WTI Part No. 14069
Rev. G

AFS-16-1

RJ45 Fallback Switch

User's Guide

Power & Console Solutions | wti.com

Warnings and Cautions:
Installation Instructions

Secure Racking

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

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

Input Supply

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

Grounding

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

No Serviceable Parts Inside; Authorized Service Personnel Only

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

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

Two Power Supply Cables

Note that the AFS-16 features two separate power inputs, and a separate power supply cable for each power input. Make certain to disconnect both power supply cables from their power source before attempting to service or remove the unit.

Disconnect Power

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

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

Disconnect Power Before Servicing

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

Agency Approvals

FCC Part 15 Regulation

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

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

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

EMC, Safety, and R&TTE Directive Compliance

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

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

  and

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

  and

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

Industry Canada - EMI Information

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

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

Table of Contents

List of Figures

1. Introduction

The AFS-16-1 is a versatile switching system, designed for applications that require routing of analog or digital signals between a common RJ45 jack and “A” and “B RJ45 jacks. The AFS is ideal for switching RS232, RS422/485, Ethernet/UTP or telephone lines.

The system consists of a Card Rack, one Power Supply Module, one Control Module, and up to 16 Circuit Modules. Each Circuit Module is capable of switching all 8 pins of the Common RJ45 jack between Jack “A” or Jack “B”. Each card can be switched by alarm, manually, or by command.

The AFS includes an assortment of alarm features, which allow the unit to monitor temperature, power interruptions, and invalid access attempts and then notify you via Email, text message, Syslog message or SNMP trap when critical conditions are detected. The AFS can also monitor device response to ping commands and then switch A/B paths and provide notification when devices fail to respond.

Security and Co-Location Features:

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

The AFS also provides four different levels of security for user accounts: Administrator, SuperUser, User and ViewOnly. The Administrator level provides complete access to all A/B switching functions, status displays and configuration menus. The SuperUser level allows control of A/B switching, but does not allow access to configuration functions. The User level allows access to only a select group of Administrator-defined A/B circuits. The ViewOnly level allows you to check unit status, but does not allow A/B switching or access to configuration menus.

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

Environmental Monitoring and Management:

The AFS can constantly monitor temperature levels, ping response and other factors. If the AFS detects that user defined thresholds for these values have been exceeded, the unit can promptly notify you via email, text message, SNMP trap, or Syslog message. The AFS also records temperature readings to a convenient log file.

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

WTI Management Utility

The AFS includes the WTI Enterprise Management Utility (WMU,) which allows you to manage multiple WTI units via a single menu. For more information on the Enterprise Management Utility, please refer to the WMU User's Guide, which can be downloaded from the WTI web site at: http://www.wti.com/t-product-manuals.aspx.

Typographic Conventions

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

2. Unit Description

The AFS consists of a frame unit, one Dual Power Supply Module, one Control Module, and up to sixteen Circuit Modules.

2.1. The Dual Power Supply Module

The Dual Power Supply Module, shown in Figure 2.1, provides AC power used by the Control Module and Circuit Module(s). The AFS will always include one Dual Power Supply Module. Note that the Power Supply Module is not designed to be removed from the AFS Rack Assembly.

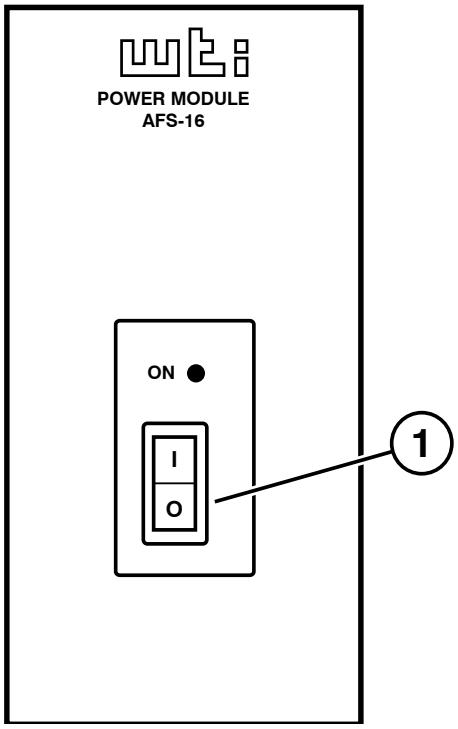

Figure 2.1: The Power Supply Module

The Power Supply Module faceplate includes the following:

① **Power Switch and ON Indicator**

② **Power Inlets:** (Not Shown) Two (2) IEC320-C14 AC inlets (located on the back panel of the Dual Power Supply Module) which are used to connect the AFS to an appropriate power source.

③ **Power Supply Indicators:** Two LEDs (located on the back panel of the Dual Power Supply Module), which will light when connected to an active power source. Note that there is one LED for Inlet "A" and one LED for Inlet "B".

2.2. The Control Module

The Control Module, shown in Figure 2.2, coordinates switching of the individual Circuit Modules. The Control Module includes a Master A/B Gang Switch, status LEDs, a 10/100Base-T Ethernet connector and an RJ-45 RS232 Serial Port for connection to your PC, control device or external modem. An AUX jack is provided to allow connection to a monitored line and optional external alarm. The AFS always includes one Control Module.

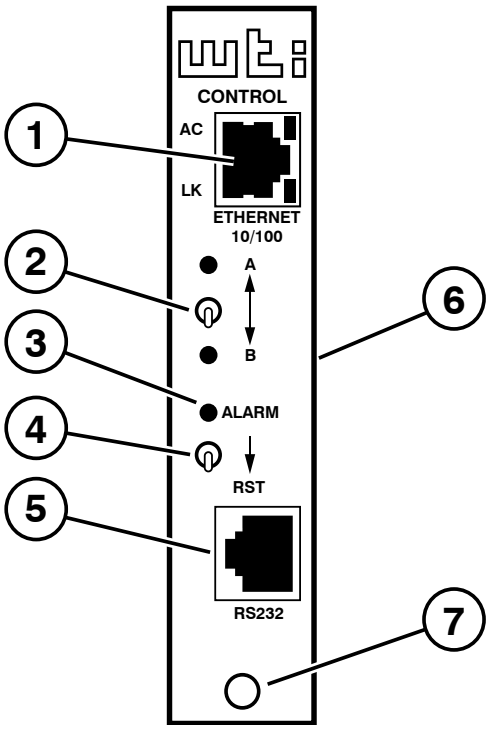

Figure 2.2: The Control Module

The AFS Control Module includes the following components:

① **Ethernet Port:** An RJ45 Ethernet port for connection to your 10Base-T or 100Base-T, TCP/IP network. Note that the AFS features a default IP address (192.168.168.168). This allows you to establish an SSH connection with the unit without first assigning an IP address. Note that the Network Port also includes two, small LED indicators for Link and Data Activity.

② **Master A/B Gang Switch:** Allows manual control of A/B switching at up to sixteen Circuit Modules. Note that the Master A/B Gang Switch can be disabled as described in Section 5.3.

③ **ALM Indicator:** The ALM Indicator will light when Monitor Input Alarm is triggered. For more information on the Monitor Input Alarm, please refer to Section 7.6.

④ **Reset Switch:** To reinitialize the AFS, hold the Reset Switch in the "down" position for approximately five seconds. When the AFS is reset, all users will be disconnected from the AFS and the operating system will be reloaded.

⑤ **RS232 Connector:** An RJ-45 Serial Port for connection to your PC, control device, or external modem. Please refer to Appendix A for a description of the RS232 interface.

⑥ **AUX Connector:** (Not Shown) A five terminal quick connector, located on the back edge of the Control Module board. The AUX Connector can be used in conjunction with the Monitor/Alarm Input feature to generate an alarm when the status of pin 4 changes. In addition, pins 1 through 3 on the AUX Connector can also be used to switch a connected device On or Off in response to signal changes at Pin 4. For more information, please refer to Section 7.

Notes:

- *The Monitor Input signal (Pin 4) is always measured relative to the signal at the common ground (Pin 5).*
- *A "Low" signal should be between Zero (0) Volts and -48 Volts and a "High" signal should be between +5 Volts and +48 Volts.*

⑦ **Release Pin:** A snap-lock pin that is used to secure the Control Module to the AFS frame.

⑧ **Monitor Input Level Jumper:** (Not Shown) A jumper located on the Control Module board, which is used to configure the AUX Connector for use with the Monitor/Alarm Input feature. The Monitor Input Level Jumper selects the non-active state for the Monitor/Alarm Input feature. When the jumper is set in the "1" position (normally high,) the Monitor/Alarm Input feature can generate an alarm when the Monitor Input signal goes low. When the jumper is set in the "0" position (normally low,) the Monitor/Alarm Input feature can generate an alarm when the Monitor Input signal goes high. For more information on the Monitor/Alarm Input feature, please refer to Section 7.6.

2.3. The Circuit Module

The AFS can accept up to sixteen Circuit Modules. Each Circuit Module includes a common jack, jacks for "A" and "B" paths, and a Manual A/B switch as described in Figure 2.3.

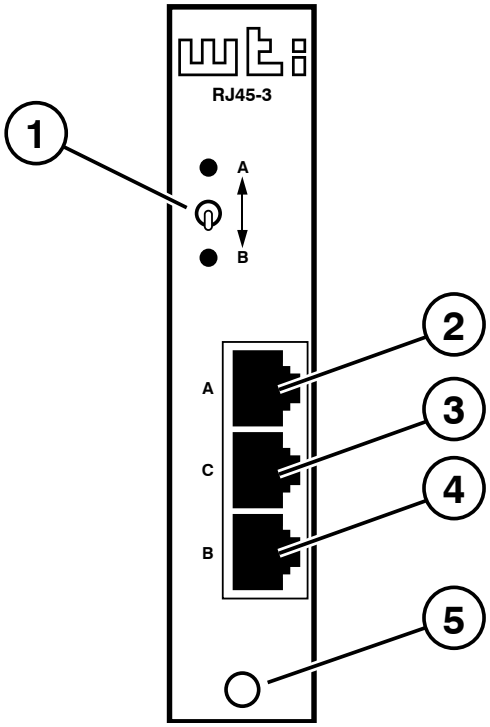

Figure 2.3: The Circuit Module

The AFS Circuit Module includes the following components:

① **A/B Switch:** Each A/B Switch can be manually switched, or activated by commands sent to the Control Module. The A/B Switch can also be operated by the Control Module's Master A/B Switch.

② **"A" Connector:** An RJ45 Port, used for connection to your primary line.

③ **"C" Connector:** An RJ45 Port, used for connection to a common line.

④ **"B" Connector:** An RJ45 Port, used for connection to your fallback line.

⑤ **Release Pin:** Used to secure the Circuit Module to the AFS frame.

⑥ **A/B Switch Jumper:** (Not Shown) A jumper, located on the Circuit Module board, which is used to enable/disable the individual Circuit Module's response to the Master A/B Gang Switch as described in Section 4.5.1.

3. Getting Started

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

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

3.1. Apply Power to the AFS

Refer to the safety precautions listed at the beginning of this User's Guide, and then connect the unit to a 100 to 240 VAC power source.

> **Note:** *The AFS includes two power inlets. You can connect either one or both of these inputs to your power source. If both power inlets are connected, they should be connected to separate power sources in order that the second power source can serve as a redundant back up in the event of failure.*

Connect the power supply cable(s) to the unit's power inlet(s) and then connect the cable(s) to appropriate power supplies.

Set the Power Switch on the AFS Power Module to the ON Position. The ON LED on the Power Module and the A/B indicators on the Control Module should light. After about 90 seconds, the A/B indicators should go out, indicating that the unit is ready to receive commands.

3.2. Connect Your PC to the AFS

The AFS can either be controlled by a local PC Serial Port, controlled via modem, or controlled via TCP/IP network. In order to select parameters or control switching functions, commands are issued to the AFS via either the Ethernet Port or RS232 Console Port.

- **Ethernet Port:** Connect your 10Base-T or 100Base-T network interface to the AFS Control Module's 10/100Base-T Network Port.
- **RS232 Port:** Use the supplied Ethernet cable and adapter to connect your PC COM port to the RS232 Console Port on the AFS Control Module as described in Section 4.3. For a description of the RS232 Port Interface, please refer to Appendix A.1.
- **Modem:** If desired, an external modem can also be installed at the RS232 Port. For more information, please refer to Section 4.4.

3.3. Communicating with the AFS

When properly installed and configured, the AFS will allow command mode access via Telnet, Web Browser, SSH client, modem, or local PC. However, in order to ensure security, both Telnet and Web Browser access are disabled in the default state. To enable Telnet and/or Web Browser access, please refer to Section 5.9.2.

Notes:

- *Default AFS serial port parameters are set as follows: 9600 bps, RTS/CTS Handshaking, 8 Data Bits, One Stop Bit, No Parity. Although these parameters can be easily redefined, for this Quick Start procedure, it is recommended to configure your communications program to accept the default parameters.*
- *The AFS features a default IP Address (192.168.168.168) and a default Subnet Mask (255.255.255.0.) This allows network access to command mode, providing that you are contacting the AFS from a node on the same subnet. When attempting to access the AFS from a node that is not on the same subnet, please refer to Section 5.9 for further configuration instructions.*

1. **Access Command Mode:** The AFS includes two separate user interfaces; the Text Interface and the Web Browser Interface. The Text Interface is available via Local PC, SSH Client, Telnet, or Modem. The Web Browser interface is only available via TCP/IP network.

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

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

   c) **Via Web Browser:** Make certain that Web Browser access is enabled as described in Section 5.9.2. Start your JavaScript enabled Web Browser, enter the default AFS IP address (192.169.168.168) in the Web Browser address bar, and then press **[Enter]**.

   d) **Via Telnet:** Make certain that Telnet access is enabled as described in Section 5.9.2. Start your Telnet client, and enter the AFS's default IP address (192.168.168.168).

   e) **Via Modem:** Use your communications program to dial the number for the external modem (optional) that you have connected to the AFS's RS232 port. For more information on connecting a modem to the AFS, please refer to Section 4.4.

2. **Username** / **Password Prompt:** A message will be displayed, which prompts you to enter your username (Login) and password. If a valid username and password are entered, the AFS will display either the Circuit Control Screen (Web Browser Interface) or the Circuit Status Screen (Text Interface.)

Notes:

- *The default Username is* "**`super`**".
- *The default Password is* "**`super`**"
- *If a Login Banner has been defined as described in Section 5.3, then a banner page will appear before the command interface is displayed. The Login Banner can be used to display legal warnings or other information.*

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

3.4. Fallback Switching

A/B fallback switching can be controlled via the Text Interface or Web Browser Interface.

3.4.1. Fallback Switching - Text Interface

Access the AFS Text Interface as described in Section 3.3 and then proceed as follows:

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

2. **Manual A/B Switching:** Use the manual circuit switches to change A/B paths. Note that this example assumes that the Master A/B Gang Switch and individual circuit module switches have not been disabled.

   a) **Master A/B Gang Switch:** Toggle the Master A/B Gang Switch between the “A” and “B” positions. The LED indicators should follow the Master Switch, indicating that each circuit has switched the “A” and “B” paths.

   b) **Circuit Module A/B Switch:** Choose an individual Circuit Module and toggle the module’s A/B Switch between “A” and “B”. The LED indicators should indicate that the module has switched the A/B path.

3. **Code Activated Switching:** To control A/B fallback switching using ASCII commands, invoke the following commands at the AFS command prompt:

   a) Type **`/T *,B`** and press **[Enter]**. All Circuit Modules should switch to the “B” path.

   b) Type **`/T 1,A`** and press **[Enter]**. Circuit Module number 1 should switch to the “A” path.

   c) Type **`/T 2,3,4,A`** and press **[Enter]**. Circuit Modules 2, 3, and 4 should switch to the “A” path.

3.4.2. Fallback Switching - Web Browser Interface

In the default state, the Web Browser Interface will not be available until you have enabled Web Access as described in Section 5.9.2. After Web Access has been enabled, access the AFS Web Browser Interface as described in Section 3.3 and then proceed as follows:

1. **Access the Circuit Control Menu:** Click on the "Circuit Control" link on the left hand side of the screen to display the Circuit Control menu. The Circuit Control menu includes a series of dropdown menus that are used to select the desired switching action for each Circuit Module.

   Note: *The Circuit Control menu also lists the number and user-defined name of each Circuit Module present, the name of the currently selected A/B circuit path, the A/B position of the switch, a brief description of the reason for the last switching action and a column that shows if each circuit is controlled by the Monitor/Alarm Input feature.*

2. **Select the Switching Action:** Use the dropdown menu to select an A/B switching operation for the desired Circuit Module. For example, to switch Circuit 1 to the B position, click on the down arrow in the "Action" column for Circuit 1 to display the dropdown menu, select the "B" option from the dropdown menu and then click on the "Confirm Circuit Actions" button.

   Notes:

   - *The dropdown menu for each circuit allows you to select position A, position B or the default position. Normally, the "Default" option will switch the circuit to the user-defined Default position that is selected as described in Section 5.6. However, in the case of this Quick Start procedure, the Default circuit positions have not yet been defined.*
   - *The Circuit Control Menu also includes the ability to switch all AFS Circuit Modules. If desired, the dropdown menu in the "All Circuits" row can be used to switch all AFS circuits.*

3. **Confirm Switching Actions:** After you click on the "Confirm Circuit Actions" button, the AFS will display a screen which summarizes the selected switching operation(s) and asks for confirmation before executing the command. To proceed with the selected switching operation, click on the "Execute Circuit Actions" button.

4. The AFS will execute the switching operation and then display the Circuit Status screen.

This completes the Quick Start procedure for the AFS. Prior to placing the unit into operation, it is recommended to refer to the remainder of this user's guide for important information regarding advanced configuration options and more detailed operation instructions. If you have further questions regarding the AFS unit, please contact WTI Customer Support as described in Appendix C.

4. Hardware Installation

4.1. Connecting the Power Supply Cable(s)

Refer to the cautions listed below and at the beginning of this User's Guide, and then connect the AFS to an appropriate 100 to 240 VAC power supply.

 **CAUTIONS:** 

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

Note: *The AFS includes two power inlets. You can connect either one or both of these inputs to your power source. If both power inlets are connected, they should be connected to separate power sources in order that the second power source can serve as a redundant back up in the event of failure.*

Set the Power Switch on the AFS Power Module to the ON Position. The ON LED on the Power Module and the A/B indicators on the Control Module should light. After about 90 seconds, the A/B indicators should go out, indicating that the unit is ready to receive commands. Note that if the AFS needs to download SSH keys, it may take longer than 90 seconds for the A/B indicators to switch off.

4.2. Connecting the Network Cable

Use the supplied 10/100Base-T Ethernet cable to connect the AFS Ethernet port to your TCP/IP network. Note that the AFS includes a default IP address (192.168.168.168) and a default subnet mask (255.255.255.0.) When installing the
AFS in a working network environment, it is recommended to define network parameters as described in Section 5.9.

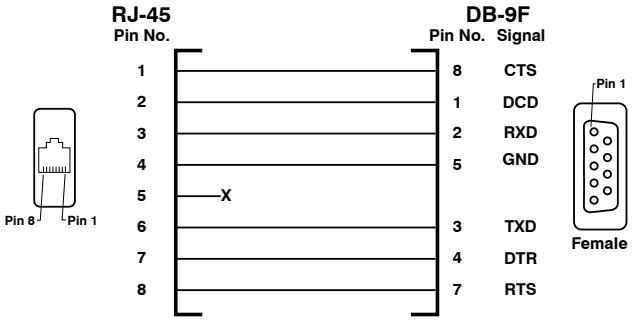

Figure 4.1: DX9F-DTE-RJ Snap Adapter Interface

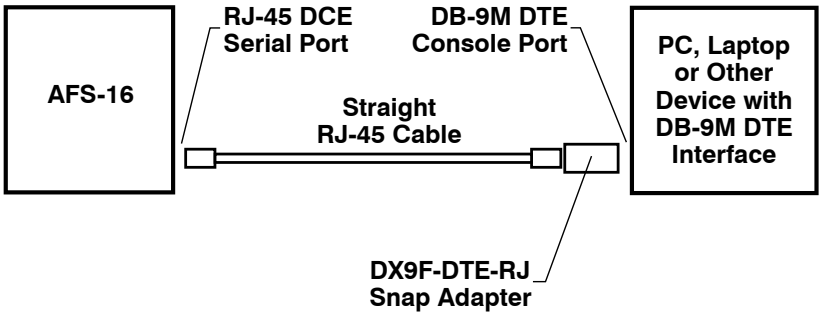

Figure 4.2: Connecting DB-9M DTE Devices to the AFS Control Module's Serial Port

4.3. Connecting a Local Control Device

Use the supplied Ethernet cable and adapter to connect your PC COM port to the RS232 Console Port on the AFS Control Module as shown in Figure 4.1 and Figure 4.2.

4.4. Connecting an External Modem (Optional)

Access the AFS Command Mode and then use the Port Parameters menu to configure the RS232 Port for Modem Mode as described in Section 5.8. Use an appropriate cable to connect your external modem the RS232 Port on the AFS's Control Module and then connect your RJ11 phone line to the external modem.

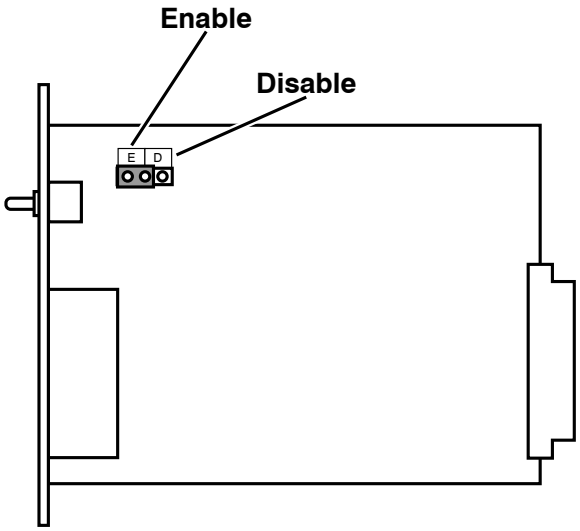

Figure 4.3: Circuit Module Jumper

4.5. Module Set Up

4.5.1. Circuit Module Set Up

The A/B Switch Jumper on the Circuit Module card (Figure 4.3) enables/disables the individual Circuit Module's A/B Switch. If you wish to disable manual A/B switching control at a specific Module, then the A/B Switch Jumper on that Module must be set in the "Disable" position.

4.5.2. Control Module SetUp

The Control Module includes a jumper that can be used to configure the AUX Connector for use with the Monitor/Alarm Input feature. If you intend to use the Input Monitor Alarm, then this jumper should be set as described in Section 7.6.

4.6. The A/C/B Connectors

Each AFS Circuit Module includes three RJ45 connectors: a "C" (Common) connector, an "A" (Primary Fallback) connector and a "B" (Secondary Fallback) connector. Use an RJ45 Ethernet cable to connect devices to the A/C/B ports as required.

This completes the AFS installation instructions. Please proceed to the next Section for instructions regarding basic unit configuration.

5. Basic Configuration

This section describes the basic configuration procedure for AFS units. For information on Alarm Functions, please refer to Section 7.

5.1. Communicating with the AFS Unit

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

In addition, the AFS also offers three different methods for accessing command mode; via network, via modem, or via local console. The Web Browser interface is only available via TCP/IP network, and the Text Interface is available via TCP/IP network (SSH or Telnet), modem or local PC.

5.1.1. The Text Interface

The Text Interface consists of a series of simple ASCII text menus, which allow you to select and define parameters by entering the number for the desired parameter using your keyboard, and then typing in the value for that parameter.

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

Once Telnet Access is enabled, you will then be able to use the Text Interface to communicate with the AFS via local PC, Telnet or SSH connection. You can also use the Text Interface to access command mode via an external modem installed at the RS232 Port on the AFS Control Module.

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

- **Access via Network:** The AFS must be connected to your TCP/IP Network, and your PC must include a communications program (such as HyperTerminal.)
- **Access via Modem:** An external modem must be installed at the Control Module's RS232 Port and the RS232 Port must be configured for Modem Mode as described in Section 5.8. A phone line must be connected to the external modem. In addition, your PC must include a communications program.
- **Access via Local PC:** Your PC must be connected to the RS232 Port on the AFS Control Module. The RS232 Port must be configured for Normal Mode, and your PC must include a communications program.

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

Note: *When communicating with the unit for the first time, you will not be able to contact the unit via Telnet until you have accessed command mode via Local PC or SSH Client and used the Network Parameters Menu to enable Telnet as described in Section 5.9.2.*

1. Contact the AFS Unit:

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

   b) **Via Network:** The AFS includes a default IP address (192.168.168.168) and a default subnet mask (255.255.255.0.) This allows you to contact the unit from any network node on the same subnet, without first assigning an IP Address to the unit.

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

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

   c) **Via Modem:** Use your communications program to dial the number for the phone line that you have connected to the AFS RS232 Serial Port.

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

3. If a valid username and password are entered, the AFS will display the Circuit Status Screen.

   Note: *If a Login Banner has been defined as described in Section 5.3, then a banner page will appear before the command prompt is displayed. The Login Banner can be used to display legal warnings or other information.*

5.1.2. The Web Browser Interface

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

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

1. Start your JavaScript enabled Web Browser, key the AFS's IP address (default = 192.168.168.168) into the web browser's address bar, and press **[Enter]**.

2. **Username** / **Password Prompt:** A message box will prompt you to enter your username and password. The default username is "**super**" (all lower case, no quotes), and the default password is also "**super**".

3. If a valid username and password are entered, the Circuit Control Screen will be displayed.

   Note: *If a Login Banner has been defined as described in Section 5.3, then a banner page will appear before the command prompt is displayed. The Login Banner can be used to display legal warnings or other information.*

5.1.3. Access Via PDA

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

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

- Product Status Screen (Unit Info)
- Circuit Status Screen
- Circuit Group Status Screen
- Circuit Control Screen
- Circuit Group Control Screen

These screens will allow PDA users to review Circuit Status and Circuit Group Status, invoke A/B switching and display the Site I.D. and firmware version. Note however, that PDA users are not allowed to change or review AFS configuration parameters.

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

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

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

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

5.2. Configuration Menus

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

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

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

Notes:

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

5.3. Defining System Parameters

The System Parameters menus are used to define the Site ID Message, set the system clock and calendar, set up log functions and select other general parameters.

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

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

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

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

- **Site ID:** A text field, generally used to note the installation site or name for the AFS unit. (Up to 64 chars.; Default = undefined.)

  Notes:

  - *The Site I.D. will be cleared if the AFS is reset to default settings.*
  - *When viewed via the Text Interface (CLI) Site I.D. messages that are over 30 characters long will be truncated. To display the entire Site I.D. message via the Text Interface, type* **`/J*`** *and press* ***[Enter]***

- **Real Time Clock:** The Real Time Clock menu is used to set the clock and calendar, and to enable and configure the NTP (Network Time Protocol) feature as described in Section 5.3.1.

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

- **Invalid Access Lockout:** This feature can be used to temporarily disable Console Port access, SSH access, Telnet access and/or Web access to the AFS command mode after a user specified number of unsuccessful login attempts are made. For more information, please refer to Section 5.3.2. (Default = Off.)

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

- **Temperature Format:** Determines whether the temperature is displayed as Fahrenheit or Celsius. (Default = Fahrenheit.)
- **Temperature Calibration:** Used to calibrate the unit's internal temperature sensing abilities. To calibrate the temperature, place a thermometer inside your equipment rack, in a location that usually experiences the highest temperature. After a few minutes, take a reading from the thermometer, and then key the reading into the configuration menu. In the Web Browser Interface, the temperature is entered at the System Parameters menu, in the Temperature Calibration field; in the Text Interface, the temperature is entered in a submenu of the System Parameters menu, which is accessed via the Temperature Calibration item. (Default = undefined.)
- **Log Configuration:** This item provides access to a submenu which is used to configure the Audit Log, Alarm Log and Temperature Log as described in Section 5.3.3.
  - **Audit Log:** When enabled, creates a record of all A/B switching at the AFS unit, including switching that was initiated by alarms. (Default = On without Syslog.)
  - **Alarm Log:** When enabled, creates a record of all alarm activity at the AFS unit. (Default = On without Syslog.)
  - **Temperature Log:** When enabled, creates a record of temperature versus time at the AFS unit. (Default = On.)
- **Callback Security:** Enables and configures the Callback Security Function as described in Section 5.3.4. In order to function properly, a Callback number must also be defined for each desired user account. (Default = On - Callback without Password Prompt, 3 attempts, 30 Minute Delay.)

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

- **Control Card A/B Switch:** This item can be used to enable/disable the Master A/B Gang Switch on the AFS Control Module. (Default = On.)
- **Control Card Reset Switch:** This item can be used to enable/disable the Reset Switch on the AFS Control Module. (Default = On.)
- **Modem Phone Number / IP Address:** If an optional external modem is connected to the AFS Serial Setup Port, the Modem Phone Number parameter can be used to denote the phone number for the external modem. In cases where the AFS application includes a cellular modem, the IP address for the cellular modem can be entered via this parameter. (Default = undefined.)

- **Management Utility:** Enables/Disables the Enterprise Management Utility (WMU.) When enabled, the WMU allows you to manage multiple WTI units via a single menu. (Default = Off.) For more information on the WMU, please refer to the WMU User's Guide, which can be found on the WTI website at:

  http://www.wti.com/t-product-manuals.aspx

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

- **Scripting Options:** Provides access to a submenu that is used to configure the Command Confirmation and Automated Mode parameters.

  Note: *In the Text Interface, the Scripting Options submenu is accessed via the System Parameters menu. To access the Scripting Options parameters via the Web Browser Interface, place the cursor over the "General Parameters" link, wait for the flyout menu to appear, then click on the "Scripting Options" link.*

- **Asset Tag:** Allows a descriptive tag or tracking number to be assigned to the AFS unit. Once defined, the Asset Tag can be displayed via the Product Status Screen in the Web Interface or via the **`/J*`** command in the Text Interface. (Default = Undefined)

- **Login Banner:** Allows definition of a banner/message that will be displayed when a valid username and password are entered during log in. The Login Banner can be used to post legal warning regarding unauthorized access to the unit or to display other user-defined information or instructions. (Default = Undefined)

  Notes:

  - *Although the Login Banner will be displayed when the AFS is accessed via both the Text Interface and Web Browser Interface, the Login Banner can only be defined via the Text Interface.*
  - *The Login Banner can be up to 1024 characters long.*
  - *The Login Banner text must begin with the* **`<banner>`** *command and end with the* **`</banner>`** *command.*
  - *Banner text can be copied and pasted from a text editor, or sent in from a file.*
  - *For best results, the individual text lines in the Login Banner should be less than 80 characters wide.*

5.3.1. The Real Time Clock and Calendar

The Real Time Clock menu is used to set the internal clock and calendar:

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

Notes:

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

- **Primary NTP Address:** Defines the IPv4 and/or IPv6 protocol IP address or domain name for the primary NTP server. (Default = undefined)

Notes:

- *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 5.9.5.*
- *The Web Browser Interface includes two separate fields that are allowed to define both an IPv4 protocol and IPv6 protocol format Primary NTP Address and Secondary NTP Address.*
- *When the Primary NTP Address and Secondary NTP Address are defined via the Text Interface, the AFS will display a prompt that instructs the user to select IPv4 or IPv6 protocol.*
- *The AFS allows parameters for both IPv4 and IPv6 protocols to be defined and saved.*

- **Secondary NTP Address:** Defines the IPv4 and/or IPv6 protocol IP address or domain name for the secondary, fallback NTP Server. (Default = undefined)

Notes:

- *In order to use domain names for web addresses, DNS Server parameters must first be defined as described in Section 5.9.5.*
- *The Web Browser Interface includes two separate fields that are allowed to define both an IPv4 protocol and IPv6 protocol format Primary NTP Address and Secondary NTP Address.*
- *When the Primary NTP Address and Secondary NTP Address are defined via the Text Interface, the AFS will display a prompt that instructs the user to select IPv4 or IPv6 protocol.*
- *The AFS allows parameters for both IPv4 and IPv6 protocols to be defined and saved.*

- **NTP Timeout:** The amount of time in seconds, that will elapse between each attempt to contact the NTP server. When the initial attempt is unsuccessful, the AFS will retry the connection four times. If neither the primary nor secondary NTP server responds, the AFS will wait 24 hours before attempting to contact the NTP server again. (Default = 3 Seconds.)
- **Test NTP Servers:** Allows you to ping the IP addresses or domain names defined via the Primary and Secondary NTP Address prompts, or to ping a new address or domain defined via the Test NTP Servers submenu in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Test NTP Servers feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Test NTP Servers option, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.3.2. The Serial Port Invalid Access Lockout Feature

When properly configured and enabled, the Invalid Access Lockout feature can watch all login attempts made via SSH connection, Telnet connection, web browser or the serial SetUp Port. If the counter for any of these exceeds the user-defined threshold for maximum invalid attempts, then the corresponding port or protocol will be automatically disabled for the length of time specified by the Lockout Duration parameter.

When Invalid Access Attempt monitoring is enabled for the serial SetUp Port, the AFS will count invalid access attempts at the serial SetUp Port. If the number of invalid access attempts exceeds the defined Lockout Attempts trigger value, the AFS will lock the serial SetUp Port for the defined Lockout Duration period. When Invalid Access Attempt monitoring for SSH, Telnet or Web are selected, a lockout will be triggered when the number of invalid access attempts during the defined Lockout Duration period exceeds the defined Hit Count for the protocol. For example, if the SSH Hit Count is set at 10 and the SSH Lockout Duration period is set at 120 seconds, then if over 10 invalid access attempts are detected within 120 seconds, the AFS will then lock out the MAC address that generated the excessive attempts for 120 seconds.

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

Notes:

- *When the Serial Port Invalid Access Lockout Alarm has been enabled, the AFS can also provide notification via email, Syslog Message, and/or SNMP trap whenever an Invalid Access Lockout occurs at the serial SetUp Port.*
- *If the Network Port has been locked by the Invalid Access Lockout feature, it will still respond to the ping command (providing that the ping command has not been disabled at the Network Port.)*

The Invalid Access Lockout configuration menus allow you to select the following parameters:

- **Serial Port Protection:** Enables/Disables the Invalid Access Lockout function for the serial SetUp Port and selects lockout parameters. When this item is enabled and excessive Invalid Access attempts are detected at the SetUp Port, the SetUp Port will be locked until the user-defined Lockout Duration period elapses, or until the /UL command is issued.
  - **Serial Port Protection:** Enables/Disables the Invalid Access Lockout feature for the serial SetUp Port. (Default = Off.)
  - **Lockout Attempts:** The number of invalid attempts that must occur in order to trigger the Invalid Access Lockout feature at the serial SetUp Port. (Default = 9.)
  - **Lockout Duration:** This option selects the length of time that the serial SetUp Port will remain locked when Invalid Access Lockout occurs. If the duration is set at "Infinite", then ports will remained locked until the /UL command is issued. (Default = 30 Minutes.)

- **SSH Protection:** Enables/Disables and configures the Invalid Access function for SSH connections. When this item is enabled and excessive Invalid Access Attempts via SSH are detected, then the AFS will lock out the offending MAC address for the user-defined SSH Lockout Duration Period or until the /UL command is issued. Note that for SSH protection, the lockout trigger is a function of the SSH Hit Count parameter and the SSH Lockout Duration Parameter.
  - **Lockout Enable:** Enables/Disables Invalid Access Lockout protection for SSH connections. (Default = Off.)
  - **SSH Hit Count:** The number of invalid attempts that must occur during the length of time specified by the SSH Lockout Duration period in order to trigger the Invalid Access Lockout feature for SSH protocol. For example, if the SSH Hit Count parameter is set to 10 and the SSH Lockout Duration parameter is set to 30 minutes, then the AFS will lock out the offending MAC address for 30 minutes when over 10 invalid access attempts occur during any 30 minute long period. (Default = 20.)
  - **SSH Lockout Duration:** This option selects both the length of time that an SSH Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When an SSH Lockout occurs, the offending MAC address will be prevented from establishing an SSH connection to the AFS for the defined SSH Lockout Duration period. (Default = 2 Seconds.)
- **Telnet Protection:** Enables/Disables and configures the Invalid Access function for Telnet connections. When this item is enabled and excessive Invalid Access Attempts via Telnet are detected, then the AFS will lock out the offending MAC address for the user-defined Telnet Lockout Duration Period or until the /UL command is issued. Note that for Telnet protection, the lockout trigger is a function of the Telnet Hit Count parameter and the Telnet Lockout Duration Parameter.
  - **Lockout Enable:** Enables/Disables Invalid Access Lockout protection for Telnet connections. (Default = Off.)
  - **Telnet Hit Count:** The number of invalid attempts that must occur during the length of time specified by the Telnet Lockout Duration period in order to trigger the Invalid Access Lockout feature for the Telnet protocol. For example, if the Telnet Hit Count parameter is set to 10 and the Telnet Lockout Duration parameter is set to 30 minutes, then the AFS will lock out the offending MAC address for 30 minutes when over 10 invalid access attempts occur during any 30 minute long period. (Default = 20.)
  - **Telnet Lockout Duration:** This option selects both the length of time that a Telnet Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When a Telnet Lockout occurs, the offending MAC address will be prevented from establishing a Telnet connection to the AFS for the defined Telnet Lockout Duration period. (Default = 2 Seconds.)

- **Web Protection:** Enables/Disables and configures the Invalid Access function for Web connections. When this item is enabled and excessive Invalid Access Attempts via Web are detected, then the AFS will lock out the offending MAC address for the user-defined Web Lockout Duration Period or until the /UL command is issued. Note that for Web protection, the lockout trigger is a function of the Web Hit Count parameter and the Web Lockout Duration Parameter.
  - **Lockout Enable:** Enables/Disables Invalid Access Lockout protection for web connections. (Default = Off.)
  - **Web Hit Count:** The number of invalid attempts that must occur during the length of time specified by the Web Lockout Duration period in order to trigger the Invalid Access Lockout feature for Web access. For example, if the Web Hit Count parameter is set to 10 and the Web Lockout Duration parameter is set to 30 minutes, then the AFS will lock out the offending MAC address for 30 minutes when over 10 invalid access attempts occur during any 30 minute long period. (Default = 20.)
  - **Web Lockout Duration:** This option selects both the length of time that a Web Lockout will remain in effect and also the time period over which invalid access attempts will be counted. When a Web Lockout occurs, the offending MAC address will be prevented from establishing a Web connection to the AFS for the defined Telnet Lockout Duration period. (Default = 2 Seconds.)

5.3.3. Log Configuration

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

- **Audit Log:** Creates a record of all switching activity at the AFS unit, including A/B switching initiated by the alarm functions. In addition, the Audit Log also includes login/logout records for all users. Each Log record includes a description of the activity that caused the A/B switching, the username for the account that initiated the action and the time date that each event occurred.
- **Alarm Log:** Creates a record of all Alarm Activity at the AFS unit. Each time that an alarm is triggered or cleared, the AFS will generate a record that lists the time and date of the alarm, the name of the Alarm triggered, a description of the Alarm and the time and date that the Alarm was cleared.
- **Temperature Log:** Provides a record of rack temperature levels over time at the AFS unit. Each Log record will include the time, date, and temperature reading.

5.3.3.1. Audit Log and Alarm Log Configuration Options

The System Parameters menu allows you to enable/disable and configuration the Audit Log and Alarm Log. The Audit Log and Alarm Log function both offer the following configuration options:

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

  Note: *In order for the Audit Log or Alarm Log to generate Syslog Messages, Syslog Parameters must first be defined as described in Section 11.*

5.3.3.2. The Temperature Log

The System Parameters menu allows you to either enable or disable the Temperature Log. When disabled, the AFS will not log temperature readings. In the default state, the Temperature Log is enabled.

5.3.3.3. Reading, Downloading and Erasing Logs

To read or download the status logs, proceed as follows:

- **Text Interface:** Type **/L** and press **[Enter]** to access the Display Log menu. Select the desired option, key in the appropriate number, press **[Enter]** and then follow the instructions in the "Display Logs" submenu.
- **Web Browser Interface:** Move the cursor over the "Logs" link on the left hand side of the screen. When the flyout menu appears, click on the desired option.

Proceed as follows to download, display or erase logged data:

- **Audit Log and Alarm Log:** The Audit Log and Alarm Log can be displayed or downloaded via either the Text Interface or Web Browser Interface. When the Audit Log or Alarm Log are displayed via the Text Interface, the AFS will also offer the option to erase Audit Log or Alarm Log data.
- **Temperature Log:** The Temperature Log can be displayed or downloaded via either the Text Interface or Web Browser Interface. When selected via the Text Interface, the AFS will also offer the option to erase Temperature Log data.

Notes:

- *The AFS dedicates a fixed amount of internal memory for log records, and if log records are allowed to accumulate until memory is filled, data will eventually "wrap around," and older data will be overwritten by newer data.*
- *Once records have been erased, they cannot be recovered.*

5.3.4. Callback Security

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

In order for Callback Security to function, you must first enable and configure the feature as described in this section, and then define a callback number for each desired user account. To access the Callback Security menu via Text Interface, type **`/F`** and press **[Enter]** and then select the Callback Security option. To access the Callback Security menu via Web Browser Interface, place the cursor over the General Parameters link, wait for the flyout menu to appear, then Click on the "Callback Security" link.

The Callback Security Menu offers the following options:

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

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

Notes:

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

5.3.5. Scripting Options

The Scripting Options submenu provides access to parameters that are used to set up the AFS unit for running various scripts.

Notes:

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

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

- **Command Confirmation:** This item can be used to suppress the command confirmation prompt, which is normally displayed before commands are executed. When Command Confirmation is "Off", the AFS will not display the "Are You Sure?" prompt before executing commands. (Default = On.)
- **Automated Mode:** When enabled, the AFS will execute commands without displaying a confirmation prompt, status screen or confirmation messages as described in Section 5.3.5.1. (Default = Off.)

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

5.3.5.1. Automated Mode

The Automated Mode allows the AFS to execute A/B switching commands, without displaying menus or generating response messages. Automated Mode is designed to allow the AFS to be controlled by a device which can generate commands to control power switching functions without human intervention.

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

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

Notes:

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

To enable/disable the Automated Mode, go to the System Parameters menu, and then set the "Automated Mode" option to "On". When Automated Mode is enabled, AFS functions will change as follows:

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

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

5.4. User Accounts

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

The AFS allows up to 128 user accounts; each account includes a username, password, command access level, circuit access rights, service access rights and an optional callback number.

5.4.1. Command Access Levels

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

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

- **Administrator:** Administrators are allowed to invoke all configuration and operation commands, can view all status screens, and can always direct A/B switching commands to all AFS Circuit Modules.
- **SuperUser:** SuperUsers are allowed to invoke A/B switching commands and view all status screens. SuperUsers can view configuration menus, but are not allowed to change configuration parameters. SuperUsers are granted access to all AFS Circuit Modules.
- **User:** Users are allowed to A/B switching commands and view all status screens, but can only apply commands to the AFS Circuit Modules that they have been specifically granted access to. In addition, Users are not allowed to view configuration menus or change configuration parameters.
- **ViewOnly:** Accounts with ViewOnly access, are allowed to view Status Menus (with restrictions,) but are not allowed to invoke A/B switching commands, and cannot view configurations menus or change configuration parameters. ViewOnly accounts can display Status screens, but can only view the status of the AFS Circuit Modules that are specifically allowed by the account.

Section 17.2 summarizes command access for all four access levels.

In the default state, the AFS includes one predefined account that provides access to Administrator commands and allows to control of all Circuit Modules. The default username for this account is "**`super`**" (lowercase, no quotation marks), and the password for the account is also "**`super`**".

Notes:

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

5.4.2. Granting Circuit Module Access

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

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

- **Administrator:** Accounts with Administrator access are always allowed to control all Circuit Modules. Circuit Module access cannot be disabled for Administrator level accounts.
- **SuperUser:** SuperUser accounts allow access to all Circuit Modules. Circuit Module access cannot be disabled for SuperUser level accounts.
- **User:** Accounts with User level access are only allowed to access the Circuit Modules that have been specifically permitted via the "Circuit Access" parameter in the Add User and Modify User menus.
- **ViewOnly:** Accounts with ViewOnly access are not allowed to invoke A/B switching commands. ViewOnly accounts can display the status of Circuit Modules, but are limited to the Circuit Modules specified by the account.

5.5. Managing User Accounts

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

- **View User Directory:** Displays currently defined parameters for any user account.
- **Add Username:** Creates new user accounts, and allows you to assign a username, password, command level, Circuit Module access and other factors.
- **Modify User Directory:** This option is used to edit or change account information.
- **Delete User:** Clears user accounts.

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

5.5.1. Viewing User Accounts

The "View User Directory" option allows you to view details about each account. The View User option will not display actual passwords; instead, the password field will read "defined". The View User Accounts function is only available when you have accessed command mode using a password that permits Administrator Level commands.

5.5.2. Adding User Accounts

The "Add Username" option allows you to create new accounts. Note that the Add User function is only available when you have accessed command mode using a password that permits Administrator Level commands. The Add User Menu can define the following parameters for each new account:

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

- **Username:** Up to 32 characters long, and cannot include non-printable characters. Duplicate usernames are not allowed. (Default = undefined.)
- **Password:** Five to 16 characters long, and cannot include non-printable characters. Note that passwords are case sensitive. (Default = undefined.)
- **Access Level:** Determines which commands this account will be allowed to access. This option can set the access level for this account to "Administrator", "SuperUser", "User" or "ViewOnly." For more information on Command Access Levels, please refer to Section 5.4.1 and Section 17.2. (Default = User)

- **Circuit Access:** Determines which AFS Circuit Modules this account will be allowed to access. (Defaults; Administrator & SuperUser = All Circuit Modules On, User and ViewOnly = All Circuit Modules Off.)

  Notes:

  - *Administrator and SuperUser level accounts will always have access to all Circuit Modules.*
  - *ViewOnly accounts are allowed to display the status of Circuit Modules, but are limited to the Circuit Modules specified by the account. ViewOnly accounts are not allowed to invoke A/B Switching commands.*

- **Circuit Group Access:** Determines which Circuit Groups this account will be allowed to control. Circuit Groups allow you to define a selection of Circuit Modules, and then quickly assign access to that group of circuits to accounts. (Default = All Circuit Groups Off.)

  Notes:

  - *In order to use this feature, Circuit Groups must first be defined.*
  - *Administrator and SuperUser level accounts will always have access to all Circuit Groups.*
  - *ViewOnly accounts are allowed to display the status of Circuit Groups, but are limited to the Circuit Groups specified by the account. ViewOnly accounts are not allowed to invoke A/B switching commands.*

- **Service Access:** Determines whether this account will be able to access command mode via Serial Port (RS232 Port), Telnet/SSH or Web and whether the account will have access to the Outbound Telnet feature. For example, if Telnet/SSH Access is disabled for this account, then this account will not be able to access command mode via Telnet or SSH. (Default = Serial Port = On, Telnet/SSH = On, Web = On, Outbound Access = Off.)

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

  Notes:

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

- **Authorization Keys:** This item can be used to assign an SSH Authorization Key to the user account, view assigned authorization keys or delete assigned authorization keys. When a valid authorization key is assigned to a given user, that user will be able to access AFS command mode without entering a password. When assigning an authorization key, the AFS offers the option to define a name for the key and upload a key from the user's server.

5.5.3. Modifying User Accounts

The "Edit User Directory" function allows you to edit existing accounts in order to change parameters, circuit access rights or Administrator Command capability. Note that the Edit/Modify User function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Once you have accessed the Modify Users menu, use the menu options to redefine parameters in the same manner employed for the Add User menu.

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

5.5.4. Deleting User Accounts

This function is used to delete individual user accounts. Note that the Delete User function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Notes:

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

5.6. Circuit Configuration

The Circuit Parameters menu allows you to select parameters for the AFS Circuit Modules. This allows you to assign names to the A, C, and B connectors on each Circuit Module, and also define a default A/B setting for each A/B Switch. Note that the Circuit Parameters menu is only available when you have logged into command mode using an account that permits Administrator commands.

To define Circuit Parameters via the Text Interface, type **/PC** and then press **[Enter]** to display the Circuit Parameters Menu. To define Circuit Parameters via the Web Browser Interface, click on the Circuit Parameters link on the left hand side of the screen to display the Circuit Parameters Menu.

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

- **Name (Common):** Assigns a name to the Common RJ45 connector on the selected Circuit Module.
- **Name (A):** Assigns a name to the "A" RJ45 connector on the selected Circuit Module.
- **Name (B):** Assigns a name to the "B" RJ45 connector on the selected Circuit Module.
- **Power Up Default:** Determines how this A/B Switch will react when the "Default All Circuits" command (/DC) is invoked, or after power to the unit has been interrupted and then restored. After the default command is invoked, or power is restored, the AFS will automatically set each A/B Switch to the "A" or "B" setting as specified by the Power-Up Default. (Default = "A").

Notes:

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

5.7. The Circuit Group Directory

The Circuit Group Directory allows you to designate "groups" of circuits that are dedicated to a similar function, and will most likely be switched at the same time or by the same user.

Circuit Groups allow you to direct A/B switching commands to a series of circuits, without addressing each circuit individually. For example, a set selection of AFS circuits could be assigned to a circuit group named, "Servers". This would allow you to quickly switch all circuits in the group, by either including the "Servers" Circuit Group name in a /T command line via the Text Interface, or by using the Circuit Group Control menu via the Web Browser Interface.

The Circuit Group Directory function is only available when you have logged into command mode using an account that permits Administrator commands. In both the Text Interface and the Web Browser Interface, the Circuit Group Directory menu offers the following functions:

- **View Circuit Group Directory:** Displays currently defined Circuit Module access rights for any AFS Circuit Group.
- **Add Circuit Group to Directory:** Creates new Circuit Groups, and allows you to assign circuit access rights to each group.
- **Modify Circuit Group Directory:** This option is used to edit or change circuit access rights for each Circuit Group.
- **Delete Circuit Group from Directory:** Clears Circuit Groups that are no longer needed.

5.7.1. Viewing Circuit Groups

The "View Circuit Group Directory" option allows you to view the configuration of each Circuit Group. Note that the View Circuit Group Directory function is only available when you have accessed command mode using a password that permits Administrator Level commands.

5.7.2. Adding Circuit Groups

The "Add Circuit Group to Directory" option allows you to create new Circuit Groups and assign circuit access rights to each group. Note that the Add Circuit Group function is only available when you have accessed command mode using a password that permits Administrator Level commands.

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

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

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

5.7.3. Modifying Circuit Groups

The "Modify Circuit Group" function allows you to edit existing Circuit Groups in order to change circuit access rights. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands.

Once you have accessed the Modify Circuit Group menu, use the menu options to redefine parameters in the same manner that is used for the Add Circuit Group menu.

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

5.7.4. Deleting Circuit Groups

This function is used to delete individual Circuit Groups. Note that this function is only available when you have accessed command mode using a password that permits Administrator Level commands.

> **Note:** *Deleted Circuit Groups cannot be automatically restored.*

5.8. Serial Port Configuration

The Serial Port Configuration menus allow you to select parameters for the AFS Control Module's RS232 Serial Port. The Serial Port can be configured for connection to a local PC or Modem. In addition, the Serial Port Configuration menu can also be used to set communications parameters, disable Administrator level commands and also select other Serial Port Parameters.

To configure the Serial Port via the Text Interface, type **`/P`** and then press **[Enter]**. To configure the Serial Port via the Web Browser Interface, click the "Serial Port Configuration" link on the left hand of the screen.

Notes:

- *Configuration menus are only available to Administrator level accounts.*
- *If you are configuring the AFS via modem, modem parameters will not be changed until after you exit command mode and disconnect from the unit.*

The Serial Port Configuration menu allows the following parameters to be defined:

Communication Settings:

The communication Settings are used to define general serial port communication parameters, such as the Baud Rate, Bits/Parity, Stop Bits and Handshake Mode.

General Parameters:

- **Administrator Mode:** Permits/denies port access to Administrator level accounts. (Default = Permit).

  Note: *Administrator Mode cannot be disabled at the Control Module RS232 Serial Port.*

- **Logoff Character:** The Logoff Character determines the command(s) or character(s) that must be issued at this port in order to disconnect. (Default = **`^X.`**)

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

- **Inactivity Timeout:** Enables and selects the Timeout Period for this port. If enabled, the Serial Port will disconnect when no additional data activity is detected for the duration of the timeout period. (Default = 5 Minutes.)

- **Command Echo:** Enables/Disables command echo. When disabled, commands sent to the Serial Port will still be invoked, but keystrokes will not be displayed. (Default = On.)

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

Port Mode Parameters:

- **Port Name:** Allows you to assign a name to the Serial Port. (Default = undefined.)
- **Port Mode:** The operation mode for this port. (Default = Normal Mode)

  The AFS offers three serial port operation modes:

  - **Normal Mode:** Allows local communication via the Control Module's RS232 Serial Port.
  - **Modem Mode:** Sets up the Control Module's RS232 Port for connection to an optional external modem.
  - **Modem PPP Mode:** Allows data that is normally sent via ethernet to be sent via phone line.

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

  - **Normal Mode:** Permits access to command mode. When Normal Mode is selected, the following mode specific parameter can also be defined:
    - **DTR Output:** Determines how DTR will react when the port disconnects. DTR can be held low, held high, or pulsed for 0.5 seconds and then held high. (Default = Pulse.)
  - **Modem Mode:** Permits access to command mode and simplifies connection to an external modem. Modem Mode ports can perform all functions available in Normal Mode, but Modem Mode also allows definition of a Hang-Up String, Reset String, and Initialization String:
    - **Modem Reset String:** Redefines the modem reset string. The Reset String can be sent prior to the Initialization string. (Default = **`ATZ`**.)
    - **Modem Initialization String:** Defines a command string that can be used to initialize an attached modem to settings required by your application. (Default = **`AT&C1&D2S0=1&B1&H1&R2`**)
    - **Modem Hang-Up String:** Although the AFS will pulse the DTR line to hang-up an attached modem, the Hang-Up string is often useful for controlling modems that do not use the DTR line. (Default = undefined.)
    - **Reset/No Dialtone Interval:** Determines how often the Reset String will be sent to a modem installed at the serial port and also sets the trigger value for the No Dialtone Alarm. For more information on the No Dialtone Alarm, please refer to Section 7.7. (Default = 15 Minutes)
    - **No Dialtone Alarm Enable:** When this item is "On" the No Dialtone Alarm can be enabled as described in Section 7.7. When the No Dialtone Alarm is enabled and properly configured, the AFS can provide notification if the unit detects that a phone line connected to a modem installed at this port is dead. (Default = Off.)

Note: *When communicating with the AFS via modem, Modem Mode parameters will not be changed until after you exit command mode and disconnect.*

- **Modem PPP Mode:** Allows data that is normally sent via ethernet to be sent via phone line. When Modem PPP Mode is selected, the following modem-related parameters will be available:
  - **Reset String:** Redefines the modem reset string. The Reset String can be sent prior to the Initialization string. (Default = **ATZ)**
  - **Initialization String:** Defines a command string that is used to initialize the modem to settings required for PPP communication (Default = **ATQ0V1E1S0=0&C1&D2**)
  - **Hang-Up String:** Although the AFS will pulse the DTR line to hang-up an attached modem, the Hang-Up string is often useful for controlling modems that do not use the DTR line. (Default = undefined)
  - **Reset/No Dialtone Interval:** Determines how often the Reset String will be sent to a modem installed at the serial port and also sets the trigger value for the No Dialtone Alarm. For more information on the No Dialtone Alarm, please refer to Section 7.7. (Default = 15 Minutes)
  - **No Dialtone Alarm Enable:** When this item is "On" the No Dialtone Alarm can be enabled as described in Section 7.7. When the No Dialtone Alarm is enabled, the AFS can provide notification if the unit detects that a phone line connected to a modem installed at this port is dead. (Default = Off)
  - **Periodic Reset Location:** The IP address or URL for the website used to keep the PPP connection alive when not in use. The AFS will regularly ping the selected IP address or URL in order to keep the connection alive. (Default = undefined)

Notes:

- *In order to select a domain name as the Periodic Reset Location, you must first define the Domain Name Servers as described in Section 5.9.5.*
- *The IP Address, P-t-P and Subnet Mask parameters cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication is started..*

  - **PPP Phone Number:** The phone number for the line that will be used for PPP communication. (Default = undefined)
  - **User Name:** The user name for the ISP account that will be used for PPP communication. (Default = undefined)
  - **Password:** The password for the ISP count that will be used for PPP communication (Default = undefined)
  - **IP Address:** The temporary IP address that will be assigned to the PPP communication session by the ISP. Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started. (Default = undefined)
  - **P-t-P:** Note that this item cannot be defined by the user and will be automatically supplied by the ISP when a PPP communication session is started. (Default = undefined)
  - **Subnet Mask:** This item is not defined by the user and will be automatically supplied by the ISP when a PPP communication session is initiated. (Default = undefined)

5.9. Network Configuration

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

Although the Web Browser Interface and Text Interface allow definition of essentially the same parameters, parameters are arranged differently in the two interfaces. In the Text Interface, most network parameters are defined via one menu. But in the Web Browser Interface, network parameters are divided into separate menus, which are accessed via the Network Configuration flyout menu.

Notes:

- *Settings for network parameters depend on the configuration of your network. Please contact your network administrator for appropriate settings.*
- *The Network Parameters Menu selects parameters for all 16 logical Network Ports.*
- *The IP Address, Subnet Address and Gateway Address cannot be changed via the Web Browser Interface. In order to change these parameters, you must access the unit via the Text Interface.*
- *When a new IP Address is selected, or the status of the DHCP feature is changed, the unit will disconnect and reconfigure itself with the new values when you exit the Network Parameters Menu. When configuring the unit via Web or Telnet, make certain your DHCP server is set up to assign a known, fixed IP address in order to simplify reconnection to the unit after the new address has been assigned.*
- *The Network Parameters menu is only available when you have logged into command mode using an account and port that permit Administrator level commands (Administrator Mode enabled.)*

Both IPv4 and IPv6 parameters can be defined for the Network port, and the unit will automatically use the appropriate protocol to match connections established via the Ethernet port. Note that both the IPv4 configuration menu and the IPv6 configuration menu offer essentially the same parameters.

- **Text Interface:**
  To define network parameters for the IPv4 protocol, type **`/N`** and press **[Enter]**.
  To define network parameters for the IPv6 protocol, type **`/N6`** and press **[Enter]**.
- **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen, wait for the fly-out menu to appear, and then click on the link to display the desired menu. Note that some submenus offer the option to define IPv4 or IPv6 parameters and that IPv4 and IPv6 menus include a link that can be used to jump to the other protocol.

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

5.9.1. Network Port Parameters

In the Text Interface, these parameters are found in the main Network Configuration menu. In the Web Browser Interface, these parameters are found by placing the cursor over the "Network Configuration" link on the left hand side of the screen, and then clicking on the "Network Port Parameters" link in the resulting fly-out menu.

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

- **Logoff Character:** Defines the Logoff Character for this port. (Default = **^x** (**[Ctrl]** plus **[X]**).)

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

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

  Notes:

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

- **Inactivity Timeout:** Enables and selects the Inactivity Timeout period for the Network Port. (Default = 5 Minutes.)

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

- **Accept Break:** Determines whether the Network Port will accept breaks received from the attached device, and pass them along to a connected port. When the Accept Break parameter is enabled and the Network Port is connected to the RS232 Serial Port, breaks received at the Network Port will be passed to the Serial Port. When disabled, breaks will be refused at the Network Port. (Default = On.)

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

5.9.2. Network Parameters

In the Text Interface, these parameters are accessed via the main Network Configuration menu, which can be activated by typing **/N** (for IPv4 parameters) or **/N6** (for IPv6 parameters) and then pressing **[Enter]**. In the Web Browser Interface, these parameters are found by placing the cursor over the "Network Configuration" link on the left hand side of the screen, and then clicking on the "Network Parameters" link in the resulting fly-out menu.

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

- **IP Address:** (Default = 192.168.168.168.)
- **Subnet Mask:** (IPv4 Only; Default = 255.255.255.0)
- **Subnet Prefix:** (IPv6 Only; Default = undefined)
- **Gateway Address:** (Default = undefined.)
- **DHCP:** Enables/Disables Dynamic Host Configuration Protocol. When this option is "On", the AFS will perform a DHCP request. Note that in the Text Interface, the MAC address for the AFS is listed on the Network Status Screen. (Default = Off.)

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

- **IP Security:** Provides access to a submenu that is used to enable and define the IP Security filter as described in Section 5.9.3. (Default = Off)

  Note: *In the Web Browser Interface, IP Security parameters are defined via the IP Security Submenu, which may be accessed via the Network Configuration Menu.*

- **Static Route:** Provides access to a submenu that is used to enable and define Static Route functions as described in Section 5.9.4. (Default = Off)

  Note: *In the Web Browser Interface, Static Route parameters are defined via the Static Route Submenu, which may be accessed via the Network Configuration Menu.*

- **DNS Servers:** Provides access to a submenu that is used to define Domain Name Server parameters as described in Section 5.9.5. (Default = undefined)

  Note: *In the Web Browser Interface, DNS Server parameters are defined via the DNS Server Submenu, which may be accessed via the Network Configuration Menu.*

- **Negotiation:** (Text Interface Only) This parameter can be used to solve synchronization problems when the AFS unit negotiates communication parameters with another device. (Default = Auto)

  Notes:

  - *If the other device is set for automatic negotiation, then the AFS's Negotiation parameter should also be set to Auto.*
  - *If the other device is not set for automatic negotiation, then the AFS's Negotiation parameter should be set to match the other device (e.g., "100/Full.)*

- **Telnet Access:** Enables/disables Telnet access. When Telnet Access is "Off," users will not be allowed to establish a Telnet connection to the unit. (Default = Off.)

- **Telnet Port:** Selects the TCP/IP port number that will be used for Telnet connections. In the Text Interface, this item is defined via a submenu, displayed when the Telnet Access parameter is selected. (Default = 23.)

- **Max. Per Source:** Specifies the maximum number of Telnet sessions that will be allowed per user MAC address. (Default = 4.)

  Notes:

  - *In the Text Interface, the "Per Source" parameter is defined via a submenu of item 21 (Telnet Access) in the Network Parameters menu.*
  - *After changing the "Max Per Source" parameter, you must log out of all pre-existing Telnet sessions in order for the new maximum value to be applied.*

- **SSH Access:** Enables/disables SSH communication. (Default = On.)

- **SSH Port:** Selects the TCP/IP port number that will be used for SSH connections. (Default = 22.)

  Note: *In the Text Interface, this item is defined via a submenu, which is displayed when the SSH Access parameter is selected.*

- **HTTP Access (Web Access):** Enables/disables the Web Browser Interface. When disabled, users will not be allowed to contact the unit via the Web Browser Interface. (Default = Off.)

- **HTTP Port:** Selects the TCP/IP port number that will be used for HTTP connections. (Default = 80.)

- **HTTPS Access:** Enables/disables HTTPS communication. For instructions on setting up SSL encryption, please refer to Section 14. (Default = Off.)

- **HTTPS Port:** Selects the TCP/IP port number that will be used for HTTPS connections. (Default = 443.)

Notes:

- *In the Text Interface, HTTP and HTTPS parameters reside in a separate submenu. To enable and configure HTTP and HTTPS Access via the Text Interface, access the Network Configuration Menu, key in the number for the "Web Access" parameter and then press **[Enter]**.*
- *When the Web Access parameter is accessed via the Text Interface, the resulting submenu will also allow you to select SSL (encryption) parameters.*

- **Harden Web Security:** When the Harden Web Security feature is On (default,) only the high and medium cypher suites for SSLv3 and TLSv1 will be enabled. When the Harden Web Security feature is Off, all SSL protocols will be enabled, allowing compatibility with older browsers. (Default = On.)

Note: *In the Text Interface, this option is enabled/disabled via the Web Access submenu.*

- **TLS Mode:** Selects TLSv1 or TLSv1.1. Although TLSv1.1 provides better security, the default settings of most browsers do not support TLSv1.1. For more information, please refer to Section 14.4. (Default = TLSv1)

Note: *In the Text Interface, the TLS Mode parameter is located in the Web Access submenu.*

- **SYSLOG Addresses:** The IP Addresses or domain names (up to 64 characters) for the Syslog Daemons that will receive log records generated by the AFS. (Default = undefined.)

Notes:

- *The Syslog Address submenu in the Text Interface and the Network Parameters submenu in the Web Browser Interface both include a Ping Test function that can be used to ping the user-selected Syslog IP Addresses in order to verify that valid IP addresses have been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping the currently defined Syslog Addresses in order to make certain that the IP addresses are responding.*

- **Ping Access:** Enables/Disables response to ping commands. When Disabled, the AFS will not respond to Ping commands. Note that disabling Ping Access at the Network Port will not effect the operation of the Ping-No-Access Alarm. (Default = On.)

- **Outbound Access:** Enables/Disables the ability to create outbound Telnet and/or SSH connections via the Network Port and/or Serial Port. When enabled, users who have accessed command mode via the RS232 Serial Port will be able to connect to the Network Port, and invoke the /TELNET and/or /SSH commands to create an outbound connection. Likewise, when enabled, users who have accessed command mode via the Network port can also create an outbound connection via the Serial port. For example, to create an outbound Telnet connection, first make certain that this option is enabled for both the RS232 Serial Port and user account, then access command mode via the Text Interface at the RS232 Port. At the AFS> prompt, invoke the /TELNET command as described in Section 10.3. (Default = Off.)

- **Outbound Secure Level:** When Outbound Access is enabled, this parameter is used to determine whether outbound connections will be allowed to be established via both the Serial Port and Network Port, or via the Serial Port only. (Default = Serial Only.)

  Note: *In the Text Interface, the Outbound Secure Level prompt can be found in the Outbound Access submenu.*

- **Ping Syslog Servers:** (Ping Test) Pings the IP addresses which have been defined for the SYSLOG Severs in order to check for a response.

  Notes:

  - *The Syslog Address submenu in the Text Interface and the Network Parameters submenu in the Web Browser Interface both include a Ping Test function that can be used to ping the user-selected Syslog IP Addresses in order to verify that valid IP addresses have been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
  - *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping the currently defined Syslog Addresses in order to make certain that the IP addresses are responding.*

5.9.3. IP Security

The IP Security feature allows the AFS to restrict unauthorized IPv4 or IPv6 format IP addresses from establishing inbound Telnet connections to the unit. This allows you to grant Telnet access to only a specific group of IP addresses, or block a particular IP address completely. In the default state, the AFS accepts incoming IP connections from all hosts.

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

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

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

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

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

Notes:

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

5.9.3.1. Adding IP Addresses to the Allow and Deny Lists

To add an IPv4 or IPv6 format IP Address to the Allow or Deny list, and begin configuring the IP Security feature, proceed as follows.

Notes:

- *Both the Allow and Deny list can include Linux operators, wild cards, and net/mask pairs.*
- *In some cases, it is not necessary to enter all four "digits" of the IP Address. For example, if you wish to allow access to all IP addresses that begin with "192," then you would only need to enter "192."*
- *The IP Security Configuration menu is only available when the Administrator Mode is active.*
- *In order to use domain names in the Allow List and/or Deny List, you must first define IP address(es) for the desired Domain Name Servers.*

1. Access the IP Security Configuration Menu.

   a) **Text Interface:** Type **`/N`** **[Enter]** to define addresses in IPv4 format, or type **`/N6`** and press **[Enter]** to define addresses in IPv6 format. The Network Configuration Menu will be displayed. From the Network Configuration Menu, type **`5`** **[Enter]** to display the IP Security Menu.

   b) **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears, click on the "IP Security" Link to display the IP Security Menu. The IP Security menu in the Web Browser Interface will accept addresses in either IPv4 or IPv6 format.

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

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

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

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

5.9.3.2. Linux Operators and Wild Cards

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

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

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

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

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

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

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

5.9.3.3. IP Security Examples

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

   - Allow List:
     1. 192.255.255.192
     2. 168.112.112.05

   - Deny List:
     1. ALL

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

   - Allow List:
     1. ALL EXCEPT 192.255.255.192, 168.112.112.05
   - Deny List:
     1. 192.255.255.192, 168.112.112.05

Notes:

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

5.9.4. Static Route

The Static Route menu allows you to type in Linux routing commands that will be automatically executed each time that the unit powers up or reboots. In the Text Interface, the Static Route menu is accessed via the Network Configuration menu. In the Web Browser Interface, the Static Route menu is accessed via the flyout menus under the Network Configuration link. Note that parameters defined via this menu will be applied to both IPv4 and IPv6 communication

5.9.5. Domain Name Server

The DNS menu is used to select IPv4 or IPv6 format IP addresses for Domain Name Servers. When web and network addresses are entered, the Domain Name Server interprets domain names (e.g., www.wti.com), and translates them into IP addresses. In the Text Interface, the DNS menu is accessed via the Network Configuration menu. In the Web Browser Interface, the DNS menu is accessed via the flyout menus under the Network Configuration link. Note that if you don't define at least one DNS server, then IP addresses must be used, rather than domain names. Note that parameters defined via this menu will be applied to both IPv4 and IPv6 communication.

The Domain Name Server menu includes a Ping Test feature, that allows you to ping the IP addresses for each user-defined domain name server in order to check that a valid IP address has been entered.

Note: *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

5.9.6. SNMP Access Parameters

These menus are used to select access parameters for the SNMP feature. The SNMP Access Parameters menus allow the following parameters to be defined:

Notes:

- *After you have configured SNMP Access Parameters, you will then be able to manage the AFS's User Directory and display unit status via SNMP, as described in Section 13.*
- *In the Text Interface, SNMP Access Parameters are defined via two separate menus that are accessed via either the* **/N** *command (IPv4) or the* **/N6** *command (IPv6.)*
- *In the Web Browser interface, both IPv4 and IPv6 SNMP Access Parameters are defined via a single menu. When defining IPv6 parameters, make certain that the IPv6 checkbox in the SNMP Access Parameters menu is checked.*

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

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

- **Version:** This parameter determines which SNMP Version the AFS will respond to. For example, if this item is set to V3, then clients who attempt to contact the AFS using SNMPv2 will not be allowed to connect. (Default = V1/V2 Only.)

- **Read Only:** Enables/Disables the "Read Only Mode", which controls the ability to access configuration functions and invoke switching commands. When Enabled, you will not be able to change configuration parameters or invoke other commands when you contact the AFS via SNMP. (Default = No.)

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

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

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

Notes:

- *The Authentication / Privacy item is not available when the Version parameter is set to V1/V2.*
- *If the Version Parameter is set to V1/V2/V3 (all) and Authentication / Privacy parameter is set to "Auth/Priv", then only V3 data will be encrypted.*
- *The AFS does not support "noAuth/noPriv" for SNMPv3 communication.*

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

Notes:

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

- **Privacy Protocol:** (SNMPv3 Only) Selects AES or DES encryption support. (Default = DES)

  Note: *SNMPv2 does not support encryption.*

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

  Note: *If identical names are defined for the Read Only Community and Read/Write Community, then the unit will give priority to the Read/Write Community option.*

5.9.7. SNMP Trap Parameters

These menus are used to select parameters that will be used when SNMP traps are sent. For more information on SNMP Traps, please refer to Section 12. In the Text Interface, the SNMP Trap Parameters menu is accessed via the Network Configuration menu. In the Web Browser Interface, the SNMP Trap Parameters menu is accessed via the flyout menus under the Network Configuration link. The SNMP Trap Parameters menu allows the following parameters to be defined:

Notes:

- *In the Text Interface, SNMP Trap parameters are defined via two separate menus that are accessed via either the* **/N** *command (IPv4) or the* **/N6** *command (IPv6.)*
- *In the web browser interfrace, SNMP Trap parameters are defined via two separate submenus that are accessed via the IPv4 or IPv6 flyout menus, under the SNMP Traps link.*

- **SNMP Manager 1:** The IP Address for the first SNMP Manager. (Default = Undefined.)

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

- **SNMP Manager 2:** (Default = Undefined.)
- **Trap Community:** (Default = Public.)
- **Trap Version:** The assigned security level for SNMP traps. (Default = V1)
- **V3 Trap Engine ID:** The V3 SNMP agent's unique identifier. (Default = undefined)
- **Ping Test:** Allows you to ping the IP addresses or domain names defined via the SNMP Manager 1 and SNMP Manager 2 prompts in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping the currently defined SNMP Managers in order to make certain that the IP addresses are responding.*

5.9.8. LDAP Parameters

The AFS supports LDAP (Lightweight Directory Access Protocol,) which allows authentication via the "Active Directory" network Directory Service. When LDAP is enabled and properly configured, command access rights can be granted to new users without the need to define individual new accounts at each AFS unit, and existing users can also be removed without the need to delete the account from each AFS unit. This type of authentication also allows administrators to assign users to LDAP groups, and then specify which circuits the members of each group will be allowed to control at each AFS unit.

In order to apply the LDAP feature, you must first define User Names and associated Passwords and group membership via your LDAP server, and then access the AFS command mode to enable and configure the LDAP settings and define port access rights and command access rights for each group that you have specified at the LDAP server. Note that in order to access the LDAP Parameters menu, you must login to AFS command mode using a password that permits Administrator level commands.

Notes:

- *In the Text Interface, the LDAP Parameters menu is accessed via the Network Configuration menu (/N for IPv4 parameters or /N6 for IPv6 parameters.)*
- *In the Web Browser Interface, both IPv4 and IPv6 parameters are defined via a single LDAP Parameters menu, which is accessed via the flyout menus under the Network Configuration link.*
- *Circuit access rights are not defined at the LDAP server. They are defined via the LDAP Group configuration menu on each AFS unit and are specific to that AFS unit alone.*
- *When LDAP is enabled and properly configured, LDAP authentication will supersede any passwords and access rights that have been defined via the AFS user directory.*
- *If no LDAP groups are defined on a given AFS unit, then access rights will be determined as specified by the "default" LDAP group.*
- *The "default" LDAP group cannot be deleted.*

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

- **Enable:** Enables/disables LDAP authentication. (Default = Off.)
- **Primary Host IPv4:** Defines the IP address or domain name for the primary LDAP server when IPv4 protocol is used to communicate with the AFS unit. (Default = undefined)
- **Primary Host IPv6:** Defines the IP address or domain name for the primary LDAP server when IPv6 protocol is used to communicate with the AFS unit. (Default = undefined)
- **Secondary Host IPv4:** Defines the IP address or domain name for the secondary (fallback) LDAP server when IPv4 protocol is used. (Default = undefined)
- **Secondary Host IPv6:** Defines the IP address or domain name for the secondary (fallback) LDAP server when IPv6 protocol is used. (Default = undefined)

- **LDAP Port:** Defines the port that will be used to communicate with the LDAP server. (Default = 389.)
- **TLS/SSL:** Enables/Disables TLS/SSL encryption. Note that when TLS/SSL encryption is enabled, the LDAP Port should be set to 636. (Default = Off.)
- **Bind Type:** Sets the LDAP bind request password type. In the Text Interface, when the Bind Type is set to "Kerberos" LDAP, the menu will include an additional prompt, used to select Kerberos parameters. In the Web Browser Interface, Kerberos parameters are defined via the main LDAP Parameters menu. (Default = Simple.)
- **Search Bind DN:** The username that will be allowed to search the LDAP directory. (Default = undefined.)
- **Search Bind Password:** Sets the Password for the user who is allowed to search the LDAP directory. (Default = undefined.)
- **User Search Base DN:** Sets the directory location for user searches. (Default = undefined.)
- **User Search Filter:** Selects the attribute that lists the user name. Note that this attribute should always end with "=%s" (no quotes.) (Default = undefined.)
- **Group Membership Attribute:** Selects the attribute that lists group membership(s). (Default = undefined.)
- **Group Membership Value Type:** (Default = DN.)
- **Fallback:** Enables/Disables the LDAP fallback feature. When enabled, the AFS will revert to it's own internal user directory if no defined users are found via the LDAP server. In this case, port access rights will then be granted as specified in the default LDAP group. (Default = Off.)
- **LDAP Group Setup:** Provides access to a submenu, which is used to view, add,, modify and delete LDAP Groups as described in Sections 5.9.8.1 through 5.9.8.4.
- **LDAP Kerberos Setup:** Kerberos is a network authentication protocol, which provides a secure means of identity verification for users who are communicating via a non-secure network. In the Text Interface, Kerberos parameters are selected via a submenu that is only available when Kerberos is selected as Bind Type. In the Web Browser Interface, Kerberos parameters are defined via the main LDAP Parameters menu. The following parameters are available:
  - **Port:** (Default = 88.)
  - **Realm:** (Default = Undefined.)
  - **Key Distribution Centers (KDC1 through KDC5):** (Default = Undefined.)
  - **Domain Realms 1 through 5:** (Default = Undefined.)

- **Debug:** This option is used to assist WTI Technical Support personnel with the diagnosis of LDAP issues.
- **Ping Test:** Allows you to ping IP addresses or domain names that have been defined via the LDAP Parameters menus in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.9.8.1. Viewing LDAP Groups

If you need to examine an existing LDAP group definition, the "View LDAP Groups" function can be used to review the group's parameters and Circuit Access settings.

5.9.8.2. Adding LDAP Groups

Once you have defined several users and passwords via your LDAP server, and assigned those users to LDAP Groups, you must then grant access rights to each LDAP Group at each AFS unit. In order to add LDAP groups, you must log in to command mode using a password that permits access to Administrator level commands. The Add LDAP Group menu allows the following parameters to be defined:

- **Group Name:** Note that this name must match the LDAP Group names that you have assigned to users at your LDAP server. (Default = undefined.)
- **Access Level:** Sets the command access level. (Default = User.)
- **Circuit Access:** This item is used to select the AFS Circuit Modules that members of this LDAP group will be allowed to connect. (Default = All Circuits Off.)
- **Circuit Group Access:** This item is used to determine which Circuit Groups the members of this LDAP Group will be allowed to control. (Default = undefined.)
- **Service Access:** Selects access methods for this LDAP Group. Determines whether members of this LDAP Group will be allowed to access command mode via Serial Port, Telnet/SSH, Web and/or to establish outbound connections. Also enables/disables Outbound Telnet. (Default; Serial Port = On, Telnet/SSH = On, Outbound Access = Off.)

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

5.9.8.3. Modifying LDAP Groups

If you need to modify an existing LDAP Group in order to change parameters or circuit access rights, the "Modify LDAP Group" function can be used to reconfigure group parameters. To Modify an existing LDAP Group, access the AFS command mode using a password that permits access to Administrator Level commands. Once you have accessed the Modify LDAP Group menu, use the menu options to redefine parameters in the same manner that is used for the Add LDAP Group menu.

> **Note:** *After you have defined LDAP Group parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Modify LDAP Group" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the "Saving Configuration" message is displayed.*

5.9.8.4. Deleting LDAP Groups

The Delete LDAP Group function is used to delete LDAP Groups that are no longer needed. To delete an existing LDAP Group, you must access command mode using a password that permits access to Administrator Level commands.

5.9.9. TACACS Parameters

The TACACS Configuration Menus offer the following options:

- **Enable:** Enables/disables the TACACS feature at the Network Port. (Default = Off.)
- **Primary Address:** Defines the IP address or domain name (up to 64 characters) for your primary TACACS server. (Default = undefined.)
- **Secondary Address:** Defines the IP address or domain name (up to 64 characters) for your secondary, fallback TACACS server (if present.) (Default = undefined.)
- **Secret Word:** Defines the shared TACACS Secret Word for both TACACS servers. (Default = undefined.)
- **Fallback Timer:** Determines how long the AFS will continue to attempt to contact the primary TACACS Server before falling back to the secondary TACACS Server. (Default = 15 Seconds.)
- **Fallback Local:** Determines whether or not the AFS will fallback to its own password/username directory when an authentication attempt fails. When enabled, the AFS will first attempt to authenticate the password by checking the TACACS Server; if this fails, the AFS will then attempt to authenticate the password by checking its own internal username directory. This Parameter offers three options:
  - **Off:** Fallback Local is disabled (Default.)
  - **On (All Failures):** Fallback Local is enabled, and the unit will fallback to it's own internal user directory when it cannot contact the TACACS Server, or when a password or username does not match the TACACS Server.
  - **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to it's own internal user directory when it cannot contact the TACACS Server.
- **Authentication Port:** The port number for the TACACS function. (Default = 49.)
- **Default User Access:** When enabled, this parameter allows TACACS users to access the AFS command mode without first defining a TACACS user account on the AFS. When new TACACS users access the AFS command mode, they will inherit the default Access Level, Circuit Access, Circuit Group Access and Service Access that are defined via the items listed below: (Default = On.)
  - **Enable:** Enables/disables the Default User Access function. (Default = On.)
  - **Access Level:** Selects the default Access Level setting for new TACACS users. This option can set the default access level to "Administrator", "SuperUser", "User" or "ViewOnly." (Default = User.)

➤ **Circuit Access:** Selects the default Circuit Access setting for new TACACS users. The Circuit Access setting determines which Circuit Module(s) each account will be allowed to control. (Defaults; Administrator and SuperUser = All Circuits On, User = All Circuits Off, ViewOnly = All Circuits Off.)

Notes:

- *Administrator and SuperUser level accounts always have access to all circuits.*
- *User level accounts will only have access to the circuits that are defined via the "Circuit Access" parameter.*
- *ViewOnly accounts are not allowed to invoke switching commands.*

➤ **Circuit Group Access:** Selects the default Circuit Group Access setting for new TACACS users. (Defaults; Administrator and SuperUser = All Circuit Groups On, User = All Circuit Groups Off, ViewOnly = All Circuit Groups Off.)

Notes:

- *In order to use this feature, Circuit Groups must first be defined as described in Section 5.7.*
- *Administrator and SuperUser level accounts will always have access to all Circuit Groups.*
- *User Level accounts will only have access to the Circuit groups that are defined via the Circuit Group Access parameter.*
- *ViewOnly accounts are not allowed to invoke switching commands.*

➤ **Service Access:** Selects the default Service Access setting for new TACACS users. Determines whether each account will be able to access command mode via Serial Port, Telnet/SSH or Web. In addition, the Service Access setting also determines whether each account will be able to employ the Outbound Access function. (Default = Serial Port = On, Telnet/SSH = On, Web = On.)

Note: *If Outbound Access has been disabled via the Network Parameters menu, then the Service Access parameter will not be allowed to grant Outbound Access to new TACACS users.*

- **Ping Test:** Allows you to ping IP addresses or domain names that have been defined via the TACACS Parameters menus in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.9.10. RADIUS Parameters

In the Text Interface, the RADIUS Parameters menu is accessed via the Network Configuration menu (/N for IPv4 parameters or /N6 for IPv6 parameters.) In the Web Browser Interface, both IPv4 and IPv6 parameters are defined via a single RADIUS Parameters menu, which is accessed via the flyout menus under the Network Configuration link. The RADIUS Configuration Menus offer the following options:

- **Enable:** Enables/disables the RADIUS feature at the Network Port. (Default = Off.)
- **Primary Address IPv4:** Defines the IP address or domain name for your primary RADIUS server when IPv4 protocol is used. (Default = undefined)
- **Primary Address IPv6:** Defines the IP address or domain name for your primary RADIUS server when IPv6 protocol is used. (Default = undefined)
- **Primary Secret Word:** Defines the RADIUS Secret Word for the primary RADIUS server. (Default = undefined.)
- **Secondary Address IPv4:** Defines the IP address or domain name for your secondary, fallback RADIUS server when IPv4 protocol is used. (Default = undefined)
- **Secondary Address IPv6:** Defines the IP address or domain name for your secondary, fallback RADIUS server when IPv6 protocol is used. (Default = undefined)
- **Secondary Secret Word:** Defines the RADIUS Secret Word for the secondary RADIUS server. (Default = undefined.)
- **Fallback Timer:** Determines how long the AFS will continue to attempt to contact the primary RADIUS Server before falling back to the secondary RADIUS Server. (Default = 3 Seconds.)
- **Fallback Local:** Determines whether or not the AFS will fallback to its own password/username directory when an authentication attempt fails. When enabled, the AFS will first attempt to authenticate the password by checking the RADIUS Server; if this fails, the AFS will then attempt to authenticate the password by checking its own internal username directory. This parameter offers three options:
  - **Off:** Fallback Local is disabled (Default.)
  - **On (All Failures):** Fallback Local is enabled, and the unit will fallback to it's own internal user directory when it cannot contact the Radius Server, or when a password or username does not match the Radius Server.
  - **On (Transport Failure):** Fallback Local is enabled, but the unit will only fallback to it's own internal user directory when it cannot contact the Radius Server.
- **Retries:** Determines how many times the AFS will attempt to contact the RADIUS server. Note that the retries parameter applies to both the Primary RADIUS Server and the Secondary RADIUS Server. (Default = 3.)
- **Authentication Port:** The Authentication Port number for the RADIUS function. (Default = 1812.)

- **Accounting Port:** The Accounting Port number for the RADIUS function. (Default = 1813.)
- **Debug:** (Text Interface Only) When enabled, the AFS will put RADIUS debug information into Syslog. (Default = Off.)
- **OneTime Auth:** This feature should be enabled when using Two Factor Authentication with the One Time Password scheme enabled. When enabled, the One Time Password will be valid for the time specified under the OneTime Auth Timer parameter. (Default = Off)
- **OneTime Auth Timer:** When the OneTime Auth parameter is enabled, this parameter determines how long (in minutes) the One Time Password will be valid. (Default = 5 Minutes)
- **Ping Test:** Allows you to ping IP addresses or domain names that have been defined via the RADIUS Parameters menus in order to check that a valid IP address or domain name has been entered.

Notes:

- *In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *In addition to the Ping Test feature, the /TEST command in the Text Interface or the "Test" option in the Web Browser Interface can also be used to ping any user defined IP address in order to make certain that the IP address is responding.*

5.9.10.1. Dictionary Support for RADIUS

The RADIUS dictionary file can allow you to define a user and assign command access rights and port access rights from a central location. The RADIUS dictionary file, "dictionary.wti" is included on the CDROM along with this user's guide. To install the dictionary file on your RADIUS server, please refer to the documentation provided with your server; some servers will require the dictionary file to reside in a specific directory location, others will require the dictionary file to be appended to an existing RADIUS dictionary file. The WTI RADIUS dictionary file provides the following commands:

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

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

  `WTI-Super="2"`

- **`WTI-Circuit-Access`** - Determines which circuit(s) the user will be allowed to access. This command provides an argument that consists of a four character string, with one character for each the AFS's Circuit Modules. The following options are available for each switched circuit:
  `0` = Off (Deny Access)
  `1` = On (Allow Access)

  For example, to allow access to Circuits 2 and 4, the command line would be:

  `WTI-Circuit-Access="0101"`

- **`WTI-Group-Access`** - Determines which Circuit Group(s) the user will be allowed to access. The argument for this command includes a character for each, defined Circuit Group, with the first character in the string being used to represent the first Circuit Group defined, and the last character in the string representing the last Circuit Group defined. The following options are available for each Circuit Group:
  `0` = Off (Deny Access)
  `1` = On (Allow Access)

  For example, to allow access to the first three defined Circuit Groups out of a total of six defined Circuit Groups, the command line would be:

  `WTI-Group-Access="111000"`

Example:
The following command could be used to set the command access level to "User", allow access to Circuits 1 and 2, and also allow access to the first two of five defined Circuit Groups:

```
tom  Auth-Type:=Local, User-Password=="tom1"
   Login-Service=Telnet,
   Login-TCP-Port=Telnet,
   User-Name="HARRY-tom",
   WTI-Super="1",
   WTI-Circuit-Access="1100",
   WTI-Group-Access="11000",
```

5.9.11. Email Messaging Parameters

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

- **Text Interface:** Type **/N** (for IPv4 parameters) or /N6 (for IPv6 parameters) and press **[Enter]** to access the Network Configuration Menu. Key in the number for the Email Messaging option and press **[Enter]** to display the Email Messaging Menu.
- **Web Browser Interface:** Place the cursor over the "Network Configuration" link on the left hand side of the screen. When the fly-out menu appears select either the link for IPv4 parameters or IPv6 parameters to display the Email Messaging Menu.

The Email Configuration menu offers the following options:

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

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

5.10. Save User Selected Parameters

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

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

5.10.1. Restore Configuration

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

Notes:

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

To restore the previously saved configuration, proceed as follows:

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

6. Ping-No-Answer Fallback Switching

The Ping-No-Answer function can be used to automatically switch one or more circuit modules when an attached device fails to respond to a Ping Command. In addition, the Ping-No-Answer function can also be configured to send an email, text message, Syslog Message or SNMP Trap to notify you whenever a Ping-No-Answer Action occurs. Please refer to Section 7.3 for instructions on setting up alarm notification for Ping-No-Answer Actions.

To set up a Ping-No-Answer Profile, you must access command mode using a password that permits Administrator level commands. In the Text Interface, type **/PNA** and press **[Enter]** to access the Ping-No-Answer Configuration menu and then select the desired option from the resulting submenu. In the Web Browser Interface, the Ping-No-Answer Configuration menu is accessed via the link on the left hand side of the screen.

Notes:

- *In order for the Ping-No-Answer Reboot feature to work properly, your network and/or firewall as well as the device at the target IP address must be configured to allow ping commands.*
- *After defining or editing Ping-No-Answer parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Ping No Answer" button to save parameters; in the Text Interface, press **[Esc]** several times until the AFS displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.1. Adding Ping-No-Answer Profiles

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

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

  Notes:

  - *In order to use domain names, DNS Server parameters must first be defined as described in Section 5.9.5.*
  - *In the Text Interface, a submenu will be displayed that allows the user to choose either IPv4 protocol or IPv6 protocol.*
  - *In the Web Browser Interface, the Add Ping-No-Answer Reboot menu includes a menu item that is used to select IPv4 protocol or IPv6 protocol.*

- **Protocol:** Allows definition of an IPv4 format IP Address or an IPv6 format IP Address. Note that if desired, both an IPv4 and an IPv6 format IP Address may be defined. (Default = IPv4)

  Note: *In the Text Interface, the protocol is specified via the IP Address or Domain Name prompt.*

- **Ping Interval:** Determines how often the Ping command will be sent to the selected IP Address. The Ping Interval can be any whole number, from 1 to 3,600 seconds. (Default = 60 Seconds.)

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

- **Interval After Failed Ping:** Determines how often the Ping command will be sent after a previous Ping command receives no response. (Default = 10 Seconds.)

- **Ping Delay After PNA Action:** Determines how long the AFS will wait to send additional Ping commands, after Ping-No-Answer A/B switching has been initiated. (Default = 15 Minutes.)

- **Consecutive Failures:** Determines how many consecutive failures of the Ping command must be detected in order to initiate Ping-No-Answer fallback switching. For example, if this value is set to "3", then after three consecutive Ping failures, the specified Circuit Module(s) will then be switched. (Default = 5.)

- **Toggle:** Enables/Disables the Ping-No-Answer Fallback function for the specified IP address. When enabled, the AFS will switch the selected circuit(s) or Circuit Group(s) when the target device fails to respond to a ping command. When disabled, the AFS will not switch the specified circuit(s) when a ping failure is detected, but will continue to send notification, providing that notification parameters have been defined and the Ping-No-Answer Answer alarm has been enabled. (Default = No.)

  Notes:

  - *In order for Email/Text Message Notification to function, you must first define Email/Text Message parameters.*
  - *In order for Syslog Message Notification to function, you must first define a Syslog Address.*
  - *In order for SNMP Trap Notification to function, you must first define SNMP parameters.*

- **Circuit Access:** Determines which Circuit Modules will be switched when the IP address for this Ping-No-Answer Profile fails to respond. In the Text Interface, Circuit Access is defined via a separate submenu; in the Web Browser Interface, Circuit Access is defined via a drop down menu, accessed by clicking on the "plus" sign in the "Configure Circuit Access" field. (Default = undefined.)

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

- **PNA Action:** Determines how the AFS will react when the IP address fails to respond. The PNA Action parameter allows you to select one of the following options. (Default = Continuous.)
  - **Continuous:** (Default) If the target device fails to respond, the AFS will continuously restart the PNA Check cycle until the IP address responds. Each time the device fails to respond to a ping command, the AFS will continue to switch the specified circuit(s) or group(s).
  - **Single:** If the target device fails to respond, the AFS will switch the specified circuit(s) or groups only once.
  - **Recover Mode:** If the target device fails to respond, the AFS will continue to ping the target device. If the target device eventually responds, the AFS will then switch the specified circuit(s) or group(s) to their original A/B status.
- **Ping Test:** Sends a test Ping command to the IP Address or domain name that has been defined for this Ping-No-Answer Profile.

Notes:

- *In order for the Ping Test function to work properly, your network and/or firewall as well as the device at the target IP address must be configured to allow ping commands.*
- *After you have finished defining or editing Ping-No-Answer Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Add Ping No Answer" button to save parameters; in the Text Interface, press the **[Esc]** key several times until the RSM-8R8 Series unit displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.2. Viewing Ping-No-Answer Profiles

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

6.3. Modifying Ping-No-Answer Profiles

After you have defined a Ping-No-Answer profile, you can modify the configuration of the profile using the Modify Ping-No-Answer function. To modify the configuration of an existing Ping-No-Answer profile, you must access the command mode using a password that allows Administrator level commands. The AFS will display a screen which allows you to modify parameters for the selected Ping-No-Answer Profile. Note that this screen functions identically to the Add Ping-No-Answer menu.

> **Note:** *After you have finished defining or editing Ping-No-Answer Reboot parameters, make certain to save the changes before proceeding. In the Web Browser Interface, click on the "Change Ping No Answer" button to save parameters; in the Text Interface, press the* ***[Esc]*** *key several times until the RSM-8R8 Series unit displays the "Saving Configuration" message and the cursor returns to the command prompt.*

6.4. Deleting Ping-No-Answer Profiles

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

7. Alarm Configuration

The AFS offers an assortment of user configurable alarm functions, that can be used to provide notification or perform user specified tasks when high rack temperatures, power supply instability, lost dialtone to a modem and other significant conditions are detected. In addition, the AFS can also generate an alarm when the Monitor/Alarm Input feature detects a signal change at the Control Module AUX connector. When an alarm condition is detected, the AFS can send an "Alarm" to user selected personnel via Email, text message, Syslog Message or SNMP trap.

Notes:

- *In order to send alarm notification via email or text message, email addresses and parameters must first be defined.*
- *In order to send alarm notification via Syslog Message, a Syslog address must first be defined .*
- *In order to send alarm notification via SNMP Trap, SNMP Trap parameters must first be defined .*
- *After defining parameters via the Text Interface, make certain to press the **[Esc]** key several times to completely exit from the configuration menu and save newly defined parameters. When parameters are defined via the Text Interface, newly defined parameters will not be saved until the "Saving Configuration" message is displayed.*

To configure the AFS's Alarm functions, first access command mode using a password that allows Administrator level commands. If you are communicating with the unit via the Text Interface, type **/AC** and then press **[Enter]**. If you are communicating via the Web Browser Interface, click on the "Alarm Configuration" link on the left hand side of the screen. The Alarm Configuration Menu will be displayed.

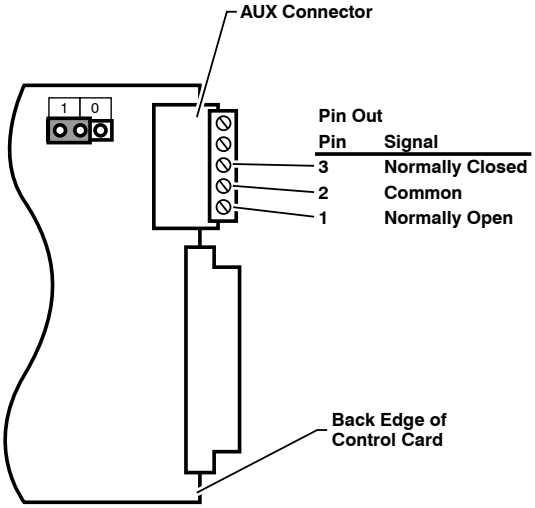

Figure 7.1: Control Module AUX Connector - Output Contacts

7.1. The Output Contacts

In addition to providing notification when an alarm is generated, the Over Temperature Alarms, Ping-No-Answer Alarm, Invalid Access Lockout Alarm and Monitor Input Alarm all offer the option to switch the output contacts on the Control Module AUX Connector when an alarm is triggered. The output contacts can then be used to activate an audible alarm or other device in response to these alarms.

When the Contact Output Enable parameter is enabled for any of these alarms, the Common line will be switched from the Normally Closed contact to the Normally Open contact in order to drive an attached device.

Figure 7.1 above shows the location of the Normally Closed, Common and Normally Open contacts on the Control Module AUX Connector.

7.2. The Over Temperature Alarms

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

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

If the user-defined trigger levels for temperature are exceeded, the AFS can also enable the Contact Output on the AFS Control Module's AUX connector.

To configure the Over Temperature Alarms, access the AFS command mode using a password that permits Administrator Level commands, and then use the Alarm Configuration menu to select the desired alarm feature. Note that both the Initial Threshold menus and Critical Threshold menus offer essentially the same set of parameters, but the parameters defined for each alarm are separate and unique. Therefore, parameters defined for the Critical Threshold Alarm will not be applied to the Initial Threshold Alarm and vice versa.

Notes:

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

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

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

Notes:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message, Address 1, 2 and 3 and Contact Output Enable Parameters all include "Copy to All Triggers" options that allow you to assign the corresponding parameter for all AFS alarms. For example, if the Over Temperature Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other AFS alarms will also be enabled.*

- **Alarm Set Threshold:** The trigger level for this alarm. (Initial Threshold: Default = 110°F or 43°C, Critical Threshold: Default = 120°F or 49°C.)

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

- **Alarm Clear Threshold:** Determines how low the temperature must drop in order for the Alarm condition to be cancelled. (Initial Threshold: Default = 100°F or 38°C, Critical Threshold: Default = 110°F or 43°C.)

  Note: *The System Parameters menu is used to set the temperature format for the AFS unit to either Fahrenheit or Celsius.*

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

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

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

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

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

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

- **Contact Output Enable:** Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when an Over-Temperature Alarm is generated. (Default = On.)

  Note: *For more information on the Output Contacts, please refer to Section 7.1.*

7.3. The Ping-No-Answer Alarm

The Ping-No-Answer Alarm is intended to provide notification when one of the IP addresses defined via the Ping-No-Answer function fails to respond to a Ping command. When one of the user-defined IP addresses fails to answer a Ping command, the AFS can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *In order for the Ping-No-Answer Alarm to work properly, your network and/or firewall, as well as the device at the target IP address, must be configured to allow ping commands.*
- *In order for this alarm to function, at least one target IP Address for the Ping No Answer Alarm must be defined as described in Section 6.*
- *In order for the AFS to provide Email alarm notification, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the AFS to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2.*
- *In order for the AFS to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7.*

7.3.1. Defining Ping-No-Answer IP Addresses

In order for the Ping-No-Answer Alarm to function, you must first define at least one Ping-No-Answer profile. In the Text Interface, the **/PNA** command provides access a submenu that is used to define Ping-No-Answer profiles. In the Web Interface, Ping-No-Answer profiles are defined via the "Ping-No-Answer Configuration" option on the left hand side of the screen. For more information regarding definition of Ping-No-Answer profiles and associated IP address, please refer to Section 6.

Note: *To define Ping-No-Answer IP addresses for the Ping-No-Answer Alarm, without enabling the A/B switching function, make certain that the "Toggle" option in the Add Ping-No-Answer Profile menu is set to "No."*

7.3.2. Configuring the Ping-No-Answer Alarm

To configure the Ping-No-Answer Alarm, access the AFS command mode using a password that permits Administrator Level commands. The Ping-No-Answer alarm configuration menu offers the following parameters:

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

  Notes:

  - *In order for this alarm to function, at least one target IP Address for the Ping No Answer Alarm must be defined as described in Section 6.*
  - *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter to Off and then back On again.*
  - *The Trigger Enable, Notify on Clear, Email Message, Address 1, 2 and 3 and Contact Output Enable Parameters all include "Copy to All Triggers" options that allow you to assign the corresponding parameter for all AFS alarms. For example, if the Ping No Answer Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other AFS alarms will also be enabled.*

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

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

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

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

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

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

- **Contact Output Enable:** Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when a Ping-No-Answer Alarm is generated. (Default = On.)

  Note: *For more information on the Output Contacts, please refer to Section 7.1.*

7.4. The Serial Port Invalid Access Lockout Alarm

The Serial Port Invalid Access Lockout Alarm can provide notification when the AFS has locked the serial SetUp Port due to repeated, invalid attempts to access command mode. Normally, the Invalid Access Lockout feature can lock the serial SetUp Port whenever the unit detects that a user-defined threshold for invalid access attempts at the SetUp Port is exceeded. When a serial port lockout occurs, the unit can provide notification via Email, Syslog Message or SNMP Trap.

Notes:

- *Note that Serial Port Invalid Access Lockout Alarm is only intended to provide notification when the Invalid Access Lockout feature has locked the serial SetUp Port. To apply the Invalid Access Lockout feature to the Network Port, please refer to Section 5.3.2.*
- *In order for this alarm to function, Invalid Access Lockout parameters for the serial port must first be configured and enabled.*
- *If desired, the AFS can be configured to count Invalid Access attempts at the serial SetUp port, and provide notification when the counter exceeds a user defined trigger level, without actually locking the port in question. To do this, enable the Invalid Access Lockout Alarm as described here, but when you configure Invalid Access Lockout parameters as described in Section 5.3.2, set the Lockout Attempts and Lockout Duration as you would normally, and then set the "Lockout Enable" parameter to "Off."*
- *In order for the AFS to provide Email alarm notification, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the AFS to provide Syslog Message notification, Syslog parameters must first be defined and Syslog Messages must be enabled.*
- *In order for the AFS to provide SNMP Trap notification when this alarm is triggered, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Serial Port Invalid Access Lockout Alarm, access the AFS command mode using a password that permits Administrator Level commands. The Invalid Access Lockout alarm configuration menu offers the following parameters:

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

Notes:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message, Address 1, 2 and 3 and Contact Output Enable Parameters all include "Copy to All Triggers" options that allow you to assign the corresponding parameter for all AFS alarms. For example, if the Invalid Access Lockout Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then other AFS alarms will also be enabled.*

- **Resend Delay:** Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes.)
- **Notify Upon Clear:** When this item is enabled, the AFS will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the AFS will send initial notification when it detects that an Invalid Access Lockout has occurred, and then send a second notification when it determines that the port has been unlocked. (Default = On.)
- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

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

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: Invalid Access Lockout")
- **Contact Output Enable:** Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when a Ping-No-Answer Alarm is generated. For more information, please refer to Section 7.1. (Default = On.)

  Note: *For more information on the Output Contacts, please refer to Section 7.1.*

7.5. The Power Cycle Alarm

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

Notes:

- *In order for the AFS to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the AFS to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the AFS to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Power Cycle Alarm, you must access the AFS command mode using a password that permits Administrator Level commands. The Power Cycle Alarm configuration menu offers the following parameters:

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

  Notes:

  - *When an alarm is generated, to cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
  - *The Trigger Enable, Email Message and Address 1, 2 and 3 Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all applicable AFS alarms. For example, if the Power Cycle Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then other AFS alarms will also be enabled.*

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

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

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

7.6. Monitor/Alarm Input

The Monitor/Alarm Input feature allows the AFS to monitor Pin 4 on the Control Module's AUX connector, and then switch circuit modules, and/or activate an audible alarm or other external device and/or send notification when the signal at Pin 4 changes.

Notes:

- *In order for the AFS to provide alarm notification via Email, communication parameters must first be defined as described in Section 5.9.11.*
- *In order for the AFS to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the AFS to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

To configure the Monitor/Alarm Input feature, you must access the AFS command mode using a password that permits Administrator Level commands. The Monitor/Alarm Input configuration menu offers the following parameters:

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

Notes:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify on Clear, Email Message, Address 1, 2 and 3 and Contact Output Enable Parameters all include "Copy to All Triggers" options that allow you to assign the corresponding parameter for all AFS alarms. For example, if the Monitor/Alarm INput Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then other AFS alarms will also be enabled.*

- **Monitor/Alarm Input Level:** Determines whether a high or low signal at the Monitor Input contact (Pin 4 on the Control Module's AUX Connector) will generate an alarm. For example, if the Monitor/Alarm Input Level is set at "Low", then an alarm will be triggered when a low signal is detected at Pin 4. Note that the Monitor/Alarm Input Level is always set to compliment the setting for the Monitor Input Level Jumper as described in Section 7.6.1. (Default = Low.)
- **Monitor/Alarm Input Delay:** Determines how long the signal at the Monitor Input Contact must remain high/low in order to generate an alarm. (Default = 0.5 Seconds.)
- **Resend Delay:** Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt to send notification was unsuccessful. (Default = 60 Minutes.)

- **Notify Upon Clear:** When this item is enabled, the AFS will send additional notification when the signal at the Monitor Input contact (Pin 4 on the Control Module's AUX Connector) returns to the normal (non-alarm) state. (Default = On.)
- **Email Message:** Enables/Disables email notification for this alarm. (Default = On.)
- **Address 1, 2, and 3:** These parameters are used to select which of the three email addresses defined via the "Email Messages" menu will receive the email alarm notification messages generated by this alarm. The Address parameters can be used to select one, or any combination of the addresses defined via the Email Messages menu. (Default = All On.)

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

- **Subject:** Define the text that will appear in the "Subject" field for email notification messages generated by this alarm. (Default = "Alarm: Monitor/Alarm Input".)
- **Contact Output Enable:** Activates/deactivates the Output Contacts on the Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact. (Default = On.)

  Note: *For more information on the Output Contacts, please refer to Section 7.1.*

- **Circuits to Switch:** Selects the Circuit Module(s) and Circuit Group(s) that will be switched when the Monitor/Alarm Input feature is triggered, determines the A/B switch position and enables/disables the "Return" feature. This item provides access to a submenu which is used to define the following:

  - **Enable:** Enables/disables A/B switching in response to the Monitor/Alarm Input feature. When disabled, the AFS will not perform A/B switching with the Monitor/Alarm Input feature is triggered. (Default = Off.)
  - **Circuit State:** Specifies the A/B position that circuits will be switched to when the Monitor/Alarm Input feature is triggered. (Default = B.)
  - **Return:** Enables/Disables the Return feature, which allows the AFS to switch circuits back to their original state after a Monitor/Alarm Input event has been cleared. (Default = On.)
  - **Circuit Access:** Determines which Circuit Modules will be switched when the Monitor/Alarm Input feature is triggered. Note that in the Text Interface, Circuit Access is defined via a separate submenu; in the Web Browser Interface, Circuit Access is defined via a drop down menu, which is accessed by clicking on the "plus" sign in the "Configure Circuit Access" field. (Default = undefined.)
  - **Circuit Group Access:** Determines which Circuit Group(s) the Monitor/Alarm Input feature will be applied to. Note that in the Text Interface, Circuit Group Access is defined via a separate submenu; in the Web Browser Interface, Circuit Group Access is defined via a drop down menu, which is accessed by clicking on the "plus" sign. (Default = undefined.)

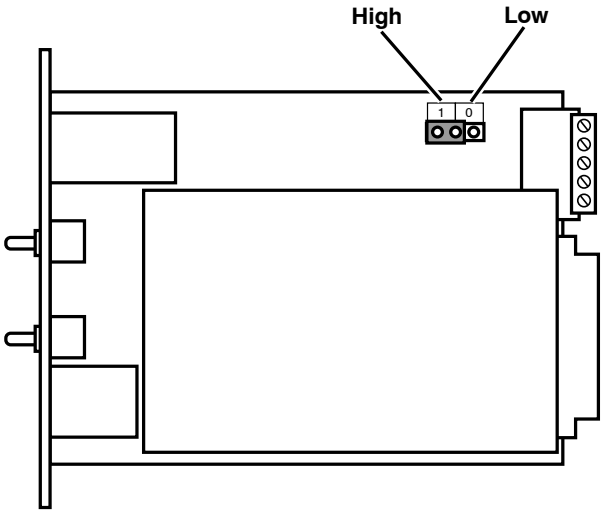

Figure 7.2: Control Module Jumper

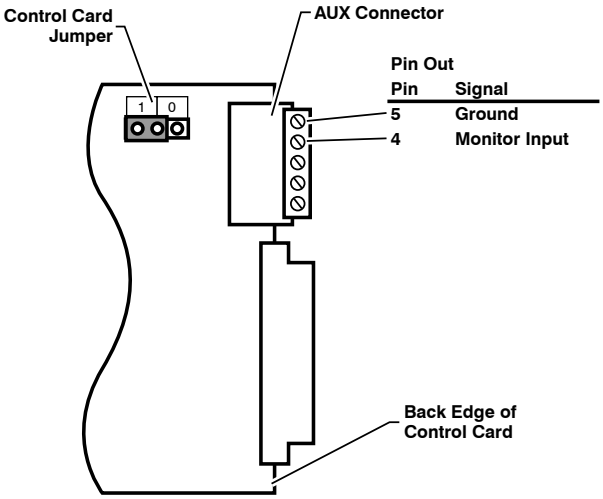

Figure 7.3: Control Module AUX Connector - Monitor Input and Ground

7.6.1. Monitor Input Level Settings

When the Monitor/Alarm Input feature is properly configured, the AFS can trigger an alarm and/or perform A/B switching operations when the signal at Pin 4 (Monitor Input) on the Control Module AUX connector goes high or low. In set up this feature, you must first use the Control Card Jumper to select the non-active (non-alarm) state, and then use the Monitor/Alarm Input configuration menu to select the active/alarm state (the signal level that will trigger an alarm) as described in the Sections that follow.

Notes:

- *The Monitor Input signal (Pin 4) is always measured relative to the signal at the common ground (Pin 5).*
- *A "Low" signal should be between Zero (0) Volts and -48 Volts and a "High" signal should be between +5 Volts and +48 Volts.*

7.6.1.1. Monitor Input Signal - Trigger When Low

To set up the Monitor/Alarm Input feature to trigger an alarm when the signal at AUX connector pin 4 (the Monitor Input) goes Low, configure the AFS as follows:

1. **Control Card Jumper Setting:** Set the Jumper to the "1" position (default.) This will set the non-active, non-alarm signal state to "High".
2. **Monitor/Alarm Input Level:** Use the Monitor/Alarm Input configuration menu to set the Monitor Alarm Input Level to "Low". This will configure the Monitor/Alarm Input feature to generate an alarm when the Monitor Input signal goes Low.
3. **Set the Remaining Parameters:** Use the Monitor/Alarm Input configuration menu to select the remaining parameters.
4. **Connect Monitor Input:** Connect the signal line that you wish to monitor to Pin 4 (Monitor Input) on the Control Module AUX Connector as shown in Figure 7.3.

7.6.1.2. Monitor Input Signal - Trigger When High

To set up the Monitor/Alarm Input feature to trigger an alarm when the signal at AUX Connector pin 4 (the Monitor Input) goes High, configure the AFS as follows:

1. **Control Card Jumper Setting:** Set the Jumper to the "0" position. This will set the non-active, non-alarm signal state to "Low" as shown in Figure 7.2.
2. **Monitor/Alarm Input Level:** Use the Monitor/Alarm Input configuration menu to set the Monitor Alarm Input Level to "High". This will configure the Monitor/Alarm Input feature to generate an alarm when the Monitor Input signal goes High.
3. **Set the Remaining Parameters:** Use the Monitor/Alarm Input configuration menu to select the remaining parameters.
4. **Connect Monitor Input:** Connect the signal line that you wish to monitor to Pin 4 (Monitor Input) on the Control Module AUX Connector as shown in Figure 7.3. Connect your ground line to the Ground Connector (Pin 5).

7.7. The No Dialtone Alarm

The No Dialtone Alarm enables the AFS to monitor a telephone line connected to an external modem installed at the AFS serial RS232 port, and then provide notification if the AFS detects that the phone line is dead or no dialtone is present.

If the No Dialtone Alarm is enabled and the AFS determines that there is no dialtone signal, the No Dialtone Alarm can provide notification via email using a network connection. In addition, The AFS will also create an entry in the Alarm Log, indicating that the No Dialtone Alarm has been triggered.

Notes:

- *In order for this alarm to function, the No Dialtone Alarm parameter must be enabled and the Rest/No Dialtone Interval must be defined. Both parameters are defined via the Serial Port Parameters menu as described in Section 5.8.*
- *In order for the AFS to provide alarm notification via Email, communication parameters must first be defined.*
- *In order for the AFS to provide alarm notification via Syslog Message, Syslog parameters must first be defined and Syslog Messages must be enabled as described in Section 5.9.2 and Section 11.*
- *In order for the AFS to provide alarm notification via SNMP Trap, SNMP parameters must first be defined, and SNMP Traps must be enabled as described in Section 5.9.7 and Section 12.*

The configuration menu for the No Dialtone Alarm allows the following parameters to be defined:

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

Note:

- *To cancel an alarm without correcting the condition that caused the alarm, simply toggle the Trigger Enable parameter Off and then back On again.*
- *The Trigger Enable, Notify Upon Clear, Email Message, Address 1, 2 and 3, and Contact Output Enable Parameters all include "Copy to All Triggers" options that allow you to enable/disable the corresponding parameter for all AFS alarms. For example, if the No Dialtone Alarm's Trigger Enable parameter is set to "On (Copy to All Triggers), then all other AFS alarms will also be enabled.*

- **Resend Delay:** Determines how long the AFS will wait to resend an email message generated by this alarm, when the initial attempt to send the notification was unsuccessful. (Default = 60 Minutes.)
- **Notify Upon Clear:** When this item is enabled, the AFS will send additional notification when the situation that caused the alarm has been corrected. For example, when Notify Upon Clear is enabled, the AFS will send initial notification when it detects that the dialtone for the external modem has been lost, and then send a second notification when it determines that the dialtone has been restored. (Default = On.)

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

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

- **Subject:** This parameter is used to define the text that will appear in the "Subject" field for all email notification messages generated by this alarm. (Default = "Alarm: No Dial Tone")
- **Contact Output Enable:** Activates/deactivates the Output Contacts on the AFS Control Module AUX Connector. When the Contact Output Enable parameter is set to "On", the Common line will be switched from the Normally Closed contact to the Normally Open contact when a Ping-No-Answer Alarm is generated. For more information, please refer to Section 7.1. (Default = On.)

  Note: *For more information on the Output Contacts, please refer to Section 7.1.*

8. The Status Screens

The Status Screens are used to display status information about the AFS hardware and firmware, Network Port, Circuit Modules, Circuit Groups and other features. The Status Screens are available via both the Text Interface and Web Browser Interface.

8.1. Product Status

The Product Status Screen lists the model number, power rating and software version and other information regarding your local AFS unit. To display the Product Status Screen via the Text Interface, type `/J*` and press **[Enter]**. To display the Product Status Screen via the Web Browser Interface, click on the "Product Status" link.

8.2. The Network Status Screen

The Network Status screen shows activity at the AFS's virtual network ports, and lists the TCP Port Number, Active/Free Status and current user name for each virtual network port. To view the Network Status Screen, access command mode using a password that permits access to Administrator Level commands. To display the Network Status Screen via the Text Interface, type `/SN` and press **[Enter]**. To display the Network Status Screen via the Web Browser Interface, click on the Network Status link.

8.3. The Circuit Status Screen

The Circuit Status Screen shows the current status of the AFS's Circuit Modules, and also lists the unit's current temperature, Monitor/Alarm Input status, and Alarm Contact Output status.

Note:

- *When the Circuit Status screen is viewed by an account with Administrator or SuperUser command access, all AFS Circuit Modules present are listed. When the Circuit Status screen is viewed by an account with User or ViewOnly command access, then the screen will list only the Circuit Modules that are allowed by the account.*
- *If a Circuit Module slot is empty, then the Circuit Status screen will display a row of dashes for that Circuit Module position.*

To display the Circuit Status Screen via the Text Interface, type `/S` and then press **[Enter]**. To display the Circuit Status Screen via the Web Browser Interface, click on the "Circuit Status" link.

8.4. The Circuit Group Status Screen

The Circuit Group Status screen shows the configuration details and A/B switching status for the AFS's user-defined Circuit Groups.

Notes:

- *When the Circuit Group Status Screen is viewed by an account with Administrator or SuperUser command access, all AFS Circuit Modules and Circuit Groups will be shown. When the Circuit Status Screen is viewed by an account with User or ViewOnly command access, then the unit will only display the Circuit Modules and Circuit Groups that are allowed by the account.*
- *In order to display the Circuit Group Status screen, you must first define at least one Circuit Group.*

To display the Circuit Group Status Screen via the Text Interface, type **/SG** and then press **[Enter]**. To display the Circuit Group Status Screen via the Web Browser Interface, click on the "Circuit Group Status" link.

8.5. The Port Diagnostics Screen

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

Note: *The Port Diagnostics Screen is only available via the Text Interface.*

8.6. IP Alias Status Screen

The IP Alias Status Screen displays the user defined IP alias for the serial port, along with the user-defined port name. To display the Alias Status Screen via the Text Interface, type **/SA** and press **[Enter]**.

8.7. The Alarm Status Screen

The Alarm Status Screen lists all available user-defined alarms and indicates whether or not each alarm has been triggered. The resulting screen will display "Yes" (or 1) for alarms that have been triggered or "No" (or 0) for alarms that have not been triggered. If desired, the /AS command line can also include an optional alarm argument that will cause the unit to display the status of one individual alarm. For a list of alarm arguments, please refer to Section 17.3.1.

8.8. The Port Parameters Screens

The /W (Who) command displays currently selected configuration parameters for the serial port and network port. Rather than listing general connection information for the ports, the Port Parameters screen lists all defined parameters for each port.

When the /W command is invoked by an Administrator or SuperUser level account, it can be used to display parameters for either the serial port or the Network Port. If the /W command is invoked by a User or ViewOnly level account, then it will only display parameters for the serial port.

The /W command offers the following options:

- **Display Serial Port Parameters:** (Administrators and SuperUsers Only) **`/w 1` [Enter]**
- **Display Network Port Parameters: `/w` [Enter]**

Note: *The Port Parameters screens are only available via the Text Interface.*

8.9. The Event Logs

8.9.1. The Audit Log

The Audit Log provides a record of most command activity at the AFS unit, including A/B switching, and login and logout activity. Note that the Audit Log does not include user information regarding access to configuration menus or status screens.

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

- **Text Interface:** Type **/L** and press **[Enter]**. The "Display Logs" menu will be shown. At the Display Logs menu, key in the number for the Audit Log, press **[Enter]** and then follow the instructions in the resulting submenu.
- **Web Browser Interface:** Place the cursor over the "Logs" link on the left hand side of the screen wait for the fly-out menu to appear. When the fly-out menu appears, click on the desired option.

8.9.2. The Alarm Log

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

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

- **Text Interface:** Type **/L** and press **[Enter]**. The "Display Logs" menu will be shown. At the Display Logs menu, key in the number for the Alarm Log, press **[Enter]** and then follow the instructions in the resulting submenu.
- **Web Browser Interface:** Place the cursor over the "Logs" link on the left hand side of the screen wait for the fly-out menu to appear. When the fly-out menu appears, click on the desired option.

8.9.3. The Temperature Log

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

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

- **Text Interface:** Type **/L** and press **[Enter]**. The "Display Logs" menu will be shown. At the Display Logs key in the number for the Temperature Log, press **[Enter]** and then follow the instructions in the resulting submenu.
- **Web Browser Interface:** Place the cursor over the "Logs" link on the left hand side of the screen wait for the fly-out menu to appear. When the fly-out menu appears, click on the desired option.

9. Operation

As discussed in Section 5, the AFS offers two separate command interfaces; the Web Browser Interface and the Text Interface. Both interfaces offer essentially the same options and features, and in most cases, parameters defined via the Web Browser Interface will also apply when communicating via the Text Interface (and vice versa.)

9.1. A/B Switching - Web Browser Interface

When using the Web Browser Interface, A/B switching commands are invoked via the Circuit Control Screen and Circuit Group Control Screen.

9.1.1. The Circuit Control Screen - Web Browser Interface

The Circuit Control Screen lists the current A/B status of the AFS's Circuit Modules and is used to control switching and rebooting of each A/B circuit. To perform A/B switching or set circuits to user-defined default states, proceed as follows:

1. Access the AFS Command Mode, and then click on the "Circuit Control" link on the left hand side of the screen to display the Circuit Control Screen.

   Notes:

   - *When the Circuit Control Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched circuits will be displayed.*
   - *When the Circuit Control Screen is displayed by an account that permits User or ViewOnly command access, the screen will only include the circuits that are specifically allowed by the account.*

2. **A/B Switching:** From the Circuit Control Menu, click the down arrow in the "Action" column for the desired circuit(s), then select position "A" or position "B" from the dropdown menu and click on the "Confirm Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Actions" button to complete the command.

3. **Setting Circuits to the Default State:** From the Circuit Control Menu, click the down arrow in the "Action" column for the desired circuits, then select "Default" from the dropdown menu and click on the "Confirm Actions" button. Next the AFS will display a screen which lists the selected switching actions and asks for confirmation before proceeding. Click on "Execute Actions" to complete the command; all selected circuits will be set to their user-defined default state.

4. **Applying a Command to All Circuits:** From the Circuit Control Menu, click the down arrow in the "Action" column in the "All Circuits" row, then select the desired operation from the dropdown menu and click on the "Confirm Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Actions" button to apply the selected command to all AFS Circuits.

   Note: *When each command is complete, the Circuit Status Screen will be displayed. At that time, the Status Screen will list the updated A/B status of each circuit.*

9.1.2. The Circuit Group Control Screen - Web Browser Interface

The Circuit Group Control Screen is used to apply A/B switching commands to all circuits in a user-defined Circuit Group. Circuit Groups allow you to define a group of circuits, dedicated to a similar purpose or client, and then direct switching commands to the group, rather than switching one circuit at a time.

To invoke A/B switching commands, proceed as follows:

1. Access the AFS Command Mode, and then click on the "Circuit Group Control" link on the left hand side of the screen to display the Circuit Group Control Screen.

   Notes:

   - *When the Circuit Group Control Screen is displayed by an account that permits Administrator or SuperUser command access, all user-defined Circuit Groups will be displayed.*
   - *When the Circuit Control Screen is displayed by an account that permits User or ViewOnly level commands, the screen will only include the Circuit Groups that are allowed by the account.*

2. **A/B Switching - Circuit Groups:** From the Circuit Group Control Menu, click the down arrow for the desired Circuit Group(s), then select "A" or "B" from the dropdown menu and click on the "Confirm Group Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Group Actions" button to execute the command(s.)

3. **Switching Circuit Groups to Defaults:** From the Circuit Group Control Menu, click the down arrow for the desired group(s), then select "Default" from the dropdown menu and click on the "Confirm Group Actions" button. Next the AFS will display a screen which lists the selected switching action(s) and asks for confirmation before proceeding. Click on the "Execute Group Actions" button to execute the command; all selected circuit groups will be set to their user-defined default states.

   Note: *When each Circuit Group command is completed, the Circuit Status Screen will be displayed. At that time, the Status Screen will show the updated A/B status of each circuit.*

9.2. A/B Switching - Text Interface

When using the Text Interface, all A/B switching functions are performed by invoking simple, ASCII commands. The Text Interface includes a Help Menu, which summarizes all available AFS commands. To display the Text Interface Help Menu, type **/H** and press **[Enter]**.

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

9.2.1. The Circuit Status Screen - Text Interface

The Circuit Status Screen lists the current status of the Circuit Modules, and also displays the current temperature, Monitor/Alarm Input status, Alarm Contact Output status and the user-defined Site I.D. Message. The Circuit Status Screen will be re-displayed each time a command is successfully executed.

9.2.2. A/B Switching Commands - Text Interface

These commands can be used to switch AFS's circuit modules, and can also be used to set circuits to the user-defined default A/B positions. Circuits may be specified by number, name or Circuit Group Name.

Notes:

- *When the Port and Circuit Status Screen is displayed by an account that permits Administrator or SuperUser level commands, all switched circuits will be displayed.*
- *When the Port and Circuit Status Screen is displayed by an account that permits ViewOnly or User command access, the screen will only include the switched circuits that are specifically allowed by the account.*
- *When you have accessed command mode using an account that permits Administrator or SuperUser level commands, switching commands can be applied to all circuits.*
- *When you have accessed command mode using an account that permits only User level commands, switching commands can only be applied to the circuits that are specifically allowed by that account.*
- *Text Interface commands are **not** case sensitive. When used in command lines, circuit names and Circuit Group names are also **not** case sensitive.*

When A/B switching commands are executed, the AFS will list specified switching actions for each applicable Circuit Module, then display a "Sure?" prompt and wait for a user response before completing the command. The unit will then return to the Circuit Status Screen.

To switch Circuits or Circuit Groups, proceed as follows:

1. **Switch Circuit(s) to "A" Position:** Type **/TA *n*** and press **[Enter]**. Where "***n***" is the number or name of the desired Circuit or Circuit Group. For example:

   /TA 1 [Enter] or **/TA DATACENTER [Enter]**

2. **Switch Circuit(s) to "B" Position:** Type **/TB *n*** and press **[Enter]**. Where "***n***" is the number or name of the desired Circuit or Circuit Group. For example:

   /TB 2 [Enter] or **/TB SERVERS [Enter]**

3. **Set All Permitted Circuits to Default A/B Positions:** Type **/DC** and press **[Enter]**. All circuits permitted by your account will be set to their default A/B status, which can be defined via the Circuit Parameters Menu.

   Notes:

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

4. **The "Toggle" Command:** As an alternative to the /TA and /TB commands, the /T (Toggle) command can also be used to perform A/B switching. Type **/T *n,p*** and press **[Enter]**. Where "***n***" is the number or name of the desired Circuit or Circuit Group and "***p***" is the desired A/B position. For example:

   /T 2,B [Enter] or **/T SERVERS,A [Enter]**

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

   /TA ROUTER,Y or **/T 2,B,Y**

9.2.2.1. Applying Commands to Several Circuits - Text Interface

As described below, A/B switching commands can be applied to only one Circuit Module, or to an assortment of circuits.

1. **Switch Several Circuits:** To apply the /TA, TB or /T command to several circuits, enter the numbers or names for the circuits, separated by a "plus sign" (**+**) or a comma (**,**). For example to switch circuits 1, 3, and 4 to the "B" position, enter one of the following commands:

   /TB 1+3+4 [Enter]
   or
   /T 1+3+4,B [Enter]

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

2. **Switch a Range of Circuits:** To apply the /TA or /TB command to a series of circuits, enter the numbers for the circuits that mark the beginning and end of the range, separated by a colon. For example to switch circuits 1 through 3 to the "A" position, enter the following:

   `/TA 1:3` [Enter]

   Note: *The "Range" argument is not available when using the /T command to switch circuits. The Range (:) argument can only be used with the /TA and /TB commands.*

4. **All Circuits:** To apply a command to all circuits, enter an asterisk in place of the name or number. For example, to switch all circuits to the "B" position, enter one of the following commands:

   `/TB *` [Enter] or **`/T *,B` [Enter]**

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

9.3. The SSH/Telnet Connect Function (Web Browser Interface Only)

The SSH/Telnet Connect function allows you to open an SSH Shell Session or Telnet Session without leaving the Web Browser interface. Once you have successfully opened an SSH Shell Session or Telnet Session, you can then use ASCII commands to configure and operate the AFS unit as described in Section 9.2 and Section 17.

9.3.1. Initiating an SSH Shell Session via the Web Browser Interface

To initiate an SSH Shell Session from the AFS Web Browser Interface, proceed as follows:

1. Place the cursor over the "SSH/Telnet Connect" button on the left hand side of the screen. When the flyout menu appears, click on the SSH option.

   Note: *If the RSP displays a message that indicates that your browser does not include the Java plugin, go to the Java website and download the latest version of the Java plugin.*

2. Start Java: Click on the File menu and select "Open Shell Session"

3. The AFS will display a prompt that asks the user to enter a valid username and host name (IP Address.) Key in the username and host name (IP address) using the following format and then click on the "OK" button:

   `username@ip_address`

   Notes:

   - *The username entered must be a valid username that has been previously defined via the AFS User Directory as described in Section 5.5.*
   - *The IP Address (host name) can either be the address to the machine that you are currently communicating with via the Web Browser Interface, or you can enter the IP address for another AFS unit, providing that the username entered is present on the other AFS unit too.*

4. After the username and host name are entered, the AFS will prompt you to enter your password. Key in the password that has been defined for the username entered in step 3 above and then click on the "OK" button.

5. The AFS will display the Circuit Status Screen, followed by the command prompt. You may now invoke AFS commands as described in Section 9.2 and 17.

6. To terminate the SSH Session, type **`/x`** and press **[Enter]**.

9.3.2. Initiating a Telnet Session via the Web Browser Interface

To initiate a Telnet Session from the AFS Web Browser Interface, proceed as follows:

1. Place the cursor over the "SSH/Telnet Connect" button on the left hand side of the screen. When the flyout menu appears, click on the Telnet option.

   Note: *If the RSP displays a message that indicates that your browser does not include the Java plugin, go to the Java website and download the latest version of the Java plugin.*

2. Log in to the Telnet Session:

   a) The AFS will display the "login" prompt. Key in a valid username that has been previously defined via the AFS User directory and then press **[Enter]**.

   b) The AFS will display the "password" prompt. Key in the valid password for the username entered above and then press **[Enter]**.

   Notes:

   - *The username entered must be a valid username that has been previously defined via the AFS User Directory as described in Section 5.5.*
   - *The IP Address (host name) can either be the address to the machine that you are currently communicating with via the Web Browser Interface, or you can enter the IP address for another AFS unit, providing that the username entered is present on the other AFS unit too.*

3. The AFS will display the Circuit Status Screen, followed by the command prompt. You may now invoke AFS commands as descrived in Section 9.2 and 17.

4. To terminate the Telnet Session, type **`/x`** and press **[Enter]**.

9.4. Manual Operation

In addition to the command driven A/B switching functions that are available via the Web Browser Interface and Text Interface, the Circuit Modules can also be manually switched. Circuit Modules can be individually controlled using the A/B switch on the Circuit Module front panel, or all 16 Circuit Modules can be manually switched using the Master A/B Gang Switch on the Control Module front panel.

If desired, the manual A/B Switch on each individual Circuit Module can also be disabled using the A/B Switch Jumper. In addition, the Master A/B Gang Switch can also be completely disabled via the System Parameters Menu.

9.5. Logging Out of Command Mode

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

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

10. Telnet & SSH Functions

10.1. SSH Encryption

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

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

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

The /K command uses the following format:

`/K <k>` [Enter]

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

1. SSH1
2. SSH2 RSA
3. SSH2 DSA

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

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

10.2. Creating an Outbound Telnet Connection

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

Notes:

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

To create an outbound Telnet connection, access the Text Interface via the Control Module's RS232 Serial Port, using an account that permits Telnet Access and Outbound Access and then invoke the /TELNET command using the following format:

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

Where:

`ip` Is the target IP address.

`port` Is an optional argument which can be included to indicate the target port at the IP address.

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

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

`/TELNET 255.255.255.255 2000 raw` [Enter]

10.3. Creating an Outbound SSH Connection

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

Notes:

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

To create an outbound SSH connection, access the Text Interface via the Control Module's RS232 Serial Port using an account that permits SSH Access and Outbound Access and then invoke the /SSH command using the following format:

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

Where:

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

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

`/SSH 255.255.255.255 -l employee` [Enter]

11. Syslog Messages

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

11.1. Configuration

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

To configure the Syslog function, please proceed as follows:

1. **Access command mode:** Note that the following configuration menus are only available to accounts that permit Administrator level commands.
2. **System Parameters Menu:** Access the System Parameters Menu, then set the following parameters:
   a) **Set Clock and Calendar:** Set the Real Time Clock and Calendar and/or configure and enable the NTP server feature.
3. **Network Parameters Menu:** Access the Network Parameters Menu, then set the following parameters:
   a) **Syslog IP Addresses:** Determine the IP addresses for the devices that will run the primary and secondary Syslog Daemons, then use the Network Port Configuration menu to define the IP Addresses for the Syslog Daemons.

Notes:

- *The Network Parameters Menu allows the definition of IP addresses for both a primary Syslog Daemon and an optional secondary Syslog Daemon.*
- *The Ping Test function can be used to ping the user-selected Syslog IP Addresses to verify that valid IP addresses have been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*

4. **Syslog Daemon:** In order to capture messages sent by the AFS, a computer must be running a Syslog Daemon (set to UDP Port 514) at the IP address specified in Step 3 above.

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

12. SNMP Traps

The SNMP Trap function allows the AFS to send Alarm Notification messages to two different SNMP managers, each time one of the Alarms is triggered.

Note:

- *The SNMP feature cannot be configured via the SNMP Manager.*
- *SNMP reading ability is limited to the System Group.*
- *The SNMP feature includes the ability to be polled by an SNMP Manager.*
- *Once SNMP Trap Parameters have been defined, SNMP Traps will be sent each time an Alarm is triggered and/or when a Buffer Mode serial port reaches the user-defined Buffer Threshold value.*

12.1. Configuration:

To configure the SNMP Trap function, proceed as follows:

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

2. **SNMP Trap Parameters:** Access the SNMP Trap Parameters Menu and then set the following parameters:

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

Notes:

- *To enable the SNMP Trap feature, you must define at least one SNMP Manager. SNMP Traps are automatically enabled when at least one SNMP Manager has been defined.*
- *The SNMP Trap submenu in the Text Interface includes a Ping Test function that can be used to ping the user-selected SNMP Managers to verify that a valid IP address has been entered. In order for the Ping Test feature to function, your network and/or firewall must be configured to allow ping commands.*
- *Addresses for SNMP Managers can be defined in either IPv4 or IPv6 format, as described in Section 5.9.7.*

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

Once SNMP Trap Parameters have been defined, the AFS will send an SNMP Trap each time an alarm is triggered.

13. Operation via SNMP

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

13.1. AFS SNMP Agent

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

13.2. SNMPv3 Authentication and Encryption

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

For SNMPv3, the AFS supports two forms of Authentication/Privacy: Auth/noPriv which requires a username/password, but does not encrypt data going over the internet and Auth/Priv which requires a username/password AND encrypts the data going over the internet using DES or AES (in the case of the AFS, the default encryption format for SNMPv3 is DES.) For the Password protocol, the SRM supports either MD5 or SHA1.

13.3. Configuration via SNMP

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

- **`userTable::userName`** – 32 character username
- **`userTable::userPasswd`** – 16 character password
- **`userTable::userAccessLevel`** – Account access level.
  - `0` ViewOnly Access
  - `1` User Access
  - `2` Superuser Access
  - `3` Administrator Access

- **`userTable::userCircuitAccess`** – A string of up to 16 characters, with one character for each of the 16 possible Circuit Modules on the AFS unit. A '`0`' indicates that the account **does not** have access to the circuit, and a '`1`' indicates that the user *does* have access to the circuit.

  Note: *The number of circuits specified in the userCircuitAccess string must not exceed the number of Circuit Modules available on your AFS unit. If the userCircuitAccess string specifies more circuits than are available on the unit, an error message will be generated.*

- **`userTable::userGroupAccess`** – A string of 54 characters, with one character for each of the 54 possible Circuit Groups in the system. A '`0`' indicates that the account **does not** have access to the Circuit Group, and a '`1`' indicates that the user *does* have access to the Circuit Group.
- **`userTable::userSerialAccess`** – Access to the serial interface
  - `0` No access
  - `1` Access
- **`userTable::userTelnetSshAccess`** – Access to the Telnet/SSH interface
  - `0` No access
  - `1` Access
- **`userTable::userOutboundTelSshAccess`** – Access to Outbound Telnet/SSH
  - `0` No access
  - `1` Access
- **`userTable::userWebAccess`** – Access to the Web interface
  - `0` No access
  - `1` Access
- **`userTable::userCallbackNum`** – 32 character callback number for account
- **`userTable::userSubmit`** – Set to `1` to submit changes.

13.3.1. Viewing Users

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

13.3.2. Adding Users

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

13.3.3. Modifying Users

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

13.3.4. Deleting Users

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

13.4. Circuit Control via SNMP

13.4.1. Controlling Circuits

A/B Switching and Default commands can be issued for circuits via SNMP. Circuits are arranged in a table of N rows, where N is the number of circuits in the system. Circuit parameters are described below.

- **`circuitTable::circuitID`** – String indicating the circuit's ID
- **`circuitTable::circuitName`** - String indicating the circuit's user-defined name.
- **`circuitTable::circuitStatus`** – Current state of the circuit
  - `0` Switch Position B
  - `1` Switch Position A
- **`circuitTable::circuitAction`** – Action to be taken on circuit
  - `1` Mark to Switch to A (does not execute)
  - `2` Mark to Switch to B (does not execute)
  - `3` N/A
  - `4` Mark to DEFAULT Circuit (does not execute)
  - `5` Mark to Switch to A and execute circuit actions
  - `6` Mark to Switch to B and execute circuit actions
  - `7` N/A
  - `8` Mark to DEFAULT Circuit and execute circuit actions

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

13.4.2. Controlling Circuit Groups

A/B Switching and Default commands can be issued for circuit groups via SNMP. Circuit Groups are arranged in a table of 54 rows, one row for each circuit group in the system. Circuit Group parameters are described below.

- **`circuitGroupTable::circuitGroupName`** – String indicating the circuit groups name
- **`circuitGroupTable::circuitGroupAction`** – Action to be taken on circuit group
  - `1` Mark to Switch to A (does not execute)
  - `2` Mark to Switch to B (does not execute)
  - `3` N/A
  - `4` Mark to DEFAULT Circuit (does not execute)
  - `5` Mark to Switch to A and execute circuit group actions
  - `6` Mark to Switch to B and execute circuit group actions
  - `7` N/A
  - `8` Mark to DEFAULT Circuit and execute circuit group actions

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

13.5. Viewing AFS Status via SNMP

Status of various components of the AFS can be retrieved via SNMP. Circuit Status, and Environmental Status are currently supported.

13.5.1. System Status - Ethernet Port Mac Addresses

The Mac Address for the Ethernet Port can be displayed using the command below:

- **`environmentUnitTable::environmentMacEth0`** The Mac Address for Ethernet Port 0.

13.5.2. Circuit Status

The status of each circuit in the system can be retrieved using the command below.

- **`circuitTable::circuitStatus`** – The status of the circuit.
  - `0` Switch Position B
  - `1` Switch Position A
  - `155` No Circuit Installed in this Slot
- **`circuitTable::circuitReason`** – Returns a numeric code, which describes the reason for the last successful A/B switching operation as follows:
  - `0` Power Up
  - `1` User
  - `2` PNA
  - `3` External Alarm
  - `4` Circuit Switch
  - `5` Control Switch
  - `6` Demo

13.5.3. Unit Environment Status

The temperature status and Control Module Jumper status can be retrieved. The environmentUnitTable contains one row.

- **`environmentUnitTable::environmentUnitTemperature`** – The temperature of the AFS unit.
- **`environmentUnitTable::environmentUnitName`** – Returns the specific model number for the AFS unit.
- **`environmentUnitTable::environmentUnitMonitorAlarm`** – Returns the current state of the Monitor Input Signal.
  - `0` Monitor Input Signal is Low.
  - `1` Monitor Input Signal is High

13.5.4. Alarm Status

The status of the AFS unit's alarm functions can be retrieved and displayed using the following commands:

Notes:

- *When an alarm status command returns a zero (0), this indicates that the alarm is inactive.*
- *When an alarm status command returns a one (1), this indicates that the alarm is active (triggered.)*

- **`alarmTables::alarmOverTemperatureInitial`** - Displays the status of the Over Temperature (Initial) Alarm.
- **`alarmTables::alarmOverTemperatureCritical`** - Displays the status of the Over Temperature (Critical) Alarm.
- **`alarmTables::alarmPingNoAnswer`** - Displays the status of the Ping-No-Answer Alarm.
- **`alarmTables::alarmInvalidAccessLockout`** - Displays the status of the Serial Port Invalid Access Lockout Alarm.
- **`alarmTables::alarmPowerCycle`** - Displays the status of the Power Cycle Alarm.
- **`alarmTables::alarmNoDialtone`** - Displays the status of the No Dialtone Alarm.

13.6. Sending Traps via SNMP

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

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

The AFS can send an SNMP trap to notify you when one of the AFS alarms have been triggered. In all cases except the Power Cycle Alarm, there will be one trap sent when the alarm is triggered, and a second trap sent when the alarm is cleared.

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

14 Setting Up SSL Encryption

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

> **Note:** *SSL parameters cannot be defined via the Web Browser Interface. In order to set up SSL encryption, you must contact the AFS via the Text Interface.*

There are two different types of https security certificates: "Self Signed" certificates and "Signed" certificates.

Self Signed certificates can be created by the AFS, without the need to go to an outside service, and there is no need to set up your domain name server to recognize the AFS. The principal disadvantage of Self Signed certificates, is that when you access the AFS command mode via the Web Browser Interface, the browser will display a message which warns that the connection might be unsafe. Note however, that even though this message is displayed, communication will still be encrypted, and the message is merely a warning that the AFS is not recognized and that you may not be connecting to the site that you intended.

Signed certificates must be created via an outside security service (e.g., VeriSign®, Thawte™, etc.) and then uploaded to the AFS unit to verify the user's identity. In order to use Signed certificates, you must contact an appropriate security service and set up your domain name server to recognize the name that you will assign to the AFS unit (e.g., service.wti.com.) Once a signed certificate has been created and uploaded to the AFS, you will then be able to access command mode without seeing the warning message that is normally displayed for Self Signed certificate access.

```
WEB ACCESS: [eth0] IPv4

HTTP:
1.  Enable: On
2.  Port:   80

HTTPS:
3.  Enable: Off
4.  Port:   443

SSL Certificates:
5.  Common Name:
6.  State or Province:
7.  Locality:
8.  Country:
9.  Email Address:
10. Organization Name:
11. Organizational Unit:              15. Export Server Private Key:
12. Create CSR:                       16. Import Server Private Key:
13. View CSR:                         17. Harden Web Security: On
14. Import CRT:                       18. TLS Mode: TLSv1

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

Figure 14.1: Web Access Parameters (Text Interface Only)

14.1. Creating a Self Signed Certificate

To create a Self Signed certificate, access the Text interface via Telnet or SSH, using a password that permits access to Administrator level commands and then proceed as follows:

1. Type **/N** and press **[Enter]** to display the Network Parameters menu.
2. At the Network Parameters menu, key in the number for the Web Access option and press **[Enter]** to display the Web Access menu (Figure 14.1.) Next, key in the number for the HTTPS Enable option and press **[Enter].** Then follow the instructions in the resulting submenu to enable HTTPS access.
3. Next, use the Web Access menu to define the following parameters.

   Note: *When configuring the AFS, make certain to define all of the following parameters. Although most SSL applications require only the Common Name, in the case of the AFS all of the following parameters are mandatory.*

   - **5. Common Name:** A domain name, that will be used to identify the AFS unit. If you will use a Self Signed certificate, then this name can be any name that you choose, and there is no need to set up your domain name server to recognize this name. However, if you will use a Signed certificate, then your domain name server must be set up to recognize this name (e.g., service.yourcompanyname.com.)
   - **6. State or Province:** The name of the state or province where the AFS unit will be located (e.g., California.)
   - **7. Locality:** The city or town where the AFS unit will be located (e.g., Irvine.)
   - **8. Country:** The two character country code for the nation where the AFS will be located (e.g., US.)
   - **9. Email Address:** An email address, that can be used to contact the person responsible for the AFS (e.g., jsmith@yourcompany.com.)
   - **10. Organizational Name:** The name of your company or organization (e.g., Yourcompanyname, Inc.)
   - **11. Organizational Unit:** The name of your department or division; if necessary, any random text can be entered in this field (e.g., tech support.)

4. After you have defined parameters 5 through 11, type `12` and press **[Enter]** (Create CSR) to create a Certificate Signing Request. By default, this will overwrite any existing certificate, and create a new Self Signed certificate.

   a) The AFS will prompt you to create a password. Key in the desired password (up to 16 characters) and then press **[Enter]**. When the AFS prompts you to verify the password, key it again and then press **[Enter]** once. After a brief pause, the AFS will return to the Web Access Menu, indicating that the CSR has been successfully created.

   b) When the Web Access Menu is re-displayed, press **[Esc]** several times until you exit from the Network Parameters menu and the "Saving Configuration" message is displayed.

5. After the new configuration has been saved, test the Self Signed certificate by accessing the AFS via the Web Interface, using an HTTPS connection.

   a) Before the connection is established, the AFS should display the warning message described previously. This indicates that the Self Signed certificate has been successfully created and saved.

   b) Click on the "Yes" button to proceed. The AFS will prompt you to enter a user name and password. After keying in your password, the main menu should be displayed, indicating that you have successfully accessed command mode.

14.2. Creating a Signed Certificate

To create a Signed certificate, and eliminate the warning message, first set up your domain name server to recognize the Common Name (item 5) that you will assign to the unit. Next, complete steps one through five as described in Section 14.1 and then proceed as follows:

1. **Capture the Newly Created Certificate:** Type `13` and press **[Enter]** (View CSR). The AFS will prompt you to configure your communications (Telnet) program to receive the certificate. Set up your communications program to receive a binary file, and then press **[Enter]** to capture the file and save it. This is the Code Signing Request that you will send to the outside security service (e.g., VeriSign, Thawte, etc.) in order to have them sign and activate the certificate.

2. **Obtain the Signed Certificate:** Send the captured certificate to the outside security service. Refer to the security service's web page for further instructions.

3. **Upload the Signed Certificate to the AFS:** After the "signed" certificate is returned from the security service, return to the Web Access menu.

   a) Access the AFS command mode via the Text Interface using an account that permits Administrator level commands as described previously, then type **/N** and press **[Enter]** to display the Network Parameters menu, and then type **23** and press **[Enter]** to display the Web Access menu.

   b) From the Web Access menu, type **14** and press **[Enter]** (Import CRT) to begin the upload process. At the CRT Server Key submenu, type **1** and press **[Enter]** to choose "Upload Server Key."

   c) Use your communications program to send the binary format Signed Certificate to the AFS unit. When the upload is complete, press **[Escape]** to exit from the CRT Server Key submenu.

   d) After you exit from the CRT Server Key submenu, press [Escape] several times until you have exited from the Network Parameters menu and the "Saving Configuration" message is displayed.

4. After the configuration has been saved, test the signed certificate by accessing the AFS via the Web Browser Interface, using an HTTPS connection. For example, if the common name has been defined as "service.wti.com", then you would enter "**https://service.wti.com**" in your web browser's address field. If the Signed Certificate has been properly created and uploaded, the warning message should no longer be displayed.

14.3. Downloading the Server Private Key

When configuring the AFS's SSL encryption feature (or setting up other security/ authentication features), it is recommended to download and save the Server Private Key. To download the Server Private Key, access the Text interface via Telnet or SSH, using a password that permits access to Administrator level commands and then proceed as follows:

1. Type **/N** and press **[Enter]** to display the Network Parameters menu.

2. At the Network Parameters menu, type **23** and press **[Enter]** to display the Web Access menu (Figure 14.1.)

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

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

14.4. TLS Mode

The TLS Mode parameter in the Web Access menu (Text Interface Only) allows the TLS Mode to be set to either TLSv1 or TLSv1.1. Although TSLv1.1 provides better security, the default settings of most browsers do not support TLSv1.1. The default setting for this parameter is TLSv1.

15. Saving and Restoring Configuration Parameters

Once the AFS is properly configured, parameters can be downloaded and saved as an ASCII text file. Later, if the configuration is accidentally altered, the saved parameters can be uploaded to automatically reconfigure the unit without the need to manually assign each parameter.

Saved parameters can also be uploaded to other identical AFS units, allowing rapid set-up when several identical units will be configured with the same parameters.

The "Save Parameters" procedure can be performed from any terminal emulation program (e.g. HyperTerminal™, TeraTerm©, etc.), that allows downloading of ASCII files.

> **Note:** *Configuration parameters can be downloaded and saved via either the Web Browser Interface or Text Interface. Saved configuration parameters can only be uploaded to the AFS unit via the Text Interface.*

15.1. Sending Parameters to a File

15.1.1. Downloading & Saving Parameters via Text Interface

1. Start your terminal emulation program and access the Text Interface command mode using an account that permits Administrator level commands.
2. When the command prompt appears, type `/u` and press **[Enter]**. The AFS will prompt you to configure your terminal emulation program to receive an ASCII download.
   a) Set your terminal emulation program to receive an ASCII download, and the specify a name for a file that will receive the saved parameters (e.g. AFS.PAR).
   b) Disable the Line Wrap function for your terminal emulation program. This will prevent command lines from being broken in two during transmission.
3. When the terminal emulation program is ready to receive the file, return to the AFS's Save Parameter File menu, and press **[Enter]** to proceed. AFS parameters will be saved on your hard drive in the file specified in Step 2 above.
4. The AFS will send a series of XML command lines which specify currently selected parameters. When the download is complete, press **[Enter]** to return to the command prompt.

15.1.2. Downloading & Saving Parameters via Web Browser Interface

The Web Browser Interface also includes a download function that can be used to save AFS parameters to an XML format file on your PC or laptop. To save parameters via the Web Browser Interface, proceed as follows:

Notes:

- *Although AFS parameters can be saved to a file via either the Text Interface or Web Browser Interface, saved parameters can only be restored via the Text Interface. The Restore Parameters function is not available via the Web Browser Interface.*
- *This procedure may differ slightly, depending on the operating system and browser used. In some cases, your system may perform a security scan before proceding with the download.*

1. Access the Web Browser Interface command mode using an account that permits Administrator level commands.

1. When the Web Browser Interface appears, click on the "Download Unit Configuration" button on the left hand side of the screen.

2. After a brief pause, your browser may display a prompt asking if you want to open or save the downloaded file. At this point, you can either select the "Save" option to save the parameters file to the download folder on your PC, or select "Save As" to pick a different location and/or filename for the saved parameters file.

15.2. Restoring Saved Parameters

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

Note: *The Restore Parameters feature is only available via the Text Interface.*

1. Start your terminal emulation program and access the AFS's Text Interface command mode using an account that permits Administrator level commands.

2. Configure your terminal emulation program to upload an ASCII text file.

3. Upload the ASCII text file with the saved AFS parameters. If necessary, key in the file name and directory path.

4. Your terminal emulation program will send the ASCII text file to the AFS. When the terminal program is finished with the upload, make certain to terminate the Upload mode.

   Note: *If the AFS detects an error in the file, it will respond with the "Invalid Parameter" message. If an error message is received, carefully check the contents of the parameters file, correct the problem, and then repeat the Upload procedure.*

5. If the parameter upload is successful, the AFS will send a confirmation message, and then return to the command prompt. Type `/s` and press **[Enter]**, the Status Screen will be displayed. Check the Status Screen to make certain the unit has been configured with the saved parameters.

15.3. Restoring Previously Saved Parameters

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

Notes:

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

To restore the previously saved configuration, proceed as follows:

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

16. Upgrading AFS Firmware

When new, improved versions of the AFS firmware become available, either the Firmware Upgrade Utility (recommended) or the "Upgrade Firmware" function (Text Interface only) can be used to update the unit. The following Section describes the procedure for updating the AFS unit using the Firmware Upgrade Utility or the Upgrade Firmware function.

16.1. WMU Enterprise Management Software (Recommended)

The preferred method for updating AFS units is via the WMU Enterprise Management Software that is included with the unit. The WMU software allows you to manage firmware updates for multiple WTI units from a single interface. For a description of the process for managing firmware updates via the WMU, please refer to the WMU user's guide, which can be downloaded from the WTI User's Guide Archive at:

http://www.wti.com/t-product-manuals.aspx

Note that in order to use the WMU software, the firmware version for the AFS must be at least v2.30 or higher. When upgrading older AFS units that feature pre v2.30 firmware, it is recommended to use the WTI Firmware Upgrade Utility. A zip file that contains the installation files and other documentation for the WTI Firmware Upgrade Utility can be downloaded from WTI's FTP server, located at:

ftp://wtiftp.wti.com/pub/TechSupport/Firmware/Upgrade_Utility/

Please refer to the documentation included in the zip file for further instructions.

16.2. The Upgrade Firmware Function (Alternate Method)

The Upgrade Firmware function provides an alternative method for updating the AFS firmware. Updates can be uploaded via FTP or SFTP protocols.

Notes:

- *The FTP/SFTP servers can only be started via the Text Interface.*
- *All other ports will remain active during the firmware upgrade procedure.*
- *If the upgrade includes new parameters or features not included in the previous firmware version, these new parameters will be set to their default values.*
- *The upgrade procedure will require approximately 15 minutes.*

1. Obtain the update file. Firmware modifications can either be mailed to the customer, or downloaded from WTI. Place the upgrade CDR in your disk drive or copy the file to your hard drive.
2. Access Text Interface command mode via Serial Port, Telnet or SSH client session, using a username/password and port that permit Administrator level commands.

3. When the command prompt appears, type **/UF** and then press **[Enter]**. The AFS will display a screen which offers the following options:

   a) **Start FTP/SFTP Servers Only (Do NOT default parameters):** To proceed with the upgrade, while retaining user-defined parameters, type **1** and press **[Enter]**. All existing parameter settings will be restored when the upgrade is complete.

   b) **Start FTP/SFTP Servers & Default (Keep IP parameters & SSH Keys):** To proceed with the upgrade and default al user-defined parameters except for the IP Parameters and SSH Keys, type **2** and press **[Enter]**. When the upgrade is complete, all parameter settings except the IP Parameters and SSH Keys, will be reset to factory default values.

   c) **Start FTP/SFTP Servers & Default (Default ALL parameters):** To proceed with the upgrade, and reset parameters to default settings, type **3** and press **[Enter]**. When the upgrade is complete, all parameters will be set to default values.

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

   Note that after any of the above options is selected, the AFS will start the receiving servers and wait for an FTP/SFTP client to make a connection and upload a valid firmware binary image.

4. To proceed with the upgrade, select either option 1 or option 2. The AFS will display a message that indicates that the unit is waiting for data. Leave the current Telnet/SSH client session connected at this time.

5. Open your FTP/SFTP application and (if you have not already done so,) login to the AFS unit, using a username and password that permit access to Administrator Level commands.

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

7. After the file transfer is complete, the AFS will install the upgrade file and then reboot itself and break all port connections. Note that it will take approximately 10 minutes to complete the installation process. The unit will remain accessible until it reboots.

   a) Some FTP/SFTP applications may not automatically close when the file transfer is complete. If this is the case, you may close your FTP/SFTP client manually after it indicates that the file has been successfully transferred.

   b) When the upgrade process is complete, the AFS will send a message to all currently connected network sessions, indicating that the AFS is going down for a reboot.

   Note: *Do not power down the AFS unit while it is in the process of installing the upgrade file. This can damage the unit's operating system.*

8. If you have accessed the AFS via the Network Port, in order to start the FTP/SFTP servers, the AFS will break the network connection when the system is reinitialized.

   - If you initially selected "Start FTP/SFTP Servers and Save Parameters", you may then reestablish a connection with the AFS using your former IP address.
   - If you initially selected "Start FTP/SFTP Servers and Default Parameters", you must then login using the AFS's default IP address (Default = 192.168.168.168) or access command mode via Serial Port 1 or via Modem.

When firmware upgrades are available, WTI will provide the necessary files. At that time, an updated Users Guide or addendum will also be available.

17. Command Reference Guide

17.1. Command Conventions

Most commands described in this section conform to the following conventions:

- **Text Interface:** Commands discussed in this section, can only be invoked via the Text Interface. These commands *cannot* be invoked via the Web Browser Interface.
- **Slash Character:** Most AFS Text Interface commands begin with the Slash Character (**/**).
- **Apply Command to All Circuits:** When an asterisk is entered as the argument of the **/T** (Toggle), **/TA** (Toggle to A) or **/TB** commands (Toggle to B) the command will be applied to all circuits. For example, to switch all circuits to "A", type **/TA * [Enter]**.
- **Circuit Name Wild Card:** It is not always necessary to enter the entire circuit name. Circuit names can be abbreviated in command lines by entering the first character(s) of the name followed by an asterisk (*****). For example, a circuit named "SERVER" could be specified as "**S***". Note however, that this command would also be applied to any other circuit name that begins with an "S".
- **Command Queues:** If a toggle command is directed to a circuit that is already being switched by a previous command, then the new command will be placed into a queue until the circuit is ready to receive additional commands.
- **Suppress Command Confirmation Prompt:** When the commands are invoked, the "**,Y**" option can be included to override the Command Confirmation ("Sure?") prompt. For example, to switch Circuit 4 to the "B" position without displaying the Sure prompt, type **/TB 4,Y [Enter]**.
- **Enter Key:** Most commands are invoked by pressing **[Enter]**.

17.2. Command Summary

Function	Command Syntax	Command Access Level			
		Admin.	SuperUser	User	ViewOnly
Display					
Circuit Status	**/S [Enter]**	X❶	X❶	X❶	X❶
Serial Port Diagnostics	**/SD [Enter]**	X❶	X❶	X❶	X❶
Serial Port Parameters (Who)	**/W [Enter]**	X	X	X	X
Circuit Group Status	**/SG [Enter]**	X❷	X❷	X❷	X❷
Network Status	**/SN [Enter]**	X	X		
Network Config. Summary	**/RN [Enter]**	X	X	X	X
IP Alias Status	**/SA [Enter]**	X	X		
Alarm Status	**/AS [Enter]**	X			
Help Menu	**/H [Enter]**	X❸	X❸	X❸	X❸
Log Functions	**/L [Enter]**	X	X		
Site ID / Unit Information	**/J[*] [Enter]**	X	X	X	X
Control					
Exit Command Mode	**/X [Enter]**	X	X	X	X
Connect - Local <Remote>	**/C 1 [Enter]**	X	X	X❹	
Switch Circuit *c* to Position A	**/TA <c>[,Y] [Enter]❺**	X	X	X	
Switch Circuit *c* to Position B	**/TB <c>[,Y] [Enter]❺**	X	X	X	
Switch Circuit *c* to Position *p*	**/T <c>,<p>[,Y] [Enter]❺**	X	X	X	
Default All Circuits	**/DC[,Y] [Enter]❺**	X	X	X❻	
Send Parameter File	**/U [Enter]**	X			
Send SSH Keys	**/K <n> [Enter]**	X			
Unlock Invalid Access	**/UL [Enter]**	X			
Outbound Telnet	**/TELNET <ip> [port] [raw] [Enter]**	X❼	X❼	X❼	
Outbound SSH	**/SSH <ip> -l <username> [Enter]**	X❼	X❼	X❼	
Configuration					
System Parameters	**/F [Enter]**	X	❽		
Serial Port Parameters	**/P [Enter]**	X	❽		
Circuit Parameters	**/PC [Enter]**	X	❽		
Circuit Group Parameters	**/G [Enter]**	X	❽		
Network Configuration (IPv4)	**/N [Enter]**	X	❽		
Network Configuration (IPv6)	**/N6 [Enter]**	X	❽		
Ping-No-Answer Function	**/PNA [Enter]**	X	❽	❾	❾
Alarm Configuration	**/AC [Enter]**	X	❽		
Reboot System	**/I [Enter]**	X	X❿		
Upgrade Firmware	**/UF [Enter]**	X			
Test Network Configuration	**/TEST [Enter]**	X	X		

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

❷ In Administrator and SuperUser modes, all Circuit Groups are displayed. In User and ViewOnly modes, the Circuit Group Status Screen will only include the Circuit Groups allowed by the account.

❸ In Administrator Mode, Help Menus will list all commands. In SuperUser, User and ViewOnly modes, Help Menus will only list the commands allowed by the access level.

❹ User Mode accounts will be allowed to connect to the Serial Port only if Serial Access is enabled for the account.

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

❻ The "Default All Circuits" command will only be applied to the Circuits that are allowed by the account.

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

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

❾ User Mode and ViewOnly accounts are allowed to view existing Ping-No-Answer settings, but are not allowed to add or modify settings.

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

17.3. Command Set

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

17.3.1. Display Commands

/S Display Circuit Status Screen

Displays the Circuit Status Screen, which lists the current status of the AFS Circuit Modules.

> **Note:** *In Administrator Mode and SuperUser Mode, all AFS circuits are displayed. In User Mode and ViewOnly Mode, the Circuit Status Screen will only include the circuits allowed by your account.*

Availability: Administrator, SuperUser, User, ViewOnly
Format: `/S` **[Enter]**

/SD Display Port Diagnostics

Provides detailed information regarding the status of the serial Setup Port.

Availability: Administrator, SuperUser, User, ViewOnly
Format: `/SD` **[Enter]**
Response: Displays Port Diagnostics Screen.

/W Display Port Parameters (Who)

Displays configuration information for the serial Setup Port, but does not allow parameters to be changed.

Availability: Administrator, SuperUser, User, ViewOnly
Format: `/W` **[Enter]**

/SG Display Circuit Group Status Screen

Displays the Circuit Group Status Screen, which lists the available Circuit Groups, the Circuits included in each Circuit Group, the current A/B state and other factors.

> **Note:** *In Administrator and SuperUser Mode all user defined Circuit Groups are displayed. In User Mode and ViewOnly Mode, the Circuit Group Status Screen will only include the Circuit Groups allowed by your account.*

Availability: Administrator, SuperUser, User, ViewOnly
Format: `/S` **[Enter]**

/SN Display Network Status

Displays the Network Status Screen, which lists current network connections to the AFS Network Port.

Availability: Administrator, SuperUser

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

/RN Network Configuration Summary

Displays a screen that lists currently selected communication settings, LDAP status, RADIUS status, Email Messaging status, NTP status and PPP status.

Availability: Administrator, SuperUser, User ViewOnly

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

/SA IP Alias Status

Displays the Alias Status Screen, which lists currently selected port name, alias IP address and Direct Connect status for the AFS serial port. For more information, please refer to Section 8.6.

> **Note:** *When the Alias Status Screen is displayed by an Administrator or SuperUser level account, the screen will display the status of all ports. If the Alias Status Screen is displayed by a User or ViewOnly level account, the screen will only display the status of the ports specifically allowed by the account.*

Availability: Administrator, SuperUser, User, ViewOnly

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

/H Help

Displays a Help Screen, which lists all available Text Interface commands along with a brief description of each command.

> **Note:** *In the Administrator Mode, the Help Screen will list the entire AFS command set. In SuperUser Mode, User Mode and ViewOnly Mode, the Help Screen will only list the commands that are allowed for that Access Level.*

Availability: Administrator, SuperUser, User, ViewOnly

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

/L Log Functions

Provides access to a menu which allows you to display, download or erase the Audit Log, Alarm Log and Temperature Log.

Availability: Administrator, SuperUser

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

/AS Alarm Status Screen

Lists all available user-defined alarms and indicates whether or not each alarm has been triggered. The resulting screen will display "Yes" (or 1) for alarms that have been triggered or "No" (or 0) for alarms that have not been triggered. If desired, the /AS command line can also include an optional alarm argument that will cause the unit to display the status of one individual alarm as shown in the table below:

Alarm Name	Alarm Argument
Over Temperature (Initial)	OTI
Over Temperature (Critical)	OTC
Ping No Answer	PNA
Serial Port Invalid Access Lockout	LO
Power Cycle (Cold Boot)	CB
Alarm Input	AI
No Dialtone	ND
Emergency Shutoff	ES

Availability: Administrator

Format: **`/AS [alarm]`** **[Enter]**

Where **`alarm`** is an optional argument, which can be used to display the status of an individual alarm as shown in the table above.

/J Display Site ID / Unit Information

Displays the user-defined Site I.D. message. If the optional asterisk (*) argument is included in the command line, the command can also display the model number, serial number, software version and other information for the AFS unit.

Availability: Administrator, SuperUser, User, ViewOnly

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

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

17.3.2. Control Commands

/X Exit Command Mode

Exits command mode. When issued at the Network Port, also ends the Telnet session.

> **Note:** *If the /X command is invoked from within a configuration menu, recently defined parameters may not be saved. In order to make certain that parameters are saved, always press the **[Esc]** key to exit from all configuration menus and then wait until "Saving Configuration" message has been displayed and the cursor has returned to the command prompt before issuing the /X command.*

Availability: Administrator, SuperUser, User, ViewOnly

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

/C Connect

This command can be used to establish a bidirectional connection between the Serial Setup Port and the Network Port.

Notes:

- *User level accounts can only connect to the Serial Port if access to the port has been specifically enabled for the account.*
- *To terminate the connection, press **[Ctrl]**+**[X]** (**^x**) and then press **[Enter]**.*

Availability: Administrator, SuperUser, User

Format: **/C 1 [Enter]**

/TA Toggle to "A" Position

Toggles a Circuit or a Circuit Group to the "A" position.

Note: *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all AFS Circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the Circuits and/or Circuit Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **/TA <c>[,Y] [Enter]**

Where:

c	The number or name of the Circuit(s) or Circuit Group(s) that you wish to switch to the "A" position. To apply the command to several Circuits, enter a plus sign (+) between each Circuit number. To apply the command to a range of Circuits, enter the numbers for the first and last Circuits in the range, separated by a colon character (:). To apply the command to all Circuits allowed by your account, enter an asterisk character (*).
,Y	(Optional) Suppresses the command confirmation prompt.

Example:

Assume that your account allows access to Circuit 2 and Circuit 3. To switch Circuits 2 and 3 to the "A" position without displaying the optional command confirmation prompt, invoke the following command line:

/TA 2+3,Y [Enter]

/TB Toggle to "B" Position

Toggles a Circuit or a Circuit Group to the "B" position.

> **Note:** *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all AFS Circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the Circuits and/or Circuit Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **`/TB <c>[,Y]`** **[Enter]**

Where:

- **`c`** The number or name of the Circuit(s) or Circuit Group(s) that you wish to switch to the "B" position. To apply the command to several Circuits, enter a plus sign (+) between each Circuit number. To apply the command to a range of Circuits, enter the numbers for the first and last Circuits in the range, separated by a colon character (:). To apply the command to all Circuits allowed by your account, enter an asterisk (*).
- **`,Y`** (Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Circuit 2 and Circuit 3. To switch Circuits 2 and 3 to the "B" position without displaying the optional command confirmation prompt, invoke the following command line:

`/TB 2+3,Y` **[Enter]**

/T Toggle Command

This command can be used to toggle any Circuit or Circuit Group to either the "A" position or the "B: position.

> **Note:** *When this command is invoked in Administrator Mode or SuperUser Mode, it can be applied to all AFS Circuits and Circuit Groups. When this command is invoked in User Mode, it can only be applied to the Circuits and/or Circuit Groups that have been enabled for your account.*

Availability: Administrator, SuperUser, User

Format: **`/T <c>,<p>[,Y]`** **[Enter]**

Where:

- **`c`** The number or name of the Circuit(s) or Circuit Group(s) that you wish to switch. To apply the command to several Circuits, enter a plus sign (+) between each Circuit number. To apply the command to all Circuits allowed by your account, enter an asterisk character (*).
- **`p`** The desired switch position. Enter an "A" to switch specified circuits to the "A" position or a "B" to switch circuits to the "B" position.
- **`,Y`** (Optional) Suppresses the command confirmation prompt.

Example:
Assume that your account allows access to Circuit 2 and Circuit 3. To switch Circuits 2 and 3 to the "A" position without displaying the optional command confirmation prompt, invoke the following command line:

`/T 2+3,A,Y` **[Enter]**

/DC Set All Circuits to Default States

Sets all Circuit Modules to their user-defined default state.

> **Note:** *When this command is invoked in Administrator Mode and SuperUser Mode, it will be applied to all AFS circuits. When invoked in User Mode, the command will only be applied to the Circuits that are allowed by your account.*

Availability: Administrator, SuperUser, User

Format: **`/DC[,Y]` [Enter]**

Where ,Y is an optional command argument, which can be included to suppress the command confirmation prompt.

/U Send Parameters to File

Sends all AFS configuration parameters to an ASCII text file. This allows you to back up the configuration of your AFS unit.

Availability: Administrator

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

/K Send SSH Key

Instructs the AFS to provide you with a public SSH key for validation purposes. This public key can then be provided to your SSH client, in order to prevent the SSH client from warning you that the user is not recognized when you attempt to create an SSH connection.

Availability: Administrator

Format: **`/K k` [Enter]**

Where k is a required argument, which indicates the key type. The k argument provides the following options: 1 (SSH1), 2 (SSH2 RSA), 3 (SSH2 DSA.)

/UL Unlock Port (Invalid Access Lockout)

Manually cancels the AFS's Invalid Access Lockout feature. Normally, when a series of failed login attempts are detected, the Invalid Access Lockout feature can shut down the effected port for a user specified time period in order to prevent further access attempts. When the /UL command is invoked, the AFS will immediately unlock all ports that are currently in the locked state.

Availability: Administrator

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

/TELNET Outbound Telnet

Creates an outbound Telnet connection as described in Section 10.2.

Notes:

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

Availability: Administrator, SuperUser, User

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

Where:

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

/SSH Outbound SSH

Creates an outbound SSH connection as described in Section 10.3.

Notes:

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

Availability: Administrator, SuperUser, User

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

Where:

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

17.3.3. Configuration Commands

/F Set System Parameters

Displays a menu which is used to define the Site ID message, serial number and other items, as well as create user accounts, set the system clock, and configure and enable the Invalid Access Lockout feature. All functions provided by the /F command are also available via the Web Browser Interface.

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

/P Set Serial Port Parameters

Displays a menu that is used to select options and parameters for the AFS Control Module's serial port. All functions provided by the /P command are also available via the Web Browser Interface.

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

/PC Set Circuit Parameters

Displays a menu that is used to select options and parameters for the AFS's Circuit Modules. All functions provided by the /PC command are also available via the Web Browser Interface.

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

/G Circuit Group Parameters

Displays a menu that is used to View, Add, Modify or Delete Circuit Groups.

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

/N Network Port Parameters - IPv4

Displays a menu used to select IPv4 protocol parameters for the Network Port. All functions provided by the /N command are also available via the Web Browser Interface. For more information, please refer to Section 5.9.

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

/N6 Network Port Parameters - IPv6

Displays a menu used to select IPv6 protocol parameters for the Network Port. All functions provided by the /N6 command are also available via the Web Browser Interface. For more information, please refer to Section 5.9.

Availability: Administrator
Format: **`/N6`** **[Enter]**

/PNA Configure Ping-No-Answer Function

Displays a menu that is used to configure the Ping-No-Answer function. The Ping-No-Answer function allows the AFS to automatically perform A/B switching when a target device fails to respond to a ping command. For more information, please refer to Section 6.

> **Note:** *If desired, the Ping-No-Answer function can also be configured to send email notification whenever a target device fails to respond to a ping command. For more information, please refer to Section 7.3.*

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

/AC Alarm Configuration Parameters

Displays a menu that is used to configure and enable the Over Temperature Alarms, Lost Communication Alarm, Ping-No-Answer Alarm, Invalid Access Lockout Alarm, Power Cycle Alarm and Monitor/Alarm Input function.

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

/I Reboot System (Default)

Reinitializes the AFS unit and offers the option to keep user-defined parameters or reset to default parameters. As described in Sections 5.10.1 and 15.3, the /I command can also be used to restore the unit to previously saved parameters. When the /I command is invoked, the unit will offer four reboot options:

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

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

/UF Upgrade Firmware

When new versions of the AFS firmware become available, this command is used to update existing firmware.

Notes:

- *The Firmware Upgrade Utility is the preferred method for managing AFS firmware upgrades. The /UF command is intended to provide an alternative to the Firmware Upgrade Utility.*
- *When a firmware upgrade is performed, the AFS will require 15 minutes for the upgrade procedure.*

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

/TEST Test Network Parameters

Displays a menu which is used to test configuration of the Syslog and SNMP Trap functions and can also be used to invoke a Ping Command.

Notes:

- *In order for a ping test to function properly, your network and/or firewall and the target device must be configured to allow ping commands.*
- *In order for the ping command to function with domain names, Domain Name Server parameters must be defined.*
- *The Test Menu's Ping command is not effected by the status of the Network Parameters Menu's Ping Access function.*

Availability: Administrator, SuperUser

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

Appendix A. Interface Description

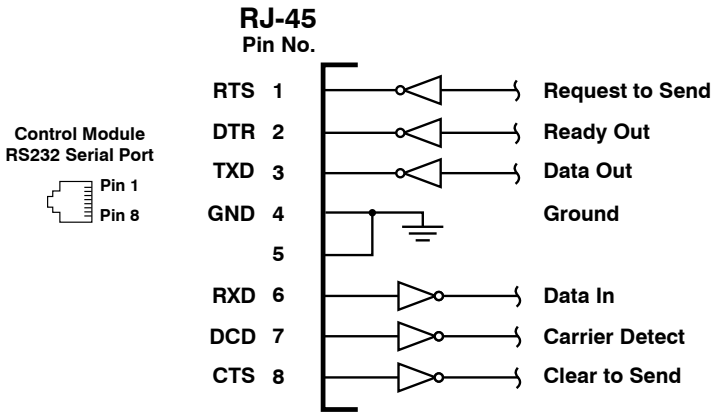

Figure A.1: Serial Port Interface

A.1. Serial Port (RS232)

DCD and DTR hardware lines function as follows:

1. **When connected:**

   a) If either port is set for Modem Mode, the DTR output at either port reflects the DCD input at the other end.

   b) If *neither* port is set for Modem Mode, DTR output is held high (active).

2. **When not connected:**

   a) If the port is set for Modem Mode, upon disconnect DTR output is pulsed for 0.5 seconds and then held high.

   b) If the port is *not* set for Modem Mode, DTR output is controlled by the DTR Output option (Serial Port Parameters Menu, Option 23). Upon disconnect, Option 23 allows DTR output to be held low, held high, or pulsed for 0.5 seconds and then held high.

Appendix B. Specifications

Switch Card: Up to 16 Modules

Interface: RJ45-3, Three Jacks, 8 Pins Switched Common Jack to A or B Jack.

Contacts: High Reliability, Mechanical Relays, Break-Before-Make Contacts with 1 Amp @ 30 VDC Rating, 100 Million Cycle Life.

Switching:

Manual: Individual Toggle Switch, Gang Switching from Control Module.

Code/Web Browser: By Slot Number or by Name.

Card Rack and Control Unit

Ethernet Port: 10/100Base-T

Serial Console Port: 1 each, RJ45, RS232C

AUX Port: 5-Pin Quick-Connect Terminal Block for External Connection for Alarm Output, Monitor Input and Ground. Monitor Input Signal is always read relative to ground signal.

Low Monitor Input Signal: 0V to -48V

High Monitor Input Signal: +5V to +48V

RS232 Port Interface:

Connectors: One (1) RJ45 connector (DTE pinout.)

Coding: 7/8 bits, Even, Odd, No Parity, 1, 2 Stop Bits.

Flow Control: XON/XOFF, RTS/CTS, Both, or None.

Data Rate: 300 to 115.2K bps (all standard rates).

Inactivity Timeout: No activity timeout disconnects port/modem sessions. Off, 5, 15, 30, 90 minutes.

Break: Send Break or Inhibit Break

Site ID: 32 Characters.

Port Name: 16 Characters per port.

Usernames & Passwords: 32 character usernames; 16 character passwords (case sensitive.) Up to 128 pairs, definable circuit module, circuit group and system access.

Physical/Environmental:

Size: 5.25” x 19.00” x 6.75” (H x W x D)

Power: 100/240 VAC 50/60 Hz, 15 watts

Weight: Shipping Weight, Fully Loaded, 15 pounds

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

Humidity: 10 - 90% RH

Venting: Side vents are used to dissipate heat generated within the unit. When mounting the unit in an equipment rack, make certain to allow adequate clearance for venting.

Appendix C. Customer Service

Customer Service hours are from 8:00 AM to 5:00 PM, PST, Monday through Friday. When calling, please be prepared to give the name and make of the unit, its serial number and a description of its symptoms. If the unit should need to be returned for factory repair it must be accompanied by a Return Authorization number from Customer Service.

WTI Customer Service
5 Sterling
Irvine, California 92618

Local Phone: (949) 586-9950
Toll Free Service Line: 1-888-280-7227
Service Fax: (949) 583-9514

Email: service@wti.com

Trademark and Copyright Information

WTI and Western Telematic are trademarks of Western Telematic Inc.. All other product names mentioned in this publication are trademarks or registered trademarks of their respective companies.

Information and descriptions contained herein are the property of Western Telematic Inc.. Such information and descriptions may not be copied, disseminated, or distributed without the express written consent of Western Telematic Inc..

August, 2014
Part Number: 14069, Revision: G

Trademarks and Copyrights Used in this Manual

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

Teraterm is a copyright of Ayera Technologies, Inc.

BlackBerry is a registered trademark of Research In Motion Limited.

JavaScript is a trademark of Sun Microsystems, Inc.

Telnet is a trademark of Telnet Communications, Inc.

Thawte is a trademark of Thawte, Inc.

VeriSign is a registered trademark of VeriSign, Incorporated

All other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.