



RFL Electronics Inc.

IMUX 2000

SNMP Access Gateway

User's Manual

**RFL Electronics Inc.
353 Powerville Road
Boonton Township, NJ 07005
(973) 334-3100**

**Publication No. MC2000SNMP
Printed In U.S.A.
Revised August 10, 2009**

TABLE OF CONTENTS - SNMP ACCESS GATEWAY USER'S MANUAL

CHAPTER 1 - PRODUCT OVERVIEW	1
Figure 1. - SNMP Access Gateway Connectivity Overview	1
1.1 - Introduction	1
1.2 - IMUX 2000 Information	2
CHAPTER 2 - INSTALLATION	3
2.1 - Mounting	3
2.2 - Power Input	3
Figure 2. - SNMP Access Gateway Module and MA-810 Module Adapter	3
2.3 - Serial Ports	4
Figure 3. - SNMP Access Gateway DB9 Pin Out	4
2.4 - Ethernet	4
2.5 - Front Panel Items	5
Figure 5. - SNMP Access Gateway Front Panel Layout	5
CHAPTER 3 - BASIC SETUP FOR OPERATION	7
3.1 - Network Setup	7
3.2 - Local Command Mode	7
3.3 - Connections	8
CHAPTER 4 - COMMAND CONTROL	9
4.1 - Command Processor Mode	9
4.2 - General Commands	10
4.2.1 - EXIT	10
4.2.2 - BYE	10
4.2.3 - ? (question mark)	10
4.2.4 - SETUP	10
4.2.5 - EVENTS	11
4.2.6 - DEFAULT	11
4.2.7 - COLDSTART	11
4.2.8 - HELP	11
4.2.9 - PING	11
4.3 - Pseudo-SNMP Commands	11
4.3.1 - GET	11
4.3.2 - GETNEXT	12
4.3.3 - GETX	12
4.3.4 - SET	12
4.3.5 - WALK	12

CHAPTER 5 - USE OF THE SETUP MENU	13
5.1 - Networking	13
5.1.1 - Network Access Enabled	13
5.1.2 - Get IP Address	13
5.1.3 - IP Address	14
5.1.4 - Network Mask	14
5.1.5 - Default Router	14
5.1.6 - FTP AutoDelete	14
5.1.7 - SNMP Manager Setup	14
5.1.8 - SNMP Trap Setup	14
5.1.9 - SNMP Community Setup	15
5.1.10 - IP Address Restrictions	15
5.1.11 - Ping Router every 10 Mins	15
5.1.12 - PPP Dialout Setup	15
5.1.13 - PPP Hosting Setup	15
5.2 - Serial/Input Ports	15
5.3 - Passwords	16
5.4 - Event Definitions	16
5.4.1 - Set Up Sensor/Analog Events	16
5.4.2 - Upload New Alarm File	17
5.4.3 - View Alarm File	17
5.4.4 - Alarm Evaluator Enabled	18
5.4.5 - Store Data Record Events	18
5.4.6 - Store Alarm Record Events	18
5.4.7 - Store Sensor Events	18
5.4.8 - Store Reset Events	18
5.4.9 - Store Command Log Events	18
5.5 - Action Definitions	18
5.5.1 - Traps	19
5.5.2 - Pagers	19
5.6 - System Date/Time	20
5.7 - General Settings	20
5.7.1 - Set UnitID	20
5.7.2 - Operational Settings	21
5.7.3 - Character Mask	21
CHAPTER 6 - PASS THROUGH MODE	22
CHAPTER 7 - CONSOLE MODE	24
CHAPTER 8 - MANAGEMENT INFORMATION BASE (MIB)	25
CHAPTER 9 - SNMP CONFIGURATION AND CONTROL	29
CHAPTER 10 - USING FTP	40

CHAPTER 11 - PROGRAMMING DATA ALARMS	41
11.1 - Alarms are the same as Events	41
11.2 - Alarm Actions	41
11.3 - How Data Alarms Are Set Up	41
11.4 - Defining Data Alarms	41
11.5 - Field Section	42
11.6 - Operators for Formulas	42
11.7 - Macro Section	43
11.8 - Data Alarm Section	43
11.9 - End Section	44
11.10 - Defining Alarm Actions	44
CHAPTER 12 - USE OF THE EVENTS COMMAND	45
12.1 - List Events File	45
12.2 - Clear Events File	45
12.3 - View Active Alarms	45
12.4 - Acknowledge Active Alarms	46
12.5 - View Alarm Action Detail	46
12.6 - View Data Alarm Counters	46
12.7 - View Action History	46
12.8 - Clear Action History	47
CHAPTER 13 - RESETTNG THE SNMP ACCESS GATEWAY	48

CHAPTER 14 - APPLICATION NOTES	49
APP NOTE A. USE OF IP RESTRICTIONS	50
APP NOTE B: MONITORING RS232 LEVELS AS ALARMS	51
Figure 8. Schematic for Sensor Inputs	51
Figure 9. Illustration of Connecting for Monitoring RS232 Control Lines	51
APP NOTE C: IMUX TRAP MESSAGES	52
C.1 Trap Format	52
C.2 Trap Codes	52
C.3 Trap Configuration Information	53
C.4 MIB Information	53
CHAPTER 15 - WARRANTY INFORMATION	54
CHAPTER 16 - CANADIAN DEPT. OF COMM. NOTICE	55

"Portions of this document are provided by and used with permission of Omnitronix, 760 Harrison, Seattle, WA, (206)624-4985. Unauthorized reproduction, distribution, or sale of this user manual is prohibited"

Chapter 1 - Product Overview

1.1 - Introduction

The SNMP Access Gateway monitors serial (RS232) data streams for alarm conditions, and provides notification of alarm conditions by audible alarm, pager messages and SNMP traps. The SNMP Access Gateway may be used to provide legacy (non-network) equipment with the ability to generate SNMP traps when alarm conditions occur. Additionally, the SNMP Access Gateway can provide pass-through access to devices connected to the serial ports of the SNMP Access Gateway, thereby providing remote access to programming or maintenance ports of equipment.

The SNMP Access Gateway has two serial ports, and one ethernet 10BaseT network port. Front panel LEDs provide status information about the ethernet connection, serial port activity, and power status.

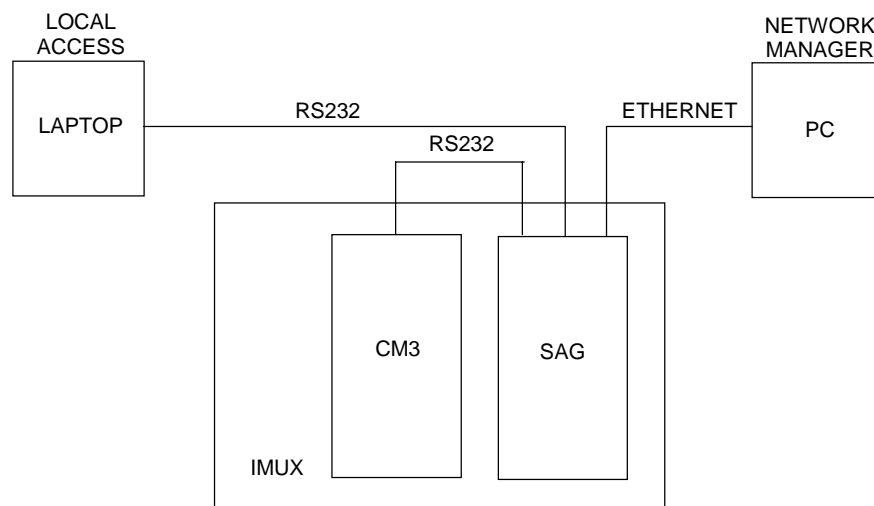


Figure 1. - SNMP Access Gateway Connectivity Overview

The serial ports can operate from 300 to 19,200 baud, and are used to monitor serial data streams and/or provide remote pass-through access to connected equipment. These serial ports are labeled IMUX (I/O 1) and REMOTE (I/O 2). An alarm configuration file can be loaded into the memory of the SNMP Access Gateway, and the SNMP Access Gateway can then monitor the data received on the serial ports for alarm conditions.

The two serial ports may also be used in a 'console' mode, in which the SNMP Access Gateway is placed in-line between two pieces of equipment. In this mode the alarm configuration file may still be used to monitor the data streams for alarm conditions, but the SNMP Access Gateway, in this case, passes data received on each serial port to the other port, so that the SNMP Access Gateway does not disrupt the data flowing between the two devices.

The serial ports may be used for pass-through access to connected serial devices, similar to a terminal server. A TCP/IP connection is made to the SNMP Access Gateway, and then characters received from the network connection is passed to the serial port, and characters received on the serial port are passed to the network connection. This pass-through mode may be used to remotely access the maintenance ports of equipment, etc.

When more than one connection is made to the SNMP Access Gateway for access to the same pass-through port, then users may be allowed to 'join' connections. This feature can be useful in providing technical support in the use of the connected equipment. Two remote users, at different locations, can both have access to the same pass-through port. This allows a person providing technical support to see what commands or data is actually being sent and received, which can be quite useful when providing technical support.

One of the serial ports (I/O 2) may also be used as a local command port, for configuration or checking on the status of the device. 'Local Command Port Mode' may be entered by using either a push-button located on the front panel of the SNMP Access Gateway or by entering a pre-defined escape sequence on the serial port itself. This local command port is especially useful when performing static allocation of network IP addresses, in which case the SNMP Access Gateway needs to be configured with an IP address prior to its use on the network.

An Events file is maintained by the SNMP Access Gateway which contains logged events, such as received alarm records, etc. Each type of item which may be recorded in the events log is enabled by its own configuration setting, so that the events file usage can be customized as appropriate for the installation site.

All settings and configuration of the SNMP Access Gateway may be made remotely, using either commands via a TCP/IP or modem connection, or by SNMP. The SNMP Access Gateway contains a customized management information base (MIB) which may be used to configure and control the SNMP Access Gateway. Configuration settings are stored in non-volatile memory for preservation in the event of a power loss.

1.2 - IMUX 2000 Information

When used with the IMUX 2000 the SNMP Access Gateway connects to the remote port of the IMUX using port 1. Port 2 is used as a craft interface to both the IMUX and SNMP Access Gateway. A serial cable is supplied for connection from I/O 1 to the REMOTE port on the IMUX CM3R. The power for the gateway is supplied via the IMUX motherboard.

The unit is programmed from the factory for the proper setup for most IMUX applications. The only required setup by the user is to program in the proper IP address for the gateway and the destination IP address for the SNMP traps.

The gateway has been designed to work specifically with version 23 of the IMUX CM3C software or any version of the CM3R software. When used with any of these versions, RS232 trap messages are created by the IMUX. This allows the gateway to generate SNMP traps as a result of a message from the IMUX. These traps will contain data that defines the fault condition on the IMUX. More information on these traps is contained in Application note C.

Chapter 2 - Installation

2.1 - Mounting

The SNMP Access Gateway module is packaged in a plug-in module, for mounting in an IMUX 2000 chassis.

When installing the SNMP Access Gateway module, a location should be selected in the front of the IMUX 2000 chassis which is directly in line with the MA-810 module adapter which is mounted in the back of the chassis. Make sure the serial port cable can reach the CM3R remote port. This cable should have enough slack so it is not in danger of being pulled out of place. Some serial port cables, especially hanging cables of any significant length, may have enough hanging weight to pull the SNMP Access Gateway out of place. In such a case, the serial port cables may need to be tied in place to provide the SNMP Access Gateway with relief from such strain.

2.2 - Power Input

The SNMP is powered through the IMUX 2000 chassis motherboard. The SNMP Access Gateway uses a maximum power input of approximately 5 watts, so the maximum current from the IMUX 2000 power supply is about 1 amp.

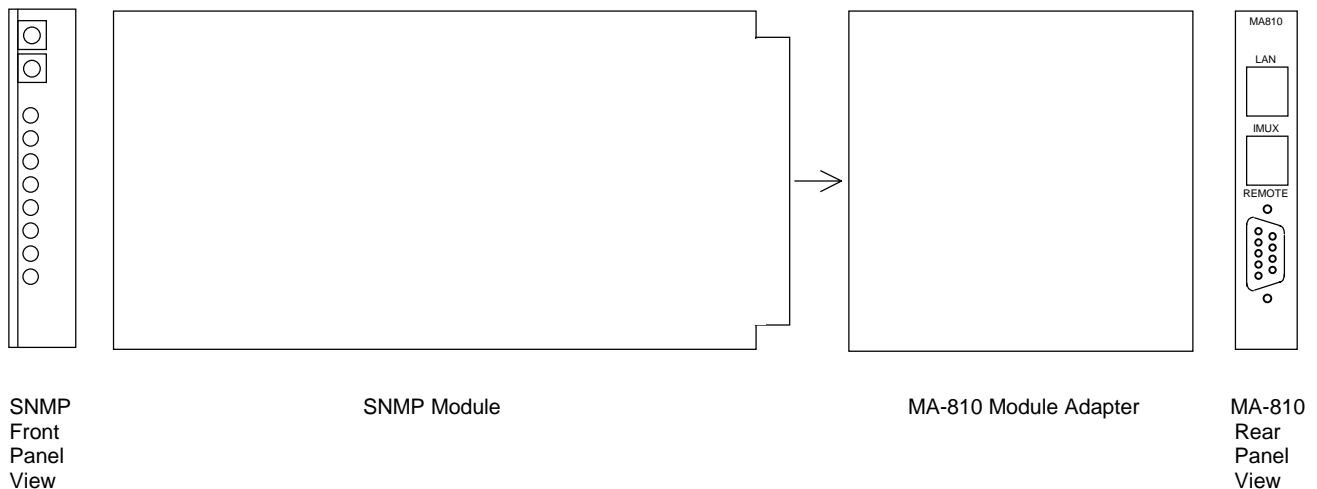


Figure 2A. – SNMP Access Gateway Module and MA-810 Module Adapter

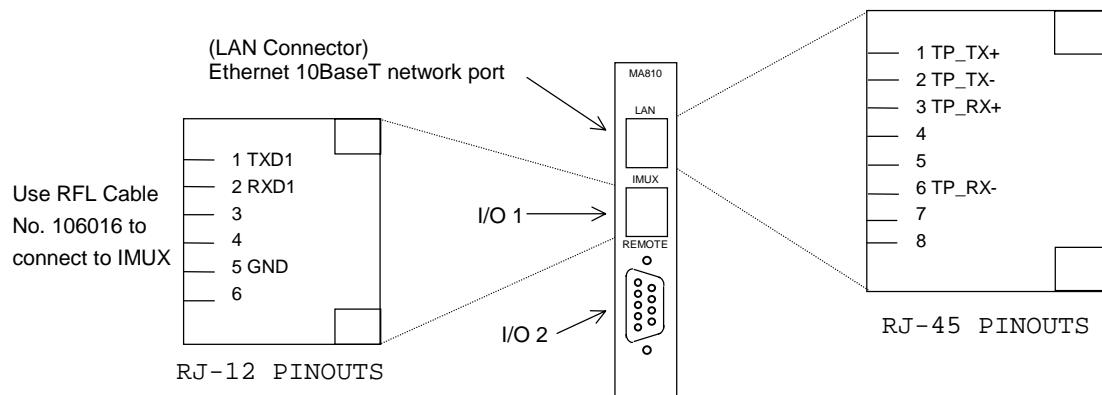


Figure 2B. – MA-810 Module Adapter Connectors

2.3 - Serial Ports

The I/O 2 serial port is configured as a DTE port using a male, DB-9 connector. The I/O 1 serial port is configured as a DTE port using an RJ-12 connector which is similar to that used on the COM ports of an IBM-compatible personal computer. Figure 3 shows the pin configuration of the I/O 2 port. Figure 2B shows the pin configuration of the I/O 1 port.

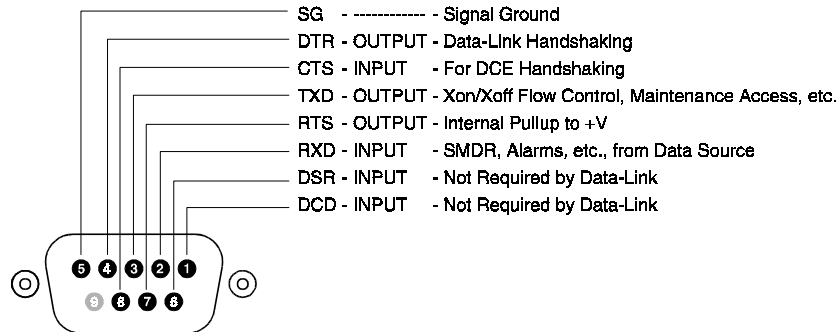


Figure 3. - SNMP Access Gateway DB9 Pin Out

The main pins which must be noted are the received data signal line on pin 2 and the signal ground on pin 5. When receiving serial data, these are the only two connections which the SNMP Access Gateway needs. However, if pass-through access to connected serial devices is required, then the transmitted data signal line on pin 3 must be connected as well. Additionally, some equipment may require an RS-232 high signal on one or more of its signal lines in order to transmit or accept data. Consult the manual for your other equipment as needed.

The DCE, DB-9 female cable ends which mate with the serial port connectors of the SNMP Access Gateway will often have a pair of screw-down cable locks. These cable locks should be used to assure a solid connection of the cable with the SNMP Access Gateway serial port connectors.

2.4 - Ethernet

The ethernet 10BaseT connector is an RJ-45 connector. This connector is the commonly used 10BaseT connector, which would connect the SNMP Access Gateway to an ethernet hub or switch.

2.5 - Front Panel Items

The front panel of the SNMP Access Gateway module has two push-buttons and 8 LED indicators representing status information about the SNMP Access Gateway.

The reset (RST) button (S2) is used to reset the SNMP Access Gateway. After the RST button is held in for about 5 seconds, the SNMP Access Gateway will start sounding its audible alarm. At this point the RST button may be released. The SNMP Access Gateway will remain in reset while the RST button is pressed, and will begin operation again once the RST button is released.

The program (PRG) button (S1) is used to silence audible alarms and to enter local command (programming) mode. When an audible (buzzer) alarm is active, pressing the PRG button clears the alarm, so that the audible alarm is silenced. If the PRG button is held in for about 3 seconds, the SNMP Access Gateway enters local command (programming) mode. In this mode serial port I/O 2 operates as a local command port. Either a time-out of no command for five minutes, an EXIT or BYE command, or a reset will take the SNMP Access Gateway out of local command mode.



Figure 5. – SNMP Access Gateway Module Layout

The ethernet status is shown as three LEDs. The yellow Link LED lights whenever an ethernet 10BaseT network link connection is found. The green Transmit LED lights briefly whenever an ethernet frame is being transmitted. The green NET LED lights whenever a TCP socket is opened to the unit, whether telnet or FTP. SNMP activity causes this NET LED to blink once per second. These LEDs can be used to see that a network cable connection is made, and when some network activity has caused the SNMP Access Gateway to transmit on the network.

Each RS-232 port has two LEDs associated with it. The left LED is a received data (RXD) LED. The right LED is a transmitted data (TXD) LED. The TXD LED is normally on and green. The RXD LED is off when no cable is connected to the serial port, and on when a cable is connected. Normally the RXD LED will be green as well. When an RS-232 line is idle, the voltage is negative, and the LED shows green. When data is transmitted, the voltage goes between positive and negative voltages and the LED turns red and green, so when data is transmitted or received on a serial port the corresponding LED will flicker between red and green, which sometimes makes the LED look yellow. These LEDs can be used to see that a cable is connected (the LED is lit) and that data is being transmitted or received (the LEDs flicker between red and green).

The power LED has two uses. Normally the power led is lit constantly, with a quick flash once every ten seconds. This 'heartbeat' signal on the power LED provides a quick indication that the SNMP Access Gateway is operating. A second mode of use of the power LED is when the SNMP Access Gateway is in local command mode. When the local serial port is in command mode, the power led flashes on and off at about a 1/2 second on, 1/2 second off rate.

Chapter 3 - Basic Setup for Operation

3.1 - Network Setup

As with all TCP/IP- or SNMP-based devices, the SNMP Access Gateway requires an IP address to be assigned to each unit in order to send and receive TCP/IP or SNMP data. The SNMP Access Gateway may operate with either a statically or dynamically allocated IP address.

When statically allocated, the SNMP Access Gateway must be configured with an IP address, network address mask, and default router prior to being used on the network. This configuration may be made by a local command port. It can not be made via a TCP/IP (network) connection, as use of such connections would first require the setting of the IP address.

The IP address may be dynamically allocated using either BOOTP or DHCP. By default, the SNMP Access Gateway is configured to use BOOTP or DHCP to dynamically obtain its IP address, network address mask, default router, etc. When booting, the SNMP Access Gateway transmits a BOOTP/DHCP request. This request is responded to by any BOOTP or DHCP servers configured to allocate an IP address to the SNMP Access Gateway. When the SNMP Access Gateway receives its first response from the BOOTP/DHCP request, then the SNMP Access Gateway either uses the BOOTP reply or engages in a DHCP session to dynamically establish the network settings of the SNMP Access Gateway.

The SNMP Access Gateway expects to be on a local area network, or to use the default router in the case where an IP destination is determined to not be a local address. The SNMP Access Gateway uses the destination IP address and the network address mask to determine if the destination IP address is a local address or not. If so, then the IP frame is sent to the destination IP address on the local network. If not, then the IP frame is sent via the default router. If no default router is configured (the address is 0.0.0.0) then no IP frame is sent when the SNMP Access Gateway determines that the IP frame must be routed and no router exists. If an SNMP management station will be used which is not on the local network, then the configuration of the default router should be verified. See the use of the PING command in verification that a route to each management station exists and is usable.

The SNMP Access Gateway provides TCP/IP connections using ports 23 and 2000. Up to three concurrent connections may be made using these port numbers. When a port address of 23 is used, the telnet character processing (interpretation of IAC codes, option negotiation, etc.) is performed in both directions of data flow. When a port address of 2000 is used, no telnet character processing is performed. Other than this difference, the use of port 23 or port 2000 is identical. The SNMP Access Gateway also uses ports 20 and 21 when providing the FTP server functions.

The SNMP Access Gateway has a configurable list of IP restrictions. This list may be used to restrict IP access to the SNMP Access Gateway to only certain networks or certain IP addresses, reject connection from certain IP networks or addresses, etc. This may be used to provide greater security features than a password alone. The IP restriction table is established using the SETUP command on the NETWORKING menu. If the IP restriction table is empty, then all networks and IP addresses are allowed to connect to the SNMP Access Gateway. By entering IP restrictions in the table, then certain networks or IP addresses can be restricted. See the App Note A. Use of IP Restrictions for more information on the use of IP restrictions. By default, no IP restrictions are established.

3.2 - Local Command Mode

The serial port labeled I/O 2 may be used for local command mode. This mode is entered by either holding in the PRG button on the front panel for about five seconds, until the power LED starts flashing on at off, or by entering the (programmable) escape character three times within 3 seconds on the I/O 2 serial port.

When in local command mode, the baud rate and serial port parameters of I/O 2 remain the same.

A user may exit local command mode by four methods. Using the EXIT or BYE command will terminate local command mode. Waiting five minutes without entering a command will also terminate local command mode. Additionally, resetting the SNMP Access Gateway with the RST button will also exit local command mode.

3.3 - Connections

A connection may be made to the SNMP Access Gateway via a network connection. When a connection is made, the user is provided with a menu from which the desired mode of the connection is established. The user may select to enter a command processor mode of operation, or may select a pass-through mode of operation. The user selects the desired mode of operation from the menu, and then the user is prompted for the password for that mode of access. If the user enters the proper password, then the desired mode of the connection is established.

A connection may be in one of four states. A first state is an idle state, in which no active connection for that possible connection has been established. In the second state, a user has established a connection and the menu selection for which type of connection is desired has not yet been made. In the third state the user has entered the command processor. In the fourth state the user has entered pass-through access mode.

Three concurrent network connections, one local command port connection, plus an FTP server connection may all exist with the SNMP Access Gateway. SNMP is connectionless, and may be use concurrently with any combination of connections. The FTP server connection does not affect the other connections or use of command or pass-through mode.

Only one valid command processor connection may exist at a time. Thus, if I/O 2 is in the local command port mode, then requests to enter command processor mode via any of the network connections must be denied. Similarly, if one of the network connections has been established as a command processor connection, then other network connection cannot access the command processor until it has been made available once again. If a network connection is in command processor mode, then the local command port mode on I/O 2 is also not allowed until the command processor is available for re-assignment.

When a user opens a connection to the SNMP Access Gateway the user is provided with a menu from which the mode of operation is selected, as shown below.

```
SNMP Access Gateway Model    Version 1.00

0. Enter Command Processor
1. Enter Pass-Through to Port 1
2. Enter Pass-Through to Port 2
X. Exit (end connection)
```

A network connection can be broken by using the 'X' selection from the main menu. The network connection is then placed into the idle state.

A network connection may also be broken from the client side using the disconnect feature of the client software. Closing of the network connection places that connection into the idle state.

When a connection has been established and is in either the command processor or pass-through mode of operation, the current operating mode should be terminated and the user should return to the main menu before closing the connection to the SNMP Access Gateway. Closing a network connection should not result in any extra characters being transmitted to either the command processor or a pass-through port.

Chapter 4 - Command Control

4.1 - Command Processor Mode

The command processor may be accessed from a network connection. A user enters command processor mode from the main menu by selecting the '0' option.

```
SNMP Access Gateway Model    Version 1.00
```

```
0. Enter Command Processor
1. Enter Pass-Through to Port 1
2. Enter Pass-Through to Port 2
X. Exit (end connection)
<user enters 0>
```

```
Command Processor Password: ---- <user enters password>
Command Password Accepted
```

```
Enter Command (Setup, Events, ?, Help or other command)
>
```

The > is the command prompt. At this point the user may enter any of the commands for the SNMP Access Gateway. After a command is executed, a new prompt > is provided. The command reminder line is only provided again if a blank (enter only) line is entered.

If the command processor is currently in use by any of the other connections, then after the user has entered the command processor password the user gets a message as below:

```
Command Processor Currently In Use.  Access Denied
```

Thus, only one command processor connection may be made at a time. In this case the user is returned to the main selection menu.

The EXIT command is used to exit the command processor and return to the main menu. The BYE may also be used to exit the command processor. However, the BYE command also terminates the connection after the command processor access is terminated.

If no command is entered for 4 minutes and 30 seconds then a reminder message is sent out, followed by the prompt:

```
Command Processor Time-out in 30 seconds
>_
```

If no command is entered within this 30 seconds then the BYE command is executed, terminating the command processor access and terminating the connection, due to no command in 5 minutes. This automatic logout occurs on any of the command connections, including all network connections, and the local command port.

Command may be entered in upper, lower or mixed case. Only a few commands are needed to control and manage the SNMP Access Gateway. The commands available are:

Session control commands	
EXIT	Exit command processor back to main menu
BYE	Exit command processor and close connection
Setup and status commands	
?	Shows the SNMP Access Gateway status
SETUP	Most SNMP Access Gateway setup is done with this command
EVENTS	List, clear events file
RELAYS	Setup and status of relays
DEFAULT	Set settings to defaults

COLDSTART	Clear events file, all settings to default
Other commands	
HELP	Show list of commands
PING	Ping an IP Address for testing
Pseudo-SNMP Commands	
GET	Get the value of an object with a specific object ID
GETNEXT	Get the value of the next object after an object ID
GETX	Get the value of the object last retrieved
SET	Set the value of an object
WALK	Get the value of the object after the last retrieved

4.2 - General Commands

4.2.1 - EXIT

The EXIT command terminates the command processor access and returns the user to the main menu. This command can be used if the user wants to change the access mode from command processor mode to pass-through access mode. If the user wants to simply exit the command processor and then terminate the connection, the BYE command may be used instead to perform both these actions with one command.

4.2.2 - BYE

The BYE command terminates both the command processor access and the connection being used to access the command processor. The BYE command can be used at the end of a command session to exit the command processor and terminate the command connection. Alternatively, the EXIT command could be used to exit the command processor and return to the main menu, and then the 'X' main menu command can be used to terminate the connection which was used for command access.

4.2.3 -? (question mark)

The ? command provides a status display for the SNMP Access Gateway. This display shows the firmware version, unit ID, current date and time, setup of the serial ports, sensor and relay status, etc. This command can be used to check the operational status and configuration of the SNMP Access Gateway unit.

```
SNMP->Link V0.50m    #
Unit ID : SNMP->Link
Date    : MON 04/06/98      Time    : 17:55:38
Modem   : 33600 8,N,1
Network : Yes              FAFile  : Yes
IP Add  : 192.168.100.131
MAC Add : 00:10:A3:00:00:09
-----
                I/O 1      I/O 2
Baud Rate    19200      19200
Parity, etc. 8,N,1      8,N,1
-----
Event Records 0
Current Event Status:
Data Alarms  -----
Sensors  A1 :Open   A2 :Open   A3 :Open   A4 :Open   A5 :Open   A6 :Open
Relays   A8 :Open   A9 :Open
```

4.2.4 - SETUP

The SETUP command provides a series of menus from which the user may select configuration items for setup and configuration purposes. These setup menus include setup items for the networking settings, serial port settings,

password settings, event (alarm) definition settings, alarm action settings, and other settings. See Chapter 5 - Use of the SETUP Menu for further details of the use of the SETUP command.

4.2.5 - EVENTS

The EVENTS command is used to view the current status of the events (alarms), view the contents of the events log file, clear contents of the events log file, view the current active alarm actions, acknowledge alarms, and view the history log of alarm actions. See Chapter 12 - Use of the EVENTS Command for further details of the use of the EVENTS command.

4.2.6 - DEFAULT

The DEFAULT command resets certain variables and settings to their default values. The network settings and serial ports settings are not affected by the use of the DEFAULT command. The events log file is not cleared. The configuration variables and settings affected by the DEFAULT command are:

Setting	Value Set To
Store data record events	1 (on)
Store alarm record events	1 (on)
Store command log	1 (on)
Store reset events	1 (on)
Store sensor events	1 (on)

4.2.7 - COLDSTART

The COLDSTART command is used to completely re-initialize the SNMP Access Gateway. All network and other settings are re-initialized to their default values. The events log file is cleared.

4.2.8 - HELP

The HELP command provides a list of the command available with the SNMP Access Gateway. The display looks something like this:

```
?          SETUP  EVENTS  RELAYS  EXIT
GET        GETNEXT GETX    SET
```

4.2.9 - PING

The PING command executes an ICMP PING test to determine if an IP address is reachable and responding. The PING command may be used to test the network connectivity of the SNMP Access Gateway. For example, if a default router is used, the SNMP Access Gateway should be able to PING the default router, which demonstrates network connectivity and proper network connections.

4.3 - Pseudo-SNMP Commands

The pseudo-SNMP commands are manual commands which can be entered via a dialup or telnet connection and which may be used with the object IDs developed for SNMP for setting and retrieving the value of SNMP-manageable objects. These objects may be part of the standard (MIB-II) MIB (as described in RFC 1213), or part of the custom MIB of the SNMP Access Gateway. The pseudo-SNMP management section of this manual provides further details and examples of use of the pseudo-SNMP commands.

4.3.1 - GET

The GET command is used with a specific object ID to obtain the value of that object.

4.3.2 - GETNEXT

The GETNEXT command is used with an object ID, and the value returned is the object ID and value of the object which follows the object ID included with the GETNEXT command.

4.3.3 - GETX

The GETX command is used without an object ID, and the value returned is that of the last object retrieved by pseudo-SNMP.

4.3.4 - SET

The SET command is used with an object ID and a value, and the object with the object ID included with the command is set to the value included with the command.

4.3.5 - WALK

The WALK command is used without an object ID, and may be used to 'walk' through the MIB. The WALK command acts like the GETNEXT command, but uses the object ID of the last object retrieved by pseudo-SNMP as the included address. Thus, repeated uses of the WALK command allow the user to progress through all items of the MIB.

Chapter 5 - Use of the SETUP Menu

Upon selecting 'Enter Command Mode' from the main SNMP Access Gateway menu, the password prompt as shown below is presented for entry of the Command Mode Password.

```
Command Processor Password: ----
Command Password Accepted
```

Upon entry of a valid password the Command Mode Prompt (a 'greater than' sign) is shown and commands can be entered. The first time the command prompt is presented, an additional line is printed (as shown below) to remind the user of a few basic commands and this prompt can be redisplayed by pressing ENTER on a blank line of the command prompt. The SETUP command presents the user with a menu of basic setup functions.

```
>SETUP

Setup Main Menu
A. Networking
B. Serial/Input Ports
C. Passwords
D. Event Definitions
E. Action Definitions
F. System Date/Time
G. Other Settings
Selection?
```

Many of the above menu items have extensive sub-menus for configuration of all the possible SNMP Access Gateway settings. The following sections take each of the above menu items and go through the possible options and selections.

5.1 - Networking

Selecting the Menu Letter of NETWORKING from the Setup Main Menu presents the following submenu for setting various network related options. The Networking menu appears as follows. Each of the menu items shown below is discussed in order in this section.

```
Setup: Networking
A. Network Access Enabled [Y]
B. Get IP Address via [BOOTP/DHCP]
C. IP Address [192.168.100.131]
D. Network Mask [255.255.255.0]
E. Default Router [192.168.100.254]
F. FTP AutoDelete [N]
G. SNMP Manager Setup
H. SNMP Trap Setup
I. SNMP Community Setup
J. IP Address Restrictions
K. Ping Router every 10 Mins [N]
L. PPP Dialout Setup
M. PPP Hosting Setup
```

5.1.1 - Network Access Enabled

This option is toggled by pressing its Menu Letter. The default for this option is Y but communication via the ethernet interface can be inhibited by disabling this selection.

5.1.2 - Get IP Address

This option is toggled by pressing its Menu Letter. The default selection is BOOTP/DHCP and the alternate selection is STATIC. The default selection has the SNMP Access Gateway request and respond to BOOTP/DHCP

assignment for the unit IP Address. STATIC implies that the IP address is manually entered and in this mode the BOOTP/DHCP sequence is not initiated or allowed by the SNMP Access Gateway.

5.1.3 - IP Address

By pressing the Menu Letter of this option a prompt is presented for entry of the Static IP address. Note that after changing the IP address and exiting the SETUP menu the SNMP Access Gateway will reboot itself and any current network connections will be terminated (unless Get IP Address Via is set to Bootp/DHCP in which case the IP address change will not be accepted).

5.1.4 - Network Mask

By pressing the Menu Letter of this option a prompt is presented for entry of the Network Mask.

5.1.5 - Default Router

By pressing the Menu Letter of this option a prompt is presented for entry of the Default Router.

5.1.6 - FTP AutoDelete

This option is toggled by pressing its Menu Letter. FTP AutoDelete controls whether data is automatically deleted as TCP packets are acknowledged during an FTP transfer of the Events File data. The default is N.

5.1.7 - SNMP Manager Setup

Selecting the Menu Letter of this option presents the following submenu for entry of the IP addresses of up to eight possible SNMP managers. The addresses entered here will be referred to in other setup and alarm parameters as T1, T2, etc., to specify which managers traps should be sent to.

```
Setup: Networking: SNMP Managers
1. Manager 1 [192.168.100.20]
2. Manager 2 [192.168.100.1]
3. Manager 3 []
4. Manager 4 []
5. Manager 5 []
6. Manager 6 []
7. Manager 7 []
8. Manager 8 []
Selection?
```

5.1.8 - SNMP Trap Setup

Selecting the Menu Letter of this option presents the following submenu for selection of various options relating to sending SNMP traps.

```
Setup: Networking: SNMP Traps
A. SNMP Traps Enabled? [Y]
B. SNMP Authentication Failure Traps Enabled? [Y]
C. SNMP Traps Repeat Time (0 for no repeat) [2]
D. Enterprise-Specific Traps Enabled? [Y]
Selection?
```

A. This selection enables/disables the sending of SNMP Traps in general. The default is 'Y'.

This selection enables the sending of a trap to all SNMP Managers if an invalid community name is used in an SNMP GET or SET. The default is 'N'.

C. This selection enables and selects the interval at which SNMP Traps will repeat being sent until the alarm generating the trap is explicitly acknowledged. See Chapter 12 - Use of the EVENTS Command for more on Acknowledging Alarms.

D. This selection enables/disables sending traps relating to SNMP Access Gateway contact closures and data alarms. The default is 'Y'.

5.1.9 - SNMP Community Setup

Selecting the Menu Letter of this option presents the following submenu for specifying SNMP Community Names. Whenever you do an SNMP operation, whether a SET or a GET, the community name needs to be included as part of that operation. Additionally the community name is sent within any SNMP traps. While the default for all of these community names is 'public', these can be individually changed by using this menu.

```
Setup: Networking: SNMP Community Names
A. Read Community [public]
B. Write Community [public]
C. Trap Community [public]
Selection?
```

5.1.10 - IP Address Restrictions

Selecting the Menu Letter of this option presents the following submenu for selection of various options relating to IP Address Restrictions. Essentially, if there are no addresses entered in this table then connection from any IP address is allowed. Entries in this table will limit and explicitly allow connection from various IP addresses. For further information see the Application Note - Using IP Restrictions at the end of this manual

```
1. 192.169.100.0
A. Add Item to Table
B. Delete Item From Table
X. Delete All Items From Table
Selection?
```

5.1.11 - Ping Router every 10 Mins

This option enables pinging the Default Router's IP address every 10 minutes.

5.1.12 - PPP Dialout Setup

This option leads to a sub-menu which is described in the PPP chapter. The sub-menu contains the options to setup PPP dialout functionality for actions such as sending traps.

5.1.13 - PPP Hosting Setup

This option leads to a sub-menu which is described in the PPP chapter. The sub-menu contains the options to setup the Data-Link as a PPP Host.

5.2 - Serial/Input Ports

Selecting the Menu Letter of SERIAL/INPUT PORTS from the Setup Main Menu presents the following submenu for setting the baud rate and parity settings of the SNMP Access Gateway serial ports. The following two menus are displayed in order. The default settings for both serial ports is 19200 Baud, 8 Bits, No Parity, 1 Stop Bit.

```
Setup: Serial Ports
1. I/O 1: 19200,8,N,1
2. I/O 2: 19200,8,N,1
Selection? 1
```

```
Setup: Serial Ports: I/O 1 Baud Rate
A. 300
B. 600
```

C. 1200
 D. 2400
 E. 4800
 F. 9600
 G. 19200
 Selection [G]?

Setup: Serial Ports: I/O 1 W,P,S
 A. 8,N,1
 B. 7,E,1
 C. 7,O,1
 D. 7,N,1
 Selection [A]?
 DTR Low Except When Pass-Through Active [N]?

This last option turns on or off DTR handshaking with the device connected to I/O port 1 or 2 that one is accessing directly. In its default state, DTR is always high to the device on the respective port. With this option set to Y(es), DTR will go low to the device when no direct serial access is occurring. This is useful if one wants the device to close any maintenance or administrative session automatically in the case where a connection was not terminated properly.

5.3 - Passwords

Selecting the Menu Letter of PASSWORDS from the Setup Main Menu presents the following submenu for setting the SNMP Access Gateway passwords. The menu below shows the default passwords.

Setup: Passwords
 A. Command Password [SL60]
 B. Pass-Through Port 1 Password [ACCESS1]
 C. Pass-Through Port 2 Password [ACCESS2]
 D. FTP Server Password [SL60]
 Selection?

5.4 - Event Definitions

Selecting the Menu Letter of EVENT DEFINITIONS from the Setup Main Menu presents the following submenu for setting up the various events and alarm capabilities of the SNMP Access Gateway.

Setup: Event Definitions
 A. Set up Sensor / Analog Events
 B. UpLoad New Filter and Alarm File
 C. View Current Filter and Alarm File
 D. Alarm Evaluator Enabled [Y]
 E. Store Data Record Events [Y]
 F. Store Alarm Record Events [Y]
 G. Store Sensor Events [N]
 H. Store Reset Events [N]
 I. Store Command Log Events [N]

5.4.1 - Set Up Sensor/Analog Events

Selecting the Menu Letter of this option presents the following submenu for selection of various options relating to enabling and configuring the Contact Closure/Analog inputs for use.

Setup: Event Definitions: Sensor Events

Sensor	Set Type	Name	Active	Thrsh	Actions
1. Sensor 1	Y CC	fire	Closed	1	(T)12

2. Sensor 2	Y	CC	smoke	Closed	3 (T)1,(P)2
3. Sensor 3	Y	CC	flood	Closed	3 (T)1,(P)3
4. Sensor 4	Y	CC	famine	Closed	3 (T)1,(P)4
5. Sensor 5	Y	CC	pestilence	Closed	3 (T)1,(P)5
6. Sensor 6	Y	CC	layoffs	Closed	3 (T)1,(P)6

Selection?

Selection of any one of the sensors displayed on this list presents the following menu for sensor configuration.

```
Setup: Event Definitions: Sensor Events
Sensor 1
Enable Event [Y]?
Sensor Type, (C=Contact Closure, A=Analog) [CC]?
Sensor Event Name [fire]?
Sensor Event State (O=Open C=Closed) [Closed ]?
Sensor Event Threshold in Seconds [1]?
(T)rap Actions [12]?
(P)ager Actions []?
(B)uzzer Action []?
(R)elay Actions []?
```

Enable Event - This enables/disables any alarm action occurring from this sensor changing states.

Sensor Type - This selects whether the input type is a dry contact closure or an analog voltage.

Sensor Event Name - This is the name assigned to this sensor by the user.

Sensor Event State - This selects whether the alarm state, if selected as a contact closure, is open or closed.

Sensor Event Threshold in Seconds - This selects how long the contact closure sensor must be in the alarm state before it is considered an alarm. The default is 3 seconds.

(T)rap Actions - This assigns which traps should occur if this sensor changes to the alarm state. The numbers 1 through 8 may be entered indicating the SNMP Manager addresses 1 through 8 set up elsewhere.

(P)ager Actions - This assigns which pager numbers should be called when this alarm state occurs.

(B)uzzer Action - This allows specification of buzzer noise one or two (beeping or solid) when this alarm state occurs.

(R)elay Actions - This assigns which relays will activate when this alarm state occurs. The relay must be configured to be in Individual-Controlled mode as described in the chapter on Relay Management for this option to work.

5.4.2 - Upload New Alarm File

For uploading an alarm file over TCP/IP see the section on FTP.

5.4.3 - View Alarm File

Selecting the Menu Letter of this option displays any existing alarm file resident in the memory, looking something like this:

```
[fields]
flag=1,1
number=2,3
lastdigit=5,1
therest=6,95

[dataalarms]
equalfour=all,1,T1,Alhours
```

```

equalfour_1=lastdigit="4"
greatfour=all,1,T1,Alhours
greatfour_1=lastdigit>"4"
lessfour=all,1,T1,Alhours
lessfour_1=lastdigit<"4"
notfour=all,1,T1,Alhours
notfour_1=lastdigit!"4"

```

[end]

5.4.4 - Alarm Evaluator Enabled

Selecting the Menu Letter of this option enables/disables the operation of any existing alarm file loaded into the memory.

5.4.5 - Store Data Record Events

Selecting the Menu Letter of this option enables/disables the storage in the Events file of 'Data' records. A Data record is classified as any serial string received by the . (Note that for a string to be accepted as a 'record' it must a) be terminated by a CR, CL/LF, 03, or b) exceeds 200 characters or c) resides without meeting the previous two conditions for 10 seconds). Therefore, enabling this feature will cause all records received by the UNIT to be stored in the Events File.

5.4.6 - Store Alarm Record Events

Selecting the Menu Letter of this option enables/disables the storage in the Events file of 'Alarm' records. An Alarm record is classified as any serial string received by the UNIT which matches any existing alarm definition. Enabling this feature will cause Alarm records received by the UNIT to be stored in the Events File. Note that if 'Store Data Records' is also enabled the records matching alarm formulas will be stored twice, once as a data record and once as an alarm record.

5.4.7 - Store Sensor Events

Selecting the Menu Letter of this option enables/disables the storage in the Events file of Sensor Event records. A Sensor Event is classified as any sensor moving from a 'non-alarm' condition to an alarm condition. In this case a message will be placed in the Events File registering this occurrence.

5.4.8 - Store Reset Events

Selecting the Menu Letter of this option enables/disables the storage in the Events file of Reset Event records. A Reset Event is classified as any reboot of the UNIT. In this case a message will be placed in the Events File registering this occurrence.

5.4.9 - Store Command Log Events

Selecting the Menu Letter of this option enables/disables the storage in the Events file of Command Events. A Command Event is the sending of a command to the UNIT via command mode. In this case a message will be placed in the Events File registering each command which is sent to the UNIT.

5.5 - Action Definitions

Selecting the Menu Letter of ACTION DEFINITIONS from the Setup Main Menu presents the following submenu for setting up the various event notifications which can be associated with SNMP Access Gateway events and alarms.

```

Setup: Action Definitions
A. Traps
B. Pagers
Selection?

```

5.5.1 - Traps

Selecting the Menu Letter of this option presents a set of options to define the 'payload' variable which is included in all SNMP traps when sent. The current trap configuration is illustrated at the top of this menu. The default configuration is shown below.

```
Setup: Action Definitions: Trap Format
MM/DD HH:MM Type AlarmName Number Alarm Text String or Alarm Record
```

- A. Include Date/Time [Y]
- B. Include Alarm Type [Y]
- C. Include Alarm Name [Y]
- D. Include Alarm Number [Y]
- E. Include Alarm String [Y]

5.5.2 - Pagers

Selecting the Menu Letter of this option presents a set of options to define the phone numbers and other parameters for the eight possible pagers which can be associated with SNMP Access Gateway events and alarms. Note that the amount of information for each pager is too long to display on a single line, so two lines are used for the information for each pager definition.

```
Setup: Action Definitions: Pagers
# Type      Retry # Delay Repeat Delay TxID TxRSN DialDly HangupDly
  PagerID      Message
1. Numeric   01    05   N    05   N   N    15     10
   345#
2. Numeric   01    05   N    05   Y   Y    15     10
   456#
3. Numeric   01    05   N    05   N   Y    15     10
   567#
4. Numeric   01    05   N    05   N   Y    15     10
   678#
5. Numeric   01    05   N    05   N   Y    15     10
   789#
6. Numeric   01    05   N    05   N   Y    15     10
   890#
7. Numeric   03    05   N    05   N   Y    10     10
8. Numeric   03    05   N    05   N   Y    10     10
```

Selection?

By selecting any of the pager entries 1 through 8 the following prompts are displayed for selection and entry of the pager settings for that particular pager.

```
Setup: Action Definitions: Pagers: Callout 1
Pager Phone Number [9,6480769]?
Pager ID           []?
Pager Message      [345#]?
Pager Type (A-Alpha, N-Numeric) [Numeric]?
Repeat Until Source Acked [N]?
Time (minutes) Between Repeats [05]?
Transmit UnitID [N]?
Transmit Reason for Action [N]?
Numeric Pager Dial Delay [15]?
Numeric Pager Hangup Delay [10]?
```

Pager Phone Number - This is the number the modem should dial to connect to the pager service.

Pager ID - This is the ID used by the pager service to identify that specific pager.

Pager Message - In the case of an Alphanumeric pager this entry contains an optional text message which is included in the pager message whenever an alarm is sent to this pager. In the case of a numeric pager, this is the number which is transmitted as the message to the numeric pager.

Pager Type (A-Alpha, N-Numeric) - This selection indicates whether the protocol used for this pager should be numeric (numbers only, keyed in by touch-tones) or TAP protocol for sending alphanumeric messages.

Repeat Until Source Acked - This option indicates whether paging should repeat at intervals until the SNMP Access Gateway is specifically connected to and the alarm acknowledged.

Time (minutes) Between Repeats - This value indicates the duration between repeats mentioned above.

Transmit UnitID - This option selects whether the Unit ID should be included in the pager message transmitted. This only applies to alphanumeric pagers.

Transmit Reason for Action - This option selects whether a condensed code indicating the reason for the pager alarm should be transmitted as part of the alarm message. This only applies to alphanumeric pagers.

Numeric Pager Dial Delay - This value sets the number of seconds between the initial modem dialing of the numeric pager phone number and the subsequent dialing of the pager ID number.

Numeric Pager Hang-up Delay - This value indicates how long the SNMP Access Gateway waits after sending the final digits to the numeric pager before the SNMP Access Gateway disconnects.

5.6 - System Date/Time

Selecting the Menu Letter of SYSTEM DATE/TIME from the Setup Main Menu presents the following prompts for entry of the date/time information to set the SNMP Access Gateway internal clock.

```
Setup System Date/Time
MON 04/06/98 17:58:22

Time (24-Hour HH:MM) [17:58]?
Date (MM/DD/YY) [04/06/98]?
Day of Week (1-7, 1=SUN - 7=SAT) [2]?
Adjust for Daylight Savings? [Y]?
MON 04/06/98 17:58:00
```

5.7 - General Settings

Selecting the Menu Letter of GENERAL SETTINGS from the Setup Main Menu presents the following submenu for setting a number of miscellaneous operational settings of the SNMP Access Gateway.

```
Setup: General Settings
A. Set UnitID
B. Operational Settings
C. Misc. Modem-Related Settings
D. Character Mask
Selection?
```

5.7.1 - Set UnitID

By pressing the Menu Letter of this option a prompt is presented for entry of the Unit ID.

```
UnitID [SNMP Access Gateway]?
```

5.7.2 - Operational Settings

Selecting the Menu Letter of this option presents the following submenu for setting several general operational settings of the SNMP Access Gateway.

```
Setup: General Settings: Operational Settings
A. Escape Character [27]
B. Console Mode [N]
C. Strip Pass-through LFs sent to Device on I/O Port 1 [N]
D. Strip Pass-through LFs sent to Device on I/O Port 2 [N]
E. Strip Pass-through LFs received from Device on I/O Port 1 [N]
F. Strip Pass-through LFs received from Device on I/O Port 2 [N]
```

Escape Character - This is the ASCII value of the ESCAPE character used to exit Pass-Through mode. This value is required to be pressed three times in Pass-Through mode to escape this mode back to the main login menu.

Console Mode - This setting indicates whether the serial ports of the SNMP Access Gateway should be independent inputs or whether they should operate jointly as a transparent pass-through connection (what goes in one port comes out the other and vice versa) for inline transparent monitoring of alarm messages.

Strip Pass-through LFs - Settings C through F strip linefeeds being sent to or received from the devices connected to I/O's 1 and 2, respectively. Some devices were found that didn't tolerate linefeeds being sent to them. And sometimes, linefeeds being received from the devices were not tolerated by the telnet client being used. Therefore, these options have been added to handle these situations.

5.7.3 - Character Mask

Selecting the Menu Letter of this option presents the following submenu for setting the serial input character mask. By customizing this selection you can screen out specified characters from the serial input stream. The numbers shown in the display indicate the characters which are allowed, displayed as their ASCII values.

```
Setup: General Settings: Character Mask
          2  3                10          13
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79
80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95
96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111
112 113 114 115 116 117 118 119 120 121 122 123 124 125 126
```

```
A. Mask Enabled [Y]
B. Default Mask
C. Add a Character
D. Delete a Character
E. Enter Mask Specification
Selection?
```

Chapter 6 - Pass Through Mode

Pass-through mode may be accessed from a network connection. A user enters pass-through mode from the main menu by selecting either the '1' or '2' option. The '1' option provides pass-through access to serial port I/O 1, and the '2' option provides pass-through access to serial port I/O 2.

```
SNMP Access Gateway Model unit   Version 1.00
```

```
0. Enter Command Processor
1. Enter Pass-Through to Port 1
2. Enter Pass-Through to Port 2
X. Exit (end connection)
<user enters '1'>
```

```
Pass-Through Port 1 Password: ----- <user enters password>
Pass-Through Port 1 Password Accepted
Exit Pass-Through Mode by Entering ESC-ESC-ESC
```

A pass-through connection accepts characters on the network connection and passes those characters to the selected serial I/O port. Characters received on the serial I/O port are passed to the network connection.

When pass-through mode is entered, the escape character which may be used to exit pass-through mode is displayed. In the example shown above, the ESC (27) character is shown as the escape character. The escape character may be changed by using the SETUP command. When the escape character is entered on the network connection three times within three seconds, the SNMP Access Gateway exits the pass-through mode connection and returns the connection to the main menu.

When the escape character is entered the first and second times, the SNMP Access Gateway collects these characters and does not pass them on to the serial I/O port. After the third escape character is collected, the SNMP Access Gateway exits the pass-through connection. Thus, the escape characters are not passed through to the pass-through port when the escape sequence is used to exit the pass-through mode. However, if three seconds passes between escape characters, or if one or two escape characters are collected and then a character which is not the escape character is collected, then all collected characters are passed through to the serial I/O port. The escape character could then, for example, be changed to a capital letter 'X'. Then pass-through access to the serial I/O port could be terminated with three 'X' characters entered within three seconds, with no intervening characters. But use of a single or two 'X' characters in the pass-through command session would still result in the 'X' characters being passed through to the serial I/O port.

In the case where a user establishes a connection and selects an access port from the main menu and another user is already logged into the same serial I/O port for pass-through access, the new user is given the opportunity to join in the connection. Since the new user must have entered a valid password to access the port, a joining of the ports is allowed. In this case the message which the SNMP Access Gateway sends to the new participant is:

```
Pass-Through Port 1 Password: ----- <user enters password>
Pass-Through Port 1 Password Accepted
```

```
A Session with Port 1 is Already Established with:
    Network at IP 192.168.100.118
```

```
Do You Wish to Join the Session (Y/N) y
Session Joined.
```

After the user enters a letter, the SNMP Access Gateway either joins the connection or, if the user entered anything other than a 'Y', drops the user back into the main menu. If joining the connection, the SNMP Access Gateway provides a message to the user which shows what the escape character is.

If the connection is joined, then the user becomes an active participant in the connection.

In pass-through access mode, each character the user inputs by network connection is passed to the serial I/O port, and each character which is received by the serial I/O port is passed through to the network connection. During this time, the data from the port is NOT processed by the event and alarm evaluator, so no alarm records are detected during this pass-through access.

If more than one network connection is established for a serial I/O port (the 'join' has been used) then each character which is received from the serial I/O port is sent to each participant, and each character received from each participant is sent to each other participant and the serial I/O port. Joins may be used to observe the use of the pass-through mode by another user, for technical support or other purposes.

When joined, breaking a pass-through connection only affects the connection on which the escape sequence (or network or modem disconnection) was used. The other participants in the joined connection do not have their pass-through access terminated. When the last participant in a joined connection terminates the pass-through connection, then the serial I/O port reverts to the normal data collection mode automatically.

Pass-through access to serial I/O ports in console mode may also be made. See the section on console mode for more information on how pass-through connections are handled when the serial I/O ports are in console mode.

Chapter 7 - Console Mode

When the serial I/O ports are in console mode, characters which are received on one serial I/O port are sent out the other serial I/O port. This allows the SNMP Access Gateway to be placed in-line between two piece of equipment (such as a control console and a piece of equipment, hence the console mode name), and monitor the data flow between the devices for alarm conditions.

Console mode is enabled and disabled via the menus of the SETUP command, or by SNMP. By default console mode is not enabled.

When data is received from a serial I/O port while in console mode, the data is processed by the alarm evaluator as well as being passed to the other serial I/O port. Thus, the alarm evaluator can analyze the data flow from both serial I/O ports and log alarm events while simultaneously passing the data between the two serial I/O ports.

When a user attempts to establish a pass-through access to one of the serial I/O ports when the I/O ports are in console mode, the pass-through connection is allowed, as a joined connection. In this case characters which are received on the network connection are passed to the selected serial I/O port, and characters which are received on either of the serial I/O ports are passed to the network connection, in addition to being passed to the other serial I/O port. Thus, pass-through mode may be used to monitor the activities in console mode, and also provide the user with access to the equipment being controlled by the console. However, the characters received from the network connection are not processed by the alarm evaluator, so that they do not generate any alarm events.

Chapter 8 - Management Information Base (MIB)

The following illustrates the SL-60 MIB in tree format. The function of each of these objects is explained in the chapter following this one. This MIB is supplied on a disk with your unit in ASN.1 format. The various object Ids are listed out with their complete prefixes omitted. The full prefix to use with the following object Ids is shown below.

Omnitronix Private Enterprise MIB for SNMP Access Gateway
Prefix: 1.3.6.1.4.1.3052.2

1 - productIds

- 1.1 - snmplinkThisProduct
- 1.2 - thisTrapString

2 - productConfig

- 2.1 - productname
- 2.2 - systemversion
- 2.3 - appversion
- 2.4 - hardware
 - 2.4.1 - numberports
 - 2.4.2 - nets
 - 2.4.3 - modems
 - 2.4.4 - hardware sensors
 - 2.4.5 - hardware relays
- 2.5 - factorysetup
 - 2.5.1 - modemreport
 - 2.5.2 - modemportspeed
 - 2.5.3 - modemsetupstring
 - 2.5.4 - modemcddelay
 - 2.5.5 - modemtype
 - 2.5.6 - serialnumber
 - 2.5.7 - dateofmanufacture

3 - unitIds

- 3.1 - snmplinkSiteId

4 - serialPorts

- 4.1 - numberPorts
- 4.2 - portSetupTable
 - 4.2.1 - portSetupEntry
 - 4.2.1 - portIndex
 - 4.2.2 - portBaud
 - 4.2.3 - portWord
 - 4.2.4 - portParity
 - 4.2.5 - portStopbits

5 - time

- 5.1 - currenttime
- 5.2 - autoDstAdjust

6 - snmpsetup

- 6.1 - snmpTrapsEnabled
- 6.2 - snmpManagerTable
 - 6.2.1 - snmpTableEntry

- 6.2.1.1 - snmpMgrIndex
- 6.2.1.2 - snmpManagerIp
- 6.2.1.3 - snmpManagerName
- 6.3 - snmpTrapsAutoRepeatTime
- 6.4 - snmpSendTestTrap

7 - ftpsetup

- 7.1 - ftpAutoDelete

8 - events

- 8.1 - eventsControl
 - 8.1.1 - storeDataEvents
 - 8.1.2 - storeAlarmEvents
 - 8.1.3 - storeResetEvents
 - 8.1.4 - storeCommandLog
 - 8.1.5 - storeSensorEvents
- 8.2 - alarmEvaluator
- 8.3 - dataAlarmTable
 - 8.3.1 - dataAlarmEntry
 - 8.3.1.1 - dataAlarmIndex
 - 8.3.1.2 - dataAlarmActive
 - 8.3.1.3 - dataAlarmName
 - 8.3.1.4 - dataAlarmCounter
 - 8.3.1.5 - dataAlarmThreshold
 - 8.3.1.6 - dataAlarmClearMode
 - 8.3.1.7 - dataAlarmClearTime
 - 8.3.1.8 - dataAlarmAcked
 - 8.3.1.9 - dataAlarmBeeperActions
 - 8.3.1.10 - dataAlarmPagerActions
 - 8.3.1.11 - dataAlarmTrapActions
 - 8.3.1.12 - dataAlarmString
 - 8.3.1.13 - dataAlarmPort
 - 8.3.1.14 - dataAlarmAutoClear
- 4 - sensorAlarmTable
 - 4.1 - sensorAlarmEntry
 - 4.1.1 - sensorAlarmIndex
 - 4.1.2 - sensorAlarmActive
 - 4.1.3 - sensorAlarmName
 - 4.1.4 - sensorType
 - 4.1.5 - sensorAlarmMode
 - 4.1.6 - sensorRangeMin
 - 4.1.7 - sensorRangeMax
 - 4.1.8 - sensorAlarmState
 - 4.1.9 - sensorAlarmCounter
 - 4.1.10 - sensorAlarmThreshold
 - 4.1.11 - sensorAlarmAcked
 - 4.1.12 - sensorAlarmBeeperActions
 - 4.1.13 - sensorAlarmPagerActions
 - 4.1.14 - sensorAlarmTrapActions

9 - actions

- 9.1 - actionsBuzzer
 - 9.1.1 - actionsBuzzerState
- 9.2 - actionsPagerTable
 - 9.2.1 - actionsPagerTableEntry

- 9.2.1.1 - pagerTableIndex
- 9.2.1.2 - pagerType
- 9.2.1.3 - pagerPhonenumber
- 9.2.1.4 - pagerID
- 9.2.1.5 - pagerDialDelay
- 9.2.1.6 - pagerHangupDelay
- 9.2.1.7 - pagerMessage
- 9.2.1.8 - pagerSendId
- 9.2.1.9 - pagerSendReason
- 9.2.1.10 - pagerMaxAttempts
- 9.2.1.11 - pagerAttempts
- 9.2.1.12 - pagerAttemptDelay
- 9.2.1.13 - pagerRepeat
- 9.2.1.14 - pagerRepeatDelay
- 9.3 - actionsTraps
 - 9.3.1 - actionsTrapsEntSpecific
 - 9.3.2 - trapFormat
 - 9.3.2.1 - trapDateTime
 - 9.3.2.2 - trapAlarmType
 - 9.3.2.3 - trapAlarmName
 - 9.3.2.4 - trapAlarmID
 - 9.3.2.5 - trapAlarmString
 - 9.3.3 - actionsTrapsEntSpecCount

10 - relays

- 10.1 - numberRelays
- 10.2 - relaysTable
 - 10.2.1 - relaysTableEntry
 - 10.2.1.1 - relaysTableIndex
 - 10.2.1.2 - relaysTableName
 - 10.2.1.3 - relaysTableMode
 - 10.2.1.4 - relaysTableState
 - 10.2.1.5 - relaysTableResetState

11 - controls

- 11.1 - opSettings
 - 11.1.1 - consoleMode
 - 11.1.2 - charmask
- 11.2 - modemSettings
 - 11.2.1 - modemParity
 - 11.2.2 - modemTapSetup
 - 11.2.3 - modemInactivityTimer
 - 11.2.4 - modemTimeBetweenOutbound
- 11.3 - passThrough
 - 11.3.1 - ptconn1
 - 11.3.2 - ptconn2
- 11.4 - connections
 - 11.4.1 - connectionsTable
 - 11.4.1.1 - connectionsTableEntry
 - 11.4.1.1.1 - connectionsTableIndex
 - 11.4.1.1.2 - connectionsState
 - 11.4.1.1.3 - connectionsMode
 - 11.4.1.1.4 - connectionsAddress
 - 11.4.1.2 - connectionsCmdActive
 - 11.4.1.3 - connectionsCmdConn
 - 11.4.1.4 - connctionsEndchar

11.4.1.5 - connectionsPTTimelimit

12 - alarmhistory

- 12.1 - actionQueue
 - 12.1.1 - actionCount
 - 12.1.2 - actionTable
 - 12.1.2.1 - actionTableEntry
 - 12.1.2.1.1 - actionTableIndex
 - 12.1.2.1.2 - actionAked
 - 12.1.2.1.3 - actionReason
 - 12.1.2.1.4 - actionReasonID
 - 12.1.2.1.5 - actionReasonLevel
 - 12.1.2.1.6 - actionType
 - 12.1.2.1.7 - actionTypeID
 - 12.1.2.1.8 - actionRepeatTime
 - 12.1.2.1.9 - actionAttempts
 - 12.1.2.1.10 - actionNextAttempt
 - 12.1.2.1.11 - actionTimeStamp
- 12.2 - actionHistory
 - 12.2.1 - historyCount
 - 12.2.2 - historyTable
 - 12.2.2.1 - historyTableEntry
 - 12.2.2.1.1 - historyTableIndex
 - 12.2.2.1.2 - historyEntryType
 - 12.2.2.1.3 - historyReason
 - 12.2.2.1.4 - historyReasonID
 - 12.2.2.1.5 - historyReasonLevel
 - 12.2.2.1.6 - historyType
 - 12.2.2.1.7 - historyTypeID
 - 12.2.2.1.8 - historyTimeStamp
 - 12.2.2.1.9 - historyClearLog

13 - iprestrictions

- 13.1 - iprestrictTable
 - 13.1.1 - iprestrictTableEntry
 - 13.1.1.1 - iprestrictTableIndex
 - 13.1.1.2 - iprestrictIpAddress

99 - techsupport

- 99.1 - techsupportInt1
- 99.2 - techsupportInt2
- 99.3 - techsupportInt3
- 99.4 - techsupportInt4
- 99.5 - techsupportInt5

snmplinkMainTrap TRAP-TYPE
 ENTERPRISE snmplinkThisProduct
 VARIABLES { thisTrapString }
 DESCRIPTION

“An snmplinkMainTrap is issued when a sensor or data alarm trap is to be issued. The thisTrapString contains a string formatted using the trap format controls. The string may contain a data alarm record if the trap is a data alarm trap.”

::= 10

Chapter 9 - SNMP Configuration and Control

The following section describes in detail the contents of the custom SNMP Access Gateway MIB, including notes about how these MIB object may be used.

9.1 - productIds	Items in this section are either factory-configured or read-only.
snmplinkThisProduct	This is a text string with the product name.
thisTrapString	This string is used in traps, and the contents of this string contain the trap alarm type, name, index number, and alarm string, as configured by the trap format variables.
productConfig	Items in this section are all factory-configured.
productname	This is a text string with the product name.
systemversion	This integer is the version of the 'system' section of the SNMP Access Gateway firmware.
appversion	This text string is the version of the 'application' section of the SNMP Access Gateway firmware. It will usually have a format of V1.00, V1.01, etc.
hardware:numberports	This integer is the number of serial ports found. In the standard SNMP Access Gateway this will be 2.
hardware:nets	This integer is the number of network interfaces found. In the standard SNMP Access Gateway this will be 1.
hardware:modems	This integer is the number of modem ports found. If the optional internal modem is installed, this will be 1, otherwise it will be 0.
factorysetup:modemreport	This is the text string reported in the status display to show the type of modem installed.
factorysetup:modemportspeed	This is the baud rate used when communicating with the internal modem
factorysetup:modemsetupstring	This text string is the modem setup string used with the internal modem. It may be factory-customized for use with different internal modems.
factorysetup:cddelay	This integer is the number of seconds the SNMP Access Gateway waits after sensing an activation of carrier from the modem before recognizing the availability of the internal modem. This is used to avoid transmitting data to the internal modem before it is actually ready for the data, which can cause the modem to auto-disconnect or miss transmitting the data.
factorysetup:modemtype	This integer is a factory-assigned modem type number to track the type of modem installed in the SNMP Access Gateway.
factorysetup:serialnumber	This is a factory-assigned serial number assigned to this SNMP Access Gateway unit at final testing and configuration time.
factorysetup:dateofmanufacture	This text string is a factory-assigned date of manufacture assigned to this SNMP Access Gateway unit at final testing and configuration time.
9.2 - unitIds	This section contains objects for the user-configurable identification of a particular SNMP Access Gateway unit. Only one object is contained in this section.
snmplinkSiteId	This text string is user configured to indicate the installation site or identification of a particular SNMP Access Gateway unit.
9.3 - serialPorts	

numberPorts	This integer is the number of serial ports found installed in the SNMP Access Gateway unit. For the standard SNMP Access Gateway this will be 2.
portSetupTable	This table is used to retrieve and set the serial port settings, for the baud rate, word length and parity. This table is indexed by the serial I/O port number (i.e., 1 or 2 for the standard SNMP Access Gateway unit).
portSetupTable:portBaud	This integer is the baud rate of the port. Valid entries are 300, 600, 1200, 2400, 4800, 9600 and 19200 baud.
portSetupTable:portWord	This integer is the word length of the port. Valid entries are 7 or 8 bit word lengths.
portSetupTable:portParity	This single-character text string is the parity of the port. Valid entries are 'N' for no parity, 'E' for even parity and 'O' for odd parity.
portSetupTable:portStopbits	This integer is the number of stop bits for the port. It is always 1.
9.4 - Time	
currenttime	This text string is the current date and time of the SNMP Access Gateway clock. This read-write variable may be used to retrieve or set the system clock.
autoDstAdjust	This integer controls the automatic adjustment of the system clock for daylight savings time. If enabled, the clock is advanced one hour at 2:00 a.m. on the first Sunday in April, and turned back an hour at 2:00 a.m. on the last Sunday in October.
9.5 - snmpsetup	
snmpTrapsEnabled	This integer enables the SNMP Access Gateway to send traps. If disabled, no traps are sent by the SNMP Access Gateway. To use the trap transmission features of the SNMP Access Gateway this object should be set to 1.
snmpManagerTable	This table contains the IP addresses and optional names of SNMP managers to which the SNMP Access Gateway will send traps.
snmpManagerTable:snmpManagerIp	This IP Address is the IP address of an SNMP manager to which the SNMP Access Gateway may send traps. If the entry is not valid, it contains 0.0.0.0 as the IP address. In order for the SNMP Access Gateway to send traps to an SNMP manager, the IP address of the manager must be set in this table.
snmpManagerTable:snmpManagerName	This text string is an optional text description of the name of the SNMP manager. It is not used by the SNMP Access Gateway in transmitting traps, but may be used to keep a name associated with the IP address of an SNMP manager.
snmpTrapsAutoRepeatTime	This integer is the number of minutes between repeated transmissions of the same trap, due to an event which requires a trap to be sent. This timer is only active on enterprise-specific traps, it does not affect the transmission of the cold-start or warm-start standard traps. If this integer is set to 0, then traps are sent once and not repeated. In an environment where repetitions of traps is not desired, this object should be set to 0. If set to a value between 1 and 255, then enterprise-specific traps are repeated at the interval described by this object.

snmpSendTestTrap	When this object is set to any value, then the SNMP Access Gateway sends a 'test' trap by sending a trap to all of the managers in the snmpManagerTable. This test trap may be used to assure that the proper SNMP managers are set up in the smpManagerTable, and that each manager is properly responding to traps.
9.6 - ftpsetup	
ftpAutoDelete	This object controls the auto deletion of the events log file when it is retrieved by FTP. When set to 0, the file is not automatically deleted. When set to 1, the events file entries which were retrieved by FTP are automatically deleted from the events log file as the data is retrieved by FTP.
9.7 - events	
storeDataEvents	The events section of the MIB is used to control which events are stored in the events log file, provide status information on the configuration of the data alarms, enable the processing of data alarms, retrieve and set the sensor alarm configuration.
storeAlarmEvents	This object, when set to 1, allows all data records received on the serial I/O ports to be stored as events. This object can be enabled to store all data records in the events log file. The storage of all data records which are received would be most useful when each data record received by the SNMP Access Gateway is an alarm record, a no data alarm processing is performed by the SNMP Access Gateway.
storeResetEvents	This object, when set to 1, allows all data alarm records to be stored in the events log file. A received data record is determined to be a data alarm record if the alarm evaluator determines that the data record matches any of the defined alarm criteria, regardless of the count of such data alarm records received.
storeCommandLog	This object, when set to 1, allows all resets from any source to be stored as events in the events log file. This may be useful in detecting power outages which might affect the operation of the SNMP Access Gateway or other equipment.
storeSensorEvents	This object, when set to 1, allows all command lines entered at the command processor to be stored in the events log file. This allows a system administrator to examine the usage of the commands.
alarmEvaluator	This object, when set to 1, allows all sensor activation and in-activation events to be stored in the events log.
dataAlarmTable	This object enables and disables the alarm evaluator. When set to 0, no alarm evaluation is performed on data records, so no data alarm records are stored in the events file, and no data alarms are activated. When set to 1, the alarm evaluator is used to detect data alarm records and sense when data alarm events must be performed.
dataAlarmActive	This table provides retrievable information on the status and configuration of the data alarms. The data alarms are configured using an alarms configuration file, so objects in the dataAlarmTable are read-only. The number of table entries provided is equal to the number of defined data alarms in the alarms configuration file.
	This object shows that a particular data alarm is active. This object always reads as 1

dataAlarmName	This object is a text string which is the name associated with the data alarm, as defined in the alarms configuration file.
dataAlarmCounter	This integer is the current count of received alarm records which match the data alarm equation corresponding to this data alarm. This counter is reset at some pre-determined time interval, as determined by the dataAlarmClearMode and dataAlarmClearTime. The counter counts up as data alarm records are detected which match the corresponding data alarm equation. When the dataAlarmThreshold is reached, the data alarm actions are performed and the dataAlarmCounter is also reset.
dataAlarmThreshold	When a data record is received and matches the data alarm equation corresponding to this data alarm, and the dataAlarmCounter is incremented and now is equal to the dataAlarmThreshold, then the data alarm actions are taken.
dataAlarmClearMode	This integer represents the frequency of clearing of the dataAlarmCounter. Accepted values are 0 - every hour, 1 - every 2 hours, 2 - every 4 hours, 3 - every 6 hours, 4 - every 8 hours, 5 - every 12 hours, 6 - every 24 hours (daily) and 8 - cleared daily, but at a specified time (this time is specified in the dataAlarmClearTime object).
dataAlarmClearTime	This text string holds a time (e.g., '01:20') at which the dataAlarmCounter is cleared each day if the dataAlarmClearMode is set to 8.
dataAlarmAcked	Setting this object to any value acknowledges the data alarm actions associated with the current activity of this data alarm, which stops the repetitions of traps and pager actions, and silences the buzzer if this data alarm is the reason why the buzzer is active. This is the only read-write object in this section of the MIB.
dataAlarmBeeperActions	This object indicates the buzzer (audible alarm) actions associated with this data alarm. The object value may be 0 - no action, 1 - beep once every 10 seconds or 2 - beep continuously.
dataAlarmPagerActions	This object shows which pagers are to be paged when the actions associated with the data alarm are activated. Each bit in this integer is assigned to one of the pagers 1-8. Bit 0 (value of 1) is assigned to pager 1, bit 1 (value of 2) is assigned to pager 2, etc. If a bit in the dataAlarmPagerActions integer is cleared, then that pager is not activated by this data alarm. If a bit in the dataAlarmPagerActions is set, then that pager is activated by this data alarm.
dataAlarmTrapActions	This object shows which SNMP managers are sent traps when the actions associated with the data alarm are activated. Each bit in this integer is assigned to one of the SNMP managers 1-8. Bit 0 (value of 1) is assigned to SNMP manager 1, bit 1 (value of 2) is assigned to SNMP manager 2, etc. If a bit in the dataAlarmTrapActions integer is cleared, then that SNMP manager is not sent a trap based on this data alarm. If a bit in the dataAlarmTrapActions is set, then that SNMP manager is sent a trap based on this data alarm.

dataAlarmString	This text string object contains the last data record which was received which matched the data alarm equation associated with this data alarm. Since data records may be received after a data alarm initiates its actions, retrieval of this object after a data alarm is activated may not result in the retrieval of the data record which activated the data alarm. However, this object will contain the last data record which was received which did match the alarm equation associated with this data alarm.
dataAlarmPort	This integer object contains the serial I/O port number upon which the text string contained in the dataAlarmString was received.
sensorAlarmTable	This table contains the configuration objects for the sensor alarms. This table always has as many entries as there are sensors available to configure in the SNMP Access Gateway.
sensorAlarmActive	When this object is set to a value of 0, the associated sensor is not enabled for activating alarms. When this object is set to a value of 1, the associated sensor is enabled for activating alarms.
sensorAlarmName	This text string object holds a name associated with this sensor alarm.
sensorType	When this integer object is set to a value of 0, the sensor is processed as a contact closure sensor, with states of Opened and Closed. The sensor is normally opened, and is treated as closed when the sensor contact is connected to ground. When this object is set to a value of 1, the sensor is processed as an analog voltage sensor. In this case the sensor takes on values from 0-255, when the analog input voltage goes from 0 to 5 volts.
sensorAlarmMode	This integer object controls the mode of activation of the sensor. When the sensorType is 0 (a contact closure sensor) then the sensorAlarmMode may be set by the user to values of 0 (active when contact is opened) or 1 (active when contact is closed). When the sensorType is 1 (analog sensor) then the sensorAlarmMode may be set by the user to values of 0 (active when voltage drops below normal range minimum), 1 (active when voltage goes above normal range maximum) and 2 (active when voltage goes outside of normal range). The current sensor state is then reflected in sensorAlarmState.
sensorRangeMin	This integer is the minimum A/D value for the 'normal' operating range for the sensor attached to an analog input. For an analog sensor alarm which is triggered by dropping below the minimum A/D value the sensorRangeMin object sets the A/D value under which the voltage must drop.
sensorRangeMax	This integer is the maximum A/D value for the 'normal' operating range for the sensor attached to an analog input. For an analog sensor alarm which is triggered by exceeding the maximum A/D value the sensorRangeMax object sets the A/D value which the voltage must exceed.
sensorAlarmState	The sensorAlarmState object is a read-only object which holds the current state of the sensor (opened or closed when in contact closure mode, or the current A/D value being read if in analog mode).

sensorAlarmCounter	This read-only object holds the number of seconds that the sensor alarm has been in its active state. For a contact closure input this counter is the number of seconds that the contact closure has been sensed in the (opened or closed) active state. For an analog sensor this counter is the number of seconds that the sensor has been in the (overmax, undermin, outsidersrange) active state.
sensorAlarmThreshold	This object holds the number of seconds that the sensor alarm must be in the active state to trigger the sensor alarm actions.
sensorAlarmAcked	This object, when set to any value, acknowledges the active state of this sensor alarm, and stops the repeating of any traps or pager actions, and turns off the buzzer if the buzzer activation is based on the active state of this sensor.
sensorAlarmBeeperActions	This object indicates the buzzer (audible alarm) actions associated with this sensor alarm. The object value may be 0 - no action, 1 - beep once every 10 seconds or 2 - beep continuously.
sensorAlarmPagerActions	This object shows which pagers are to be paged when the actions associated with this sensor alarm are activated. Each bit in this integer is assigned to one of the pagers 1-8. Bit 0 (value of 1) is assigned to pager 1, bit 1 (value of 2) is assigned to pager 2, etc. If a bit in the sensorAlarmPagerActions integer is cleared, then that pager is not activated by this sensor alarm. If a bit in the sensorAlarmPagerActions is set, then that pager is activated by this sensor alarm.
sensorAlarmTrapActions	This object shows which SNMP managers are sent traps when the actions associated with this sensor alarm are activated. Each bit in this integer is assigned to one of the SNMP managers 1-8. Bit 0 (value of 1) is assigned to SNMP manager 1, bit 1 (value of 2) is assigned to SNMP manager 2, etc. If a bit in the sensorAlarmTrapActions integer is cleared, then that SNMP manager is not sent a trap based on this sensor alarm. If a bit in the sensorAlarmTrapActions is set, then that SNMP manager is sent a trap based on this sensor alarm.
9.8 - actions	
actionsBuzzerState	This object holds the current operating state of the buzzer. Values for this object may be 0 - no buzzer action, 1 - buzzer active one second out of each 10 seconds, 2 - buzzer on continuously.
actionsPagerTable	This table holds the settings for the 8 pagers. Each pager may have a different phone number, pagerID, etc., so that a combination of pagers may be used to manage the alarms generated by the SNMP Access Gateway.
pagerType	The pager may be either an alphanumeric pager, or a numeric pager. If the pager is numeric, this object should be set to a value of 0, if the pager is alphanumeric this object should be set to a value of 1.
pagerPhonenumber	This text string is the phone number what is dialed to reach the paging service.
sensor pagerID	When the pager is alphanumeric, the pagerID is a text string which must match the pager ID as assigned by the pager company. When the pager is a numeric pager, the pagerID is the second number sequence which is sent, to activate the page.

pagerDialDelay	This integer is the number of seconds that the SNMP Access Gateway waits for modem carrier after dialing the pagerPhonenumber when the pager is in alphanumeric mode, or the number of seconds the SNMP Access Gateway waits after dialing the pagerPhonenumber to transmit the pagerID when in numeric mode.
pagerHangupDelay	This integer is the number of seconds the SNMP Access Gateway waits before hanging up the modem after transmitting the pagerID or pagerMessage when in numeric pager mode.
pagerMessage	This text object is a text message transmitted to an alphanumeric pager by the SNMP Access Gateway, or a second pager message which is transmitted by the SNMP Access Gateway when in numeric mode.
pagerSendId	When this integer object is set to 0, the SNMP Access Gateway does not transmit the unitId to the alphanumeric pager, and when set to 1 the SNMP Access Gateway does transmit the unitId to the alphanumeric pager when performing an alphanumeric page
pagerSendReason	When this integer object is set to 0, the SNMP Access Gateway does not transmit the reason for the pager to the alphanumeric pager, and when set to 1 the SNMP Access Gateway does transmit the reason for the page to the alphanumeric pager when performing an alphanumeric page.
pagerMaxAttempts	This integer is the maximum number of pager attempts which are allowed before the pager action is automatically retried. If set to 0, then the pager action is never automatically retried.
pagerAttempts	This integer is the number of pager attempts which have been made for this pager.
pagerAttemptDelay	This integer holds the number of minutes which must expire before the pager action will again be attempted.
pagerRepeat	This object controls if a successful page is repeated at some time interval, to ensure that the alarm is serviced. When set to 0, no pager repeats are performed for this pager. When set to 1, pager repeats are performed for this pager. These repeats only are done on a successful pager action.
pagerRepeatDelay	This integer controls the number of minutes which must pass after a successful page before the page is repeated, when pager repeat mode is active.
9.9 - actionsTraps	The actionsTraps section of the MIB controls enterprise-specific traps sent by the SNMP Access Gateway, and the format of these traps.
trapDateTime	When the trapDateTime object is set to 0, then the date and time of the activation of the alarm which caused the trap to be issued are not included in the trap alarm string. When the trapDateTime object is set to 1, then the date and time of the activation of the alarm which caused the trap to be issued are included in the trap alarm string.
trapAlarmType	When the trapAlarmType object is set to 0, then the type of alarm (sensor, data alarm) which caused the trap to be issued is not included in the trap alarm string. When the trapAlarmType object is set to 1, then the type of alarm which caused the trap to be issued is included in the trap alarm string.

trapAlarmName	When the trapAlarmName object is set to 0, then the name associated with the alarm (sensor, data alarm) which caused the trap to be issued is not included in the trap alarm string. When the trapAlarmName object is set to 1, then the name associated with the alarm which caused the trap to be issued is included in the trap alarm string.
trapAlarmID	When the trapAlarmID object is set to 0, then the identifier number for the of alarm (sensor, data alarm) which caused the trap to be issued is not included in the trap alarm string. When the trapAlarmID object is set to 1, then the identifier number for the alarm which caused the trap to be issued is included in the trap alarm string.
trapAlarmString	When the trapAlarmString object is set to 0, then the alarm string associated with the alarm (for a data alarm, this is the alarm record) is not included in the trap alarm string. When the trapAlarmType object is set to 1, then the type of alarm which caused the trap to be issued is included in the trap alarm string.
actionsTrapsEntSpecCount	This integer is the number of enterprise-specific traps which have been sent by the SNMP Access Gateway since its last reset.
9.10 - Relays	
numberRelays	This integer is the number of controllable relays which the SNMP Access Gateway has installed.
RelaysTable	This table is used to retrieve and set the operating modes for the relays.
relaysTableName	This text string holds a name which is associated with this relay.
relaysTableMode	This integer controls the operating mode of the relay. Valid settings are 0 - command-controlled mode, 1 - sensor-controlled mode, and 2 - anyalarm-controlled mode.
relaysTableState	This integer is used to retrieve the current relay state and open and close the relays when they are in sensor-controlled mode. When this object has a value of 0, the relay is opened. Setting the value of this object to 0, when in command-controlled mode, opens the relay. When this object has a value of 1, the relay is closed. Setting the value of this object to 1, when in command-controlled mode, closes the relay.
relaysTableResetState	This integer controls the state into which the relay is placed when the SNMP Access Gateway is reset. This may be used to ensure that a relay powers up in the proper state. Another use for this may be to have a management station field a trap from the SNMP Access Gateway indicative of an alarm, close the relay using the relaysTableState object, and then set the relaysTableResetState object to the same value as that of the relaysTableState, to ensure that if the SNMP Access Gateway is reset the relay will still maintain its state.
9.11 - Controls	
consoleMode	This integer object controls if console mode is enabled or not. When set to 0, console mode is disabled. When set to 1, console mode is enabled.
charmask	The charmask holds a text string which is an ASCII HEX representation of the character masking which is performed on incoming characters.

modemParity	This integer controls the parity of the modem port. Values are 1 - 7 bits, even parity, 2 - 7 bits, odd parity, and 3 - 8 bits, no parity. The value of 3 would normally be used with the SNMP Access Gateway.
modemTapSetup	This text string is sent to the modem when executing the TAP (alphanumeric) paging protocol. This string may be used to custom-configure the dialing settings of the modem to ensure successful alphanumeric paging.
modemInactivityTimer	This integer object controls the number of minutes that the SNMP Access Gateway waits during an idle modem connection before automatically closing the modem connection.
modemTimeBetweenOutbound	This integer object controls the number of seconds that the SNMP Access Gateway waits between outbound call uses of the modem. Normally this is set to 60 seconds. This timer ensures that some intervening time exists between modem outbound calls, so that attempts to connect to the SNMP Access Gateway by modem have a chance of making a connection.
ptconn1	This read-only integer indicates the current connection status of any pass-through connections to serial I/O port 1. One bit of this integer is used for each possible connection. The three network connections are assigned bit positions 0, 1 and 2, with values of 1, 2 and 4, respectively. The modem connection is assigned bit 3, with a value of 8. The serial I/O port 1 (for a joined connection) is assigned bit 4, with a value of 16, and serial I/O port 2 if assigned bit 5, with a value of 32. A bit is set if that connection has an active pass-through (or join) connection with serial I/O port 1, and is otherwise cleared.
ptconn2	This read-only integer indicates the current connection status of any pass-through connections to serial I/O port 2. One bit of this integer is used for each possible connection. The three network connections are assigned bit positions 0, 1 and 2, with values of 1, 2 and 4, respectively. The modem connection is assigned bit 3, with a value of 8. The serial I/O port 1 (for a joined connection) is assigned bit 4, with a value of 16, and serial I/O port 2 if assigned bit 5, with a value of 32. A bit is set if that connection has an active pass-through (or join) connection with serial I/O port 2, and is otherwise cleared.
9.12 - ConnectionsTable	The connectionsTable provides status information on the network and modem connections to the SNMP Access Gateway.
connectionsTableState	This integer indicates what state this connection is in. The states are 0 - waiting for a connection, 1 - sending the main menu, 2 - getting a menu item selection, 3 - unused, 4 - sending password prompt, 5 - collecting a password, 6 - doing command processor actions, 7 - doing pass-through actions, 8 - dropping the connection, 9 - disconnecting, and 10 waiting after carrier for a modem connection.
connectionsMode	This integer shows what connection mode the connection is in. 0 - command connection, 1 - pass-through to port 1, 2 - pass-through to port 2.

connectionsAddress	This object holds the IP address of the remote end of a connection. If the connection is a modem connection, this will show in the object as 0.0.0.0.
connectionsCmdActive	This object shows if any command connection is active. When this object is 0, no command processor session is active. When set to 1, some command processor connection session is active.
connectionsCmdConn	This object shows the connection number (1-3 are network connections, 4 is the modem connection and 5 is a the local command port) for an ongoing command processor session.
connectionsEndchar	This object holds the character which acts as the escape character for ending pass-through connections and initiating a local command port command session.
connectionsPTTimelimit	This object controls the number minutes the SNMP Access Gateway waits during an idle pass-through connection before automatically terminating the connection to due to lack of activity.
9.13 - Alarmhistory	The alarmhistory section of the MIB provides information on the currently active alarm actions, and the history log of actions which have been taken by the SNMP Access Gateway.
actionCount	This integer holds the count of active action entries in the action queue.
actionAcked	This object, when set to any value, acknowledges the active alarm action, removing the alarm action from the alarm action queue.
actionReason	This object contains an integer which indicates the reason for the alarm action.
actionReasonID	This integer object contains an identifier for which alarm reason (e.g., data alarm 3 vs. data alarm 4) was the source for the alarm action.
actionReasonLevel	If more than one alarm level is associated with an alarm, this object can report the level of the alarm. In the SNMP Access Gateway, this will always be 1.
actionType	This integer value indicates the type of action which will be performed.
actionTypeID	This integer object holds the identifier of which pager is to be used, which management stations are to receive traps, or which buzzer level is to be activated.
actionRepeatTime	This integer object holds a counter for the number of minutes left until the next repeated attempt to perform this alarm action.
actionAttempts	This integer holds a counter of the number of attempts which have been performed for this alarm action.
actionNextAttempt	This integer holds a counter of the number of minutes until the next attempt of this action, where a repeated action which was successful or another attempt of the action when it was not successful.
actionTimeStamp	This text string object holds the date and time of the sensing of the alarm which is causing this alarm action to be performed.
historyCount	This integer object holds the number of entries in the action history table.
historyEntryType	This integer object indicates the type of history entry (e.g., pager OK, pager FAIL, etc.).
historyReason	This integer object indicates the reason why the action was taken, as is shown in the actionReason object.

historyReasonID	This integer object indicates the identifier for the reason why the action was taken as shown in the actionReasonID object.
historyReasonLevel	This integer object indicates the alarm level for the reason why the action was taken as shown in the actionReasonLevel object.
historyType	This integer object indicates the type of action which is logged in the history log table (e.g., pager, trap, etc.).
historyTypeID	This integer object indicates the which of the historyType objects was used in relation to this history log entry.
historyTimeStamp	This text string contains the date and time at which the history log entry was made.
historyClearLog	When this integer object is set to any value, the history log entries are all cleared.
9.14 - IPRestrictions	This section of the MIB contains IP access restriction entries.
iprestrictIpAddress	Each IpAddress type entry in this table contains an IP restriction. See the section on network setup and IP restrictions on more information on using the IP restriction table.
9.15 - Tech Support	The techsupport section of the MIB contains objects which are used for technical support of the SNMP Access Gateway. These objects should not be set by the user. Contents of these objects when retrieved are not defined for public use. These objects will read with integer values, which allows these objects to be read by SNMP managers.
	<pre> 99 techsupport 1 techsupportInt1 2 techsupportInt2 3 techsupportInt3 4 techsupportInt4 5 techsupportInt5 </pre>

Chapter 10 - Using FTP

The SNMP Access Gateway contains an FTP server which may be used with TCP/IP FTP client software. The FTP server may be used to retrieve or delete the events log file, load or retrieve the alarms configuration file, load a settings file, and load new application software into the SNMP Access Gateway.

The FTP server requires the use of a User ID and password to log into the server. The User ID is collected but not presently used. The password must match the FTP server password, which may be changed using the SETUP command menus.

The FTP server supports the DIR command, which indicates the events log file exists and the number of records in the events log file. The FTP Get and Delete commands may be used with the events log file, using the filename of EVENTS. Thus, GET EVENTS will retrieve the current contents of the events log file.

The alarms configuration file does not show up in the directory listing via the FTP server. However, the alarms configuration file may be loaded into the SNMP Access Gateway and retrieved from the SNMP Access Gateway using the filename of 'ALMFILE'.

A settings file contains pseudo-SNMP set instructions and may also contain the contents of an alarm configuration file. A settings file may be loaded into the SNMP Access Gateway using the filename of 'SETTINGS'.

A new software application may be loaded into the SNMP Access Gateway by loading a file named 'NEWAPP' into the SNMP Access Gateway. Only an application program file made available by RFL should ever be loaded into the SNMP Access Gateway as an application file. Other files will not properly execute, and will thus result in the SNMP Access Gateway simply entering load mode, awaiting the loading of a valid application.

Chapter 11 - Programming Data Alarms

Data Alarms (or Alarm Formulas) are formulas set up to define what record(s) constitute an alarm condition. Alarm Formulas can be defined to activate upon the receipt of a single record, or only after X number of matching records have been received within X duration.

A Data Alarm defines a record pattern to watch for in incoming data received by the SNMP Access Gateway. A good example of a data alarm would be to watch PBX SMDR records for any call with 900 in the area code or 976 in the prefix. When the SNMP Access Gateway receives an a matching record, the assigned action(s) for that alarm can be taken.

11.1 - Alarms are the same as Events

An 'Event' is an occurrence which the SNMP is designed to monitor and log, and on which in some cases a notification action occurs. The word Event is used in some places in the manual and in other places the word Alarm is used. Some circumstances which are Events are not strictly speaking Alarms. For example, an SNMP Access Gateway reboot occurrence is logged in the Events Log. However, in most cases the terms Event and Alarm can be used interchangeably.

11.2 - Alarm Actions

The SNMP Access Gateway supports the definition of up to 8 pager definitions and up to 8 SNMP Managers for trap addresses, plus 2 Buzzer tones. Each of these is considered an 'Action' for a total of 18 possible actions which can be assigned to any individual alarm event. For example, one single Toll-Fraud alarm (someone made a call to 976-GIRL) can be set to call 6 pagers and send Data Alarm traps to 3 SNMP Managers, and to beep the SNMP Access Gateway beeper also.

11.3 - How Data Alarms Are Set Up

All settings of the SNMP Access Gateway can be entered manually using a terminal connected to the SNMP Access Gateway, with the exception of Data Alarms . Data Alarms are written into a text file as defined below and then uploaded into the SNMP Access Gateway. Two methods are provided to upload an alarm file to the SNMP Access Gateway.

Once a file has been created in accordance with the guidelines below, it can be uploaded into the SNMP Access Gateway over a modem using an Xmodem Protocol by selecting the Upload a New Alarm File found under Event Definitions, or by using FTP over the TCP/IP connection, as further explained in the section Using FTP.

This same alarm file, once uploaded, can be viewed using the View Alarm File option found under Event Definitions in the Setup Menu.

11.4 - Defining Data Alarms

The SNMP Access Gateway has a setup within the uploadable text file which looks similar to Windows INI file. In this text file the field names and positions to be used in the alarm formulas are defined. Once fields are defined, the alarm formulas and parameters for each alarm are individually defined. A sample alarm text file is shown below:

```
[fields]
outext=12,6
inext=18,6
outtrunk=18,7
intrunk=12,7
date=38,5
time=44,5
duration=50,8
phone=63,7
onefield=63,1
```

```

areacode=64,3
localprefix=63,3
anyphrase=*,10

[macros]
Outgoing=
Incoming=intrunk="DN===="
LongDistance=onefield="1"

[dataalarms]
TollFraud1=all,1,P12B1S3C1256,2Hours
TollFraud1_1= areacode="900" or (longdistance=FALSE and localprefix="976")
TollFraud2=12,20,T12,1Hours
TollFraud2_1=Outgoing=FALSE and duration<"00:00:01"

[end]

```

This sample alarm text file shows the definition of Fields, Macros, and Data Alarms. In all cases, the above text entry is not case sensitive, except for the literal text specified for record matching (if you say `xyz="cat"` it will not match `xyz="CAT"`).

11.5 - Field Section

The above field definitions were designed for some sample SL1 CDR records. Field definitions must be the first section in the definition text file. The field definition section starts with the definition header [fields]. After the field definition header comes all the field definitions. Up to 30 fields can be defined. The syntax for a field definition is:

```
fieldname = startpos , length
```

Fieldname is whatever you want to call that field. Only the first 12 characters of the field name are significant. *Startpos* is the starting character position for the field (with the first character of the record considered to be 1). *Length* is the length of the field specified. If an asterisk is placed in the *startpos* entry then use of the field will result in the record being searched for a match in any position of the record. Examples:

```
Field1=30,5      (Field1 starts at position 30 and ends at position 34)
Field2=*,5      (Field2 is 5 characters long and a match anywhere in the record will be valid)
```

11.6 - Operators for Formulas

Valid operators for use in writing formulas are:

Operator	Definition
>	Greater Than
<	Less Than
>=	Greater Than or Equal To
<=	Less Than or Equal To
! or <>	Not Equal To
=	Equal To
=	Wildcard (note this wildcard character is intended to be changed later to *)
()	(Parenthesis) Used to Combine Operations
OR	Logical OR
AND	Logical AND

11.7 - Macro Section

Macros are similar to alarm formulas, in that they are designed to test conditions against an incoming record. Before the evaluation of any alarm formulas, all defined macros are evaluated against the incoming record, resulting in a TRUE or FALSE evaluation of each macro. Macro definitions which are referenced in alarm formulas then use the TRUE or FALSE results of those tests to evaluate if an alarm has occurred. Macros eliminate the need to retest for the same conditions more than once.

Macro definitions, if used, must be the second section in the definition text file. The macro definition section starts with the definition header [macros]. After the macro definition header comes all the macro definitions. Up to 30 macros can be defined. The syntax for a macro definition is:

```
macroname = formula
```

The *macroname* is the name you want to use to reference this macro condition in later formulas. The *formula* is the formula which defines the condition being tested for.

So, how are macros used? If you wanted several alarms which tested for a group of identical conditions, your formulas might look like:

```
Alarm1_e=(ext="103" OR ext="107" OR ext="111" OR ext="114" OR ext="116" OR
ext="121" OR ext="133" OR ext="140" OR ext="145" OR ext="167") AND
(localprefix="976" or areacode="900")
Alarm2_e=( ext="103" OR ext="107" OR ext="111" OR ext="114" OR ext="116" OR
ext="121" OR ext="133" OR ext="140" OR ext="145" OR ext="167") AND
duration>"00:00:10"
```

All the extensions tested for in the first alarm formula are retested in the second formula, resulting in duplicate testing for the same conditions. By defining a macro, these extensions can be tested for once, and then the resulting TRUE or FALSE condition can be referenced in your formulas without having to retest the record. For example:

```
[macros]
MyExtensions= ext="103" OR ext="107" OR ext="111" OR ext="114" OR ext="116" OR
ext="121" OR ext="133" OR ext="140" OR ext="145" OR ext="167"

[dataalarms]
Alarm1_e=MyExtensions=TRUE AND (localprefix="976" or areacode="900")
Alarm2_e=MyExtensions=TRUE AND duration>"00:00:10"
```

Not only is this easier to type, its is much more efficient within the SNMP Access Gateway as the test for extensions only has to be done once. The above data alarm formulas are not complete, see the next section.

11.8 - Data Alarm Section

Data Alarm definitions, if used, must follow the Macro section. The Data Alarm section of the alarm file starts with the definition header [dataalarms]. After the definition header comes all the data alarm definitions. Up to 30 data alarms can be defined. The syntax for a data alarm definition is:

```
alarmname = applicableports , threshold , actions , cleartime
alarmname_e = formula
```

To prevent alarm definitions from becoming too long, each data alarm is split into two lines. The first line of the data alarm definition contain the following entries:

alarmname - This entry specifies the name of the alarm, whatever you want to call it. This name will be used as part of the alarm action process to inform you what event you are being notified about.

applicableports - This entry specifies the I/O ports to which this data alarm will apply. Either or both of the 2 SNMP Access Gateway serial I/O ports can be listed here, for example:

```
ports=1      - Only Port 1
ports=12     - Ports 1 and 2
ports=all    - Ports 1 and 2
```

threshold - This entry specifies how many matching records must be received before the alarm action is initiated. With most alarms this entry will usually be 1, but you may wish with other alarms to have a value of 30 or more.

actions - This entry specifies one or more actions to be taken when this alarm occurs. The syntax for specifying what alarm actions to take is covered later in the following section Defining Alarm Actions.

cleartime - This entry specifies when to clear the counters on the alarm back to zero occurrences. Options include:

```
1Hours      - Clears every hour
2Hours      - Clears every other hour
4Hours      - Clears every four hours
6Hours      - Clears every six hours
8Hours      - Clears every eight hours
12hours     - Clears every twelve hours
24hours     - Clears every twenty-four hours
daily       - Same as 24Hours
nn:nn      - Clears at the specified time every day
```

Important Note: If you add an 'A' before any of the above clearing parameters (as in 'A24Hours'), this will also select the alarm counters to AUTOCLEAR to zero each time the alarm occurs. Otherwise an alarm notification can occur only once within the designated period.

The second line of the alarm definition is the formula itself, with the following requirements:

alarmname_e - This is the same name as specified in the prior line with the addition of an 'underscore' and letter e (for 'equation') after the name.

formula - This formula

11.9 - End Section

The alarm text file must end in the text [end].

11.10 - Defining Alarm Actions

When an alarm occurs, one or more alarm actions can be initiated by the SNMP Access Gateway. Any alarm can include any one or all of the following actions (except only one beeper action):

Action	ActionKey	Options
Pagers	P	1 to 8 different pager callouts
SNMP Traps	T	1 to 8 different SNMP Managers
Beeper	B	1 of 2 different beeper severity's

Multiple actions are defined by using 'action keys' as shown above, plus the numbers to indicate which of those actions should be done. For example, if you wanted to specify calling pagers 1 and 2, plus traps 1 and 3 you would use specify alarm actions P12T13. By using this syntax each alarm can easily be assigned multiple alarm actions.

Chapter 12 - Use of the EVENTS Command

The EVENTS command enters a menu which allows you to view and control matters relating to existing or past Event (Alarm) conditions. Within this section you can view the current condition of sensor inputs and serial alarm parameters, records of all past events, and view and clear currently outstanding alarm conditions.

Events Main Menu

- A. List Events File (0 Records)
- B. Clear Events File
- C. View Active Alarms
- D. Acknowledge Active Alarms
- E. View Alarm Action Detail
- F. View Data Alarm Counters
- G. View Action History
- H. Clear Action History

12.1 - List Events File

Selecting the Menu Letter of this option allows you to view and optionally or clear the Events File. The Events File is a stored log of all events recorded by the SNMP Access Gateway. This log can also be transferred and deleted using FTP, which is covered in another chapter. Upon selection of this menu item the events log will be listed out as shown below and a prompt will allow you to pause and clear the records which have been shown. Below is an example of an Events File listing. Notice that the last 'DATA' record which was received also matched an Alarm Formula and so this record was stored in the events file twice, once as a data record and once as an alarm record.

```
04/08/98 11:59 DATA                2  N 021 00 T002014 DN6502 02/25 09:22 00:00:10
04/08/98 11:59 DATA                2  N 022 00 T007002 DN5700 02/25 09:19 00:02:36
04/08/98 11:59 DATA                2  E 023 00 T002024 DN1006 02/25 09:22 00:00:58
04/08/98 11:59 DATA                2  N 024 00 T002042 DN6000 02/25 09:21 00:00:46
04/08/98 11:59 ALARM equalfour 2  N 024 00 T002042 DN6000 02/25 09:21 00:00:46
```

<enter>-More C-Clear Events X-Exit

12.2 - Clear Events File

Selecting the Menu Letter of this option clears any existing records currently logged in the Events File. Upon selection of this menu item you are prompted with a Sure prompt, and answering 'Y' to this prompt clears the log.

Sure? (Y/N) Y

12.3 - View Active Alarms

Selecting the Menu Letter of this option shows the following display representing the current state and alarm status of sensor inputs and data alarms. Note the asterisks in the display below. These indicate an active alarm condition for the associated alarm. Since there can potentially be more data alarms than can be displayed on a screen, this display is intended to give a quick indication of the presence of data alarms which can then be queried in more detail using another option in this section. The position of the asterisks in the display below correspond to the order of the data alarm formulas as defined in the Alarm File (covered in another section herein).

```
Data Alarms      :          *-----*-----*-----
Sensor Alarms   :
 1 fire          CC Closed   *
 2 smoke         CC Closed   *
 3 flood         CC Open     -
 4 famine        CC Open     -
 5 pestilence    CC Open     -
 6 layoffs       CC Open     -
```

12.4 - Acknowledge Active Alarms

Selecting the Menu Letter of this option acknowledges any and all alarms currently in the queue for alarm notification. These are alarms for which the associated alarm actions are in the Action Queue for handling, whether in progress or not. This also applies to acknowledgment of 'Repeat' alarms (which are marked to repeat until explicitly acknowledged) which are also acknowledged using this selection. Acknowledging Alarms will remove all actions them from the Action Queue. Any alarm action which is in progress at the time such as a pager callout will complete and then clear. Before the Alarms are acknowledged you will be presented with a Sure prompt.

Sure? (Y/N) Y

12.5 - View Alarm Action Detail

Selecting the Menu Letter of this option shows the following display representing all of the actions currently in the Alarm Queue. An explanation of the meaning of each column follows.

#	Date	Time	Type	Name	Level	Action	ID	Try	NXt	Rpt
01:	04/08	11:59	DA	greatfour	01	Pager	001	00	05	N
02:	04/08	11:59	DA	greatfour	01	Trap	001	02	02	Y
03:	04/08	11:59	DA	equalfour	01	Trap	001	02	02	Y

<END - Hit any Key>

Date - The date the action was entered into the queue.

Time - The time the action was entered into the queue.

Type. The alarm type. DA for Data Alarm, ES for Sensor Alarm.

Name - The alarm name as assigned in the Alarm File or elsewhere in the Setup Menu.

Level - This parameter indicates the escalation level of the alarm. At this time there are no levels above 1 and so this value will always indicate '1', except when the buzzer alarm is used which has the 'severity' levels of 1 and 2.

Action - This indicates the type of action, either Pager, Trap, or Buzzer.

ID - This indicates which pager or trap alarm, from 1 to 8, this action is registered to go to.

Try - This indicates how many times this alarm has been attempted and failed, typically useful for pager callouts.

Nxt - Indicates the duration which will be waited if a failure occurs, assuming Tries is greater than one.

Rpt - This indicates whether this alarm is set to repeat after successfully completing.

12.6 - View Data Alarm Counters

This section displays the current counter thresholds for any programmed data alarms. These thresholds indicate how many such alarms have been received since the last 'Clearing' period as specified within the data alarm formula for that alarm.

Alarm Name	Count	Threshold	Alarm Name	Count	Threshold
equalfour	0	1	greatfour	0	1

12.7 - View Action History

This display indicates the past history of alarm actions which have occurred.

#	Date	Time	Type	Name	Level	Action	ID
---	------	------	------	------	-------	--------	----

01:	04/08	12:01	DA	equalfour	01	Trap	OK	01
02:	04/08	12:01	DA	greatfour	01	Trap	OK	01
03:	04/08	12:00	DA	greatfour	01	Pager	OK	01
04:	04/08	12:00	DA	equalfour	01	Buzzer		02
05:	04/08	11:59	DA	greatfour	01	Trap	OK	01
06:	04/08	11:59	DA	greatfour	01	Trap	OK	01
07:	04/08	11:59	DA	equalfour	01	Trap	OK	01
08:	04/08	11:59	DA	greatfour	01	Trap	OK	01
09:	04/06	10:41	DA	greatfour	01	Trap	OK	01
10:	04/06	10:41	DA		01	Trap	OK	01
11:	04/06	10:41	DA	greatfour	01	Trap	OK	01
12:	04/06	10:40	DA		01	Trap	OK	01
13:	04/06	10:40	DA		01	Trap	OK	01
14:	04/06	10:39	DA	greatfour	01	Trap	OK	01
15:	04/06	10:39	DA		01	Trap	OK	01
16:	04/06	10:39	DA	greatfour	01	Trap	OK	01

12.8 - Clear Action History

Selecting the Menu Letter of this option clears all entries in the Action History. Before clearing you will be prompted with a Sure Prompt.

Sure? (Y/N) Y

Chapter 13 - Resetting the SNMP Access Gateway

There are several methods for resetting the SNMP Access Gateway to various degrees.

The RST (RESET) button is located on the front panel. The RST button "reboots" the SNMP Access Gateway when you press the button for three seconds. Valid data in the SNMP Access Gateway will be preserved and SNMP Access Gateway configuration will not be changed.

If you have an alarm going off and you want to shut the alarm off, one quick press of the PRG button while acknowledge the alarm.

The RESTART command "reboots" the SNMP Access Gateway as if you had pressed the RESET button. Valid data present in the SNMP Access Gateway and configuration settings will be preserved.

The DEFAULT command sets all the settings back to their default values with the following exceptions: a) Network settings including the IP address and IP Restrictions, and b) any existing data and event or history logs.

The COLDSTART command causes a complete SNMP Access Gateway reset. The SNMP Access Gateway will be re-booted and all data will be cleared from memory. The settings in the SNMP Access Gateway will be restored to their factory defaults as per the DEFAULT command. This excludes network settings including the IP address and IP Restrictions but does include any existing data and event or history logs.

Chapter 14 - Application Notes

The following chapter contains various articles which discuss in more technical detail specific application examples and peculiarities in using the SNMP Access Gateway. This section may be frequently updated as new articles are written covering various subjects. Inquire with RFL Technical Support regarding ensuring you have all current Application Notes for use of the SNMP Access Gateway.

App Note A. Use of IP Restrictions

IP Restrictions can be established to limit which IP Addresses are allowed access to the SNMP Access Gateway. The IP Restrictions menu can be found in the Networking section of the SETUP menu. By using this menu you can enter in IP addresses into a table to specify which addresses are allowed access and which addresses are denied access to the unit.

The following rules apply to IP addresses entered into this table.

1) By default, there are no entries in the IP Restriction table. With no entries in the table, all IP addresses are allowed access to the unit. However, once any entry is placed into the IP Restriction table, only those IP addresses which are explicitly specified in the table will be allowed access to the unit. For this reason you should be very careful with this feature to avoid accidentally prohibiting your own network access to the unit.

1) A ZERO placed anywhere in the IP address acts as a wildcard to ALLOW access to any IP address matching the other values of that table entry. For example, 192.168.100.0 entered into the table will allow access to any IP address starting with 192.168.100 and prohibiting access in any form from ALL other IP addresses.

2) A 255 placed anywhere in the IP address acts as a wildcard to PROHIBIT access to any IP address matching the other values of that table entry. For example, 192.168.200.255 entered into the table will prohibit access to any IP address starting with 192.168.200.

3) A full address entered into the table will explicitly allow access to that IP address. For example, entering 192.168.200.001 explicitly allows that address access to the unit.

4) Each IP address attempting access to the unit is evaluated against the table of entries, from the first entry down to the last entry of the table. The first match which explicitly PROHIBITS an IP address will immediately cause access to the unit to be denied. The first match found which explicitly ALLOWS an IP address will immediately cause access to be allowed. You need to be careful that the logical order of your entries does not cause an earlier entry to deny access to a latter entry which you allow access to, and vice versa.

5) If no match is found by the time all entries of the table have been examined, the IP address will be denied access to the unit. However, you can approach it in the opposite fashion if you place 0.0.0.0 as the last entry in the table. Then, all prior entries can be those for which access is specifically denied, with all other addresses being allowed access.

6) If you make a mistake and deny your own IP address access, you will have to fix this using the dialup connection or the local command mode connection to change the IP restriction back so you can have access again.

App Note B: Monitoring RS232 Levels as Alarms

The following diagram shows the circuit design of the Sensor Inputs. This design allows these inputs to be used either as a dry contact closure input, or as an analog input.

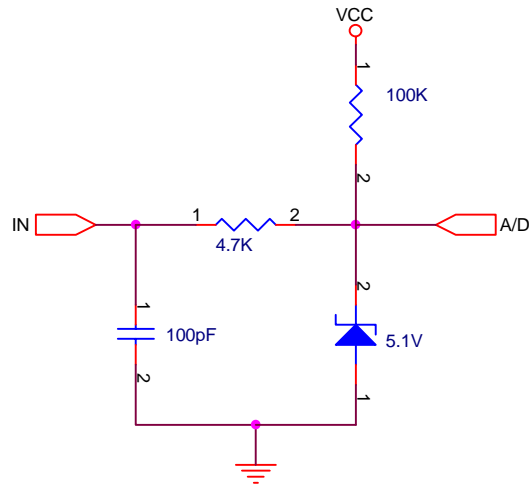


Figure 8. Schematic for Sensor Inputs

Sensor inputs can be used to monitor the state of an RS232 control line such as DTR. A wire can be attached to the line to be monitored and routed to one of the sensor inputs. The Sensor Input should be set to operate as a 'Contact Closure', not an 'Analog Input'. When the control line is LOW the contact input will be seen as OPEN. When the control line is HIGH the contact input will be seen as CLOSED.

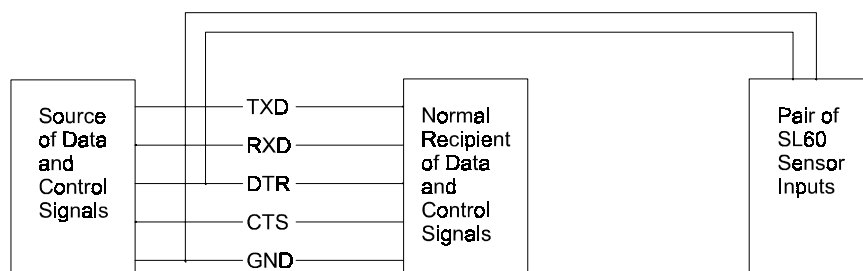


Figure 9. Illustration of Connecting for Monitoring RS232 Control Lines

Note that RS232 control signal lines are not specifically designed to drive more than one input, therefore connecting the output signal to two input connections will cause the overall voltage level of the RS232 control line to be lower than it otherwise would be if connected to a single input. This circumstance will vary from device to device and in 19 out of 20 cases should not present any problem. However you should be aware of this factor if you experience any problems with the other device which would normally be the single device receiving the RS232 output signal you are monitoring.

App Note C: IMUX TRAP messages

C.1 Trap Format

The gateway has been designed to work specifically with all versions of CM-4 software. RS232 trap messages are created by the IMUX and sent to the SAG. This allows the gateway to generate SNMP traps as a result of a message from the IMUX. These traps will contain data that defines the fault condition on the IMUX.

The trap messages contain the following information, which is unique to the IMUX

- Generic trap number 6
- Specific trap number 1-9999 (from serial data string)
- Enterprise ID 1.3.6.1.4.1.2743
- Varbind (including)
 - Trap ID 1.3.6.1.4.1.2743.1.1.1.3
 - Community string x|y|z (from serial string, x=network(1),y=node address(1-999), z=interface(1-99))
 - Message string text (from serial string)

C.2 Interface Codes

The following codes represent interfaces within the IMUX

- 1-36 IMUX channel cards with a matching SCB address
- 37 Terminal CM-4
- 38 D&I-A CM-4
- 39 D&I-B CM-4
- 40 Term or D&I-A standby CM-4
- 41 D&I-B standby CM-4
- 43 R-DACS or MDACS

C.2 Trap Codes

The table provided below lists all of the possible traps from the system.. Alarm numbering begins at 100 and is structured as follows:

NO.	SOURCE	DESCRIPTION	O/VIEW STATUS	VARBIND	
				Variable	Value Range
101	Interface	ALERT AT CHANNEL CARD #	CRITICAL	Channel #	1-36, 40, 41, 43
102	Interface	Reset ALERT AT CHANNEL CARD #	CRITICAL	Channel #	1-36, 40, 41, 43
103	Interfaces	ALERT AT MULTIPLE CARDS	CRITICAL	# of Cards	2-36
104	Interfaces	Reset ALERT AT MULTIPLE CARDS	CRITICAL	# of Cards	2-36
105	CM-4	Redundant power supply failure	CRITICAL	n/a	
106	CM-4	Reset Redundant power supply failure	CRITICAL	n/a	
107	CM-4	Shelf status (alert)	CRITICAL	n/a	
108	CM-4	Reset Shelf status (alert)	CRITICAL	n/a	
109	CM-4	Shelf status (alarm)	CRITICAL	n/a	
110	CM-4	Reset Shelf status (alarm)	CRITICAL	n/a	
111	CM-4	D&I-B Configuration alarm	CRITICAL	n/a	
112	CM-4	Reset D&I-B Configuration alarm	CRITICAL	n/a	
113	CM-4	XMIT timing not correct	CRITICAL	n/a	
114	CM-4	Reset XMIT timing not correct	CRITICAL	n/a	
115	CM-4	RCV carrier loss	CRITICAL	n/a	
116	CM-4	Reset RCV carrier loss	CRITICAL	n/a	
117	CM-4	Excess receive jitter	CRITICAL	n/a	
118	CM-4	Reset Excess receive jitter	CRITICAL	n/a	
119	CM-4	RCV out of frame	CRITICAL	n/a	
120	CM-4	Reset RCV out of frame	CRITICAL	n/a	
121	CM-4	Other side (DI-A) out of frame	CRITICAL	n/a	
122	CM-4	Reset Other side (DI-A) out of frame	CRITICAL	n/a	
123	CM-4	Other side (DI-B) out of frame	CRITICAL	n/a	
124	CM-4	Reset Other side (DI-B) out of frame	CRITICAL	n/a	
125	CM-4	RCV all ones	CRITICAL	n/a	
126	CM-4	Reset RCV all ones	CRITICAL	n/a	
127	CM-4	RCV remote alarm	CRITICAL	n/a	
128	CM-4	Reset RCV remote alarm	CRITICAL	n/a	
129	CM-4	XMIT clock free-running	CRITICAL	n/a	
130	CM-4	Reset XMIT clock free-running	CRITICAL	n/a	
131	CM-4	XMIT using fallback timing	CRITICAL	n/a	
132	CM-4	Reset XMIT using fallback timing	CRITICAL	n/a	
2000	CM-4	Power Up	NORMAL	0	
2005	Interfaces	Clear All Alarms for Subaddress	NORMAL	Subaddress	1-43

Chapter 15 - Warranty Information

Except where noted, all RFL Electronics Inc. products come with a one-year warranty from date of delivery for replacement of any part which fails during normal operation. RFL will repair or, at its option, replace components that prove to be defective at no cost to the Customer. All equipment returned to RFL Electronics Inc. must have an RMA (Return Material Authorization) number, obtained by calling the RFL Customer Service Department. A defective part should be returned to the factory, shipping charges prepaid, for repair or replacement FOB Boonton, N.J.

RFL Electronics Inc. is not responsible for warranty of peripherals, such as printers and external computers. The warranty for such devices is as stated by the original equipment manufacturer. If you have purchased peripheral equipment not manufactured by RFL, follow the written instructions supplied with that equipment for warranty information and how to obtain service.

WARRANTY STATEMENT

The RFL SNMP Access Gateway is warranted against defects in material and workmanship for twelve months from date of shipment. This warranty does not apply if the equipment has been damaged by accident, neglect, misuse, or causes other than performed or authorized by RFL Electronics Inc. This warranty specifically excludes damage incurred "in shipment" to or from RFL. In the event that an item is received in damaged condition, the carrier should be notified immediately. All claims for such damage should be filed with the carrier.

NOTE

If you do not intend to use the product immediately, it is recommended that it be opened immediately after receiving and inspected for proper operation and signs of impact damage.

This warranty is in lieu of all other warranties, whether expressed, implied or statutory, including but not limited to implied warranties of merchantability and fitness for a particular purpose. In no event shall RFL be liable, whether in contract, in tort, or on any other basis, for any damages sustained by the customer or any other person arising from or related to loss of use, failure or interruption in the operation of any products, or delay in maintenance or for incidental, consequential, indirect or special damages or liabilities, or for loss of business or other financial loss arising out of or in connection with the sale, lease, maintenance, use, performance, failure or interruption of the products.

Chapter 16 - Canadian Dept. of Comm. Notice

NOTICE: The Canadian Department of Communications Label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protections that the electrical ground connections of the power utility, telephone lines and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Load Number (LN) assigned to each terminal device denotes the percentage of total load to be connected to a telephone loop which is used by the device, to prevent overloading. The termination of a loop may consist of any combination of devices subject only to the requirement that the total of the Load Numbers of all the devices does not exceed 100. The load number of this unit is 5.

This digital apparatus does not exceed the Class A limits for Radio noise emissions from digital apparatus set out in the interference-causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.

AVIS: - L'étiquette du ministère des Communications du Canada identifie le matériel homologué. Cette étiquette certifie que le matériel est conforme à certaines normes de protection, d'exploitation et de sécurité des réseaux de télécommunications. Le Ministère n'assure toutefois pas que le matériel fonctionnera à la satisfaction de l'utilisateur.

Avant d'installer ce matériel, l'utilisateur doit s'assurer qu'il est permis de le raccorder aux installations de l'entreprise locale de télécommunication. Le matériel doit également être installé en suivant une méthode acceptée de raccordement. Dans certains cas, les fils intérieurs de l'entreprise utilisés pour un service individuel à ligne unique peuvent être prolongés au moyen d'un dispositif homologué de raccordement (cordon prolongateur téléphonique interne). L'abonné ne doit pas oublier qu'il est possible que la conformité aux conditions énoncées ci-dessus n'empêche pas la dégradation du service dans certaines situations. Actuellement, les entreprises de télécommunication ne permettent pas que l'on raccorde leur matériel à des jacks d'abonné, sauf dans les cas précis prévus par les tarifs particuliers de ces entreprises.

Les réparations de matériel homologué doivent être effectuées par un centre d'entretien Canadien autorisé désigné par le fournisseur. La compagnie de télécommunications peut demander à l'utilisateur de débrancher un appareil à la suite de réparations ou de modifications effectuées par l'utilisateur ou à cause de mauvais fonctionnement.

Pour sa propre protection, l'utilisateur doit s'assurer que tous les fils de mise à la terre de la source d'énergie électrique, des lignes téléphoniques et des canalisations d'eau métalliques, s'il y en a, sont raccordés ensemble. Cette précaution est particulièrement importante dans les régions rurales.

Avertissement. - L'utilisateur ne doit pas tenter de faire ces raccordements lui-meme; il doit avoir recours a un service d'inspection des installations électriques, ou a un electricien, selon le cas.

L'indice de charge (IC) assigné a chaque dispositif terminal indique, pour éviter toute surcharge, le pourcentage de la charge totale qui peut être raccordée a un circuit téléphonique bouclé utilisé par ce dispositif. La terminaison du circuit bouclé peut être constituée de n'importe quelle combinaison de dispositif, pourvu que la somme des indices de charge de l'ensemble des dispositifs ne dépasse pas 100. L'indice de charge de cet produit est 5.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur : "Appareils Numériques", NMB-003 édictée par le ministre des Communications.