- 2 – Expansion Card slots
- Internal battery backup that preserves clock operation when power is not present. Data records and settings are stored in non-volatile memory and therefore do not require backup.

In addition to the above components, the standard unit is shipped the following accessories:
- This product manual and Asentria Alarm Manager software on the Documentation and Software CD
- RJ45 M-M unshielded serial cable and RJ45/DB9 straight thru adapter for each serial port ordered
- RJ45 Ethernet cables for each Ethernet port
- Power supply adapter (for AC units), or wiring harness and Molex plug (for DC units)

Options
Each of the following components is optional and may be installed on a T830:
- Additional RJ45 DTE serial ports in sets of 4
- On-board 56K dialup modem
- Run-time battery (enables the unit to function for a period of time without power, if enabled).
- Expansion Cards configured as wireless modem, ADSL modem, contact closures, analog sensors, and relays.

The T830 may come with any of the following accessories as well, depending on the configuration or order:
- Modem cable if that option is ordered

LEDs, Ports, DIP Switches and Buttons

Fig 2: Front panel (T830-2)

LEDs – Front Panel

Note: When the T830 firmware is upgraded, the front panel LEDs flash in a specific pattern. This is described, along with FTP upgrade procedures in the Upgrading the T830 section of the Features chapter.

Power
The Power LED is green and has two operational states. During the boot up cycle, it will blink once every second until the boot sequence is complete. During normal operation, it is steady on with a blink every 5 seconds.

MDM (Modem)
The MDM LED lights solid green whenever the modem is connected and blinks when the modem is dialing out.

ETH (Ethernet)
The Link LED lights solid green whenever an active Telnet or FTP connection is made to the unit.

ALM (Alarm)
This LED is reserved for future use.

25% - 75% - 100%
The T830 has three LEDs to indicate file full status. A blinking percentage full LED indicates the database has less than the amount indicated by that LED, but more than the previous. A solid lit LED indicates the database percentage is at or over the value for that LED.

Expansion Card *n*
Each optional Expansion Card has eight LEDs associated with it.

LEDs – Back Panel

Each RJ45 port on the back panel has two LEDs associated with it – one on the Right of the port, one on the Left of the port.

Ethernet Ports (ETH1 and ETH2)

- Right – Lights solid red when an Ethernet cable is connected to the port and an active Ethernet network. The LED is off when the cable is disconnected from the network, or the Ethernet Port.
- Left – Flashes yellow/green when network data (tcp packets) is being transmitted or received across the port. When no data is actually being transmitted/received, this LED is off.

I/O Port 1 & 2 (and any additional 4-I/O Port cards that may be installed)

- Right – Lights solid green when a correctly configured cable from another device is connected to it. Otherwise this LED remains off. As the I/O Port receives or transmits data, this LED will flash red.
- Left – Lights solid green when power is applied to the T830, regardless of whether a cable is connected to the I/O Port or not.

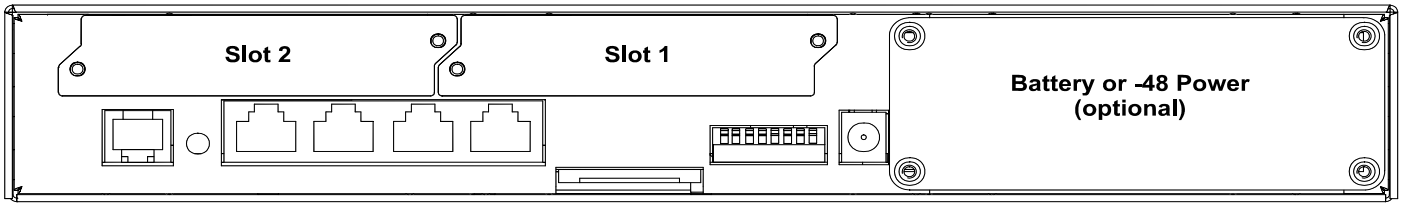


Fig 3: Back panel T830-2 (11”- wide model)

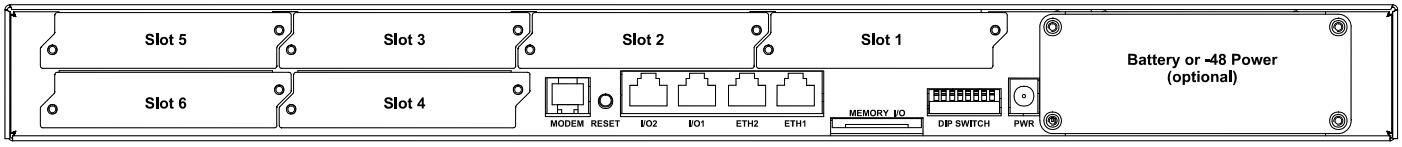


Fig 4: Back panel T830-6 (17”- wide model)

The above drawings show the T830 configured (from right to left) with a bay for the optional run-time battery, (bottom) AC power jack, bank of 8 DIP switches, MMC memory I/O card slot, two RJ45 Ethernet ports, two RJ45 RS232 serial ports, Reset button, one RJ11 POTS modem port, and either two or six "slots“ or expansion bays for optional Expansion Cards that expand the functionality of the unit with wireless modem, ADSL card, and a variety of sensor and relay I/O.

Ports

Memory I/O
The slot labeled Memory I/O is reserved for future use. Eventually T830’s may be upgraded using a MultiMedia Card (MMC) in this slot.

Ethernet
The Ethernet 10/100Mb interfaces are standard RJ45. Either of these standard connectors will connect the T830 to an Ethernet hub or switch. Refer to the Telnet/TCP Connections section in the Features chapter for further information regarding a number of different types of telnet connection options. LEDs by each Ethernet connection on the back panel flicker when packets are being transmitted/received on that port.

Serial Ports
Each of the two (or more) serial ports is configured as a DTE port using an RJ45 connector. This is the standard recommended pinout for EIA/TIA-561 for 8 pin RJ45 connector:

PIN1 =RI =RING INDICATOR, INPUT to the T830
PIN2 =DCD =CARRIER DETECT, INPUT to the T830
PIN3 =DTR =DATA TERMINAL READY, OUTPUT from the T830
PIN4 =SIGNAL GROUND
PIN5 =RXD =RECEIVED DATA, INPUT to the T830
PIN6 =TXD =TRANSMITTED DATA, OUTPUT from the T830
PIN7 =CTS =CLEAR TO SEND, INPUT to the T830
PIN8 =RTS =REQUEST TO SEND, OUTPUT from the T830

The DB9 female cable end which mates with the serial port connectors of connected devices will often have a pair of screw-down cable screws. These cable screws should be used to assure a solid connection of the cable with the device.

Default settings for the serial ports are 19200-baud, 8-bit word length, no parity, and one stop bit (19200, 8N1). Use the internal setup menu to adjust these settings.

Internal Modem
If a dialup POTS modem is installed, an RJ11 (typical U.S. phone) connector is used. A POTS (analog) dialup phone line is inserted into this connector.

The modem installed within this unit is FCC certified. For further information, consult the Internal Modem Guidelines appendix or the serial number label on the bottom of the T830.

DIP Switches

The bank of 8 DIP switches on the back panel of the T830 are used to control the baud and parity settings of I/O2, to set the operational mode for I/O2, and to put the unit into "boot load mode" where it can be forced to load a new application (firmware image). The following table shows how to set the various DIP switches to obtain certain settings:

I/O 2 Baud	**SW1**	**SW2**
2400	OFF	OFF
9600	ON	OFF
19200	OFF	ON
115200	ON	ON
I/O 2 Word, Parity	**SW3**	
8N1	OFF	
7E1	ON	
I/O 2 Mode	**SW4**	
Command Mode	OFF	
Data Mode	ON	
Boot Load Mode	**SW8**	**SW1 thru SW7**
No Forced App Reload (Default)	OFF	X (don't care)
Forced Application Reload	ON	ON

Note: Boot Load Mode can only be set by flipping ALL DIP switches to the ON or UP position. This is not a setting that can be configured via internal menu settings, or Setting Keys.

Note: For settings that can be set either via DIP switch, internal menu settings, or Setting Keys, the T830 always pays attention to the last setting, regardless of how it was done. So if the internal setting for I/O2 Mode is Command, and someone flips SW4 to the ON or UP position, the Mode is immediately set to Data.

Buttons

The only button on the T830 is the Reset button located on the back panel next to the left of serial port I/O 2.

Getting Connected

Power Up Sequence

On startup, the T830 goes through the following boot sequence in approximately 55 seconds:

1) The power LED flashes once each second for 30 seconds.
2) The LED for Expansion Card 1 go through a 15 second flashing sequence.
3) All LED's then go off for approximately 5 seconds.
4) Power, Modem (if installed) and Ethernet LEDs light for 5 seconds, then Modem and Ethernet go off.
5) Power LED will blink once every 5 seconds as a "heartbeat" while the T830 is powered on.

Default Passwords

The T830 uses a very flexible system for managing users, passwords, and access rights. By default, the following four user profiles are enabled. Note that if a password is defined without a user name, the profile is defined just by the user name. All of the default profiles are password-only. All passwords are masked: ********

The default settings are configured to low security for your convenience in setup. It is highly recommended that you change these passwords and record them in a secure location.

User	Password	Login To
User1	SMDR	Command processor
User2	SUPER	Command processor
User3	ACCESS1	Passthrough/File 1
User4	ACCESS2	Passthrough/File 2

The Status Screen

The T830 Status screen is the unit's one-stop informational source. Most of the information that a user would need to know about the unit is available through this display. This section outlines this data and highlights why it is useful.

```
TeleBoss 830 2.03.050 STD  -  Status
Site Name       : 830-830000085
Serial Number   : 830000085        Eth 1    : STATIC
Date            : TUE 03/25/2008   IP Addr  : 0.0.0.0
Time            : 12:53:03         MAC Addr : 00:10:A3:60:01:20
Memory          : 2048K            Eth 2    : STATIC
% Full Alarm    : OFF              IP Addr  : 0.0.0.0
No-Data Alarm 1 : OFF              MAC Addr : 00:10:A3:60:01:21
No-Data Alarm 2 : OFF              Modem    : Yes
Duplex          : HALF
-------------------------------------------------------------------------
Port   Baud/Etc.  Recs     Bytes    Full Wrap Name
IO1  : 19200,8N1  00000000 00000000   0% OFF  I/O 1
IO2  : 19200,8N1  00000000 00000000   0% OFF  I/O 2

COMPLETE
>
```

TeleBoss 830 indicates that this product is the T830, followed by **2.03.050,** the currently loaded firmware version.

Site Name is the identifier assigned to each T830 by the end user in the General Settings menu.

Serial Number is the factory-assigned, unique serial number for this T830.

Date and **Time** display the current date and time.

Memory indicates the amount of flash memory configured for storage of data.

% Full Alarm / No Data Alarm *n* indicates the current ON/OFF status of the % Full Alarm, and No Data Alarms 1 and 2, respectively.

Duplex controls the echo settings for the command processor. Full duplex causes the T830 to echo all characters sent to the remote device. Half duplex turns off character echo.

Eth 1 and **Eth 2** displays STATIC, or DHCP, depending on which mode each of the two Ethernet interfaces is configured for.

IP Add and **MAC Add** immediately following Eth 1 and Eth 2 are the network IP address assigned to each Ethernet card, and that cards MAC address. The MAC address of both Ethernet cards can also be found on the unit's serial number label.

Modem indicates whether the optional internal modem is installed.

The default serial port names of **I/O 1, 2, etc** are displayed for each of the installed serial ports along with the following information:

Baud/Etc. displays the baud rate, word length, parity, and stop bit settings for each installed serial port.

Recs shows the number of carriage return-delimited records stored within the file associated with each serial port.

Bytes displays the amount of storage allocated for the above records.

Full is a rough percentage indicator of how much data is stored in a particular file.

Wrap indicates the ON/OFF status of whether file wrapping is enabled on a particular port. When ON, a unit that is 100% full will overwrite the oldest buffered records with new ones.

Name displays the target name, which is an optional name given to the device connected to the port. This target name is used in event notifications and can be configured in the Serial Settings menu for each port.

Setup Menu

Overview

This section displays screen shots and descriptions taken from the command prompt menu system. However, the menu structure and options are the same as the web interface.

The Setup menu contains all of the configuration options available on the T830. It is organized in a logical tree structure with all settings classified under the following groups:

```
TeleBoss 830 - Main Setup Menu
A) Network Settings
B) Serial Settings
C) Modem Settings
D) User Profile Settings
E) Alarm/Event Definitions
F) Action Definitions
G) General Settings
H) Event Log Settings
I) Audit Log Settings

Enter your Selection:
```

Each section in this chapter will go over one of the above setup branches, outlining the options within.

Press either <ESC> or <ENTER> to go back one level in the menu tree, or <CTRL + C> to exit any menu and return to the command prompt.

Since this product allows for multiple simultaneous command processors, two administrators could conceivably change the same option at the same time, but due to the multitasking nature of the T830, the changes are processed in the order received.

The T830 processes setup changes in real time. In other words, the unit begins to implement changes to its configuration as soon as they are entered. There is no need to exit a setup menu or reboot the unit to apply changes. The exception to this rule is IP-specific network settings. Changes to these settings are implemented only after all open Telnet command processors are closed.

Option Types

String entry

There are several different types of inputs employed within the setup menu. The most common is the string type entry:

```
  A) Site Name                    [Test Site]
```

When selected, this setting will provide a prompt requesting a new value. You may press <ENTER> or <ESC> to abort the option entry or press <SPACE> and <ENTER> to delete the current value and leave it blank. Some numerical or required settings will not allow an you to leave an option blank, so pay attention to the unit's response when attempting to delete a setting's value.

Toggle

The second most common option type is the toggle type option:

```
  A) Enable Web Interface       [OFF]
```

When selected, this option will not prompt for a new value. It will simply cycle to the next available option in its list. This switch type is typically used for options with two or three choices. Most often it is in an ON/OFF form, but could be a series of options such as "NONE", "1", and "2".

Alarm actions (action list)
Alarm actions have their own unique method of entry. Refer to the Action List section in the Features chapter for more information.

Option list
The option list type is similar to the toggle type in that it has a list of options to choose from:

```
TeleBoss 830 - Serial Port 2 Baud Rate
A) 300
B) 600
C) 1200
D) 2400
E) 4800
F) 9600
G) 19200
H) 38400
I) 57600
J) 115200
```

After selecting an option, you are immediately returned to the previous menu. The new value will be displayed to the right of the setting name, letter, or number.

Web Interface

The T830 has a built-in HTTP web server that can be used to configure the unit from anywhere the unit can be accessed on the network or Internet. Once you have enabled it through the network section of the Setup Menu, simply connect to ***http://<IP address of T830>***

You will be greeted by a login screen. Log in with your Login ID (Username) and Password. These are the same credentials you would use to log into the command prompt. Once logged in, the General Status screen will be displayed, with a menu bar across the top of the page that displays the same menu options as the command prompt menu system. From here, you can alter any setting in the same way you could via the prompt.

Main Setup Menu

```
TeleBoss 830 - Main Setup Menu
A) Network Settings
B) Serial Settings
C) Modem Settings
D) User Profile Settings
E) Alarm/Event Definitions
F) Action Definitions
G) General Settings
H) Event Log Settings
I) Audit Log Settings
```

Network Settings contains settings for network communication, SNMP, FTP, Email, and more.

Serial Settings contains settings pertaining to the function of each serial port.

Modem Settings contains modem init settings and modem-specific security options.

User Profile Settings contains all of the user profiles and global security settings.

Alarm/Event Definitions contains all of the settings that define events within the T830.

Action Definitions contains configurations for all of the actions possible when events are detected.

General Settings contains the site name, answer string, confirmation prompt, date/time, and other general settings.

Event Log Settings allows for configuration and displaying of the Events Log.

Audit Log Settings allows for configuration and displaying of the Audit Log.

Network Settings

The Network Settings menu contains all of the options pertaining to network communication.

```
TeleBoss 830 - Network Settings
A) Ethernet Settings
B) Default Router                       [192.168.100.2]
C) Name Resolution Settings
D) Telnet Duplex                        [FULL]
E) Inactivity Timeout                   [0]
F) IP Record Collection Settings        [OFF]
G) Web Interface Settings               [ON]
H) SNMP Settings
I) FTP Settings
J) Email Settings
K) Real-Time Socket Settings
L) Static Route Settings
M) DSL Settings
N) VPN Settings
   Note: Changes to IP Address, Subnet Mask, or Router
         Address will not take effect until any open
         Telnet command processor sessions are ended.
```

Ethernet Settings displays the menu where you can configure each of the two Ethernet interfaces.

Default Router displays the configured default router (gateway) for the unit. Refer to the Default Router section in the Features chapter for more information.

Name Resolution Settings allows you to configure the IP addresses of up to two Domain Name Servers (DNS).

Telnet Duplex controls the echo settings for Telnet. Full duplex causes the unit to echo all characters sent to the remote device. Half duplex turns off character echo. Default setting is Full.

Inactivity Timeout sets the number of minutes (0 - 255) before a network connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated. Default setting is 0.

IP Record Collection Settings displays the IP Record Collection Settings menu where the Avaya Reliable Session Protocol (RSP) can be configured to collect data from Avaya IP-enabled switches that support RSP.

Web Interface Settings displays the Web Interface Settings menu where you can toggle the web interface ON or OFF, set the session timeout (0 - 65535 minutes), and set the TCP port number for the web connection.

SNMP Settings displays the SNMP Settings menu where you can configure the SNMP community name, and spoofed PPP/Trap IP address.

FTP Settings displays the FTP Settings menu, where you can configure automatic FTP pushes of buffered data.

Email Settings displays the Email settings menu, where you can configure the SMTP server address, Email domain name, and authentication parameters.

Real-Time Socket Settings displays the Real-Time Socket Settings menus where you can configure real-time socket settings for each file of buffered data. Real-Time Sockets are used to collect data on TCP port 2201 from a serial port in real-time, while buffering data if the network connection goes down.

Static Route Settings displays the Static Route Settings menu where you can configure static network routes.

DSL Settings displays the DSL Settings menu where settings are configured so the T830 can communicate using the optional ADSL Modem.

VPN Settings displays the VPN Settings menu where settings are configured so the T830 can communicate with the optional Asentria SitePath secure, unified administration portal software.

Ethernet Settings

Ethernet Settings displays the following menu where each of the two installed Ethernet cards can be configured:

```
TeleBoss 830 - Ethernet Settings
A) Ethernet 1
B) Ethernet 2

Enter your Selection: a

TeleBoss 830 - Ethernet 1 Settings
A) Mode                                [STATIC]
B) IP Address                          [0.0.0.0]
C) Subnet Mask                         [255.255.255.0]
D) Router Address                      [0.0.0.0]
E) NAT                                 [ON]
```

Mode toggles between STATIC or DHCP – whichever is appropriate for this Ethernet port. Default setting is STATIC.

IP Address is the network address assigned to this Ethernet card. Default setting is 0.0.0.0

Subnet Mask sets the network subnet mask provided by the network administrator. Default setting is 255.255.255.0

Router Address sets the router address provided by the network administrator. Default setting is 0.0.0.0

NAT is an ON/OFF toggle to enable Network Address Translation. Default setting is ON.

Note: The T830 does not heed changes to network configurations while you are connected to a command processor via Telnet or web interface. Changes, including population of the candidate default router set, are pended until all network-based command processor sessions have ended. Open FTP and RTS connections will fail if these settings are changed during an open connection.

Name Resolution Settings

```
TeleBoss 830 - Name Resolution Settings
A) DNS Server 1                        [0.0.0.0]
B) DNS Server 2                        [0.0.0.0]
C) DNS Mode                            [MANUAL]
```

DNS Server 1 / **2** are the IP addresses of Domain Name Servers that you may want to configure so that you can use host names rather than IP addresses in functions where name resolution may be needed, such as; Email server, RTS push hosts, action IP settings, network time servers, etc. Default setting for each DNS Server is 0.0.0.0.

DNS Mode toggles between MANUAL, ETH1-DHCP and ETH2-DHCP. Default setting is MANUAL.

IP Record Collection Settings

```
TeleBoss 830 - IP Record Collection (IPRC) Setup
A) IP Record Collection                 [OFF]
B) Store Collected Data In              [FILE1]
C) Data Alarm/Filter Enable             [OFF]
```

IP Record Collection selects and displays a configuration menu for Avaya Reliable Session Protocol, the only IPRC protocol that the T830 supports. Default setting is OFF.

Store Collected Data In sets the data file in which to store records received via IPRC. Default setting is FILE1.

Data Alarm/Filter Enable is an ON/OFF toggle to enable alarming or filtering of incoming data. Default setting is OFF.

» **Note:** Refer to the IPRC chapter for a detailed explanation of IPRC.

Web Interface Settings

```
TeleBoss 830 Web Interface Settings
A) Enable Web Interface                          [ON]
B) Web Session Timeout                           [30]
C) Web Connection Port                           [80]
```

Enable Web Interface is an ON/OFF toggle to enable the T830's internal web server. Default setting is ON.

Web Session Timeout sets the number of minutes (0 - 65535 minutes) a connection may remain idle before expiring. A setting of 0 means the connection will never automatically expire. Default setting is 30.

Web Connection Port is the TCP port through which the web connection is made. Default setting is Port 80.

SNMP Settings

```
TeleBoss 830 - SNMP Settings
A) SNMP Community                       [public]
B) PPP/Trap IP Address Spoofing         [0.0.0.0]
```

SNMP Community sets the SNMP community name to use. Default setting is Public. (Max length is 23 chars)

PPP/Trap IP Address Spoofing allows you to configure the IP address to be displayed in an SNMP trap sent over a PPP connection. If undefined, the T830 PPP IP is used. Default setting is 0.0.0.0

» **Note:** SNMP traps are *not* a guaranteed means of delivering notifications. Traps are a one-way network datagram and the device receiving traps does not acknowledge them. Therefore, if the trap does not reach its intended destination for whatever reason, the T830 has no way of recognizing this and resending the trap.

FTP Settings

```
TeleBoss 830 - FTP Settings
A) FTP Push Enable                      [OFF]
B) FTP Server Address                   []
C) Username                             [Default FTP Username]
D) Password                             [********]
E) Account                              []
F) Directory                            []
G) Minutes Between Push Attempts        [1440]
H) Select Files to Push
I) Remote File Names
```

FTP Push Enable toggles between OFF and REGULAR. Default setting is OFF.

FTP Server Address is the IP address or host name of the FTP server to push to. (Max length 64 chars)

Username/Password defines the login credentials that are able to access the remote FTP server. (Max length Username is 126 chars) (Max length Password is 31 chars)

Account is a third login option used only on some FTP servers. Consult your network administrator to see if this is necessary. (Max length 126 chars)

Directory is the path used to transfer the file(s). The file(s) is transferred to the root login directory if this option is left blank. (Max length 253 chars)

Minutes Between Push Attempts sets the number of minutes (1 to 9999) between FTP push attempts. Default setting is 1440 minutes.

Select Files to Push displays the FTP File Selection menu where you can select which files are pushed by toggling ON or OFF. Default setting for all is ON, except for Audit Log, which is OFF.

```
TeleBoss 830 - FTP File Selection
A) Data File 1                          [ON]
B) Data File 2                          [ON]
C) Events File                          [ON]
D) Audit Log                            [OFF]
```

Remote File Names displays the FTP File Names menu where you can give each file a name other than the default name, and/or prepend a date, time, and/or unique sequence # to the file name.

```
TeleBoss 830 - FTP File Names
A) Include Date in Filename             [OFF]
B) Include Time in Filename             [OFF]
C) Include Sequence #s in Filename      [OFF]
D) Data File 1                          [FILE1]
E) Data File 2                          [FILE2]
F) Events File                          [EVENTS]
```

Include Date/Time in Filename is an ON/OFF toggle to enable the addition of the file transfer date and/or time to the beginning of the name of each transferred file of data. Default setting is OFF.

Include Sequence #s in Filename is an ON/OFF toggle to enable the addition of a unique sequence number to the beginning of the name of each transferred file of data. This ensures that no two transfers will have the same file name. Default setting is OFF.

Data File *n* / Events File are text-entry fields where the name each data file will have on the remote server (not including any date, time, or sequence numbers) can be configured.

Once FTP Push has been configured, entering the **PUSHTEST** command will test the connectivity to the FTP server and write a "log in" and "log out" entry to the Status File in the directory you configured. No data is pushed with this command. Connection data displayed on the terminal screen is useful if the connection fails.

An immediate push of data can be done using the **PUSHNOW** command.

Email Settings

```
TeleBoss 830 - Email Settings
A) SMTP Server Hostname/IP Address      []
B) Email Domain Name                    [asentria.com]
C) Authentication (LOGIN)               [OFF]
```

SMTP Server IP Address sets the hostname or IP address of the outbound mail server. (Max length 64 chars)

Email Domain Name sets the *@domain_name.com* to use when the T830 sends an Email. Default setting is "asentria.com". (Max length 48 chars)

Authentication (LOGIN) displays a menu to configure the credentials that may be required by your server for SMTP authentication. Some SMTP servers require an authentication to relay Emails. Default setting is OFF.

```
TeleBoss 830 - Email Authentication Settings
A) Authentication Enabled               [OFF]
B) Username                             []
C) Password                             [********]
```

Authentication Enabled is an ON/OFF toggle to enable Email authentication. Default setting is OFF.

Username/Password defines the login credentials. (Max length for each is 48 chars)

A typical Email notification for a No Data alarm might look like the following:

```
From: Asentria TeleBoss 830  [mailto:Asentria_ TeleBoss 830 @Asentria.com]
Sent: Wednesday, March 12, 2008 3:59 PM
To: support@Asentria.com
Subject: Event

03/12 15:59 :: 830000085 :: No-Data 1 Alarm :: No Data Alarm Message
```

Real-Time Socket Settings

```
TeleBoss 830 - Real-Time Socket Setup
A) FILE1
B) FILE2
C) EVENTS

Enter your Selection: a

TeleBoss 830 - FILE1 Real-Time Data Socket Setup
A) Real-Time Socket Mode                [LISTEN]
B) Show Answer String on Connection     [ON]
C) Require Xon to Start Data Flow       [OFF]
D) Idle Connection Close Timer          [0]
E) Close Socket When File Empty         [OFF]
F) Real-Time Socket Push Hostname/IP    []
G) Real-Time Socket Push Port Number    [3000]
H) Real-Time Socket Push Retry Timer    [5]
```

Real-Time Socket Mode can be toggled to LISTEN, PUSH, and OFF. When set to LISTEN this functions like traditional real-time sockets on TCP port 2201. When set to PUSH the unit tries to make a TCP connection on the TCP port specified in G) Real-Time Socket Push Port Number. As long as a connection exists, the unit sends all data in the specified file on the connection as data become available. Default setting is LISTEN.

Show Answer String on Connection is an ON/OFF toggle to enable the prompt indicating successful connection to the Real-Time Socket (RTS) port. Default setting is ON.

Require Xon to Start Data Flow is an ON/OFF toggle to enable the Xon/Xoff data flow control requirement. Default setting is OFF.

Idle Connection Close Timer sets the number of seconds (0 – 255) to wait before disconnecting an idle connection. A setting of 0 means the connection will never automatically close. Default setting is 0.

Close Socket When File Empty is an ON/OFF toggle to set whether or not the T830 will automatically terminate the RTS connection when the file for this port has been emptied. Default setting is OFF.

Real-Time Socket Push Hostname/IP sets the hostname or IP address of the server where the unit will push the data if the RTS Mode is set to Push. (Max length is 64 chars)

Real-Time Socket Push Port Number sets the TCP port number the RTS push should use. Default setting is port 3000.

Real-Time Socket Push Retry Timer sets the number of minutes (1 – 255) to wait before retrying an RTS push that has previously failed. Default setting is 5 minutes.

Static Route Settings

```
TeleBoss 830 - Static Route Settings
A) Route 1
. . .
H) Route 8

Enter your Selection: a

TeleBoss 830 - Static Route 1 Settings
A) Enable                               [OFF]
B) Destination Network                  [0.0.0.0/0]
C) Gateway                              [0.0.0.0]
D) Interface                            [NONE]

Enter your Selection:
```

Static routes are network routes that specify in a more or less permanent way (*static*) that traffic to a certain destination (destination host or destination network) gets *routed* out a certain interface or via a certain gateway. Static routes gives you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different routes.

Enable is an ON/OFF toggle to enable a static route. Default setting is OFF

Destination Network is the network notation, i.e., w.x.y.z/s, where s is the significant bits. Default is 0.0.0.0/0.

Gateway is the IP address of the gateway. Default setting is 0.0.0.0

Interface toggles through all of the interfaces' available on this T830 – Ethernet 1, Ethernet 2, Dialup Modem PPP, Wireless Modem PPP (WPPP), and NONE. Default is NONE.

Refer to the Static Routes section in the Features chapter for a detailed explanation of Static Routes.

DSL Settings

```
TeleBoss 830 - DSL Settings
A) Start Mode                          [MANUAL]
B) Type                                [PPPOA]
C) VPI                                 [0]
D) VCI                                 [0]
E) Encapsulation                       [VCM]
F) Mode                                [BRIDGED]
G) Username                            []
H) Password                            [********]
I) IP Address                          [0.0.0.0]
J) Mask                                [0.0.0.0]
K) Router                              [0.0.0.0]
```

Following describes the menu options for configuring the optional ADSL Modem. For more information regarding the operation of the ADSL modem, Setting Keys, DSL Routing example, and DSL Glossary, please refer to the ADSL Modem chapter later in this manual.

Start Mode toggles between MANUAL and AUTO to set how the DSL interface is to be raised. Set this to MANUAL to require user intervention to raise the DSL interface, or to let a VPN (if it is configured to use DSL) raise the DSL interface when the VPN needs to use DSL. Set this to AUTO to tell the unit to automatically raise the DSL interface upon boot. Default setting is MANUAL.

Type toggles between PPPoA, PPPoE, Static, or DHCP. This should be set as directed by your ADSL provider. This is the most important DSL setting since its value determines what other DSL settings are applicable to the DSL configuration. Default setting is PPPoA.

VPI sets the VPI (Virtual Path Identifier) used on the DSL interface. This should be set as directed by your ADSL provider and is required for DSL operation. Values are: 0 to 4095 Default setting is 0.

VCI sets the VCI (Virtual Channel Identifier) for the DSL interface. This should be set as directed by your ADSL provider and is required for DSL operation. Values are: 0 to 65535. Default setting is 0.

Encapsulation toggles between VCM and LLC to control whether the encapsulation is LLC (Logical Link Control) or VCM (Virtual Channel Multiplexed). This should be set as directed by your ADSL provider and is required for DSL operation. Default setting is VCM.

Mode toggles between BRIDGED and ROUTED to control whether the DSL is set up for Bridged mode or Routed mode when the DSL type is STATIC. Default setting is BRIDGED.

Username and **Password** specify the PPP Username and PPP Password for the DSL interface when the DSL type is set to PPPoA or PPPoE. These should be set as directed by your ADSL provider and are required for DSL operaton. Values are text strings, max length 64 characters.

IP Address sets the public IP address of the unit in the case where the DSL link is active. If the DSL type is STATIC, the user needs to set this. If the DSL Type if DHCP, it is set automatically. This should be set as directed by your ADSL provider. Value is a dotted quad IP address. Default setting is 0.0.0.0

Mask sets the subnet mask used on the DSL interface. If the DSL type is STATIC, the user needs to set this. If the DSL Type if DHCP, it is set automatically. This should be set as directed by your ADSL provider. Value is a dotted quad subnet mask. Default setting is 0.0.0.0

Router sets the router for the DSL interface. If the DSL type is STATIC, the user needs to set this. If the DSL Type if DHCP, it is set automatically. This should be set as directed by your ADSL provider. Value is a dotted quad IP address. Default setting is 0.0.0.0

VPN Settings

```
TeleBoss 830 - VPN Settings
A) VPN 1
B) VPN 2
C) CPE Settings
D) Commissioning Settings
```

Following describes the menu options for configuring VPN Settings. These settings are only for use with the Asentria SitePath secure, unified administration portal software. Contact Asentria Technical Support for further information.

VPN 1 and **VPN 2** display a sub-menu where each of two VPN connections can be configured.

CPE Settings displays a series of sub-menus where the IP address (both Real and Alias), name, description, and keep-alive period for up to 64 CPE (Customer Premises Equipment) can be set.

Commission Settings displays a sub-menu where all the parameters for commissioning the T830 with the SitePath application are configured.

Serial Settings

```
TeleBoss 830 - Serial Settings
A) 1-I/O 1 Settings
B) 2-I/O 2 Settings
```

Note: All serial ports are set to function in Data mode, except for I/O 2, which can also be set to function in one of two other modes: Command and Inline. Default is Command Mode. Therefore the I/O 2 Settings menu has all the options of I/O 1, plus a few others that I/O 1 does not have. Those options that are exclusive to I/O 2 will be indicated as such below – all others are applicable to all ports.

Serial Port Menu

```
TeleBoss 830 - Serial 2
A) Target Name                          [I/O 2]
B) Baud Rate                            [19200]
C) Data Format                          [8N1]
D) Handshaking                          [NONE]
E) Wrap Around                          [OFF]
F) Record Stamping
G) Character Masking                    [ON]
H) Data Alarm Enable                    [OFF]
I) Store Data To                        [2]
J) Store Alarms During Pass-Through     [OFF]
K) Duplex                               [FULL]
L) Inactivity Timeout                   [0]
M) Port Mode                            [COMMAND]
N) Inline Mode Handshaking              [XON/XOFF]
O) Strip Sent Pass-Through LFs          [OFF]
P) Strip Received Pass-Through LFs      [OFF]
Q) Disable Serial Setup via DIP Switch  [OFF]
R) Data Type                            [ASCII]
S) Change ETX to CR/LF                  [OFF]
```

Target Name is the name given to the device connected to the other end of each port. The target name is used in event notifications. Default setting is I/O n. (Max length is 24 chars)

Baud Rate displays a selection menu for baud rates available for the port. These values range from 300 baud to 115200 baud. Default setting is 19200.

Data Format toggles settings for word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, 7N1, and 8O2. Default setting is 8N1.

Handshaking is a toggle item with the following options: None, Xon/Xoff, Both, and DTR. Default setting is None.

Wrap Around is an ON/OFF toggle to set whether the incoming data will wrap (overwrite) the oldest data in the file should it become full. Default setting is OFF.

Record Stamping displays a menu that allows you to select whether the Date/Time and/or the Unit ID are pre-pended to each incoming data string. Default setting for Date/Time and Unit ID is OFF.

Character Masking is an ON/OFF toggle to enable the character mask. The character mask allows you to block most non-printing ASCII characters. Specifically, the following ASCII character values are blocked: 0, 1, 4-9, 11, 12, 14-31, and 128-255. Default setting is ON.

Data Alarm Enable is an ON/OFF toggle to enable data alarm monitoring for this port. Default setting is OFF.

Store Data To displays a menu that allows you to toggle ON/OFF the files to which incoming data on this port should be stored, if any.

Store Alarms During Pass-Through is an ON/OFF toggle to determine whether data strings that meet data alarm criteria are stored in the Events File when a pass-through session is active on this port. Default setting is OFF.

Duplex (Port 2 only) toggles between Full and Half. Full duplex causes the unit to echo all characters sent to the connected terminal when in Command mode. Half duplex turns off character echo. Default setting is FULL.

Inactivity Timeout (Port 2 only) is the time (1 - 255 minutes) before a serial connection with no activity will be terminated. A setting of 0 means an inactive connection will not be terminated. Default setting is 0.

Port Mode sets the port function. This is set to DATA for I/O 1 and cannot be changed. This can be toggled between COMMAND, DATA, and INLINE for I/O 2. COMMAND allows for serial command processor access, DATA configures the port as an inbound data port just like I/O 1, and INLINE causes the unit to perform a direct connection between I/O 1 and I/O 2.

Inline Mode Handshaking (Port 2 only) toggles the handshaking method used during Inline mode operation. Available options are XON/XOFF, DTR, Both, and None. Default setting is XON/XOFF.

Strip Sent Pass-Through LFs is an ON/OFF toggle to enable the stripping of linefeeds on pass-through data *sent out* of the T830. Default setting is OFF.

Strip Received Pass-Through LFs is an ON/OFF toggle to enable the stripping of linefeeds on pass-through data *received* by the T830. Default setting is OFF.

Disable Serial Setup via DIP Switch is an ON/OFF toggle to disable the DIP switches. Default setting is OFF.

Data Type toggles between ASCII and Binary to indicate the type of data being collected on this port. Default setting is ASCII.

Change ETX to CR/LF is an ON/OFF toggle to set whether ETX characters in the incoming data should be converted to CR/LF characters. Default setting is OFF.

Modem Settings

```
TeleBoss 830 - Modem Settings
A) Dialup Modem
B) Wireless Modem
```

The Modem Settings menu displays two sub-menus for configuring either the internal 56K modem, or a optional wireless modem expansion card.

Dialup Modem

```
TeleBoss 830 - Dialup Modem Settings
A) Data Format                          [8N1]
B) Duplex                               [FULL]
C) Init String                          [ATM1]
D) TAP Init String                      [ATM0]
E) Inactivity Timeout                   [0]
F) Upon Modem Connect Go Directly To    [LOGIN]
```

Note: If the optional 56K dialup modem is not installed in the T830, this menu is displayed, but changing any of the settings will not do anything.

Data Format toggles settings for word length, parity, and stop bit settings. The available options are: 8N1, 7E1, 7O1, and 7N1. Default setting is 8N1.

Duplex controls the echo settings for the modem command processor. Full duplex causes the T830 to echo all characters sent to the remote device. Half duplex turns off character echo. Default setting is FULL.

Init String sets the user-defined modem initialization string. This string is sent to the modem before important factory modem initialization settings, so certain settings in this init string may be overridden. Default setting is ATM1. (Max length 126 chars) Note: Make sure to enter 'AT' at the beginning of this initialization string.

TAP Init String is the user-defined modem initialization string used only when the modem is making an alphanumeric modem callout. Default setting is ATM0. (Max length 126 chars) Note: Make sure to enter 'AT' at the beginning of this initialization string.

Inactivity Timeout sets the number of minutes (0 – 255) to wait before disconnecting an idle modem connection. A setting of 0 means the connection will never automatically expire. Default setting is 0.

Upon Modem Connect Go Directly To toggles through a list of actions to control what a user sees directly after connecting via modem. LOGIN requires the user to login with username and password, and will then take them to a command prompt. A serial port (I/O1, I/O2, etc.) redirects a modem user directly to that serial port upon connecting. In this passthrough mode, the command processor of the T830 is transparent. Default setting is Login.

Wireless Modem

```
TeleBoss 830 - Wireless Modem Settings
A) Mode                                 [OFF]
B) APN                                  []
C) PIN                                  []
D) Idle Timeout (minutes)               [5]
E) Band (GPRS only)                     [DUAL-850/1900]
F) PPP/Wireless User Name               []
G) PPP/Wireless Password                [********]
H) Default Route Enable                 [OFF]
```

Note: If the optional wireless modem expansion card is not installed in the T830, this menu is displayed, but changing any of the settings will not do anything.

Note: For a complete description of the setup and operation of the wireless modem, please refer to the Wireless Modem chapter later in this manual.

Mode toggles between OFF (disable modem), PERMANENT-EDGE (maintain "always-on" connection with EDGE modem), and PERMANENT-GPRS (maintain "always-on" connection with GPRS modem). Default setting is OFF.

APN sets the Access Point Name (APN) as defined by your wireless provider. Default setting is " ". (Max length is 31 chars)

PIN sets the PIN associated with the SIM card (if any). Default setting is " ". (Max length is 15 chars)

Idle Timeout sets the number of minutes (3 – 255) to wait before disconnecting an inactive modem connection. The purpose of this setting is to allow the modem to get reset after a period of inactivity to ensure the modem connection is working properly. Default setting is 5 minutes.

Band (GPRS only) toggles between DUAL - 850/1900, DUAL – 900/1800, DUAL – 900/1900, MONO – 850, MONO – 900, MONO-1800, and MONO – 1900. This sets the GSM bands on which the modem will operate. Default setting is DUAL - 850/1900.

Note: This setting is only used with the GPRS modem. For this setting to take effect, the wireless modem must be reset; this can be accomplished by restarting the host unit, or by setting the wireless modem mode to OFF for at least 10 seconds, then back to a GPRS setting.

PPP Wireless User Name/Password sets the login credentials for the PPP connection. (Max length for each is 64 chars)

Default Route Enable is an ON/OFF toggle to enable the wireless interface to be the default route when connected. Default setting is OFF.

User Profile Settings

```
TeleBoss 830 - User Profile Settings Menu
A) User 1: User1/********/COMMAND/FILE1
B) User 2: User2/********/COMMAND/FILE1
C) User 3: User3/********/PASSTHROUGH/FILE1
D) User 4: User4/********/PASSTHROUGH/FILE2
E) User 5:
F) User 6:
G) User 7:
H) User 8:
I) User 9:
J) User 10:
K) User 11:
L) User 12:
M) Global Password/Security Settings
```

User n displays the configuration menu for each user profile.

Global Password/Security Settings displays a menu of global security options.

» **Note:** Passwords are case sensitive and are masked in all menus and while typing them from the command line, for security reasons. If a user without permissions accesses the User Profile Settings menus, they will see all fields in this menu either masked or with no data in them. If they select an option, a message will be displayed that says: "You do not have permission to change this setting."

» **Note:** When configuring a new username, and an invalid or duplicate username is entered, the T830 responds as follows:

```
Invalid Entry.
Press any key to continue...
```

» **Note:** When configuring a new password, the T830 will ask you to re-enter the password. If the second entry of the password does not match the first, the T830 responds as follows:

```
Invalid Entry - Confirm Password does not match.
Press any key to continue...
```

User Setup Menu

```
TeleBoss 830 - User Setup Menu
A) Enable This User Access              [ON]
B) User Name                            [User1]
C) Password                             [********]
D) Allow User Connection via            [LMTFRSs]
E) Upon Login then Go To                [COMMAND]
F) Set Access/Pass-through Pointer To   [FILE1]
G) Pass-through Permissions
H) After PT, ESC Takes User To          [MENU]
I) Setup/Status Rights                  [ADMIN1]
J) File Release Permissions
K) File Delete Permissions
```

Enable This User Access is an ON/OFF toggle to enable access for this user profile.

User Name/Password sets the username and/or password for this profile. (Max length for each is 31 chars)

Allow User Connection via displays a menu to toggle ON or OFF access via Local (I/O 2), Modem, Telnet, FTP, Real-Time Socket, and Secure Shell (SSH). These are abbreviated: LMTFRSs and default setting for all is ON.

Upon Login then Go To toggles the action this user will be directed to upon logging in, with the following options: Menu, Command, and Passthrough as shown here:

Menu

```
TeleBoss
Password: ********

TeleBoss 830 Version 2.03.050
at 830-830000085

1. Pass-Through to I/O 1
2. Pass-Through to I/O 2
P. 830 Command Prompt
M. 830 Setup Menu
S. 830 Status Menu
X. Exit (end connection)
```

Command

```
TeleBoss
Password: ********

READY
>
```

Passthrough

```
TeleBoss
Password: ********

Connected to I/O 1
```

Set Access/Pass-through Pointer To is in effect if the “Upon Login then Go To” action is set to Passthrough. This option toggles the serial port the user will be routed to. Default setting is FILE1.

Pass-through Permissions is in effect if the “Upon Login then Go To” action is set to Menu. This option displays a menu showing all serial ports, and toggles ALLOW or DENY for each port as needed. If a port is set as ALLOW, then that serial port is displayed in the Menu after the user logs in. If a port is set as DENY, then that serial port is not displayed in the Menu. Default setting for all ports is ALLOW.

After PT, ESC Takes User To sets the action this user can perform when they exit out of a passthrough connection.

Setup/Status Rights toggles through the actions available to the user if they are given access to the command prompt. Options are MASTER, NONE, VIEW, ADMIN1, ADMIN2, and ADMIN3. See the User Rights Table for more information on each access level. Default setting is MASTER.

File Release / Delete Permissions displays a menu showing all data files, Events Log and Audit Log, and toggles ALLOW or DENY for each as needed. Default setting for all is ALLOW.

Global Password/Security Settings

```
TeleBoss 830 - Global Password/Security Settings Menu
A) Show Username/Password Prompt         [OFF]
B) Local Command Requires Password       [OFF]
C) Modem Callin Requires Password        [OFF]
D) Globally Allow Access via             [MTFRSs]
E) TCP/IP Port 23 Requires Password      [ON]
F) TCP/IP Port 210x Requires Password    [OFF]
G) TCP/IP Port 220x Requires Password    [OFF]
H) Username and/or Password Required     [PASSWORD ONLY]
```

Global Password/Security Settings set parameters for passwords and security that are required for ***every*** user who attempts to log into the T830.

Show Username/Password Prompt is an ON/OFF toggle to set whether a prompt for logging in is displayed. Default setting is OFF.

Local Command Requires Password is an ON/OFF toggle to set whether a password for I/O 2 users is required. Default setting is OFF.

Modem Callin Requires Password is an ON/OFF toggle to set whether a password for modem users is required. Default setting is OFF.

Globally Allow Access via displays a menu allowing you to toggle ON or OFF access via Modem, Telnet (ports 23, 200x, 210x), FTP, Real-Time Socket and Secure Shell (SSH). These are abbreviated: MTFRSs. Default setting for all is ON.

TCP/IP Port 23 Requires Password is an ON/OFF toggle to set whether a password for Telnet (port 23) users is required. Default setting is ON.

TCP/IP Port 210x Requires Password is an ON/OFF toggle to set whether a password for passthrough (port 210x) users is required. Default setting is OFF.

TCP/IP Port 220x Requires Password is an ON/OFF toggle to set whether a password for real-time socket (port 220x) users is required. Default setting is OFF.

» **Note:** If any of the above options is set to OFF, users connecting via that method are automatically granted all access.

Username and/or Password Required toggles between requiring: PASSWORD ONLY, USERNAME/PASSWORD (PW), or PASSWORD(PW)/USERNAME. Default setting is PASSWORD ONLY.

Alarm/Event Definitions

» **Note:** Refer to the Data Events section in the Features chapter for an example-driven approach to defining alarm definitions.

```
TeleBoss 830 - Alarm/Event Definitions Menu
A) Class Table
B) Data Alarm/Filter Settings
C) EventSensor Device Settings
D) No-Data 1 Alarm Settings              [OFF]
E) No-Data 2 Alarm Settings              [OFF]
F) Percent Full Alarm Settings           [OFF]
G) Scheduled Event 1 Settings            [OFF]
H) Scheduled Event 2 Settings            [OFF]
I) Data Filter Action                    [REJECT]
J) Asentria Alarm Version                [1.1]
K) Require Asentria Alarm ACKs           [OFF]
```

Class Table displays the menu for configuring event classification settings.

Data Alarm/Filter Settings displays the menus for configuring serial data event monitors.

EventSensor Device Settings displays the menus for configuring internal and external sensors and modules that may be installed.

Note: Currently the T830 cannot detect any external EventSensors.

No-Data *n* Alarm Settings displays the menus for configuring alarms based on period of time when no-data is received on a specific serial port.

Percent Full Alarm Settings displays the menu for configuring alarms based on how full the call record database of the T830 is.

Scheduled Event *n* Settings displays the menus for configuring alarm notifications for specific times and days of the week.

Data Filter Action toggles between REJECT and ACCEPT to indicate whether data filters are configured to reject or accept specific incoming data string(s). Default setting is REJECT.

Asentria Alarm Version toggles between 1.0 and 1.1 to indicate which type of Asentria Alarm notification will be displayed. Refer to the Asentria Alarms section in the Features chapter for a detailed explanation of Asentria Alarms.

Require AsentriaAlarm ACKs is an ON/OFF toggle to enable or disable forcing the unit to require an acknowledgment when first connecting, and after each Asentria Alarm. If disabled, the T830 will allow non-CRC mode where Asentria Alarms are delivered without waiting for any indication that the messages were properly delivered. If enabled, CRC mode is required by the T830. Refer to the Asentria Alarms section for more information about CRC and non-CRC modes.

Class Table

```
TeleBoss 830 - Class Table
A) Class 1                                          [Info]
B) Class 2                                          [Minor]
C) Class 3                                          [Major]
D) Class 4                                          [Critical]
E) Class 5                                          []
   ...
L) Class 12                                         []
```

Class *n* defines the event classification assignable to events detected by the T830. (Max length 47 chars)

Info, Minor, Major, and Critical are the default class names assigned to the first four classes. These can be changed and others added as desired to meet your specific needs.

The class number and name are reported in Asentria Alarms, and SNMP traps. It is a mechanism for you to provide varying severities for different alarms so that you can act on them upon receipt.

Data Alarm/Filter Settings

```
TeleBoss 830 - Data Alarm/Filter Settings
A) Data Alarm Field Settings
B) Data Alarm Macro Settings
C) Data Alarm Settings
D) Display Alarm Status
E) Exit Upon True Data Alarm            [OFF]
```

Data Alarm Field Settings displays the menu for configuring up to 16 data alarm fields.

Data Alarm Macro Settings displays the menu for configuring up to 100 macros to be used for data alarming.

Data Alarm/Filter Settings displays the menu for configuring up to 64 data alarms or filters.

Display Alarm Status displays real time information on data event monitors you've configured.

Exit Upon True Data Alarm is an ON/OFF toggle to set whether the T830 will stop processing more data event evaluations on a single record after it has found one match. This should be disabled if it is possible to have more than one event in a record. This is a global setting – it applies to ALL configured data alarms. Default setting is OFF.

Data Alarm Field Settings

```
TeleBoss 830 - Data Alarm Field Definition Table
                    Start    Length   Type       Name
A) Definition A     0        0        [Alpha]
B) Definition B     0        0        [Alpha]
...
P) Definition P     0        0        [Alpha]

Enter your Selection: a

TeleBoss 830 - Data Alarm Field Definition
Data Field: A
A) Start Position                    [0]
B) Field Length                      [0]
C) Field Name                        []
D) Field Type                        [Alpha]

Enter your Selection:
```

Start Position sets the number of the characters to begin a particular alarm field starting from position 1. Field definition is disabled if set to 0.

Field Length sets the length of this particular alarm field.

Field Name sets the name given for the alarm field. This name must be unique, is limited to 12 characters, and it must not contain any spaces. It can contain alphanumeric characters and the underscore, but it must start with a letter. These field names are case sensitive. If left blank, you can refer to the field by it's field letter (A,B, etc…).

Field Type toggles between Alpha and Numeric. Alpha is used for most alphanumeric data alarming, and Numeric is used if you need to alarm on a range of numbers. Default setting is Alpha.

Note: The T830 does not perform error checking to ensure that no two fields have the same name. Please make sure your fields all have unique names to avoid conflicts.

Data Alarm Macro Settings

```
TeleBoss 830 - Data Alarm Macro Settings
A) Macro 1                           []
B) Macro 2                           []
   ...
P) Macro 16                          []
Q) Next Macro Page

Enter your Selection: a

TeleBoss 830 - Settings for Data Alarm Macro 1
A) Name                              []
B) Equation                          []
```

Data alarm macros provide a way to define up to 100 equations that can be used in one or more data alarm equations. Each macro consists of an equation and an associated name that can be used to reference the macro in a data alarm equation. Refer to the Data Alarm Macros section in the Features chapter for more information.

Data Alarm/Filter Settings

```
TeleBoss 830 - Data Alarm/Filter Settings
A) Alarm/Filter Page 1 (Alarms 1-16)
B) Alarm/Filter Page 2 (Alarms 17-32)
C) Alarm/Filter Page 3 (Alarms 33-48)
D) Alarm/Filter Page 4 (Alarms 49-64)

Enter your Selection:
```

Data alarms are configured by selecting an option from the main Data Alarm/Filter Settings menu, then selecting one of the options which will give you a group of 16 data alarm/filters (1-16, 17-32, etc). This will display a menu where you can select from those 16 data alarm options as follows:

```
TeleBoss 830 - Data Alarm/Filter Settings
A) Alarm/Filter 1           []                      [OFF]   [ALARM]
   ...
P) Alarm/Filter 16          []                      [OFF]   [ALARM]
Q) Next Alarm/Filter Page
R) Setup Alarm/Filter Fields
S) Display Alarm Status
T) Exit Upon True Data Alarm                        [OFF]

Enter your Selection:
```

Alarm/Filter *n* displays the menu where an individual data alarm or filter can be configured.

Next or Previous Alarm/Filter Page displays either the next or previous set of 16 Data Alarm/Filters.

Setup Alarm/Filter Fields displays the identical Data Alarm Field Setting menu as described above. This is simply an easy way to access that menu without having to exit back through the previous menus.

Display Alarm Status displays real time information on data event monitors you've configured.

Exit Upon True Data Alarm is an ON/OFF toggle to set whether the T830 will stop processing more data event evaluations on a single record after it has found one match. This should be disabled if it is possible to have more than one event in a record. This is a global setting – it applies to ALL configured data alarms. Default setting is OFF.

Data Alarm/Filter *n* Settings

```
TeleBoss 830 - Settings For Data Alarm/Filter 1
A) Alarm/Filter Enable                  [OFF]
B) Alarm/Filter Mode                    [ALARM]
C) Alarm/Filter Name                    []
D) Alarm/Filter Equation                []
E) Threshold                            [1]
F) Auto-Clear when Threshold Reached    [ON]
G) Alarm Counter Clear Interval         [12 HOURS]
H) Alarm Counter Reset Time             [00:00]
I) Actions                              []
J) Class                                [Info]
K) Data Alarm Trap Number               [503]
L) Clear This Alarm Counter Now
```

Alarm/Filter Enable toggles each individual data event monitor ON or OFF. Default setting is OFF.

Alarm/Filter Mode toggles between Alarm and Filter to indicate whether the T830 will recognize this data event as an Alarm and take some action, or as a Filter and either accept or reject the data string. Default setting is ALARM.

Alarm/Filter Name sets the name for the event monitor. This name is reported with the specified actions. (Max length 16 chars)

Alarm/Filter Equation defines the event equation using the event fields defined in the previous menu. (Max length 160 chars) Refer to the Configuring Data Alarm Equations section in the Features chapter for more information.

Threshold sets the number of times the event equation must be matched before an event is triggered. If the event counter is allowed to grow beyond the threshold, the unit will not trigger an event again until after the counter is reset. Default setting is 1.

Auto-Clear when Threshold Reached is an ON/OFF toggle to control whether the unit will clear the event counter each time the threshold is met. Default setting is ON.

Alarm Counter Clear Interval sets an interval at which the unit should clear the match counter for an individual data event. Available options are: 2 hours, 4 hours, 6 hours, 8 hours, 12 hours, Daily, and Never. The first clear occurs at midnight. Default setting is 12 Hours.

Alarm Counter Reset Time sets the time at which the daily clear should take place if it is enabled in the Alarm Counter Clear Interval. This value is in 24-hour format. Default setting is 00:00.

Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured.

Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Data Alarm Trap Number sets the number to be sent with any SNMP traps for this event. Default is 503, but trap number can also be set in the range of 1000 – 1199 as needed.

Clear This Alarm Counter Now allows you to clear the counter for the selected data alarm manually. This happens as soon as this option is selected, so make sure you really want to clear the counter before selecting it.

Actions List

```
Enter one or more actions using this format:
(For more details see the users manual)
-------------------------------------------
Cancel : cancel(idname)
Dialup Pager : dpage(index)
Dispatcher : dispatch(phone# or index)
Email : email(email or index)
Group : group(groupname)
ID : id(id name)
Malert : malert(phone# or index)
Modem : modem(phone# or index)
Postpone : postpone(idname, seconds)
Pause : pause(seconds)
Relay : relay(action, eventsensor, point)
Talert : talert(ipaddress or index)
Trap : trap(ipaddress or index)
(separate multiple actions using semicolon)

Current Actions:
Enter Data Alarm Actions:
```

The Actions List provides you with a flexible mechanism to tell the unit how to react to events. An action list is a text string that specifies what the unit should do upon an event. It's comprised of a list of keywords and parameters

separated by semicolon. Each keyword specifies a certain action and has its own parameter set, which is enclosed in parentheses. Refer to Action List in the Features chapter for more information.

EventSensor Device Settings

Note: Currently the T830 cannot detect any external EventSensors.

The Sensor Events Menu is used to configure and control both internal and external sensors and relays. If you don't have any internal sensors or relays, or remote ES devices connected, this menu will be unpopulated. Because of the numerous ES configurations possible, menus shown in this section probably will not look exactly like the ones for your T830. (The menu below shows a T830 with 2-CC which represents the two serial ports which could be configured as contact closures.)

```
TeleBoss 830 - Sensor Events Menu
   Name                  ID         Alive      Number     Configuration
A) INTERNAL              --------   -          200        2-CC
B)  <none>
C)  <none>
   ...
Q)  <none>
R) Sensor Unresponsive Settings
```

EventSensor Slots (A thru P) displays the settings menu for each ES.

Sensor Unresponsive Settings displays the Sensor Unresponsive Menu where you can configure the actions the T830 takes if an ES becomes unresponsive.

EventSensor Slots

```
TeleBoss 830 - Internal Events Menu
A) Device Name                                    [INTERNAL]
B) Contact Closure 1                              [unnamed]
C) Contact Closure 2                              [unnamed]

Enter your Selection:
```

The display for each ES will vary depending on configuration. For example, an ES could be either internal or external. EventSensors can be configured with varying combinations of I/O types. Refer to the Event Sensor Configuration Setup section in the Features chapter that can be referred to for more information.

Sensor Unresponsive Settings

```
TeleBoss 830 - Sensor Unresponsive Menu
A) Sensor Unresponsive Timeout                    [30]
B) Sensor Unresponsive Actions                    []
C) Sensor Unresponsive Trap Number                [50]
D) Sensor Unresponsive Class                      [Info]
```

Sensor Unresponsive Timeout sets the time (10 - 65535 seconds) to wait before declaring a non-communicative EventSensor unresponsive. Default setting is 30.

Sensor Unresponsive Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Sensor Unresponsive Trap Number sets the number to be sent with any SNMP traps for this event. Default is 50, but trap number can also be set in the range of 1000 – 1199 as needed.

Sensor Unresponsive Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this alarm.

No-Data *n* Alarm Settings

No Data Alarms can be configured on the T830 to monitor data coming in via the serial ports, and take an alarm action if a certain period of time passes with no data.

```
TeleBoss 830 - No-Data Alarm 1 Settings
A) Alarm Enable                          [OFF]
B) Alarm Actions                         []
C) Alarm Message                         [No-Data Timeout 1]
D) Alarm Class                           [Info]
E) Trap Number                           [505]
F) Schedule 1 Begin Time                 [00:00]
G) Schedule 1 End Time                   [00:00]
H) Schedule 1 Duration (minutes)         [0]
I) Schedule 2 Begin Time                 [00:00]
J) Schedule 2 End Time                   [00:00]
K) Schedule 2 Duration (minutes)         [0]
L) Apply Alarm on Days                   [MTuWThF]
M) Enable Ports
N) Add Exclusion
O) Delete Exclusion
   []
   []
```

No-Data *n* Alarm Settings allows you to configure two separate No-Data Alarms, each of which can be configured for two different ranges of times with different time durations. The periods of time should be configured to match the calling patterns of your business or organization. For example, if your normal business hours are M-F 8:00 to 5:00, you will want to set lower time durations during those hours than you would “after hours” when call volumes are lighter and the periods of time where there is "no data“ might be longer.

Alarm Enable is an ON/OFF toggle to enable the no-data monitor. Default setting is OFF.

Alarm Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Alarm Message sets the text string to be delivered with this event’s alarms. Default setting is "No-Data Timeout *n*“. (Max length 126 chars)

Alarm Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this no-data alarm.

Trap Number sets the number to be sent with any SNMP traps for this event. Default is 505, but trap number can also be set in the range of 1000 – 1199 as needed.

Schedule *n* Begin Time/End Time sets the beginning and ending times (24 hr clock) for each of two ranges of time.

Schedule *n* Duration is the number of minutes (0-65535) the unit will wait without receiving data before alarming.

Apply Alarm on Days displays a menu where the seven days of the week are listed, and each can be toggled ON or OFF to designate whether this particular No-Data alarm is active on that day. Default setting is ON for Monday thru Friday, and OFF for Saturday and Sunday.

Enable Ports displays a menu where the installed serial ports are listed and each can be toggled ON or OFF to designate whether this particular No-Data alarm is active on that port. Default setting is OFF for all ports.

Add Exclusion/Delete Exclusion allow you to add or delete specific dates when this No-Data Alarm should "take the day off". For example, Christmas is a day you might want to add here. Select Add Exclusion and type in **12/25**. To delete a date, you select Delete Exclusion and type in the date you want to remove. After an exclusion date is added it appears in the brackets at the bottom of the menu. 15 dates can be entered to be excluded.

Percent Full Alarm Settings

```
TeleBoss 830 - Percent Full Alarm Settings
A) Alarm Enable                         [OFF]
B) Percent Full Threshold               [80]
C) Alarm Actions                        []
D) Alarm Message                        [DB Exceeds Threshold]
E) Alarm Class                          [Info]
F) Trap Number                          [501]
```

Alarm Enable is an ON/OFF toggle to enable the percent full alarm. Default setting is OFF.

Percent Full Threshold set the percent full level at which the alarm will be triggered. Default setting is 80 percent.

Alarm Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Alarm Message sets the text string to be delivered with the percentage full alarm. Default setting is DB Exceeds Threshold. (Max length 111 chars)

Alarm Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this percent full alarm.

Trap Number sets the number to be sent with any SNMP traps for this event. Default is 501, but trap number can also be set in the range of 1000 – 1199 as needed.

Scheduled Event Settings

Scheduled Events allow you to schedule specific a specific date/time for an alarm action to occur. For example, you might want the T830 to send you an Email every morning at 8:00 just so you know it is live on the network.

```
TeleBoss 830 - Scheduled Event 1 Setup
A) Enable Event                         [OFF]
B) Event Actions                        []
C) Event Message                        [Scheduled Event 1]
D) Event Class                          [Info]
E) Trap Number                          [506]
F) Event Time Sunday                    [OFF]
G) Event Time Monday                    [OFF]
H) Event Time Tuesday                   [OFF]
I) Event Time Wednesday                 [OFF]
J) Event Time Thursday                  [OFF]
K) Event Time Friday                    [OFF]
L) Event Time Saturday                  [OFF]
M) Add Exclusion
N) Delete Exclusion
   []
   []
```

Scheduled Event *n* Setup allows you to configure two separate Scheduled Events, each of which can be configured for any one time on any day of the week. Each day's time can be scheduled independently from the others.

Enable Event is an ON/OFF toggle to enable the Scheduled Event. Default setting is OFF.

Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Event Message sets the text string to be delivered with this event's action. Default setting is "Scheduled Event *n*". (Max length 126 chars)

Event Class sets the class for the event. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this event.

Trap Number sets the number to be sent with any SNMP traps for this event. Default is 506, but trap number can also be set in the range of 1000 – 1199 as needed.

Event Time *day* sets the time (24 hour clock) each day at which the scheduled event action will occur. If no time is configured for any day, this menu displays OFF.

Add Exclusion/Delete Exclusion allow you to add or delete specific dates when this Scheduled Event should "take the day off". For example Christmas is a day you might want to add here. Select Add Exclusion and type in **12/25**. To delete a date, you select Delete Exclusion and type in the date you want to remove. After an exclusion date is added it appears in the brackets at the bottom of the menu. 15 dates can be entered to be excluded.

Action Definitions

This menu is where you configure all of the actions possible when events are detected.

```
TeleBoss 830 - Actions Definition Menu
A) Hostname/IP Address 1                []
B) Hostname/IP Address 2                []
C) Hostname/IP Address 3                []
D) More Hostnames/IP Addresses          []
E) Email Address 1                      []
F) Email Address 2                      []
G) Email Address 3                      []
H) More Email Addresses                 []
I) Phone Number 1                       []
J) Phone Number 2                       []
K) Phone Number 3                       []
L) Phone Number 4                       []
M) Pager Number 1                       []
N) Pager Number 2                       []
O) Pager Number 3                       []
P) Pager Number 4                       []
Q) Callout Attempts                     [5]
R) Callout Delay (seconds)              [60]
S) Action Schedule                      [OFF]
```

Hostname/IP Address *n* sets the hostname or IP address of the device(s) receiving SNMP Traps. The number (1,2,3) corresponds to the "index" number for Traps as discussed in the Action List section of the Features chapter.

More Hostnames/IP Addresses displays the Hostname/IP Address Definition Menu where three more hostnames or IP Addresses (index 4,5,6) can be configured.

Email Address *n* sets the Email address of the person(s) receiving Email alerts. The number (1,2,3) corresponds to the "index" number for Email alerts as discussed in the Action List.

More Email Addresses displays the Email Address Definition Menu where three more Email Addresses (index 4,5,6) can be configured.

Phone Number *n* sets the phone number (index 1,2,3,4) to call for each dispatch, malert or modem callout as discussed in the Action List.

Pager Number *n* sets the pager phone number (index 1,2,3,4) to call for each pager callout as discussed in the Action List.

Callout Attempts sets the total number of times to attempt dispatch, malert or modem callouts if previous attempts fail. Default setting is 5.

Callout Delay sets the time in seconds (0 - 400) to wait between callout attempts. Default setting is 60 seconds.

Action Schedule displays the Action Schedule Settings Menu where actions can be limited to defined days and times.

Action Schedule

```
TeleBoss 830 - Action Schedule Settings
A) Action Schedule Enable               [OFF]
B) Begin Time                           [08:00]
C) End Time                             [17:00]
D) Weekdays Only                        [ON]
```

Actions Schedule Enable is an ON/OFF toggle to enable the action schedule. Default setting is OFF.

Begin Time/End Time sets the beginning and ending times (24 hr clock) during which alarm actions can be taken. Default settings are 08:00 (Begin Time) and 17:00 (End Time).

Weekdays Only toggles whether actions are only performed Monday thru Friday. Default setting is ON.

General Settings

```
TeleBoss 830 - General Settings
A) Site Name                            [830-830000085]
B) Answer String                        [TeleBoss]
C) Escape Key                           [27]
D) Confirmation Prompt                  [ON]
E) Time Stamp Format                    [HH:MM]
F) Date Stamp Format                    [MM/DD]
G) Space After Date/Time Stamp          [ON]
H) Prompt                               []
I) Date/Time Setup
J) Legacy Settings
```

Site Name sets the name assigned to this T830. This name is included with alarm messages (Traps, Emails, etc.) and is displayed at the top of the Status screen. The name should be unique for clarity. (Max length 40 chars) Default setting is "830 - <*serial number*>"

Answer String sets the string that is presented when a user connects to the T830 via Telnet or modem. (Max length 31 chars)

Escape Key is the decimal ASCII character code of the key you must press three times to escape from passthrough or other transparent modes. Default is 27, the <ESC> key.

Confirmation Prompt is an ON/OFF toggle to set whether a confirmation prompt (`Are you sure (y/n)?`) is displayed when the commands **`DEFAULT`** or **`COLDSTART`** are issued. If there is no response within 30 seconds, the T830 will cancel the command. Default is ON.

Time Stamp Format toggles through three options for how time stamps are formatted: HH:MM, HH:MM:SS, or Blank. Default setting is HH:MM.

Date Stamp Format toggles through four options for how date stamps are formatted: MM/DD, MM/DD/YY, MM/DD/YYYY, or Blank. Default setting is MM/DD.

Space After Date/Time Stamp is an ON/OFF toggle to set whether a space is appended to the end of the Date/Time stamp. Default setting is ON.

Prompt sets the character(s) or settings values displayed as the command line prompt. Refer to the Customizable Command Prompt section in the Features chapter for more information. (Max length 63 chars)

Date/Time Setup displays the System Date/Time menu where you can manage the clock, daylight savings control, and configure a networked time server.

Legacy Settings displays a menu for configuring legacy products that may be connected to the T830.

Date/Time Settings

```
TeleBoss 830 - System Date/Time
A) Current Date                         [03/25/2008]
B) Current Time                         [09:53:39]
C) Adjust for Daylight Savings          [ON]
D) GMT Difference (hours)               [8]
E) GMT Difference Direction             [BEHIND]
F) Enable Time Protocol                 [OFF]
G) Time Servers
```

Current Date sets the date. The unit automatically calculates the day of the week to display on the Status screen.

Current Time sets the time (24 hr clock).

Note: The date and time settings are maintained by means of an internal battery backup when power is removed from the T830.

Adjust for Daylight Savings is an ON/OFF toggle that allows automatic daylight savings time updating.
A brief explanation of daylight savings time (effective 2007): On the second Sunday in March, clocks are set ahead one hour at 2:00 a.m. local standard time, which becomes 3:00 a.m. local daylight time. On the first Sunday in November, clocks are set back one hour at 2:00 a.m. local daylight time, which becomes 1:00 a.m. local standard time.

GMT Difference (hours) sets the number of hours the current time zone is offset from GMT. Valid input ranges from 0 to 12. Default setting is 8 hours.

GMT Difference Direction sets whether you are east (ahead) or west (behind) of GMT. For example, Pacific time (GMT-8) is behind and Tokyo time (GMT +9) is ahead. Default setting is BEHIND.

Enable Time Protocol toggles between OFF, SIMPLE, and NTP.

SIMPLE - With network time set to SIMPLE the unit attempts to contact the configured time servers (see Time Servers setting below) periodically, attempting to query each using Simple Network Time Protocol (SNTP), Time, and Daytime protocols, in that order. Once a response is received for any protocol, the unit sets the system clock to the new time, updates the real time hardware clock (RTC), then the network time process dies. The interval for checking network time is hard-coded to 12 hours plus or minus a random several hours.

NTP – With network time set to Network Time Protocol (NTP), the NTP daemon is kept running at all times. Unlike the SIMPLE setting, with NTP the clock is not immediately set as soon as a time server is contacted. Rather, the NTP daemon utilizes various algorithms to set the time in an accurate and robust manner. Since the NTP daemon updates the system time asynchronously, the current time is stored in the RTC every 30 minutes while it is running. Note that if you change the clock manually, it may be a period of an hour or more before NTP resets it.

Time Servers displays a menu where the hostname or IP address of six time-servers can be configured. (Max length 64 chars) The T830 uses the following servers by default:

- time.nist.gov - 192.43.244.18 - Boulder, CO
- time-b.nist.gov - 129.6.15.29 - Gaithersburg, MD

Legacy Settings

```
TeleBoss 830 - Legacy Settings
A) Release Compressed                   [OFF]
B) Autodelete After Polling             [OFF]
C) Wait for NEXT                        [OFF]
D) Omit END DATA                        [OFF]
E) Line Tag                             [OFF]
F) Release Mode                         [LINE]
G) CBB DLE Stuffing                     [OFF]
H) CBB Retransmits                      [5]
I) CBB Timeout                          [15]
   Note: These settings are for support of older systems and
         should NOT be used for new implementations. We do
         not guarantee that these settings will be present in
         future versions or products.
```

Released Compressed is an ON/OFF toggle to enable release of data in a compressed or uncompressed format. Default setting is OFF.

Autodelete After Polling is an ON/OFF toggle to enable the deletion of data from the call record database once it has been polled. Default setting is OFF.

Wait for NEXT is an ON/OFF toggle that causes the unit to wait for the NEXT command before sending data once the RL command has been issued. Default setting is OFF.

Omit END DATA is an ON/OFF toggle that causes the unit to send or omit the string "END DATA" when a command processor poll is complete. Default setting is OFF.

Line Tag is an ON/OFF toggle that adds or omits the serial number line tags on each line of stored data. Default setting is OFF.

Release Mode toggles the following modes of releasing stored data: LINE, XMODEM, and CBB. Unless your application specifically uses XMODEM or CBB, leave this set to the default setting of LINE.

CBB DLE Stuffing/Retransmits/Timeout are specific configuration options for polling via Compressed Binary Block (CBB) mode. CBB is a release method included for compatibility and is not otherwise documented in this manual.

Event Log Settings

The Event Log is a record of all data events that occur within the T830.

```
TeleBoss 830 - Event Log Settings
A) List Events File
B) Clear Events File
C) Enable Events Log File               [ON]
D) Maximum File Size                    [32]
E) Store Data Alarm Records             [OFF]
F) Store Sensor Events                  [OFF]
G) Date/Time Stamp Data Alarm Records   [OFF]
H) Prepend Data Alarm Name              [OFF]
```

List Events File displays the contents of the Events file, if any records exist.

Clear Events File purges the records within the Events File. Records in the Events File are deleted immediately when this option is selected, so make sure you want to do this before selecting.

Enable Events Log File is an ON/OFF toggle to enable Event logging. Default setting is ON.

Maximum File Size sets the maximum number of KB the event log can reach before overwriting the oldest records. Available options are 0, 32, 64, 128, 256, 512 and 1024. Default setting is 32.

Store Data Alarm Records is an ON/OFF toggle to enable storing data alarm records. Default setting is OFF.

Store Sensor Events is an ON/OFF toggle to enable storing records generated by environmental sensors. Default setting is OFF.

Date/Time Stamp Data Alarm Records is an ON/OFF toggle to prepend a Date/Time stamp to the beginning of data alarm records. Default setting is OFF.

Prepend Data Alarm Name is an ON/OFF toggle to prepend the name of the Data Alarm to the beginning of the data alarm record. This aids in identifying which Data Alarm an alarm record is associated with. Default setting is OFF.

Audit Log Settings

The Audit Log is a record of a variety of actions that occur within the T830.

```
TeleBoss 830 - Audit Log Settings
A) List Audit Log File
B) Clear Audit Log File
C) Enable Audit Log File                [ON]
D) Maximum File Size                    [32]
E) Store Reset Events                   [ON]
F) Store Command Entry                  [ON]
G) Store Relay Activity                 [ON]
H) Store Alarm Actions Taken            [ON]
I) Store Password Failures              [ON]
J) Store Logins/Disconnects             [ON]
K) Store Pass-through Activity          [ON]
L) Store Inactivity Timeouts            [ON]
M) Store Polling Activity               [ON]
N) Store DIP Switch Changes             [ON]
```

List Audit Log File displays the contents of the Audit Log file, if any records exist.

Clear Audit Log File purges the records within the Audit Log file. Records in the Audit Log File are deleted immediately when this option is selected, so make sure you want to do this before selecting.

Enable Audit Log File is an ON/OFF toggle to enable Audit logging. Default setting is ON.

Maximum File Size is the maximum number of KB the event log can reach before overwriting the oldest records. Available options are 0, 32, 64, 128, 256, 512, and 1024. Default setting is 32.

The remaining options are ON/OFF toggles to enable logging of the action described. Default settings for all is ON.

Features and How To Use Them

Upgrading the T830

Save the update file (830-2.03.050-std-a71.udf) to a directory on your PC or an FTP server. FTP upgrades can be done in either of two ways: by using the T830's FTP client to get the update file, or sending the update file from another host to the T830's FTP server. Following are the instructions for both methods.

Note: Before upgrading it is always a good idea to make a copy of the Setting Keys file in your T830, in case settings are lost during the upgrade. This usually does not happen, but it's better to be safe than sorry.

T830 as FTP client method:

From the command line type: **xf f get <update filename> <host> <username>**

(note: you can type 'xf' at the command prompt to get usage for this command.)

Here is an actual session:

```
➢ xf f get 830-2.03.050-std-a71.udf 10.10.5.32 anonymous
Receiving 830-2.03.050-std-a71.udf via FTP
Anonymous's password:
……..
COMPLETE

<and the update starts here>
```

T830 as FTP server method:

1) Make an FTP connection to the T830 using a username and password that has MASTER rights.

2) Type **hash** at the ftp prompt. (This is optional - it just creates hash marks (###) while the file is transferring so you can see something happening.)

3) At the next ftp prompt type: **put drive:\directory\<update filename>**
For example: put C:\upgrades\830-2.03.050-std-a71.udf

4) Hash marks will now appear to show you that the file is transferring. When the transfer is complete you will be returned to an ftp prompt.

5) Type: **bye** at the ftp prompt. The unit still has to process this file, which takes about 5 minutes, at which time the unit will reboot. When the unit detects the update file and begins processing it. Wait until the unit reboots before proceeding.

6) After the T830 reboots, connect to it and either check the top line of the Status screen, or type **ver** at the command line. You should see that the unit is now upgraded to the new version.

7) Check your settings to be sure none have been lost. If they have, reload the Setting Keys file.

Setting Keys

Setting Keys (SK) provide a flat file, human readable, means of setting and retrieving settings within the unit. Setting Keys are commonly used to clone settings across multiple units or in automated processes.

Setting Keys is abbreviated when used on the command line as **SK**. Following are commands when working with the Setting Keys File from the command line of the unit.

SK [KEY[=*value*]] allows for reading or setting a single Setting Key. If the value portion of the command is omitted, the T830 will report back the value stored in that key. If the value is given, it will be stored in the key.

SK GET [X|A [CUSTOM] [*filter*]] initiates a download of unit settings. This listing can be retrieved either by Xmodem or plain ASCII using the X and A attributes, respectively. If the transfer mode attribute is omitted, the unit will prompt for the download method. The CUSTOM tag may be used to retrieve only the settings that are not set to factory defaults. A filter may be applied to limit the keys output to just the branch specified. For example, to retrieve an ASCII listing of all EventSensor settings, use the command: **SK GET A event.sensor**

SK SET [X|A] puts the unit in bulk Settings Keys upload mode. Any of the settings retrieved by SK GET can be manipulated and uploaded with new values. The unit will process settings in any order or number; not all settings need to be uploaded each session. As with SK GET, both ASCII and Xmodem transfer methods may be used to upload settings to the unit. These transfer methods are indicated by using the X and A attributes, respectively. The T830 monitors for invalid Setting Keys and will notify you after the upload if any invalid data was received.

When using SK SET in ASCII mode, the data uploaded must end with a line consisting of the word "END" followed by a return.

SK HERE allows you to set or get individual keys interactively. Typing just the key name will cause the value to be displayed. Typing the key name plus a new value will set that key. The unit will keep prompting for a new key or key/value pair until you press <Esc> or <Enter>.

SK LOG displays a list of any errors generated during an SK Set.

Setting Keys can also be retrieved and loaded via FTP.

FTP> GET SKALL FILENAME.TXT retrieves all of the Setting Keys for the unit, similar to the **SK GET A** command described above.

FTP> GET SKCUSTOM FILENAME.TXT retrieves any settings that are not set to factory default, similar to the **SK GET A CUSTOM** command described above.

FTP> PUT FILENAME.TXT SKALL and **PUT FILENAME.TXT SKCUSTOM** load the settings in FILENAME.TXT onto the T830.

Upon successful completion of loading the settings FTP will respond with "**226 - Transfer complete**". If there is a problem in the Setting Keys file then FTP will respond with "**226 - Transfer complete; errors in setting key file! Type Get SKLOG to view**"

FTP> GET SKLOG retrieves the Setting Keys log as described above.

Telnet/TCP Connections

The T830 provides support for Telnet/TCP connections via two internal Ethernet interfaces. Refer to the Ethernet Settings menu for information on how to configure these.

All Telnet connections are TCP connections but not all TCP connections are Telnet connections. A Telnet connection is made to the T830 by using the Telnet protocol and by specifying a TCP port address. 'Telnet' refers to a TCP connection made on port address 23, which specifies that characters are supposed to be handled a certain way. The T830 supports Telnet connections and also supports some custom assigned port numbers to facilitate certain connection features.

The following information assumes that you know how to run your computer to establish and use Telnet/TCP connections and only require the specific information relating to the T830 features. Port numbers below include "x" where "x" is the corresponding T830 file or port number. (ie; 2101 refers to the telnet passthrough connection made on serial port 1.)

- **Port Address 200x**: A connection to port 200x is just like a regular Telnet connection to port 23, except it sets the default file for retrieving data or the default port when the **Bypass** command is given.

- **Port Address 210x** : A connection to port 210x routes you directly to the device connected to the corresponding serial (I/O) port. A banner message will be displayed indicating you are connected to that I/O port. To disconnect from this access mode press the <ESC> key twice. Refer to the Passthrough section in this chapter for more information.

- **Port Address 220x**: A connection to port 220x is referred to as a Real-Time Socket. These are sockets that are dedicated to exporting data from file "x" in the T830. If there is any data already stored in a particular file, it will first be transferred out of the T830 to the user or machine initiating the connection. After all the data currently in the file is transferred out, any data that is coming into the T830 will be immediately transmitted out and across this connection. Refer to the Real-Time Socket Settings menu for information on how to configure these.

Secure Shell (SSH) and Secure FTP (SFTP)

Note: The T810 does not currently support SFTP but it does support Secure Shell (SSH). Please disregard any references to SFTP in this section.

This section consists of six topics regarding SSH and SFTP:

Quick Start: SSH into the unit

The T830 supports Secure Shell (SSH) version 2, including Secure FTP (SFTP). SSH version 1 is not supported. Some configuration steps are necessary before the initial SSH connection to the unit. Connect to the unit via a conventional method (serial port, telnet, modem) to make these configuration changes. The changes are:

1. Make a user profile with a username and password (required)
2. Configure network settings (required)
3. Generate the host key (optional)

These are the steps in detail:
1. Make a user profile with a username and password (required). This is done via the Setup->User Profile Settings menu.

2. Configure network settings (required) - By default the unit ships with static IP address 0.0.0.0. Change this to an appropriate static IP address on your network, as well as the default router and subnet mask if necessary.

3. Generate the host key (optional) - By default the T830 requires password authentication and does not require public key authentication. If you are not certain that you fully understand what public key authentication is, call Asentria Technical Support and ask them to explain it to you. The T830 ships with a host key already generated. You may decide to generate the host key yourself so you can be sure you are the only possessor of the host key. To generate the host key yourself, enter **SSHC –HT RSA** to create the 1024-bit rsa host key.

At this point the unit is ready to receive SSH connections. You can do the same tasks you can do on a conventional connection, like unit administration and passthrough, only now it is secured by SSH.

SFTP CDR out of the unit

The T830 uses SFTP to transfer CDR securely. SFTP runs on top of SSH version 2 and so has the same security as SSH. The unit supports password and public key authentication methods for SFTP.

If the SFTP host requires a password then the password entered in the Setup->Network Settings->FTP Settings menu is used. If the SFTP host requires public key authentication then do the following configuration steps:

1. Create a client key on the unit
2. Configure the SFTP server to make it aware that the unit is authorized to connect.
3. Configure SFTP push
4. Establish the authenticity of the SFTP host to the unit

These are the steps in detail:
1. Create a client key on the unit. - Enter **SSHC –T RSA** to create an RSA public/private key pair. The unit will generate the key and then output the key's fingerprint and public part as human-readable mostly base-64 text. The key text will begin with "ssh-" and end with "Asentria_clientkey_<serial number of unit>". You can see the unit's public client key at any time by entering **SSHC**.

2. Configure the SFTP server to make it aware that the unit is authorized to connect. - The SFTP server must know the unit's public client key in order to do public key authentication. This means taking the public client key output by the unit and configuring it in the SFTP server. For UNIX SSH servers (which typically support SFTP), this is done by appending the unit's public client key to the "authorized_keys" file in the ".ssh" directory of the user account the unit uses to SFTP-push CDR. Check with your System Administrator to determine exactly how to do this with your SFTP server.

3. Configure SFTP push - Go to the Setup->Network Settings->FTP Settings menu. Select option A until it reads "SECURE" and then configure the server address, username, password, etc.

4. Establish the authenticity of the SFTP host to the unit. - At this point the unit does not know whether to trust the configured SFTP host. (It may be a malicious host that is pretending to be your host.) Essentially you must tell the unit that you vouch for the host that is running the SFTP server; assuming you are 100% sure that the host to which the unit connects is really your host. Do this by entering **PUSHTEST**. This command is used to see that the connection between the unit and the SFTP (or FTP) host is working. For SFTP, it is also used to let you vouch for the host. The first time you make the unit connect to the SFTP host with the **PUSHTEST** command, you will see a message like the following:

> The authenticity of host <your SFTP host> can't be established.
> RSA key fingerprint is d4:1a:16:46:8a:36:59:24:22:e5:ec:6f:01:fc:74:78.
> Are you sure you want to continue connecting (yes/no)?

You may enter **YES** (you vouch for the host) or **NO** (you do not vouch for the host) at this point. To help you vouch, the unit reports the host key fingerprint. If this fingerprint is equal to the fingerprint of the host key that you know really belongs to your host, then you can safely vouch for it.

If you enter **NO** then the unit will not be able to push CDR to the SFTP host because it is un-trusted. If you enter **YES** then the unit can trust the server and the server's host key is stored on the unit. As long as the SFTP host key does not change, future connection attempts from the unit to the SFTP host will be trusted.

If the host key does change and you do not vouch for the SFTP host again to the unit (since the host has a new host key) then the unit will revert to not trusting the host (and not push CDR). If this happens and you enter **PUSHTEST**, the unit will say you have to reestablish the authenticity of the SFTP host (see next section).

Reestablishing authenticity of the SFTP host

If the host key changes, you will see something like the following when you enter **PUSHTEST**:

> @@@
> @   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!   @
> @@@
> IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
> Someone could be eavesdropping on you right now (man-in-the-middle attack)!
> It is also possible that the RSA host key has just been changed.
> The fingerprint for the RSA key sent by the remote host is
> d7:3a:05:e0:70:4d:2c:15:ae:d2:f1:c2:75:d2:af:53.
> Please contact your system administrator.

The unit will not push to a host that it sees has a different host key than the one you had vouched for. This is because the unit does not know if the host key changed due to the key of the real host actually changing or due to an imposter server coming on line to pretend to be your host (and thus having a different host key).

If you know your host key has not changed then you know the unit is being eavesdropped on. Otherwise, the host key simply changed and you must reestablish the authenticity of the host to the unit. Do this with the following steps:

1. Delete the old host key from the unit by entering **SSHC -DKM <old hostname>**
2. Enter **PUSHTEST** to vouch for the host again

Configuring authentication

By default the unit requires password authentication and does not require public key authentication in SSH. For added security you may decide to require public key authentication when connecting to the unit. Do this with the following steps:

1. Enable public key authentication by entering **SK SEC.SSH.AUTH.PUBKEY=ON**
2. Obtain the public key of the SSH client you intend to use.
3. Make the unit aware that your client is authorized to connect.
   a. On the unit, enter **SSHC -AO**
   b. Input the public key of the client. It should be a long line of ASCII text starting with "ssh-".
   c. Ensure there is a new line after the key (enter LF or CRLF if you're not sure)
   d. Enter **END** on a line by itself followed by LF or CRLF.

At this point the unit should be able to authenticate your client with public keys. You may decide that public key authentication alone is sufficient, and password authentication is not required. If so, you may disable password authentication by entering:
SK SEC.SSH.AUTH.PASSWORD=OFF

Configuring a login banner for SSH.

The unit can display a standard message when users log in via SSH. Configure this with the following steps:

1. Enter **SSHC -AN**
2. Input your authentication banner as printable ASCII text; multiple lines are allowed.
3. Input **END** on a line by itself followed by LF or CRLF.

Menu changes.

The FTP Settings Menu, FTP Push Enable option has three possible settings:

OFF, REGULAR and SECURE (for SFTP)

Default Router

The Default Router setting allows you to select the default router (gateway) for the T830. This tells the T830 which router to use if a packet is not on any of the LANs defined on the network port. The default router is selected from the routers defined for the Ethernet ports.

More information for advanced users:

The Default Router setting allows you to select the default router (gateway) for the unit. The unit uses a routing table to determine how to send any outbound IP frame. Each entry in the routing table tells the unit how to send a frame whose destination address matches a rule in the routing table. Routing table entries are examined from most-restrictive to least-restrictive, so the default routing table entry is the last entry in the table since it is the least restrictive. It is the catch-all route: it tells the unit how to send a frame when it doesn't know how else to send it. The only routes on the unit at this time are network interface routes and the default route. Network interface routes tell the unit how to send a frame bound for a machine on one of the unit's local networks (subnets). These routes are automatically configured when you configure the address of a network interface. If an outbound frame is destined for a machine off all local networks then it is sent according to what the default route specifies. The default route specifies the default router to use for these frames.

Each network interface has a router setting which you can configure; this is the machine on that interface to which frames will be sent if they do not route to the local network of that interface. However the unit uses only one of those configured routers at this time. As you configure router settings the unit will choose a default router for you. This is available for you to see (and override) via this net.default.router setting. The values you may choose for this setting (i.e., router addresses) must be in the set of routers which you have specified.

If you have configured only one router for all of your network interfaces then you don't have to worry about this setting: the unit configures it for you and there is nothing you can override it with.

Values
Values are dotted-quads and must be in the set of routers configured with net.eth.router.

Key syntax
net.default.router

Static Routes

Static routes are network routes that specify in a more or less permanent way (*static*) that traffic to a certain destination (destination host or destination network) gets *routed* out a certain interface or via a certain gateway. These give you the ability to fine-tune how outbound network traffic leaves the unit for up to eight different routes.

Configuration
The T830 has a set of 8 static route slots. Each slot has an option to enable it, set the destination net, set the gateway, and set the interface.

- **Enable** is ON/OFF, default OFF.
- **Destination Network** is network notation, i.e., w.x.y.z/s, where s is the significant bits. Default is 0.0.0.0/0.
- **Gateway** is the IP address of the gateway. Default setting is 0.0.0.0
- **Interface** is one of the allowed values: Ethernet 1, Ethernet 2, Dialup Modem PPP, Wireless Modem PPP (WPPP), and NONE. Default is NONE.

To configure a static ***host*** route you

1. Enable it
2. Specify a destination net with sigbits == 32
3. Specify gateway or interface

To configure a static ***network*** route you

1. Enable it
2. Specify a destination net with sigbits < 32
3. Specify gateway or interface

You can specify a gateway or interface. If you specify a gateway only then the frame will be IP-addressed to the destination subnet and transmitted to the gateway, and the gateway needs to be either a local Ethernet subnet or the peer of a PPP connection (be it wireless or PSTN). If you specify an interface, regardless of specifying a gateway, then the frame will be transmitted out that interface. If it is an Ethernet interface then the destination address (which matches the destination net of the route) will be arped. If it is a PPP interface then the frame which matches its route will be transmitted to the PPP peer.

» **Note:** Specifiying that certain traffic goes out a PPP interface does not cause PPP to be raised when that traffic needs to leave the unit. If a PPP interface is down then any static routes that specify a PPP interface are effectively disabled.

» **Note:** Currently there is no support for Dialup Modem PPP and Wireless Modem PPP to be functional at the same time. Eventually this will not be the case, but in the meantime the effect is that if you specify a static route with Wireless Modem PPP interface when the Dialup Modem PPP is up instead of the Wireless, then that traffic will go out the Dialup Modem PPP interface.

Setting Keys

- Net.staticroute.enable
- Net.staticroute.destnet
- Net.staticroute.gateway
- Net.staticroute.if

Example
Configure to route traffic to the the host 10.90.90.2 to go out via a special gateway 10.90.80.67.

```
net.staticroute[1].enable=on
net.staticroute[1].destnet=10.90.90.2/32
net.staticroute[1].gateway=10.90.80.67
```

Configure to route traffic to 192.168.1.0/24 (which means a subnet of 255.255.255.0) to go out the wireless interface, whenever wireless is up.

```
net.staticroute[1].enable=on
net.staticroute[1].destnet=192.168.1.0/24
```

net.staticroute[1].if=WPPP

Passthrough

Passthrough (also known as “Bypass”) is a bi-directional communication link for either a modem or Telnet connection through the T830 to a device attached to a serial port. Pass-through is useful for configuring or maintaining devices connected to the T830 without having to be in the same physical location.

Passthrough to a serial port is available on TCP ports 210*n* where ‘*n*’ is the number of the serial port.

Passthrough to a serial port is available via modem using the **BYPASS*n*** command where ‘*n*’ is the number of the serial port.

To terminate a passthrough session, press the Escape Key three times.

Following is a table showing what passthrough sub-features/behaviors are applicable to the T830 and a detailed description of each sub-feature below the table.

Sub-feature	T830
Bypass command	**Yes**
Adjustable end sequence pause	**Yes**
End sequence for network passthrough	**3 escapes (via login menu) or 1 escape (via bypass command)**
End sequence for modem passthrough	**1 escape (via bypass command)**
Joinable sessions	**Yes**
Buffered pass-through	**No**

Bypass command
The command **BYPASS*n***, where '*n*’ is the number of the serial port, is used on a modem passthrough connection.

Adjustable end sequence pause
This feature means you can control the minimum amount of time between entering escape characters that the unit will register as an authentic escape sequence. That is, you can set this to 1/4 second, meaning that in order to escape passthrough, you must enter the escape sequence with at least 1/4 second between each escape. The point is to make the unit disregard escape sequences that happen from the pass-through data itself, which is assumed to travel across the link without pauses between the escape characters. The sys.pt.endpause setting controls this.

Joinable sessions
Up to 3 pass-through sessions can be joined in that they all connect to the same serial port. Data arriving on the serial port gets passed through to all parties, and data arriving from any one party gets passed through to the connected serial port as well as the other parties.

Buffered pass-through
Buffered pass-through is where upon connecting to a passthrough session, the first thing the unit does is dump all data that has been buffered in that port's database file, instead of connecting to the port right away. Once all data from that file is output then unit connects you to the port. If no data has been buffered (or this feature is turned off) then the unit initially connects you to the port. This option is not available on the T830.

By default the unit provides passthrough access to anyone and can be further defined in the User Profile Settings menus. Various settings control its behavior, as discussed above with each sub-feature.

Data Events

This section offers a brief tutorial on how to set up a functional data event that will send an SNMP trap when the word "test" is received over a data port. Full details on how to configure data alarm equations are available in the next section, Configuring Data Alarm Equations.

Set Up a Data Event

1. From the command prompt, access the Setup menu. Select "Alarm/Event Definitions", "Data Alarm/Filter Settings", and then "Data Alarm Field Settings". The following menu allows a user to define up to 16 data event fields to be used when scanning for event data. Below is an abbreviated example of this menu:

```
TeleBoss 830 - Data Alarm Field Definition Table
                     Start    Length   Line     Type       Name
A) Definition A      0        0        0        [Alpha]
B) Definition B      0        0        0        [Alpha]
   ...
O) Definition O      0        0        0        [Alpha]
P) Definition P      0        0        0        [Alpha]
```

2. Select field A. The menu in the following example will be displayed.

```
TeleBoss 830 - Data Alarm Field Definition
Data Field: A
A) Start Position                    [0]
B) Field Length                      [0]
C) Field Name                        []
D) Field Type                        [Alpha]
```

3. Select Start Position. When prompted to enter a new value, enter "1" and press <ENTER>.
4. Select Field Length. When prompted to enter a new value, enter "4" and press <ENTER>.
5. Select Field Name and enter "test_field", then press <ENTER>.
6. Press <ENTER> to return to the Field definition Table. If configured properly, the data event field should appear in this menu.
7. Press <ENTER> to return to the Data Alarm/Filter Settings menu. From here, select the Data Alarm Settings menu, Alarm/Filter Page 1, then Alarm/Filter 1. The following menu will be displayed:

```
TeleBoss 830 - Settings For Data Alarm/Filter 1
A) Alarm/Filter Enable               [OFF]
B) Alarm/Filter Mode                 [ALARM]
C) Alarm/Filter Name                 []
D) Alarm/Filter Equation             []
E) Threshold                         [1]
F) Auto-Clear when Threshold Reached [ON]
G) Alarm Counter Clear Interval      [12 HOURS]
H) Alarm Counter Reset Time          [00:00]
I) Actions                           []
J) Class                             [Info]
K) Data Alarm Trap Number            [503]
L) Clear This Alarm Counter Now
```

8. Press “A” to toggle Alarm/Filter Enable to ON.
9. Alarm/Filter Mode should be set to ALARM. If it is set to FILTER, press “B”.
10. Select Alarm/Filter Name and enter "**`Test Event 1`**".
11. Select Alarm/Filter Equation and enter **`test_field="test"`**. This will cause an event to occur any time the word "test" is received.

12. Select Actions and enter "T1" to cause this data event to send a trap to SNMP manager #1, as configured below in the Hostname/IP Address menu.

Other Setup

1. Return to the Main Setup Menu, select “Action Definitions”, select “Hostname/IP Address 1” and enter either the hostname or IP address of the SNMP Manager where the trap will be sent.
2. Press <CTRL> + C to return to the command processor.

Testing

Connect to the unit serially on I/O 1 and type the word **`test`** followed by <ENTER>. This should trigger the above data event, and an SNMP trap should be sent to SNMP Manager #1. If this is not the case, double check the network and data event settings and then call Asentria Technical Support.

Note: There will be a 30 second delay in alarming if the terminal emulator being used does not send a LF with the CR. This may be circumvented by pressing <CTRL + J> to generate a LF.

Configuring Data Alarm Equations

The equation is the heart of any data event. The following are a few examples event equations:

- `alarm_code = "L31"`
- `ext >= "A 600" AND exit_code = "DN"`
- `(alarm_code > "1051" OR exit_code = "1Ow74x") AND switch = " 001.1.9*.**"`
- `@ = "CRITICAL"`

Here are a few tips to help you create your own data event equations:

- Multiple field references are acceptable, as long as both fields are the same length. For example, `d=c` is a valid equation if the fields that both 'd' and 'c' represent are two characters long
- Variable names are case sensitive
- Equation literals (the data contained within quotation marks) are case sensitive
- If any rule is violated in a equation, an alarm will not be generated, nor will an error be presented

Note: There may be times when two or more fields are necessary to analyze one piece of data. For example, if a time is represented in hh:mm format, some calculations may require two different fields. Other times, wildcards will do the job of masking out non-important characters just fine.

The data alarm equations used in the T830 are standard Boolean-type operators. The following table outlines each of the supported operators and their function.

Operator	Function
>	Greater Than
<	Less Than
>=	Greater Than or Equal to
<=	Less Than or Equal to
! or <>	Not Equal to
=	Equal to
*	Single character wildcard (matches any character or space)
()	Parenthesis used to combine operations
OR	Logical OR
AND	Logical AND
@	Positional wildcard (used in place of a field name to match anywhere within an incoming record)

Data Alarm Macros

Data alarm macros provide a way to define up to 100 equations that can be used in one or more data alarm equations. Each macro consists of an equation and an associated name that can be used to reference the macro in a data alarm equation. They simplify the creating of data alarm events, particularly where more than one event uses the same expression in its equation. Also, since the macro expression is evaluated only once per record, it improves the efficiency of alarm processing.

Data alarm macros can be configured using the setup menu or setting keys:

Menu

Setup -> Alarm/Event Definitions -> Data Alarm/Filter Settings -> Data Alarm Macro

Settings Keys

event.macro[].name
event.macro[}.equation

The macro equation is entered the same way as a data alarm equation. A macro equation cannot refer to another macro; in such a case, the expression involved will always evaluate to FALSE. The macro equation can be up to 160 characters in length.

The macro name is the name by which the macro is referenced in any data alarm equation, and can be up to 16 characters in length. Macro names are subject to these restrictions:

- Macro names and data field names are not case sensitive; therefore DLT35 and Dlt35 are equivalent.
- A macro cannot be given the same name as a data field or another macro.
- The following names are reserved and should not be used as macro names or data field names:
  - °IOx (where x is a number)
  - °IPRC
  - °TRAP
  - °FTP
  - °TRUE
  - °FALSE
  - °AND
  - °OR
  - °IS
  - °ISNOT

Using a macro name or data field name that starts with AND or OR will cause that part of the expression to always evaluate to FALSE.

Macro names and data field names cannot start with $.

When used in a data alarm equation, macros are always compared to TRUE or FALSE. Any other comparison yields a result of FALSE.

Example
Settings

- event.data[1].enable= ON
- event.data[2].enable= ON
- event.data[1].equation= m1=true
- event.data[2].equation= m1 = true and f2 = "0"
- event.field[1].start= 7
- event.field[2].start= 6
- event.field[1].length= 1
- event.field[2].length= 1
- event.field[1].name= f1
- event.field[2].name= f2
- event.macro[1].name= m1
- event.macro[1].equation= f1="1"

Incoming records

```
0000001 N 019 00 DN1042  T001034         02/25 09:21 00:00:50 A 5558481677
0000002 N 020 00 DN5280  T001033         02/25 09:22 00:00:08 A 5551377443
0000003 N 021 00 T002014 DN6502          02/25 09:22 00:00:10
0000004 N 022 00 T007002 DN5700          02/25 09:19 00:02:36
0000005 E 023 00 T002024 DN1006          02/25 09:22 00:00:58
0000006 N 024 00 T002042 DN6000          02/25 09:21 00:00:46
0000007 N 025 00 DN5154  T001035         02/25 09:04 00:17:50 A 5558451000
0000008 N 026 00 DN1192  T001031         02/25 09:22 00:01:10 A 5558406776
0000009 N 027 00 DN1048  T001034         02/25 09:23 00:00:26 A 5556426898
0000010 N 028 00 DN1197  T001020         02/25 09:19 00:04:30 A 5552550948
0000011 N 029 00 DN6063  T001033         02/25 09:23 00:00:16 A 5557458535
0000012 N 030 00 T002019 DN6447          02/25 09:23 00:00:10
```

Alarm records

```
0000001 N 019 00 DN1042  T001034         02/25 09:21 00:00:50 A 5558481677 (DA 1)
0000001 N 019 00 DN1042  T001034         02/25 09:21 00:00:50 A 5558481677 (DA 2)
0000011 N 029 00 DN6063  T001033         02/25 09:23 00:00:16 A 5557458535 (DA 1)
```

- The first record matches data alarm 1, because macro 'm1' is true. Macro 'm1' is true any time the character in the 7th position is '1'.
- The first record also matches data alarm 2, because macro 'm1' is true and field 'f2' contains a '0' character.
- The eleventh record matches data alarm 1, again because macro 'm1' is true. It does not match data alarm 2 because field 'f2' does not contain a '0' character.

Action List

An action list is a text string that specifies what the unit should do upon an event. It's comprised of a list of keywords and parameters separated by semicolon. Each keyword specifies a certain action and has its own parameter set, which is enclosed in parentheses.

Note: Not all actions on the Action List may be available in this product. Check with Asentria Tech Support if you have questions concerning this.

For example, the keyword *trap* has a parameter <address or index>, and has syntax *trap(address or index)* in an action list. This keyword means send a trap to the specified parameter. If the parameter is an address then it uses that address as the trap destination. If the parameter is an index then it uses the address specified in the IP action setting list, indexed by the specified index. (This IP action setting list is action.ip, so trap(1) means send a trap to the address in setting action.ip[1].)

- cancel(*idname*)
  Cancel any running action list identified by *idname*.
- dialup pager(dpage[index])
  Send a pager callout via modem; index is the phone number configured with action.page.number
- dispatcher(*phone#* or *index*)
  Send a Dispatcher alarm via modem; *index* is the phone number configured with action.call.number. E.g., action.call.number[*index*].
- email(*email* or *index*)
  Send an email to the address specified by *email*; *index* is the email address configured with action.email
- group(groupname)
  Identify this action list as part of a group identified by *groupname*; not currently used. In a future version this will be used to cancel or postpone groups of action lists.
- id(idname)
  Identify this action list by *idname*.
- malert(phone# or index)
  Send an malert (Asentria Alarm via modem); the parameters are the same as for the dispatch keyword.
- modem(phone# or index)
  Make the unit dial a phone number and start a login session (to the unit's command processor) with the answering machine. The parameters are the same as for the dispatch keyword.
- postpone(idname, seconds)
  Postpone an already-running action list identified by *idname* for a duration specified by *seconds*.
- pause(seconds)
  Pause operation for a duration specified by *seconds*.
- relay(action, EventSensor, point)
  Put a relay in a certain state specified by *action*.
  - *action*: one of the following words, by case-insensitive exact match or partial unambiguous match: *open, close, active,* or *inactive*
  - *EventSensor*: the number of the EventSensor that has the specified relay, where it is the same as that referred to by the index in an EventSensor key (e.g., 200 in event.sensor[200].* for the internal EventSensor) as well as that referred to by the SNMP esIndex object.
  - *point*: the number of the relay (1-based) on the specified EventSensor. E.g., this is the same number x in "event.sensor[200].relay[x].*"
- talert(ipaddress or index)
  Send a talert (Asentria Alarm via TCP).
  - *ipaddress* is the destination machine;
  - *index* is the IP address configured with action.ip. E.g., action.ip[*index*].
- trap(ipaddress or index)
  Send an SNMP trap. The parameters are the same as for the talert keyword. In order to send a trap there must be a route for it. Since a trap is an unacknowledgable action, the way the unit knows if a trap is successful is if it was able to leave the unit. In order for a trap to leave the unit there must be an IP route to its host. A trap action without a route to its host is considered a failure. "Without a route" means, for example, that:
  - if the host is meant to be on a local net but cannot be ARPed
  - if the host is meant to be off all local nets but the router cannot be ARPed
  - if the above two conditions exist and PPP cannot be raised as a backup route.

Each action can take a varying amount of time depending on what's going on in the unit. E.g., a trap may take less than a second to send if there is a route for it on a network interface that is already up (like Ethernet). Otherwise, if the unit is configured to bring up PPP in case the trap cannot be sent on an already-up interface, then the trap may take a minute to send while the unit brings up PPP.

The unit starts all actions up to the first pause keyword at the same time. E.g., if you have an action list like *trap(1);email(1);modem(1);pause(60);trap(2)* then the unit will start the first 3 actions, pause for a minute, then start the last action.

Wherever you can configure an event you can configure its actions. Generally this is with the *.actions setting key that applies to the event you want to monitor. You can also configure email actions (in the action list syntax) for a user profile's login challenge destination (e.g., [[sec.user.challenge.telnetsendto). Not all actions are applicable to all events: relay actions can be caused only by sensor events and data events.

Asentria Alarms

Asentria Alarms are a receipt-verified alert system delivered via modem, or TCP on port 4000.

When an Asentria Alarm is initiated, the box dials into the callout number specified by the action. Once connected, it sends a header and waits for a specific response. If the T830 receives a specific response to the header, it delivers alarms in CRC mode; otherwise, alarms are delivered in non-CRC mode. In CRC mode, each Asentria Alarm is transmitted with some extra control characters and a CRC, and the remote host is required to acknowledge each alarm in a certain format.

After all Asentria Alarms have been delivered, the box waits for 20 seconds for any type of keystroke. If a keystroke is detected, the box will present a login menu.

Asentria Alarm Protocol

Initial header

Note: Please see the Control Characters appendix for more information about special characters used within this section.

Upon dialing into the receiver, the T830 will send a message similar to the following:

```
TeleBoss 830
Server Room B
Asentria Alarm Notice ver. 1.00
(CR/LF)(ENQ)
```

The first line of the output is the T830's answer string.
The second line is the T830's unit ID.
The third line indicates the version of Asentria Alarm.
The final line is the (ENQ) control code.

Non-CRC Mode

After sending the initial header, the T830 pauses for 10 seconds to wait for an ACK from the receiver. Non-CRC mode requires the Require Asentria Alarm ACKs setting to be turned off. If the T830 sees no response or the receiver replies with:

```
(ACK)00(ACK)
```

then non-CRC mode is assumed and the sender will transmit the alarms. The control characters (SOH), (SOT), and (ETX) are not transmitted in non-CRC mode.

CRC Mode

CRC mode exists to ensure that event notifications are delivered intact. Asentria Alarms delivered in CRC mode have extra control characters and a 16-bit CRC included in each alarm to allow for error detection by the receiver. Additionally, CRC mode causes the T830 to store and later retry each alarm until a proper acknowledgement is received from the receiver.

If Require Asentria Alarm ACKs is enabled, the T830 will require a positive CRC mode response or it will disconnect and retry the call. To enable CRC, the receiver must respond with the following after the header is received:

```
(ACK)01(ACK)
```

Once CRC mode is enabled, each alarm must be acknowledged by a message in the following format:

(ACK)*XX*(ACK)

XX represents the alarm ID to acknowledge. The ID can be found in the first line of each record sent by the T830.

Alarm Transmission
After successfully initiating a session, alarms are delivered in the following format:

```
(SOH)ID=XX(SOT)
Date=12/25/07
Time=10:30:02
TargetPort=
TargetName=
AlarmType=Data Alarm
AlarmName=Test Alarm
Threshold=0
Severity=Critical
Text1=text record line
Text2=text record line
(ETX)XX
(CR/LF)
(CR/LF)
```

The alarm ID indicates the index number of each alarm delivered during a call. This number restarts at 1 for each new call.
The severity line represents the Class value defined for this alarm.
Up to twelve lines of Text*n* may be sent.
XX represents the 16-bit CRC if CRC mode is enabled. If not, this line will contain two spaces.

If additional alarms are queued to send in the same transmission, the above output is repeated, and the ID incremented with each alarm. When non-CRC alarm transmission is selected, alarms are sent with a 5 second delay between each. When all alarms and been transmitted, then T830 sends the following:

```
(EOT)
(CR/LF)
(CR/LF)
```

At this point, the T830 waits 20 seconds for the receiver to send any input, and then hangs up. If any commands are received, a command prompt is established and the connection will remain active.

Action Definition
Asentria Alarm actions are designated by "M" in action definitions. The numbers correspond to callout numbers.
Example: M1 -or- M123

EventSensor™ Configuration Setup

The T830 can be ordered with any of the following different internal I/O devices or can be connected to a number of external EventSensor devices as described in this section. The setup menus are the same regardless of whether the device is internal or external to the T830.

Input
Contact closure
Temperature
Humidity
Voltage

Output
Relays

```
EventSensor ID: 03020000
Name: unnamed
Contact Closure States:
 01 unnamed                    Open
 02 unnamed                    Open
 03 unnamed                    Open
 04 unnamed                    Open
 05 unnamed                    Open
 06 unnamed                    Open
 07 unnamed                    Open
 08 unnamed                    Open
```

Above is a representative Internal Events Menu showing 8 contact closures. Descriptions of temperature, humidity, voltage and relays will follow.

Contact Closure *n* displays the menu for configuring each of the contact closure points.

Contact Closure Setup

```
TeleBoss 830 - Internal Contact Closure Event 1
A) Sensor Name                                  [unnamed]
B) Contact Closure Enabled                      [OFF]
C) Event State                                  [OPEN]
D) Threshold                                    [2]
E) Event State Actions                          []
F) Return to Normal Actions                     []
G) Event State Class                            [Info]
H) Return to Normal Class                       [Info]
I) Event Trap Number                            [110]
J) Return to Normal Trap Number                 [110]
K) Active Alarm Alias                           []
L) Inactive Alarm Alias                         []
```

Contact closures (CC) sense the state of a circuit. A weak voltage is applied to the source pin and if pulled to ground by a connection on the circuit, the sensor reports a "closed" state. If it remains high, the sensor reports an "open" state. All of the CCs share a common ground. The contact closures may be configured to alarm in either the open or closed state, depending on the needs of the attached devices.

Sensor Name is an alphanumeric field that allows you to name this contact closure. (Max length 16 chars)

Contact Closure Enabled toggles ON/OFF to enable this contact closure. Default setting is OFF.

Event State is an OPEN/CLOSED toggle that determines whether an event will be triggered when the contact closure circuit is opened or closed. The default state is OPEN.

Threshold is the number of seconds (0-255) the sensor must remain in the event state before an actual event occurs. Default threshold is 2.

Event State/Return to Normal Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Event State/Return to Normal Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Event/Return to Normal Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Contact Closure Events is 110, but any number in the alternate range of 1000 – 1199 can be used.

Active Alarm Alias is a special sensor name used when reporting active events for this sensor.

Inactive Alarm Alias is the same as Active Alarm Alias, but used with Return to Normal events.

Temperature Sensor Setup

```
TeleBoss 830 - Internal Temperature Event
A) Temperature Sensor Enabled           [OFF]
B) Sensor Values Represented in         [FAHRENHEIT]
C) Temperature Deadband                 [3]
D) Very High Event Settings             [100] []          [120] [Info]
E) High Event Settings                  [80]  []          [120] [Info]
F) Return to Normal Settings            [-]   []          [120] [Info]
G) Low Event Settings                   [50]  []          [120] [Info]
H) Very Low Event Settings              [30]  []          [120] [Info]
```

Temperature Sensor Enabled toggles ON/OFF to enable the temperature sensor. Default setting is OFF.

Sensor Values Represented In toggles either FAHRENHEIT or CELSIUS for the desired temperature scale.

Temperature Deadband is the range, in degrees, on either side of a temperature setting that prevents the alarm from repeatedly going in and out of the "alarm state" as the actual temperature fluctuates above and below the temperature setting.

Very High/High/Low/Very Low Event Settings display a menu where the temperature at each level can be configured to alarm along with the action(s) to occur, trap number, and class. In the case of Very High or High levels, the alarm will occur as the temperature rises above the setting. In the case of Low or Very Low, the alarm will occur as the temperature drops below the setting.

Return to Normal Settings displays a menu where the actions to occur when the temperature returns to normal (drops below the High/Very High settings, or rises above the Low/Very Low settings) can be configured.

Very High/High/Low/Very Low Event Settings Setup

```
TeleBoss 830 - Internal Temperature Event Settings
A) Very High Event Temperature                  [100]
B) Very High Event Actions                      []
C) Very High Event Trap Number                  [120]
D) Very High Event Class                        [Info]
```

The menu for setting Very High Temperature settings is shown. Menus for High/Low/Very Low are identical.

Very High Event Temperature sets the temperature at which the Very High Event Actions will be triggered.

Very High Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Very High Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Temperature Events is 120, but any number in the alternate range of 1000 – 1199 can be used.

Very High Event Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Return to Normal Settings Setup

```
TeleBoss 830 - Internal Temperature Event Settings
A) Return to Normal Event Actions                    []
B) Return to Normal Event Trap Number                [120]
C) Return to Normal Class                            [Info]
```

Return to Normal Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Return to Normal Event Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Temperature Events is 120, but any number in the alternate range of 1000 – 1199 can be used.

Return to Normal Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Humidity Sensor Setup

```
TeleBoss 830 - Internal Humidity Event
A) Humidity Sensor Enabled              [OFF]
B) Humidity Deadband                    [3]
C) Very High Event Settings             [90]  []          [130] [Info]
D) High Event Settings                  [80]  []          [130] [Info]
E) Return to Normal Settings            [-]   []          [130] [Info]
F) Low Event Settings                   [20]  []          [130] [Info]
G) Very Low Event Settings              [10]  []          [130] [Info]
```

Humidity Sensor Enabled toggles ON/OFF to enable the humidity sensor. Default setting is OFF.

Humidity Deadband is the range on either side of a humidity setting that prevents the alarm from repeatedly going in and out off the "alarm state" as the actual humidity fluctuates above and below the humidity setting.

Very High/High/Low/Very Low Event Settings display a menu where the humidity at each level can be configured to alarm along with the action(s) to occur, trap number, and class. In the case of Very High or High levels, the alarm will occur as the humidity rises above the setting. In the case of Low or Very Low, the alarm will occur as the humidity drops below the setting.

Return to Normal Settings displays a menu where the actions to occur when the humidity returns to normal (drops below the High/Very High settings, or rises above the Low/Very Low settings) can be configured.

Very High/High/Low/Very Low Event Settings Setup

```
TeleBoss 830 - Internal Humidity Event Settings
A) High Event Humidity                          [80]
B) High Event Actions                           []
C) High Event Trap Number                       [130]
D) High Event Class                             [Info]
```

The menu for setting High Humidity settings is shown. Menus for Very High/Low/Very Low are identical.

High Event Humidity sets the humidity at which the High Event Actions will be triggered.

High Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

High Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Humidity Events is 130, but any number in the alternate range of 1000 – 1199 can be used.

High Event Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Return to Normal Settings Setup

```
TeleBoss 830 - Internal Humidity Event Settings
A) Return to Normal Event Actions               []
B) Return to Normal Event Trap Number           [130]
C) Return to Normal Event Class                 [Info]
```

Return to Normal Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Return to Normal Event Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Humidity Events is 130, but any number in the alternate range of 1000 – 1199 can be used.

Return to Normal Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Analog Voltage Sensor Setup

```
TeleBoss 830 Internal Events Menu
A) Device Name                                  []
B) Analog Input 1
C) Analog Input 2
D) Analog Input 3
E) Analog Input 4
F) Analog Input 5
G) Analog Input 6
H) Analog Input 7
I) Analog Input 8
J) Clear Settings for This EventSensor
```

The analog voltage sensors provide individual voltage sensing. These sensors can be used in various applications, from monitoring a power supply to verifying RS232 voltage levels.

Device Name is the option name given to the sensor.

Analog Input *n* displays a menu where each analog voltage sensor can be configured.

Clear Settings for This EventSensor when selected will immediately clear all of the configured settings for this sensor and remove it from the Sensor Events menu (except for Internal Sensors). Return to the Sensor Events menu to assign it a new slot, if desired, and reconfigure it.

Analog Input *n*

```
TeleBoss 830 Internal Analog Input Event 1
A) Analog Input Enabled                 [OFF]
B) Input Polarity                       [POSITIVE]
C) Deadband                             [30]
D) Very High Event Settings             [600]    []        [140]  [Info]
E) High Event Settings                  [600]    []        [140]  [Info]
F) Return to Normal Settings            [-]      []        [140]  [Info]
G) Low Event Settings                   [0]      []        [140]  [Info]
H) Very Low Event Settings              [0]      []        [140]  [Info]
I) Unit Conversion Settings             [Volts]
```

Analog Input Enabled toggles ON/OFF to enable this analog sensor. Default setting is OFF.

Input Polarity indicates to the unit whether the input polarity will be positive or negative.

Deadband is the range on either side of a voltage setting that prevents the alarm from repeatedly going in and out off the "alarm state" as the actual voltage fluctuates above and below the voltage setting.

Very High/High/Low/Very Low Event Settings displays a menu where the voltage at each level can be configured to alarm along with the action(s) to occur, trap number, and class. In the case of Very High or High levels, the alarm will occur as the humidity rises above the setting. In the case of Low or Very Low, the alarm will occur as the humidity drops below the setting.

Return to Normal Settings displays a menu where the optional action definition for alarms as they return to a normal state can be configured.

Unit Conversion Settings displays a menu where “real world” values can be configured

Very High/High/Low/Very Low Analog Input Event Settings

```
TeleBoss 830 Internal Analog Input Event Settings
A) Very High Event Value                        [600]
B) Very High Event Actions                      []
C) Very High Event Trap Number                  [140]
D) Very High Event Class                        [Info]
```

The menu for setting Very High Event Value settings is shown. Menus for High/Low/Very Low are identical.

Very High Event Value sets the voltage (in tenths) at which the Very High Event Actions will be triggered.

Very High Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information.

Very High Event Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for Analog Events is 140, but any number in the alternate range of 1000 – 1199 can be used.

Very High Event Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Return to Normal Settings

```
TeleBoss 830 Internal Analog Input Event Settings
A) Return to Normal Event Actions                    []
B) Return to Normal Event Trap Number                [140]
C) Return to Normal Event Class                      [Info]
```

Return to Normal Event Actions displays the Actions List, a menu where the action string for the event is configured. This field will be empty [ ] if no actions have been configured, and will show [*SET*] if one or more actions have been configured. Refer to Action List in the Features chapter for more information..

Return to Normal Event Trap Number sets the trap number which can be useful when using SNMP trap managers that employ a trap numbering system to help identify incoming traps. The default trap number for analog events is 140, but any number in the alternate range of 1000 – 1199 can be used.

Return to Normal Event Class sets the class for the alarm. When this option is selected, a list of the classes previously defined in the Class Table is displayed, from which you can select one to be assigned to this data alarm.

Unit Conversion Settings

```
TeleBoss 830 Analog Input Event Unit Conversion
A) Unit Name                                         [Volts]
B) Low Voltage Amount (tenths)                       [0]
C) Low Unit Amount (tenths)                          [0]
D) Low Unit Sign                                     [POSITIVE]
E) High Voltage Amount (tenths)                      [600]
F) High Unit Amount (tenths)                         [600]
G) High Unit Sign                                    [POSITIVE]
```

Relay Output Setup

```
TeleBoss 830 - Internal Relay Event Settings
A) Device Name                                       []
B) Relay 1                                           []
C) Relay 2                                           []
D) Relay 3                                           []
E) Relay 4                                           []
F) Relay 5                                           []
G) Relay 6                                           []
H) Relay 7                                           []
I) Relay 8                                           []
J) Clear Settings for This EventSensor
```

Internal relay outputs provide electrical output that can open or close an external circuit. Typically this is used with devices that would not otherwise be able to interface with a host product, like audio alarms, LEDs, custom circuitry, and an almost limitless number of other applications.

Device Name is the option name given to the relay module.

Relay *n* displays a menu where each relay output can be configured.

Clear Settings for This EventSensor when selected will immediately clear all of the configured settings for this relay and remove it from the Sensor Events menu (except for Internal Sensors). Return to the Sensor Events menu to assign it a new slot, if desired, and reconfigure it.

Relay *n*

```
TeleBoss 830 - Internal Relay Event 1
A) Relay Name                                    []
B) Relay Active State                            [CLOSED]
```

Relay Name is a text-entry field that allows you to name this relay.

Relay Active State toggles CLOSED/OPEN to set whether the relay will close or open when activated. Default setting is CLOSED.

Relays as Alarm Action

Relays can be used to open or close part of a circuit of your design or part of another product. You can use the S550 internal relays to control these devices. Relays can be toggled based on sensor readings, data events, or even remotely by SNMP.

Caution: Do not exceed maximum ratings for relays. T830 relays are only designed to switch relatively low voltages and amps, and are not intended to switch AC powered devices. Only a certified electrician should work with and connect AC Voltage to the T830. Improper use outside the guidelines of this manual could cause injury or death.

Max switched voltage: 60V
Max switched current: 1A
Max switched power: 30W

Remember Ohm's law: W = V x A (watts = volts x amps)
30W = 1A x 30V
30W = .5A x 60V

Note: Be aware of the inrush (startup) current of the device you are connecting to the relays. A device drawing 1A while powered up can draw many times that upon power up. This is especially true with capacitive or inductive circuits.

Action Definition
Relay action definitions are somewhat more complicated than other alarm actions in that they must declare the action to perform, which sensor the relay is on, and which relay on that sensor to switch.

Relay actions are declared with the following syntax: Raxxyy

a: The action to perform. Options are C (close), O (open), A (active), I (inactive). Active and Inactive states are determined by the relay's configuration.
xx: The EventSensor slot the relay is on. This value is a two-digit number starting with 01, corresponding to the slot (Number) the EventSensors are declared in the setup menu.
yy: Two-digit indicator of which relay to toggle.

Example: RC0107 -or- RA0103RI0104

Note: Unlike other action definitions, each relay definition must start with an R. Where other sensors may be defined as T23 (for SNMP trap managers 2 and 3), multiple relay actions must be defined in the following manner: RC0401RO0402.

Customizable Command Prompts

This feature allows the prompt in the command processor to be customized, and includes the ability to embed one or more settings values in the prompt. A customized command prompt can help simplify administration of units, particularly where multiple units are involved.

The command prompt setting is available in the General setup menu section, and via the Setting Key 'sys.prompt'. The setting can contain up to 64 characters, but the prompt itself is limited to 30 characters; any additional characters are truncated.

In addition to specifying plain text to be included in the command prompt, setting values can be embedded using a special syntax: $(setting_key_name). If this construct is used, the value of the specified setting key replaces the construct. If the setting key is not accessible for any reason (invalid key, insufficient user access level, etc), "ERROR" is displayed instead.

Note: T830 only supports the 'sys.sitename' setting key; all others return "ERROR".
To make the system prompt blank, set 'sys.prompt' to a null value (i.e. "sk sys.prompt = ").

Examples:

```
Set prompt to be ">"
        Via Setup menu:   Enter new prompt:  >
        Via Setting Key:  sk sys.prompt = >

Set prompt to be "Site Name"
        Via Setup menu:   Enter new prompt: TeleBoss (or whatever the site name is)
        Via Setting Key:  sk sys.prompt = "$(sys.sitename) "

Set prompt to be "System Date and Time>"
        Via Setup menu:   The date and time entered via the Prompt option do not
                          change as the actual date and time progress.  What you enter
                          here will always be displayed as the prompt, until you change
                          it.  If you want the date/time prompt to change with the
                          system clock, then change it via the Setting Key entry
                          describe below.
        Via Setting Key:  sk sys.prompt = $(sys.clock.date) $(sys.clock.time)>
```

IP Record Collection (IPRC)

Avaya Definity RSP

Definition
Reliable Session Protocol (RSP) is Avaya's solution to the problem of lost connections while transferring valuable call record data. This protocol is used on both the client (PBX) and server (Data-Link) sides to ensure that if the data connection breaks, no records are lost. This is accomplished by the two devices repeatedly checking in with one another. If the connection is lost, an alarm sent out by the Data-Link (and the PBX if so configured), and the PBX will begin to buffer its own data until the connection is restored.

Commands

Command	Function
IPRC or IPRC STATUS or IPRC ?	Displays a status report of the active IPRC mode.
IPRC PORT n	Changes the TCP port on which to listen for RSP connections.
IPRC RESET	Manually disconnects the current session (if connected), closes the socket (if established), and reinitializes the server.

Status Display
The IPRC command brings up a status report similar to the following report for RSP:

```
RSP Server
Status: Listening on port 9000
SAMs tx        : 0
ACKs tx        : 0
SDMs tx        : 0
SCMs rx        : 0
New data rx    : 0
Blocks rx      : 0
Dup. blocks rx : 0
```

IPRC Terms

The following terms are used in the status display accessed by the IPRC command for RSP:

Term	Meaning
SAM (Session Accept Message)	A message transmitted by the T830 to acknowledge the client's Session Connect Message.
ACK (session Acknowledgement message)	A response transmitted by the T830 to acknowledge data blocks.
SDM (Session Disconnect Message)	A command sent from the T830 to terminate the current session. This happens when the T830 encounters an anomaly in the protocol or the user resets the server.
SCM (Session Connect Message)	A request transmitted from the client to establish a session with the T830's IPRC server.
New Data	The number of non-duplicate bytes received by the server.
Blocks	Represents the number of blocks (including duplicates) received by the unit.
Dup. Blocks	The number of duplicate blocks received by the unit. If this number is high relative to the number of blocks received, either the SPDU Response Timer (ST2) on the switch needs to be increased or the T830 is full and needs to be polled.

Command Reference

User Interface Commands

Note: The HELP command can give helpful context sensitive information for most commands.

Command	Summary	Syntax	Description
BYE	Disconnect from unit	BYE	Disconnect a processor session.
EXIT	Exit command processor	EXIT	Ends the console session.
HELP	Show help menu	HELP [*command*]	Displays a list of commands or context sensitive help for a specific command.
PING	Ping IP address	PING target_address	Performs a standard network ping function on the specified IP address.
RESTART	Restart unit	RESTART	Reset the system, same as pressing the physical reset button.
SENSORS or !	Display status of internal or external sensors	SENSORS or !	Display the status of internal or external sensors
STATUS or **?**	Display status screen	STATUS or ?	Display the status screen
STATUSW or **STATUS WIRELESS** or **?WIRE** or **?WIRELESS**	Display status of wireless modem	STATUSW or STATUS WIRELESS or ?WIRE or ?WIRELESS	Display the status of the wireless modem

Setup Commands

Command	Summary	Syntax	Description
BYPASS	Access serial ports	BYPASS [port_number]	Provide pass-through terminal access between the user and the input port.
SK	Set/get key	SK [KEY[=*value*]]	Set or get a single key See Setting Keys for more information.
SK GET	Read keys	SK GET [X|A [CUSTOM] [*filter*]]	SK GET initiates a download of Setup menu options. See Setting Keys for more information.
SK HERE	Manage individual keys	SK HERE	SK HERE allows you to set or get individual keys interactively. See Setting Keys for more information.
SK LOG	Show SK error log	SK LOG	SK LOG outputs a list of any errors generated during an SK set. See Setting Keys for more information.
SK SET	Set keys	SK SET [X|A]	SK SET puts the unit in bulk settings key upload mode. See Setting Keys for more information.
SETUP	Enter setup menu	SETUP	Opens the setup menu.

System Commands

Command	Summary	Syntax	Description
COLDSTART	Cold boot unit	COLDSTART	Resets the same settings as the DEFAULT command and then reboots the unit.
DEFAULT	Restore factory defaults	DEFAULT	Resets all settings to factory default values, except does not change the following settings: • IP address • Subnet mask • Router address • Serial port baud rate and data format • Data alarm fields • Data alarm settings • Action queue Does not affect record data
DOMAIL	Test emails	DOMAIL	Sends a test email to all defined email addresses.
DOPAGE	Test pagers	DOPAGE	Sends a test page to all defined pagers.
DOTRAP	Test traps	DOTRAP	Sends a test trap to all defined trap managers.
PUSHNOW	Initiate an immediate FTP push of data	PUSHNOW	Initiates an immediate FTP push of data
PUSHTEST	Test connectivity to the FTP server	PUSHTEST	Tests connectivity to the FTP server
TYPE	Print events file contents	TYPE [EVENTS|AUDIT]	Print the contents of the Events or Audit file.
VER	Print unit version	VER	Displays unit hardware and software versions as well as the product and version build.

Wireless Modem

The wireless modem expansion card supports the same features as connecting directly to the T830 interface, including Telnet, FTP, SSH, and so on. It also supports PPP routing, which allows communication with devices connected to one of the local Ethernet interfaces. The modem is quad band GSM 850/900/1800/1900 MHZ.

The wireless EDGE modem is for use in TeleBoss products with firmware version 2.00.240 and above.
The wireless GPRS modem is for use in TeleBoss products with firmware version 2.00.330 and above.

Installation

If installing the wireless modem for the first time (not factory installed), follow these installation instructions:

- Make sure the the host T830 is powered down.
- Insert your SIM card into the slot on the wireless modem module, with the contacts on the bottom, using the card outline printed on the circuit board as a guide.
- Remove the two screws from any of the expansion port covers on the back panel of the host unit and set the port cover aside. Carefully slide the wireless modem card into the plastic rails inside the expansion port and push the card in all the way. Replace the two screws previously removed to hold the card securely in the port.
- Screw the rubber GMS antenna (or cable to an external antenna) to the SMA connector on the modem. The unit should not be powered up without an antenna connected to the modem.
- Power up the host unit.

Setup

In addition to installing an activated SIM card in the wireless modem card, certain settings on the host unit need to be configured for the wireless connection to work. These settings can be configured via either Setting Keys or the Setup Menus as described below. Changing any of these settings should be done with **net.wireless.mode** set to OFF, otherwise unexpected behavior may occur.

Setting Keys

Following are the Setting Keys used to configure the wireless modem card. All of the Setting Keys below can also be configured in the Setup menus listed in parenthesis after each.

net.wireless.mode (Setup -> Modem Settings -> Wireless Modem Settings)
Enables or disables the wireless modem. Possible values are OFF (disable modem), PERMANENT-EDGE (maintain "always-on" connection with EDGE modem), and PERMANENT-GPRS (maintain “always-on” connection with GPRS modem). The default setting is OFF.

net.wireless.apn (Setup -> Modem Settings -> Wireless Modem Settings)
The Access Point Name (APN) as defined by your wireless provider. Default setting is “ “.

net.wireless.pin (Setup -> Modem Settings -> Wireless Modem Settings)
The PIN associated with the SIM card, if any.

net.wireless.idletimeout (Setup -> Modem Settings -> Wireless Modem Settings)
The period of inactivity, in minutes, after which the modem connection is recycled. The allowed range is 3-255 minutes. The default setting is 5 minutes. The purpose of this setting is to allow the modem to get reset after a period of time to ensure the modem connection is working properly.

net.wireless.pppusername (Setup -> Modem Settings -> Wireless Modem Settings)
net.wireless.ppppassword (Setup -> Modem Settings -> Wireless Modem Settings)
Used to set the login credentials for the PPP session.

net.ppprouting.enable (Setup -> Network Settings -> PPP Settings -> IP Routing)
This setting controls whether the unit routes IP traffic from PPP to an Ethernet interface specified by the destination IP address's subnet. On products which have DIP switches, this setting is mechanically locked with a DIP switch for added security. On products with this feature but without DIP switches, there is no way to lock this.

net.eth.nat (Setup -> Network Settings -> Ethernet Settings -> Ethernet *n* Settings)
This setting controls whether the unit does Network Address Translation (NAT) on routed frames egressing the unit on the specified interface. That is, when PPP routing is operating and forwarding frames received on the PPP interface (which can be the same thing as the wireless modem interface), the unit rewrites the source IP address of forwarded frames leaving the unit to the IP address of the ethernet interface on which they leave. If this setting is disabled then forwarding may still happen since it is governed only by the PPP routing settings, but the source IP address of the forwarded frames is not rewritten.

net.wireless.defaultrouteenable (Setup -> Modem Settings -> Wireless Modem Settings)
When ON, the wireless interface is set as the default route when connected (which is either never, or all the time, with our current options). When OFF, the wireless interface will not become the default route when connected. The default is OFF. For a change to this setting to take effect and if the wireless link is already up, the wireless link must be restarted. While it is possible to detect a change to this setting and automatically restart the wireless link, it is possible that an ongoing session (such as a web session, which would not be seen as an ongoing connection) could get interrupted. To avoid this restart the wireless connection, using the **wireless restart** command. This brings down the wireless link, and it automatically comes back up with the new setting in effect.

Setup Menu

All of the **net.wireless** settings above can be accessed in the setup menu at: Modem Settings -> Wireless Modem Settings.

```
TeleBoss 830 - Wireless Modem Settings
A) Mode                                [OFF]
B) APN                                 []
C) PIN                                 []
D) Idle Timeout (minutes)              [5]
E) Band (GPRS only)                    [DUAL-850/1900]
F) PPP/Wireless User Name              []
G) PPP/Wireless Password               [********]
H) Default Route Enable                [OFF]
```

Operation

With **net.wireless.mode** set to PERMANENT-EDGE or PERMANENT-GPRS (depending on the type of modem installed), the unit attempts to maintain a connection to the wireless network at all times. If the connection goes down for any reason, including inactivity, the unit immediately attempts to reconnect. When there is no activity on the link for longer than the inactivity timeout (see below), the connection is terminated and immediately restarted. If **net.wireless.mode** is set to OFF, wireless modem operations are terminated immediately (there may be up to a minute's delay if certain operations are pending).

The **wireless restart** command causes the wireless modem to terminate the connection and restart it based on the current settings; this is useful if a setting other than "mode" is changed.

The default setting for the wireless connection is to NOT be the default route for outbound IP frames. A static route must be entered for any frame to be sent out on the wireless connection. If **Default Route Enable** is changed to ON for the wireless connection, then all IP frames that do not match an existing static route will be sent out on the wireless connection. For situations where the wireless modem is the only means of off-net access, **Default Route Enable** should be set to ON.

The front-panel MODEM LED shows the status of the wireless modem. If **net.wireless.mode** is set to OFF then the LED should remain unlit. When **net.wireless.mode** is set to PERMANENT-EDGE or PERMANENT-GPRS, the LED flashes once per second while the modem is attempting to establish a network connection. Once the connection is established, the LED blinks every 3 seconds.

Status Commands
On all products, the current status of the wireless connection can be displayed using the "**?w**" or "**statusw**" commands. (Note that "**?wire**" or "**?wireless**" or "**statusw**" or "**status wireless**" are also valid commands.) The unit will respond with: "**Wireless modem status: <state>** Possible states are:

:not installed	wireless card not detected
:not enabled	net.wireless.mode=OFF
:connecting	attempting to establish connection *
:connected	connection established, no active TCP session
:active	connection established, one or more active TCP sessions
:idle	which it may be for only a moment between sessions

* if it says "Connecting" most of the time, there is a problem and it would be advisable to contact Asentria Tech Support to check the wireless modem log.

Troubleshooting Commands
For troubleshooting, user either the "**?w log**" or "**statusw log**" command. (Note that "**?wire log**" or "**?wireless log**" or "**statusw log**" or "**status wireless log**" are also valid commands. The word "log" must be preceded by a space.) Contact Asentria Tech Support if troubleshooting is required as the log data probably will not be useful to the user.

ADSL Modem

TeleBoss units that are ADSL-modem-equipped can connect to the Internet via ADSL. This means that the unit can reach Internet hosts and have an Internet IP address but the address is completely firewalled so you will not be able to, for example, ping the unit's DSL interface IP address.

Note: Full ADSL modem functionality is only available on TeleBoss products with the "SitePath" build (version 2.03.000 or greater). If there is any question about whether your unit has the SitePath build, contact Asentria Technical Support (support@asentria.com) or 206-344-8800.

Installation

If installing the ADSL modem for the first time (not factory installed), follow these installation instructions:

- Make sure the host unit (e.g. TeleBoss device) is powered down.
- Remove the two screws from any of the expansion port covers on the back panel of the host unit and set the port cover aside. Carefully slide the ADSL modem card into the plastic rails inside the expansion port and push the card in all the way. Replace the two screws previously removed so the card is held securely in the port.
- Power up the host unit.

Description of ADSL

ADSL (Asymmetric Digital Subscriber Line) is a technology where data is modulated onto higher frequencies of copper telephone lines not used for voice in such a way that upstream and downstream data rates differ. Certain Asentria TeleBoss units can have an ADSL modem expansion card installed to provide an interface to a line. The machine on the other end of the line is a DSLAM (Digital Subscriber Line Access Multiplexer). DSLAMs exist typically inside telephone company central offices (COs) but also exist in standalone hutches (remote DSLAMs).

The abbreviations "DSL" and "ADSL" are used interchangably in this documentation; where "DSL" is written, "ADSL" also applies unless the difference is explicitly specified.

Certain terms and acronyms are used throughout this guide that may require further explanation. These are hyper-linked to the Glossary at the end of the guide.

Configuration

The ADSL modem can be configured via two methods in the TeleBoss unit: command line menus or Setting Keys. For simplicity, only the Setting Keys method is discussed in this guide. However, as you are working through the configurations you are welcome to also use the related Command Line menus (Setup ->Network Settings -> DSL Settings) or web-interface menus in your TeleBoss unit to view or configure specific settings.

There are four ways to configure ADSL depending on the specifications from your ADSL and ISP providers. In some cases the ADSL provider and ISP provider are the same. For simplicity and unless otherwise specified, "ADSL provider" means the entity that provides all settings required for the unit to use the Internet over the ADSL.

The key datum to get from your ADSL provider is what type of addressing is to be used: **PPPoA** (PPP over ATM), **PPPoE** (PPP over Ethernet), **Static**, or **DHCP**. Make note of this, then proceed with configuring the ADSL modem as described below.

Set the value of the **net.dsl.type** Setting Key to either **PPPoA**, **PPPoE**, **Static**, or **DHCP** as instructed by your ADSL provider. This is the most important DSL setting since its value determines what other DSL settings are applicable to the DSL configuration. Each of these connection protocols requires specific settings, so refer to the paragraph below for the protocol you will be using. But first, there are some settings that must be configured regardless of how **net.dsl.type** is set.

Required Settings Regardless of Connection Protocol

net.dsl.vpi
This specifies the VPI (Virtual Path Identifier) used on the DSL interface. This is provided for you by your DSL provider and is required for DSL operation. Values are: **0** to **4095**

net.dsl.vci
This specifies the VCI (Virtual Channel Identifier) for the DSL interface. This is provided for you by your DSL provider and is required for DSL operation. Values are: **0** to **65535.**

net.dsl.encap
This controls whether the encapsulation is LLC (Logical Link Control) or VCM (Virtual Channel Multiplexed). This is provided for you by your DSL provider and is required for DSL operation. Values are **LLC** or **VCM**.

Settings for PPPoA or PPPoE

net.dsl.username
This specifies the PPP username for the DSL interface. This is provided for you by your DSL provider. Values are text strings up to 64 characters.

net.dsl.password
This specifies the PPP password for the DSL interface. This is provided for you by your DSL provider. Values are text strings up to 64 characters.

Settings for Static

net.dsl.mode
This controls whether the DSL is set up for Bridged mode or Routed mode. This is provided for you by your DSL provider. Values are **BRIDGED** or **ROUTED**.

net.dsl.ip
This is the public IP address of the unit in the case where the DSL link is active. This is essentially inaccessible from the outside world because it is completely firewalled on the unit. This is provided for you by your DSL provider. Value is a dotted quad IP address.

net.dsl.mask
This controls the mask used on the DSL interface. This is provided for you by your DSL provider. It is applicable only when net.dsl.type is STATIC. Value is a dotted quad subnet mask.

net.dsl.router
The router for the DSL interface. This is provided for you by your DSL provider. This is applicable only when net.dsl.type is STATIC. Value is a dotted quad IP address.

net.dns
This specifies Domain Name System addresses to use. This is provided for you by your DSL provider. Value is a dotted quad IP address.

Settings for DHCP

If **net.dsl.type** is DHCP then no additional settings need to be configured.

Activation

Once the DSL interface is configured it must be activated. This happens automatically or manually according to how the Start Mode setting is configured:

net.dsl.startmode Set this to MANUAL to require user intervention to raise the DSL interface, or to let a VPN (if it is configured to use DSL) raise the DSL interface when the VPN needs to use DSL. Set this to AUTO to tell the unit to automatically raise the DSL interface upon boot. Values are **MANUAL** or **AUTO**. Default setting is MANUAL.

Manual Activation

net.dsl.command Set this to 1 to manually activate the DSL interface, and set this to 0 to manually deactivate the DSL interface.

In manual activation the DSL interface will not activate unless some purpose requires it: either you tell it to activate or your ADSL-based VPN, when it is being raised, tells it to activate. If you tell the interface to activate then do this by

setting **net.dsl.command=1**. The unit returns COMPLETE, meaning it has started the activation process; it does not mean that the inteface is ready to use yet. Activation is a multistep process and may take a minute or two to complete.

If the VPN tells the interface to activate, then activation happens when the VPN raises.

Read **net.dsl.command** (or **net.dsl.status**) to check the status of the DSL interface.

net.dsl.command=0 when the DSL interface is not activated
net.dsl.command=1 when DSL activation is in process
net.dsl.command=2 when the DSL interface is trained but not yet fully activated
net.dsl.command=3 when the DSL interface is fully activated (ready to use for network traffic)

If the interface doesn't activate, then first check if anything about the configuration on the unit is invalid. Then check this configuration against what was specified by the ADSL provider.

Automatic Activation

In automatic activation the unit raises the DSL interface upon boot and keeps it up until it is explicitly deactivated by the user by setting **net.dsl.command=0**.

Once the interface is activated you can use it as an outbound-only interface. It is completely firewalled to the Internet. The only traffic allowed in is traffic associated with existing connections, meaning all connections must originate from unit. Pinging (ICMP), TCP, and UDP traffic is the only traffic allowed and this traffic must originate from the unit.

Data on the ADSL connection can be viewed with the **net.dsl.info.*** key branch:

net.dsl.info.isp.ip
Read this key to see what IP address the DSL interface is using with the ISP.

net.dsl.info.isp.linktime
Read this key to see how long the unit has been connected to the ISP (i.e., how long the unit has had Internet access) since the connection was started.

net.dsl.info.isp.status
Read this key to see whether the unit is connected to the ISP; it returns "Connected" or "Not Connected". Another key that gives the same information in a different format is **net.dsl.status**.

net.dsl.info.isp.discreason
Read this key to see why, if available, DSL connectivity was lost.

net.dsl.info.link
Read this key to see whether the unit has DSL connectivity (as opposed to ISP connectivity shown with **net.dsl.info.isp.status**).

net.dsl.info.speed
Read this key to see the speed of the link (provided there is DSL connectivity, as shown with **net.dsl.info.link**).

net.dsl.info.ver.sw
Read this key to see the ADSL modem software version.

net.dsl.info.ver.fw
Read this key to see the ADSL modem firmware version.

net.dsl.info.ver.atm
Read this key to see the ADSL modem ATM driver version.

net.dsl.info.ver.dslhal
Read this key to see the ADSL modem DSL HAL version.

net.dsl.info.ver.sarhal
Read this key to see the ADSL modem SAR HAL version.

net.dsl.info.ver.pump
Read this key to see the ADSL modem data pump version.

net.dsl.info.updated
Read this key to see the last date/time at which the values in the **net.dsl.info.*** key hierarchy were last updated. These values are updated when directed by the user (by setting **net.dsl.command** to 20) or every few seconds by the unit until the ADSL modem is connected to the ISP (at which time it doesn't update until directed by the user or ISP connectivity is lost).

DSL Status

net.dsl.status is a read-only key that displays a value that reflects the current state of the DSL interface. Values are an integer >=0.

- **0** means it is not activated (the unit is not talking to the modem, no address is usable with the ISP, the DSL is not trained)
- **1** means the interface is in an intermediate level of availability: there is no address usable with the ISP and the DSL is not trained, but the unit **can** talk (but not necessarily **is** talking) to the modem.
- **2** means the interface is in an intermediate level of availability, moreso than value "1": there is no address usable with the ISP but the DSL **is** trained and the unit has good communication with its DSL modem.
- **3** means the interface is fully activated: DSL is trained and there is an address usable with the ISP.

These values are analagous to modem LEDs seen on some DSL routers: power, "link", "DSL", "Internet". 0 can be though of as "power", 1 can be thought of as "link", 2 can be thought of as "DSL", and 3 can be thought of as "Internet".

Connectivity

When the interface is activated it can be used for Internet connectivity. The simplest way to use it is as ADSL gateway via the DSL routing function (see DSL Routing section).

Deactivation

Deactivation means the unit is no longer connected to the ISP provider via ADSL. Deactivate by setting **net.dsl.command=0**. When the DSL interface is deactivated the line may still be trained.

ADSL specifications

- Full rate ANSI T1.413 Issue2, ITU-T G.992.1 and ITU-T G.992.2 standards compliant
- ITU G.992.3, ITU G.992.5 and READSL2 ADSL2/2+ standards compliant
- Annex M and Annex L specification
- Downstream and upstream data rates up to 24Mbps and 1Mbps
- Reach length up to 22Kft.
- Dying Gasp functionality
- OAM F4/F5 loop back
- VC and LLC multiplexing
- Multiple protocols over AAL5 (RFC 2684 / RFC 1483)
- PPPoA (RFC 2364)
- PPPoE (RFC 2516)
- UBR, CBR, rt-VBR and nrt-VBR traffic shaping QoS

DSL Routing

DSL routing is used to make the unit route, and do network address translation (NAT) on, NAT-capable traffic (TCP, UDP, and ICMP) from the unit's Ethernet ports to the unit's DSL peer, and hence on to the Internet. For example, a PC that uses one of the unit's Ethernet addresses as its default router can browse the web via the unit's DSL connection. The DSL interface is firewalled such that only traffic related to already-existing-outgoing connections is allowed in.

Configuration

The following Setting Keys need to be configured:

net.dsl.startmode
Set this to AUTO to tell the unit to automatically raise the DSL interface upon boot. Set this to MANUAL to require user intervention to raise the DSL interface, or to let a VPN (if it is configured to use DSL) raise the DSL interface when the VPN needs to use DSL. Values are **MANUAL** or **AUTO**. Default setting is MANUAL.

net.default.router
This setting allows you to select the default router (gateway) for the unit. Each network interface has a router setting which you can configure; this is the machine on that interface to which frames will be sent if they do not route to the local network of that interface. However the unit uses only one of those configured routers at this time. As you configure router settings the unit will choose a default router for you. This is available for you to see (and override) via this **net.default.router** setting. The values you may choose for this setting (i.e., router addresses) must be in the set of routers which you have specified, or the special value, "DSL", which means that the DSL interface peer is the default router. For DSL Routing, set **net.default.router=DSL**.

The unit uses a routing table to determine how to send any outbound IP frame. Each entry in the routing table tells the unit how to send a frame whose destination address matches a rule in the routing table. Routing table entries are examined from most-restrictive to least-restrictive, so the default routing table entry is the last entry in the table since it is the least restrictive. It is the catch-all route: it tells the unit how to send a frame when it doesn't know how else to send it. The only routes on the unit at this time are network interface routes and the default route. Network interface routes tell the unit how to send a frame bound for a machine on one of the unit's local networks (subnets). These routes are automatically configured when you configure the address of a network interface. If an outbound frame is destined for a machine off all local networks then it is sent according to what the default route specifies. The default route specifies the default router to use for these frames.

If you have configured only one router for all of your network interfaces then you don't have to worry about this setting: the unit configures it for you and there is nothing you can override it with. The default router is engaged as soon as it is configured.

net.dsl.routing.enable
Set this to ON to make the unit forward frames received on either Ethernet interface (and not addressed to the unit) out the DSL interface. Frames are NAT-ed as they leave the DSL interface. Frames arriving on the DSL interface not associated with existing connections are blocked (the unit is firewalled). Note that the unit's default router must be set to DSL (**net.default.router=DSL**) for DSL routing to work. Set this to OFF to make the unit not do this. Values are: **ON** or **OFF**. Default is OFF.

net.dsl.override
Set this to a non-zero value to enable ADSL web configuration access on the TCP port specified by the value. Set this to 0 to disable web configuration access. Values are: **0** to **65535**. Default is 0.

net.dsl.cmd
This has the same behavior as **net.dsl.command**.

net.dsl.status
Upon read this returns 0, 1, 2 or 3. Refer to the net.dsl.status description above for further details.

DSL Routing Example

1) Configure the unit so it sits on an Ethernet network.

2) Enter the following keys to configure the unit for routing:
   net.dsl.startmode=manual
   net.default.router=dsl
   net.dsl.routing.enable=on

3) Say the DSL provider sent you these settings:
   ```
   PPPoA (VCM)
   VPI: 0
   VCI: 38
   Username: dsluser
   Password: dslpassword
   ```

4) Enter the following Setting Keys to configure the unit accordingly:
   net.dsl.type=pppoa
   net.dsl.mode=vcm
   net.dsl.vpi=0
   net.dsl.vci=38
   net.dsl.username=dsluser
   net.dsl.password=dslpassword

5) Enter the following function key to raise the DSL interface:
   net.dsl.cmd=1

6) Upon setting this key to 1 the unit begins the process of raising the DSL interface. You can query the status of the DSL interface by reading the **net.dsl.status** function key. To lower the DSL interface, set:
   net.dsl.cmd=0

7) After a minute or two this key (or the **net.dsl.status** key) will return 3. If something went wrong then it will stay at 1 or 2 in which case the configuration should be rechecked.

8) To make the interface raise upon boot, enter:
   net.dsl.startmode=auto

9) Test the connection by pinging an Internet host from the unit. Once it is verified good, proceed to configure machines which will use the unit as a DSL router. On these machines set their default router to the unit's Ethernet IP address (address that is on the same subnet as these machines). Optionally you can configure this same address as a DNS server for these machines. Test the routing connection by pinging an Internet host from these machines.

DSL Glossary

ATM
Asynchronous **T**ransfer **M**ode is a network technology based on transferring data in cells or packets of a fixed size. The cell used with ATM is relatively small compared to units used with older technologies. The small, constant cell size allows ATM equipment to transmit video, audio, and computer data over the same network, and assure that no single type of data hogs the line.

DHCP
Dynamic **H**ost **C**onfiguration **P**rotocol, a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network.

DSLAM
A **D**igital **S**ubscriber **L**ine **A**ccess **M**ultiplexer is a mechanism at a phone company's central location that links many customer DSL connections to a single high-speed ATM line. When the phone company receives a DSL signal, an ADSL modem with a splitter detects voice calls and data. Voice calls are sent to the PSTN (Public Switched

Telephone Network), and data are sent to the DSLAM, where it passes through the ATM to the Internet, then back through the DSLAM and ADSL modem before returning to the customer's PC or networked-device.

LLC and VCM
Logical **L**ink **C**ontrol and **V**irtual **C**hannel **M**ultiplexing are methods of encapsulating data on an ATM communication link. Encapsulation is the process of storing cells from the foreign protocol inside PPP frames.

PPP
Point-to-**P**oint **P**rotocol is a method of connecting a PC or networked-device to the Internet.

Setting Keys
A Setting Key is a "<setting> = <value>" statement. <setting> is a series of keywords that describe a particular function of the unit, or setting. These keywords are separated by periods, for example **net.dsl.startmode**. The current value of a Setting Key can be obtained by typing **sk <setting>** at the command line and pressing the Enter key. A new value for a Setting Key can be set by typing **sk <setting> = <value>** and pressing the Enter key. The value must be valid for that particular Setting Key, and the unit will respond with COMPLETE when it is accepted. If the value is invalid, the unit will respond with Invalid Value. Contact Asentria Tech Support for more information on Setting Keys if necesary.

Signal-to-noise ratio
Signal-to-noise ratio is an electrical engineering concept defined as the ratio of a signal power to the noise power corrupting the signal. In less technical terms, signal-to-noise ratio compares the level of a desired signal to the level of background noise. The higher the ratio, the less obtrusive the background noise is.

Trained
This refers to the general ability of a modem to adjust itself to optimize the communication channel. When a modem modulates data on a line, the communication infrastructure degrades the data. Some of this degradation is due to noise and some of it is due to the modem's own echo. Part of training the modem (also sometimes referred to as "training the line") involves having the modem select optimal signal-to-noise ratio as well as teaching the modem what its own "voice" (its echo) sounds like on the line. A modem receives not only data from the other modem but also its own echoes, like when you yell to someone across a canyon and listen for their response; training helps the modem separate its own echos from the signal from the other modem.

VCI
A **V**irtual **C**hannel **I**dentifier is a unique identifier which indicates a particular virtual circuit on a network. It is a 16-bit field in the header of an ATM cell. The VCI, together with the VPI (Virtual Path Identifier) is used to identify the next destination of a cells as it passes through a series of ATM switches on its way to its destination.

VPI
Virtual **P**ath **I**dentifier refers to an 8-bit (user to network packets) or 12-bit (network-network packets) field within the header of an ATM cell. The VPI, together with the VCI (Virtual Channel Identifier) is used to identify the next destination of a cell as it passes through a series of ATM switches on its way to its destination. VPI is useful to reduce the switching table for some Virtual Circuits which have common path.

VPN
Virtual **P**rivate **N**etwork is a network that is tunneled (the virtual part), typically across a public network, and secured (the private part).

Battery Module

The TeleBoss 830 is available with an optional battery backup that provides backup power for the unit in the event of power loss.

Setup

Ensure the front panel battery enable/disable switch is in the 'enable' position. There is no other setup associated with using the battery module, nor are there any settings related to it.

Operation

As long as the front panel battery enable/disable switch is in the 'enable' position, the battery will be available in case of power loss. The amount of time that the host unit can run off battery power depends on various things including the state of battery charge at the time, and the number and type of optional devices installed in the host unit.

If the unit is running on battery power, and the front panel battery enable/disable switch is changed to the 'disable' position, the host unit will immediately shut down.

The host unit cannot be started up from the battery. This is because battery relay (which connects the battery power to the system) is open when no power is applied; it gets closed once the unit starts up and the battery manager application runs. Only at that point does battery power become available.

The status of the battery module can be determined from the command processor via the battery status command.

Basic Status

```
>status battery
Battery Status

Enable switch position: ON
Running on battery: YES (0:05:13
```

Note that the command can also be invoked in a more abbreviated format such as **"? battery"**, **"statusb"** or even **"?b"**.

When the charging current goes below 100mA, the charging voltage is switched from high (7.35 volts) to low (6.85 volts).

When running on battery power, if the battery voltage falls below 5.435 volts, the unit shuts down. Several warning messages are sent to all open command processors as the battery voltage gets low.

Appendices

User Rights Table

The following tables contain the rights available to each access level within the user profiles.

Command Permissions

Command	None	View	Admin1	Admin2	Admin3	Master
ADDLF			X	X	X	X
BYE	X	X	X	X	X	X
COLDSTART						X
DEFAULT						X
DELETE			X	X	X	X
DIR		X	X	X	X	X
DOMAIL		X	X	X	X	X
DOPAGE		X	X	X	X	X
DOTRAP		X	X	X	X	X
EXIT	X	X	X	X	X	X
FTP		X	X	X	X	X
GET		X	X	X	X	X
HELP	X	X	X	X	X	X
MODEMTALK						X
PING			X	X	X	X
RELOADALL	X	X	X	X	X	X
RESTART			X	X	X	X
RZ			X	X	X	X
SET			X	X	X	X
SETUP			X	X	X	X
SK		X	X	X	X	X
STATUS, ?		X	X	X	X	X
SUPPORT		X	X	X	X	X
TESTTIME		X	X	X	X	X
TYPE		X	X	X	X	X
VER		X	X	X	X	X

Setup Menu Permissions

Settings	View	Admin1	Admin2	Admin3	Master
Most settings	View	X	X	X	X
Authentication				View	X
Passwords					X
Event log	View	View	View	X	X
Audit log	View	View	View	X	X
PPP dial username		View	View	View	X
PPP dial password					X
Caller ID				View	X

Control Characters

Some of the following control characters may be used in various functions within the T830, including CRC mode for AsentriaAlarms and the Escape Key.

Char	Dec	Hex	Control Key	Control Action
NUL	0	00	^@	Null
SOH	1	01	^A	Start of heading
STX	2	02	^B	Start of text
ETX	3	03	^C	End of text
EOT	4	04	^D	End of transmission
ENQ	5	05	^E	Enquiry
ACK	6	06	^F	Acknowledge
BEL	7	07	^G	Bell
BS	8	08	^H	Backspace
HT	9	09	^I	Horizontal tab
LF	10	0A	^J	Line feed
VT	11	0B	^K	Vertical tab
FF	12	0C	^L	Form feed
CR	13	0D	^M	Carriage return
SO	14	0E	^N	Shift Out
SI	15	0F	^O	Shift In
DLE	16	10	^P	Data link escape
DC1	17	11	^Q	XON
DC2	18	12	^R	Device control 2
DC3	19	13	^S	XOFF
DC4	20	14	^T	Device control 4
NAK	21	15	^U	Negative acknowledge
SYN	22	16	^V	Synchronous idle
ETB	23	17	^W	End transmission block
CAN	24	17	^X	Cancel
EM	25	19	^Y	End of medium
SUB	26	1A	^Z	Substitute
ESC	27	1B	^[	Escape
FS	28	1C	^\	File separator
GS	29	1D	^]	Group Separator
RS	30	1E	^^	Record Separator
US	31	1F	^_	Unit Separator

Internal Modem Guidelines

The internal modem supplied with this product complies with Part 68 of the FCC Rules and Regulations. The labeling on the modem provides the FCC Registration number and the Ringer Equivalence Number (REN) for the modem. This information is also listed below. You must provide, upon request, this information to your telephone company.

The REN is useful to determine the quantity of devices you may connect to a telephone line and still have all of these devices ring when the number is called. In most, but not all areas, the sum of the RENs of all devices connected to one line should not exceed five (5.0). To be certain of the number of devices you may connect to a line, as determined by the REN, you should contact the local telephone company to determine the maximum REN for your calling area.

If the modem causes harm to the telephone network, the telephone company may temporarily discontinue your service. If possible, they will notify you in advance. If advance notification is not possible, you will be notified as soon as possible.

Your telephone company may make changes in its facilities, equipment, operations or procedures that could affect proper functioning of your equipment. If they do, you will be notified in advance to give you an opportunity to maintain uninterrupted telephone service.

If you experience trouble with the modem, contact Asentria at (206) 344-8800 for information on obtaining service or repairs. The telephone company may ask you to disconnect the device from the network until the problem has been corrected or until you are sure that the device is not malfunctioning.

This device may not be used on coin service lines provided by the telephone company (this does not apply to private coin telephone applications which use standard lines). Connection to party lines is subject to state tariffs.

Modem	**FCC ID**	**REN**
2400 Baud Modem	EUD-5U9-BRI4480	0.8B
33.6K Baud Radicomm Modem	406CHN-31735-PT-E REN 1.1B	1.1B
33.6K Baud OmniModem	6KMUSA-34184-MME REN 0.9B	0.9B
33.6K Baud MultiModem	AU7-USA-46014-MD-E	0.1B

Canadian Department of Communications

NOTICE: The Canadian Department of Communications Label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protections that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of total load to be connected to a telephone loop, which is used by the device, to prevent overloading.

The termination of a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100. The load number of this unit is five.

This digital apparatus does not exceed the Class A limits for Radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled "Digital
Apparatus", ICES-003 of the Department of Communications.

AVIS: - L'étiquette du ministère des Communications du Canada identify le materiel homologué. Cette étiquette certifie que le matériel est conforme a certaines normes de protection, d'exploitation et de sécurité des réseaux de télécommunications. Le Ministère n'assure toutefois pas que le matériel fonctionnera a la satisfaction de l'utilisateur.

Avant d'installer ce matériel, l'utilisateur doit s'assurer qu'il est permis de le raccorder aux installations de l'entreprise locale de télécommunication. le matériel doit également etre installé en suivant une méthod acceptée de raccordement. Dans certains cas, les fils intérieurs de l'entreprise utilisés pour un service indivuduel a linge unique peuvent etre prolongés au moyen d'un dispositif homologué de raccordement (cordon prolongateur téléphonique interne). L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées ci-dessus n'empechent pas la dégradation du service dans certaines situations. Actuellement, les entreprises de télécommunication ne permettent pas que l'on raccorde leur matériel a des jacks d'abonné, sauf dans les cas précis prévus pas les tarrifs particuliers de ces entreprises.

Les réparations de matériel homologué doivent etre effectuées pas un centre d'entretien Canadien autorisé designé par le fournisseur, La compagnie de télécommunications puet demander a l'utilisateur de débrancher un appareil a la suite de réparations ou de modifications effectuées par l'utilisateur ou a cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise a la terre de la source d'energie electrigue, des lignes téléphoniques et des canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particuliérement importante dans les régions rurales.

Avertissement. - L'utilisateur ne doit pas tenter de faire ces raccordements lui-meme; il doit avior recours a un service d'inspection des installations électriques, ou a electricien, selon le cas.

L'indice de charge (IC) assigné a chaque dispositif terminal indique, pour éviter toute surcharge, le pourcentage de la charge totale qui peut etre raccodée a un circuit téléphonique bouclé utilisé par ce dispositif. La terminaison du circuit

bouclé peut etre constituée de n'import quelle combinaision de dispositif, pourvu que la somme des indices de charge de l'ensemble des dispositifs ne dépasse pas 100. L'indice de charge de cet produit est 5.

Cet appereil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur :"Appareils Numériques", NMB-003 édictée par le ministre des Communications.

Warranty Information

Asentria Corporation hereby warrants that it will, as the buyers sole remedy, repair or replace, at its option, any part of the T830 which proves to be defective by reason of improper materials or workmanship, without charge for parts or labor, for a period of 12 (twelve) months. This warranty period commences on the date of first retail purchase, and applies only to the original retail purchaser.

To obtain service under this warranty, you must obtain, by telephone, postal letter, or email, a return authorization number from Asentria Technical Support. This authorization number may be obtained by contacting Asentria Technical Support at the address and/or phone number below. The defective unit is to be returned to Asentria with shipping prepaid, and the return authorization number must be clearly marked on the outside of the package containing the defective unit.

The dealer's bill of sale or other satisfactory proof of the date of purchase may be required to be presented in order to obtain service under this warranty.

This warranty applies if your T830 fails to function properly under normal use and within the manufacturer's specifications. This warranty does not apply if, in the opinion of Asentria Corporation, the unit has been damaged by misuse; neglect; or improper packing, shipping, modification, or servicing by other than Asentria or an authorized Asentria Service Center.

In no event shall Asentria Corporation be liable for any loss, inconvenience or damage, whether direct, incidental, consequential or otherwise, with respect to the T830. Asentria Corporation's liability shall be limited to the purchase price of the T830. No warranty of fitness for purpose, or of fitness of the T830 for any particular application is provided. It is the responsibility of the user to determine fitness of the T830 for any particular application or purpose.

This warranty gives you specific legal rights. These rights may vary from state to state, as some states do not allow limitations on liability.

You may request information on how to obtain service under this warranty by contacting Asentria Technical Support at the address and phone number below:

Asentria Technical Support
1200 North 96th St.
Seattle, WA 98103
206.344.8800
support@asentria.com