Access Security Gateway Guard and Access Security Gateway Guard Plus

User’s Guide
Notice
While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Lucent Technologies can assume no responsibility for any errors or liability for any direct or consequential damages resulting from use of the information. Changes and/or corrections to the information contained in this document may be incorporated into future issues.

Responsibility for Your System's Security
Toll fraud is the unauthorized use of your telecommunications system by an unauthorized party, for example, persons other than your company's employees, agents, subcontractors, or persons working on your company's behalf. Note that there may be a risk of toll fraud associated with your telecommunications system, and if toll fraud occurs, it can result in substantial additional charges for your telecommunications services.

You and your System Manager are responsible for the security of your system, such as programming and configuring your equipment to prevent unauthorized use. The System Manager is also responsible for reading all installation, instruction, and system administration documents provided with this product in order to fully understand the features that can introduce risk of toll fraud and the steps that can be taken to reduce that risk. Lucent Technologies does not warrant that this product is immune from or will prevent unauthorized use of common carrier telecommunication services or facilities accessed through or connected to it. Lucent Technologies will not be responsible for any charges that result from such unauthorized use.

Trademark Notice
DEFINITY and INTUYITY are registered trademarks of Lucent Technologies.

Disclaimer
Intellectual property related to this product (including trademarks) and registered to AT&T Corporation has been transferred to Lucent Technologies Incorporated.

Any references within this text to American Telephone and Telegraph Corporation or AT&T should be interpreted as references to Lucent Technologies Incorporated. The exception is cross references to books published prior to December 31, 1996, which retain their original AT&T titles.

Heritage Statement
Lucent Technologies — formed as a result of AT&T’s planned restructuring — designs, builds, and delivers a wide range of public and private networks, communication systems and software, consumer and business telephone systems, and microelectronics components. The world-renowned Bell Laboratories is the research and development arm for the company.

Ordering Information

Fraud Intervention
If you suspect you are being victimized by toll fraud and you need technical support or assistance, call the Lucent Technologies National Customer Care Center at 1 800 643-2353. For international customers, contact your local Center of Excellence.

To Get Help
If you need assistance with administration and configuration of the ASG Guard, call Ion Networks, Inc. at 1 732 494-4440. Their technical support staff is available 9:00 a.m. to 5:00 p.m. EST Monday through Friday. This call may be billable. If you believe you have a repair problem, call Lucent Technologies at 1 800 242-2121 or your local Authorized Dealer. For international customers, contact your local Center of Excellence.

To resolve the problem as quickly as possible, describe the problem and note the steps that you have taken to resolve it. Also note the status of the LEDs on the front panel.

Home Page
# Table of Contents

1. About This Guide .............................................................................................................1

2. ASG Guard/ASG Guard Plus Overview ........................................................................3
   2.1 What This Chapter Contains ....................................................................................3
   2.2 Terms ......................................................................................................................3
   2.3 Notation Used in this Guide ....................................................................................3
   2.4 ASG Guard/ASG Guard Plus Physical Overview ..................................................3
       2.4.1 ASG Guard Configuration ..............................................................................4
       2.4.2 ASG Guard Plus Configuration .................................................................4
       2.4.3 ASG Guard Front Panel ..............................................................................4
       2.4.4 ASG Guard Rear Panel ...............................................................................5
       2.4.5 ASG Guard Plus Front Panel .....................................................................5
       2.4.6 ASG Guard Plus Rear Panel .....................................................................6
   2.5 ASG Guard/ASG Guard Plus Functional Overview ...........................................7
   2.6 Security Management .............................................................................................8
       2.6.1 Access Classes .........................................................................................8
       2.6.2 User Database .........................................................................................8
   2.7 Alarm Management .................................................................................................9
   2.8 Logs ......................................................................................................................10
   2.9 Network Capabilities .............................................................................................10
   2.10 Editing Modes .....................................................................................................12
       2.10.1 TTY Mode ..............................................................................................12
       2.10.2 VT-100 Mode ........................................................................................12
   2.11 Using the Editing Keys .......................................................................................13
   2.12 Entering Commands .........................................................................................14
       2.12.1 Entering/Selecting Parameters ............................................................15

3. Physical Connections and Installation .....................................................................17
   3.1 What This Chapter Contains .............................................................................17
   3.2 LED Displays and Physical Connections ............................................................17
       3.2.1 LED Meanings ......................................................................................17
       3.2.2 Connecting a DCE device to a Host Port ............................................19
   3.3 Installation of the ASG Guard/ASG Guard Plus ..............................................20
       3.3.1 Cables and Equipment Required .......................................................20
       3.3.2 Requirements for Network Applications .......................................20
       3.3.3 Install the Unit .....................................................................................20
| 3.3.4 | Power up the ASG Guard/ASG Guard Plus | 22 |
| 3.3.5 | Verify PSTN Access | 23 |
| 4. Basic Configuration | | 25 |
| 4.1 | What This Chapter Contains | 25 |
| 4.2 | Add the First User Profile | 25 |
| 4.2.1 | Password/Callback Authentication Method | 28 |
| 4.2.2 | ASG Key Authentication Method | 30 |
| 4.3 | Specify Network Parameters | 32 |
| 4.4 | Configure the AUX Port | 33 |
| 4.5 | Initiate Security on the AUX Port | 35 |
| 4.6 | Configure a Host Port | 36 |
| 4.7 | Re-Initialize the ASG Guard/ASG Guard Plus via the AUX Port | 40 |
| 5. Modem Port Setup | | 41 |
| 5.1 | What This Chapter Contains | 41 |
| 5.2 | Overview | 41 |
| 5.3 | Modem Port Parameters | 41 |
| 5.3.1 | Display Modem Port Parameters – DM Command | 41 |
| 5.3.2 | Set Modem Port Parameters – SM Command | 43 |
| 5.4 | Verify the Settings | 47 |
| 6. Modifying the User Database | | 49 |
| 6.1 | What This Chapter Contains | 49 |
| 6.2 | Overview | 49 |
| 6.3 | Display the User Maintenance Functions Menu | 50 |
| 6.4 | Command Summary | 51 |
| 6.5 | Add a User – AU Command | 52 |
| 6.5.1 | ASG Key Authentication Method | 54 |
| 6.5.1.1 | Encryption Key Source | 55 |
| 6.5.1.2 | Encryption Key Source: Randomly Generated | 55 |
| 6.5.1.3 | Encryption Key Source: Device ID/User Code | 56 |
| 6.5.1.4 | Encryption Key Source: Fixed | 56 |
| 6.5.2 | Password/Callback Authentication Method | 57 |
| 6.5.2.1 | Access Option: Regular Callback | 57 |
| 6.5.2.2 | Access Option: Passthru | 58 |
| 6.5.2.3 | Access Option: Variable Callback | 58 |
| 6.5.3 | Page Authentication Method | 58 |
6.6  List Users – LU Command...............................................................................................60
6.7  Delete a User Profile – XU Command............................................................................62
6.8  Display a User Record – DU Command.........................................................................63
6.9  Changing User Information – CU Command.................................................................64
6.10 Set Customer Key – SCK Command ..............................................................................67
6.11 List Lucent Users – LLU Command.................................................................................68
6.12 Block/Unblock Lucent User – BLU Command.................................................................68
6.13 Display Lucent User – DLU Command............................................................................68
6.14 Block/Unblock Lucent Administration – BLA Command..................................................69

7. File Buffering ....................................................................................................................71
7.1  What This Chapter Contains............................................................................................71
7.2  Overview.........................................................................................................................71
7.3  File Management Menu...................................................................................................72
7.4  RAM Disk Organization .................................................................................................73
7.4.1 Host Port Buffer Naming..........................................................................................73
7.4.2 Buffer File Naming Conventions..............................................................................73
7.5  Set the RAM disk Protection Parameters ........................................................................75
7.6  Buffering Data Received by a Host Port.........................................................................77
7.6.1 Automatic Buffering .................................................................................................77
7.6.2 Manual Buffering......................................................................................................79
7.6.3 Displaying the Status of a Buffer .............................................................................79
7.6.4 Sending Buffer Files to the Administration PC ........................................................80
7.6.5 Using a Direct or Dial-up Connection ......................................................................80
7.6.6 Using FTP to Send Files to Another Device............................................................81
7.6.6.1 Specify the FTP Parameters ..............................................................................81
7.6.6.2 Sending the File(s) via FTP ................................................................................83
7.7  Receiving Files .............................................................................................................84
7.8  Managing Files ..............................................................................................................85
7.9  File Command Summary.................................................................................................86
7.10 RAM Drive Events .......................................................................................................86
7.11 Utility Programs ............................................................................................................88
7.11.1 CSUM.EXE ..............................................................................................................88
7.11.2 ZPAD.EXE ...............................................................................................................88
## 8. The Action and Event Tables

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1 What this Chapter Contains</td>
<td>89</td>
</tr>
<tr>
<td>8.2 Overview</td>
<td>89</td>
</tr>
<tr>
<td>8.3 Working with Action Tables</td>
<td>89</td>
</tr>
<tr>
<td>8.4 Structure of an Action Table</td>
<td>90</td>
</tr>
<tr>
<td>8.4.1 Alarm Matching Criteria</td>
<td>91</td>
</tr>
<tr>
<td>8.4.2 Multiple Actions on a Single Alarm</td>
<td>92</td>
</tr>
<tr>
<td>8.5 Planning the Action Table</td>
<td>92</td>
</tr>
<tr>
<td>8.6 Action Table Commands</td>
<td>95</td>
</tr>
<tr>
<td>8.6.1 Adding an item to the Action Table – AA Command</td>
<td>95</td>
</tr>
<tr>
<td>8.6.2 List Action Items – LA Command</td>
<td>97</td>
</tr>
<tr>
<td>8.6.3 Change Action Item – CA Command</td>
<td>98</td>
</tr>
<tr>
<td>8.6.4 Schedule Action Item – SAI Command</td>
<td>98</td>
</tr>
<tr>
<td>8.6.5 Delete Action Item – XA Command</td>
<td>99</td>
</tr>
<tr>
<td>8.7 Alarm/Event Functions Commands</td>
<td>101</td>
</tr>
<tr>
<td>8.7.1 List Alarms/Events – LE Command</td>
<td>101</td>
</tr>
<tr>
<td>8.7.2 Generate Alarm/Event – GE Command</td>
<td>101</td>
</tr>
<tr>
<td>8.7.3 Delete Alarm/Event – XE Command</td>
<td>103</td>
</tr>
<tr>
<td>8.8 Internal Alarms and Events</td>
<td>104</td>
</tr>
<tr>
<td>8.9 Action Routines</td>
<td>107</td>
</tr>
</tbody>
</table>

## 9. System Functions

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1 What This Chapter Contains</td>
<td>109</td>
</tr>
<tr>
<td>9.2 Overview</td>
<td>109</td>
</tr>
<tr>
<td>9.3 Systems Functions Menu</td>
<td>109</td>
</tr>
<tr>
<td>9.4 System Parameter Functions</td>
<td>111</td>
</tr>
<tr>
<td>9.4.1 Set System Parameters – SSP Command</td>
<td>111</td>
</tr>
<tr>
<td>9.4.1.1 Site information</td>
<td>111</td>
</tr>
<tr>
<td>9.4.1.2 Scheduling Parameters</td>
<td>113</td>
</tr>
<tr>
<td>9.4.1.3 Modem Action Routine Parameters</td>
<td>114</td>
</tr>
<tr>
<td>9.4.2 Display System Parameters – DSP Command</td>
<td>115</td>
</tr>
<tr>
<td>9.4.3 Set Host Processor Flag – SHP Command</td>
<td>116</td>
</tr>
<tr>
<td>9.4.4 Set Date and Time – SDT Command</td>
<td>117</td>
</tr>
<tr>
<td>9.5 Device Management Functions</td>
<td>118</td>
</tr>
<tr>
<td>9.5.1 Check the Software Version – VER Command</td>
<td>118</td>
</tr>
<tr>
<td>9.5.2 Upgrade the Software – UPG Command</td>
<td>119</td>
</tr>
<tr>
<td>9.5.3 Restart the ASG Guard/ASG Guard Plus – BOOT Command</td>
<td>119</td>
</tr>
<tr>
<td>9.5.4 View or Save Configuration Data on Remote Device - DUMP Command</td>
<td>120</td>
</tr>
<tr>
<td>Section</td>
<td>Page</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>9.5.5 Save Configuration Data on RAM Disk File - DUMPF Command</td>
<td>120</td>
</tr>
<tr>
<td>9.5.6 Put Customer User Table on Remote Device – CDUMP Command</td>
<td>120</td>
</tr>
<tr>
<td>9.5.7 Put Customer User Table on RAM Disk File – CDUMPF Command</td>
<td>120</td>
</tr>
<tr>
<td>9.5.8 Load a Configuration File – CONFIG Command</td>
<td>120</td>
</tr>
<tr>
<td>9.5.9 Load a Customer User Table – CCONFIG Command</td>
<td>120</td>
</tr>
<tr>
<td><strong>10. Environmental Manager</strong></td>
<td>121</td>
</tr>
<tr>
<td>10.1 What This Chapter Contains</td>
<td>121</td>
</tr>
<tr>
<td>10.2 Overview</td>
<td>121</td>
</tr>
<tr>
<td>10.3 ASG Guard/ASG Guard Plus Series Environmental Manager Options</td>
<td>121</td>
</tr>
<tr>
<td>10.4 Environmental Manager Functions and Commands</td>
<td>122</td>
</tr>
<tr>
<td>10.4.1 Set Sensor Alarms – SSA Command</td>
<td>122</td>
</tr>
<tr>
<td>10.4.2 Display Sensor Alarms – DSA Command</td>
<td>122</td>
</tr>
<tr>
<td>10.4.3 Display Sensor Inputs – DSI Command</td>
<td>122</td>
</tr>
<tr>
<td>10.4.4 Display Contact Inputs – DCC Commands</td>
<td>122</td>
</tr>
<tr>
<td>10.4.5 Set Relays – SRLY Command</td>
<td>123</td>
</tr>
<tr>
<td>10.4.6 Reset Relays – RRLY Command</td>
<td>123</td>
</tr>
<tr>
<td>10.5 The Environmental Manager</td>
<td>124</td>
</tr>
<tr>
<td>10.5.1 The Environmental Interface of the ASG Guard Plus</td>
<td>124</td>
</tr>
<tr>
<td>10.5.2 The Environmental Interface of the ASG Guard</td>
<td>126</td>
</tr>
<tr>
<td>10.6 Relays on the ASG Guard</td>
<td>128</td>
</tr>
<tr>
<td>10.7 Defining Threshold Limits – SSA Command</td>
<td>128</td>
</tr>
<tr>
<td>10.8 Analog Sensors</td>
<td>130</td>
</tr>
<tr>
<td>10.8.1 48-Volt Battery</td>
<td>130</td>
</tr>
<tr>
<td>10.8.2 Temperature</td>
<td>130</td>
</tr>
<tr>
<td>10.8.3 Voltage Inputs</td>
<td>130</td>
</tr>
<tr>
<td>10.9 Contact Closure Inputs</td>
<td>131</td>
</tr>
<tr>
<td>10.10 Displaying Analog Sensor Inputs – DSI Command</td>
<td>131</td>
</tr>
<tr>
<td>10.11 Displaying the Status of Contact Inputs</td>
<td>132</td>
</tr>
<tr>
<td><strong>11. User Connectivity</strong></td>
<td>133</td>
</tr>
<tr>
<td>11.1 What This Chapter Contains</td>
<td>133</td>
</tr>
<tr>
<td>11.2 Overview</td>
<td>133</td>
</tr>
<tr>
<td>11.3 Dial-up Preparations</td>
<td>133</td>
</tr>
<tr>
<td>11.4 Initiate a Dial-up Session</td>
<td>134</td>
</tr>
<tr>
<td>11.4.1 Password/Callback</td>
<td>134</td>
</tr>
<tr>
<td>11.4.2 Regular Callback</td>
<td>135</td>
</tr>
<tr>
<td>11.4.3 Using Variable Callback</td>
<td>137</td>
</tr>
</tbody>
</table>
12.10 Telnet Port Parameters
12.10.1 Setting Telnet Port Parameters – ST Command
12.10.2 Display Telnet Port Parameters – DT Command
12.11 Initiate a PPP Link – PPP Command
12.11.1 Designate a Port as a PPP Port
12.11.2 Initiate a PPP Connection On-Demand
12.11.2.1 ASG Guard/ASG Guard Plus Setup
12.11.2.2 Setup for PPP Client using “Dial-Up Networking” – New Connection
12.11.2.3 Setup for PPP Client using “Dial-Up Networking” – Remote Connection
12.11.2.4 Establishing a PPP Connection
12.12 Initiating a Telnet Session
12.12.1 Initiating a Telnet Session: Direct Connect
12.12.2 Telnet Session via PPP through a ASG Guard/ASG Guard Plus

13. Log Functions
13.1 What This Chapter Contains
13.2 Overview
13.3 The Log Functions Menu
13.3.1 Access History – AH Command
13.3.2 Log History – LH Command
13.3.3 Failure History – FH Command
13.3.4 Display Error Log – DER Command
13.3.5 Clear Log History – CLH Command
13.3.6 Clear Error Log – CER Command

14. Events and Action Routines
14.1 What This Chapter Contains
14.2 Overview
14.3 Internal Events
14.3.1 .AUTHFAIL Internal Event
14.3.2 .BAT48HIGH Internal Event
14.3.3 .BAT48LOW Internal Event
14.3.4 .BAT48OK Internal Event
14.3.5 .BUFREADY Internal Event
14.3.6 .C#CLOSED Internal Event
14.3.7 .C#OPEN Internal Event
14.3.8 .CCLERROR Internal Event
14.3.9 .CLKCHANGE Internal Event
14.3.10 .DAILY Internal Event
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.3.11</td>
<td>.DISKCRIT Internal Event</td>
</tr>
<tr>
<td>14.3.12</td>
<td>.DISKFULL Internal Event</td>
</tr>
<tr>
<td>14.3.13</td>
<td>.DTRHIGH, .DTRLOW, .DTRHIGH.n, and .DTRLOW.n Internal Events</td>
</tr>
<tr>
<td>14.3.14</td>
<td>.HOURLY Internal Event</td>
</tr>
<tr>
<td>14.3.15</td>
<td>.INTBATLOW Internal Event</td>
</tr>
<tr>
<td>14.3.16</td>
<td>.INTBATOK Internal Event</td>
</tr>
<tr>
<td>14.3.17</td>
<td>.LOGFULL Internal Event</td>
</tr>
<tr>
<td>14.3.18</td>
<td>.MAXRETRY Internal Event</td>
</tr>
<tr>
<td>14.3.19</td>
<td>.MDMINITERR Internal Event</td>
</tr>
<tr>
<td>14.3.20</td>
<td>.MEMLOW Internal Event</td>
</tr>
<tr>
<td>14.3.21</td>
<td>.MONTHLY Internal Event</td>
</tr>
<tr>
<td>14.3.22</td>
<td>.NETDOWN and .NETUP Internal Event</td>
</tr>
<tr>
<td>14.3.23</td>
<td>.POWERLOW Internal Event</td>
</tr>
<tr>
<td>14.3.24</td>
<td>.POWEROK Internal Event</td>
</tr>
<tr>
<td>14.3.25</td>
<td>.POWERUP Internal Event</td>
</tr>
<tr>
<td>14.3.26</td>
<td>.PPPREQ Internal Event</td>
</tr>
<tr>
<td>14.3.27</td>
<td>.RTSLOW.n and .RTSHIGH.n Internal Events</td>
</tr>
<tr>
<td>14.3.28</td>
<td>.S#HIGH, .S#LOW, or .S#OK Internal Event</td>
</tr>
<tr>
<td>14.3.29</td>
<td>.TEMPHIGH</td>
</tr>
<tr>
<td>14.3.30</td>
<td>.TEMPLOW Internal Events</td>
</tr>
<tr>
<td>14.3.31</td>
<td>.TEMPOK Internal Events</td>
</tr>
<tr>
<td>14.3.32</td>
<td>.WEEKLY Internal Event</td>
</tr>
</tbody>
</table>

14.4 ACTION ROUTINES

14.4.1 AUXCC Action Routine
14.4.2 CANCEL Action Routine
14.4.3 CLKAHEAD and CLKBACK Action Routines
14.4.4 CLKCHECK Action Routine
14.4.5 DOLIST Action Routine
14.4.6 LOG Action Routine
14.4.7 LOGCHECK Action Routine
14.4.8 NOACTION Action Routine
14.4.9 PAGE Action Routine
14.4.10 PHIRIS Action Routine
14.4.11 PHONHOME Action Routine
14.4.12 PHPPP Action Routine
14.4.13 PHSYSOP Action Routine
14.4.14 REMINIT Action Routine
| 14.4.15  | RESRELAY Action Routine | 198 |
| 14.4.16  | SCHEDULE Action Routine | 199 |
| 14.4.17  | SETHP Action Routine    | 200 |
| 14.4.18  | SETRELAY Action Routine | 201 |
| 14.4.19  | SNMPTRAP                | 202 |

**Appendix A. ASG Key User's Guide** ............................................................... 203

**Appendix B. Port Default Settings** ............................................................... 207

**Appendix C. Configuration Files** ................................................................. 211

**Appendix D. Troubleshooting** ........................................................................ 223

**Appendix E. Internal Battery Replacement** .................................................... 225

**Appendix F. Glossary of Command References** ............................................ 241

**Index** .............................................................................................................. 247
1. About This Guide

This manual describes the ASG Guard and the ASG Guard Plus. The following is an overview of each chapter.

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>About This Guide</td>
<td>Briefly describes the contents of each chapter.</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>ASG Guard/ASG Guard Plus Overview</td>
<td>Contains an overview of the ASG Guard/ASG Guard Plus operation. We recommend that all Users read this chapter.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>Physical Connections and Installation</td>
<td>Describes the required cable connections and the power-up procedure.</td>
</tr>
<tr>
<td>Chapter 4</td>
<td>Basic Configuration</td>
<td>Describes the steps to get the ASG Guard/ASG Guard Plus “up and running.”</td>
</tr>
<tr>
<td>Chapter 5</td>
<td>Modem Port Setup</td>
<td>Explains how to configure an ASG Guard/ASG Guard Plus modem port. All parameters to set-up modem ports are described. These include baud rate and parity, modem control strings, and other port settings.</td>
</tr>
<tr>
<td>Chapter 6</td>
<td>Modifying the User Database</td>
<td>Explains how to add, delete, and change information in the user database.</td>
</tr>
<tr>
<td>Chapter 7</td>
<td>File Buffering</td>
<td>Describes how the ASG Guard/ASG Guard Plus buffers data from host ports and how to manage these files.</td>
</tr>
<tr>
<td>Chapter 8</td>
<td>The Action and Event Tables</td>
<td>Explains how the ASG Guard/ASG Guard Plus manages alarms. This chapter also explains how to create, modify and test Action Tables.</td>
</tr>
<tr>
<td>Chapter 9</td>
<td>System Functions</td>
<td>Explains how to set the System Parameters and Environmental Control Functions. These parameters include site name and phone numbers, scheduling, and modem action routines.</td>
</tr>
<tr>
<td>Chapter 10</td>
<td>Environmental Manager</td>
<td>Contains information on how to use the Environmental Manager to monitor real-world events such as temperature and voltage.</td>
</tr>
<tr>
<td>Chapter 11</td>
<td>User Connectivity</td>
<td>Explains how to dial into the ASG Guard/ASG Guard Plus and authenticate. Also includes information about joining sessions that are in progress and secure port management.</td>
</tr>
<tr>
<td>-----------</td>
<td>------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Chapter 12</td>
<td>Network Functions</td>
<td>Includes instructions on how to set up the network parameters, such as the IP and Ethernet addresses.</td>
</tr>
<tr>
<td>Chapter 13</td>
<td>Log Functions</td>
<td>Describes the Access, Failure and System Error Logs maintained automatically by the ASG Guard/ASG Guard Plus. Also lists the commands to display and clear the logs.</td>
</tr>
<tr>
<td>Chapter 14</td>
<td>Events and Action Routines</td>
<td>Describes each Internal Event and standard Action Routine. Examples are also included.</td>
</tr>
<tr>
<td>Appendix A</td>
<td>ASG Key User’s Guide</td>
<td>Describes how to use the ASG Key.</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Port Default Settings</td>
<td>Describes the default Port settings for the ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>Appendix C</td>
<td>Configuration Files</td>
<td>Describes the configuration file of the ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>Appendix D</td>
<td>Troubleshooting</td>
<td>Provides a table of symptoms, causes, and possible solutions that can be used for troubleshooting problems when installing the ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>Appendix E</td>
<td>Internal Battery Replacement</td>
<td>Describes how to replace the battery in the ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>Appendix F</td>
<td>Glossary of Command References</td>
<td>Provides a list of the commands for the ASG Guard/ASG Guard Plus.</td>
</tr>
</tbody>
</table>
2. ASG Guard/ASG Guard Plus Overview

2.1 What This Chapter Contains

- Figures and descriptions of the front panel connectors for the ASG Guard and ASG Guard Plus
- Figures of the rear panel connectors for the ASG Guard and ASG Guard Plus
- ASG Guard/ASG Guard Plus Functions-Security Management, Alarm Handling, Data Buffering, SNMP Management/Reporting
- Command Organization
- How to Display Menus and Issue Commands

2.2 Terms

Authentication method - Method of verifying that the person attempting to access the ASG Guard/ASG Guard Plus or any protected resource, is an authorized user. Authentication methods supported by the ASG Guard/ASG Guard Plus include Password/Callback, ASG Key, and Pager.

Master user - A user with highest level of privileges. A master user may add and delete other users, including other users with master level privileges.

System prompt - The system prompt is the "greater than" symbol ( > ) and includes the site name. ASG Guard/ASG Guard Plus commands are typed at this prompt.

2.3 Notation Used in this Guide

Prompts appearing on the screen are typed in italics. Data entered at prompts are typed in bold.

2.4 ASG Guard/ASG Guard Plus Physical Overview

NOTE:
If your ASG Guard/ASG Guard Plus does not have a feature described in this manual, contact Lucent Technologies or your distributor for upgrade information.
2.4.1 ASG Guard Configuration

The ASG Guard has the following components:

- four Host Ports (Asynchronous DCE Ports – DB9)
- two 33.3 Mhz Internal PCMCIA Modems
- one 10Base-T Ethernet Port
- five Contact Closure Inputs
- one 0-5 VDC Analog Input
- two Temperature Sensors; Temperature Probes required
- two Solid-State Relays (Relay #1 latching, Relay #2 non-latching)
- one 48 Volt Battery Monitoring Input
- one 32 MB Ram Disk

2.4.2 ASG Guard Plus Configuration

The ASG Guard Plus has the following components:

- 16 or 28 Host Ports (Asynchronous DCE Ports – DB9)
- two 33.3 Mhz Internal PCMCIA Modems
- one 10Base-T Ethernet Port
- eight Contact Closure Inputs
- three 0-5 VDC Analog Inputs
- one Temperature Sensor; Temperature Probe required
- one 48 Volt Battery Monitoring Input
- one 32 MB Ram Disk

2.4.3 ASG Guard Front Panel

The LEDs, Aux port connector, and Key Switch are located on the front panel of the ASG Guard. Figure 2-1 shows the front panel connectors of the ASG Guard.

![ASG Guard Front Panel Connectors](image)

**Figure 2-1.** ASG Guard Front Panel Connectors
The function of each connector is explained below.

**Aux Port connector**  
You may administer the ASG Guard via a PC or terminal connected to the front Aux connector.

**Key switch**  
The key switch is used to turn the ASG Guard on and off. The key can be removed in either the on or off position. The ASG Guard cannot be turned on or off without a key.

**LEDs**  
The LEDs display status messages. When the unit is operating properly, the pulse LED will flash. The meaning of each LED is explained in *LED Meanings,* later in this chapter.

### 2.4.4 ASG Guard Rear Panel

Figure 2-2 shows the rear panel connectors of the ASG Guard.

![Figure 2-2. ASG Guard Rear Panel Connectors](image)

### 2.4.5 ASG Guard Plus Front Panel

The LEDs, Aux port connector, System Initialization Tag (SIT), and Key Switch are located on the front panel of the ASG Guard Plus. Figure 2-3 shows the front panel connectors of the ASG Guard Plus.

![Figure 2-3. ASG Guard Plus Front Panel Connectors](image)
The function of each connector is explained below.

**Aux Port connector** You may administer the ASG Guard Plus via a PC or terminal connected to either the front- or back-panel Aux connector.

**SIT** The SIT (System Initialization Tag) contains information, unique to your ASG Guard Plus, that can be transferred to the ASG Guard Plus by inserting the SIT connector.

**Key switch** The key switch is used to turn the ASG Guard/ASG Guard Plus on and off. The key can be removed in either the on or off position. The ASG Guard Plus cannot be turned on or off without a key.

**LEDs** The LEDs display status messages. When the unit is operating properly, the pulse LED will flash. The meaning of each LED is explained in [LED Meanings](#), later in this chapter.

### 2.4.6 ASG Guard Plus Rear Panel

Figure 2-4 shows the rear panel connectors of a 16-port ASG Guard Plus, and Figure 2-5 shows the rear panel connectors of a 28-port ASG Guard Plus.

![Figure 2-4. 16-Port ASG Guard Plus Rear Panel Connectors](image)

![Figure 2-5. 28-Port ASG Guard Plus Rear Panel Connectors](image)
2.5 ASG Guard/ASG Guard Plus Functional Overview

The ASG Guard/ASG Guard Plus provides the following basic functions:

- secure access to host device
- site connectivity
- alarm processing
- data buffering

<table>
<thead>
<tr>
<th>Area</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Access</td>
<td>As a front end to host devices, the ASG Guard/ASG Guard Plus provides secured access. All users connecting to the ASG Guard/ASG Guard Plus via network, modem or directly (AUX Port) need to authenticate themselves before being passed through to a host device or permitted to administer the ASG Guard/ASG Guard Plus. Several authentication mechanisms are available in the unit. The ASG Guard/ASG Guard Plus also provides a logical switching function, which allows an authorized user to connect to any host device listed in the user’s profile.</td>
</tr>
<tr>
<td>Site Connectivity</td>
<td>Acts as a central point for connection to all equipment at the site. Allows connection via a local terminal, dial-up modem, and Ethernet. A dial-up modem can also be used for PPP connections allowing remote access to network-connected devices.</td>
</tr>
<tr>
<td>Alarm Processing</td>
<td>When attached to a maintenance port of a host device, the ASG Guard/ASG Guard Plus can process alarm messages and other ASCII based data streams. Alarm messages can be delivered via modem or network connectivity. Using either PPP or network connectivity, the ASG Guard/ASG Guard Plus can deliver SNMP traps to network managers. The ASG Guard/ASG Guard Plus can convert ASCII based alarms received on its host ports to standard SNMP traps. Acting as a SNMP trap proxy agent, the ASG Guard/ASG Guard Plus allows legacy equipment to be managed and provides alarm-reporting functions.</td>
</tr>
<tr>
<td>Data Buffering</td>
<td>The ASG Guard/ASG Guard Plus can buffer all data transmitted to a host port by the attached device. Data is collected on a RAMdisk. Error messages, CDR, traffic data and other information can be subsequently delivered to a central location via dial-up or network.</td>
</tr>
</tbody>
</table>
2.6 Security Management

The ASG Guard/ASG Guard Plus maintains a database of authorized users (that is, User Database). Only users listed in the database and who successfully authenticate are allowed access. Authentication methods include password-oriented methods (Password, Callback, and Variable Callback) and token methods (ASG Key and Pager).

A Master level user assigns each user when the user's profile is added to the database. The access class determines which ports can be addressed and what information can be viewed or modified within the ASG Guard/ASG Guard Plus.

2.6.1 Access Classes

Master - Master access permits the user to change all information in ASG Guard/ASG Guard Plus. The Master user can therefore control when and how alarms are reported, add and delete users from the user database, change user profiles, modify Action and Event tables, manage data buffering and access all hosts. The Master level is the highest level of access.

Sysop 2 - A Sysop 2 level user can perform all functions listed above except modifying the user database. The Sysop 2 level user can access all hosts ports and has access to the file commands used to manage data buffering, can make changes in how ASG Guard/ASG Guard Plus responds to alarms, and change the port configuration of the unit.

Sysop 1 - The Sysop 1 level user can view pending alarms, but cannot change it. Data buffering commands are not available to the Sysop 1 user. The Sysop 1 user can access all hosts.

Host 1 to Host n - The host user only has access to a single host device. The host user cannot access any of the ASG Guard/ASG Guard Plus functions. n = number of the host user. ASG Guard can have up to four host users. ASG Guard Plus can have 16 or 28 host users. (To have 28 host users, the ASG Guard Plus must have an expansion board.)

2.6.2 User Database

Each ASG Guard/ASG Guard Plus maintains a User Database, as stated above. The database consists of a Customer User Table and a Lucent User Table. The Customer User Table contains users added by a Customer Master User (Cmaster). The Lucent User Table contains users added by a Lucent Master User (Lmaster). Lucent users provide remote maintenance support for the ASG Guard/ASG Guard Plus for warranty issues and under Service Agreements. See Chapter 6 for commands and capabilities associated with the Customer User Table and Lucent User Table.
### 2.7 Alarm Management

Alarms and events originate from a number of sources: Data received on a serial port, Timer events, Real-world measurements, as well as other activities internal to the ASG Guard/ASG Guard Plus.

When the ASG Guard/ASG Guard Plus processes an alarm or event, it checks the Action Table to determine if it is listed. If the alarm matches one listed in the Action Table, the event is placed in the Event Table for processing and listed in the system log for reference. To process the event, the ASG Guard/ASG Guard Plus performs the associated Action Routine, which performs a task associated with the alarm.

Usually the event is processed right away, and the appropriate action is taken (for example, delivering the alarm through a dial-up connection). If the event can not be acted upon immediately, it remains in the Event Table until the required time has elapsed, or the necessary resources become available (for example, the modem becomes free).

Action Routines are scripted functions that can perform a wide range of tasks associated with particular or general alarms. Certain Action Routines are included with the system, while others can be created and loaded into the ASG Guard/ASG Guard Plus in order to customize the alarm processing mechanisms and interface. Action Routines can be used to deliver alarms, take action on a host port, provide extra alarm filtering, or collect information on which subsequent alarms will be based. Action Routines can also create new alarms (called Pseudo Alarms) which allows the process to feed back on it.

---

**Event Generators**

- **Pseudo Event**
- **Internal Event**
- **Host Port**
- **Environmental Manager**

**Action Table**

"LA" to view

```
ERR000
ERR001 PAGE 555-1212
.DAILY DOLIST MIDNITE
.MIDNITE PHSYSOP
.MIDNITE.1 SCHEDULE AM PHONHOME
...
```

**Event Table**

"LE" to view

```
ERR001 000 111 222 333 System PHONHOME (ASAP)
.DAILY PHONHOME
...
```

**System Log**

"LH" to view

```
03/01/94 12:00:10 DOLIST:
03/01/94 02:10:33 Call
03/01/94 06:22:21 Event:
...
```

---

*Figure 2-6. 16-Port ASG Guard Plus Rear Panel Connectors*
2.8 Logs

The ASG Guard/ASG Guard Plus maintains logs containing details of alarms, accesses, host port activity, and system information. These logs are useful for site management, security management, and troubleshooting. All logs are maintained even if the unit is turned off. Each log type is described below.

Access History - The ASG Guard/ASG Guard Plus records each successful access. The time, date, user ID, duration of session and type of session are included in each record.

Failure History - The Failure History Log records failed access attempts. The log includes the date, time, user ID, the port accessed and the reason for failure.

Log History - This log records the activity of the ASG Guard/ASG Guard Plus and the devices to which it is connected. Activities include modem connections, received calls, Sysop sessions, and detected alarms and events.

Error Logs - The Error Log contains information regarding errors in System or User written routines.

2.9 Network Capabilities

The ASG Guard/ASG Guard Plus has both an Ethernet and PPP TCP/IP network connections. Network connections support TELNET to the ASG Guard/ASG Guard Plus, FTP for buffer and file delivery, and SNMP for TRAP delivery to network management stations. In addition, ASG Guard/ASG Guard Plus will route traffic between its network interfaces, allowing it to act as a secure remote access server for maintenance applications.

To administer information inside the ASG Guard/ASG Guard Plus, you must establish a SYSOP session. This can be done at the locally connected terminal (AUX port), through a dial-up connection, or through a TELNET session. Once a SYSOP session has been established, administration of the ASG Guard/ASG Guard Plus is through SYSOP Commands that are grouped by function into menus.

Menus are displayed by typing one of the single character SYSOP commands listed below and continued on the following page:

<table>
<thead>
<tr>
<th>Command</th>
<th>Menu</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>User Maintenance Functions</td>
<td>Commands to modify the user database are displayed.</td>
</tr>
<tr>
<td>S</td>
<td>System Functions</td>
<td>Commands to specify site and scheduling information are displayed.</td>
</tr>
<tr>
<td>A</td>
<td>Action and Alarm Functions</td>
<td>Commands to view and modify the Action Table are displayed.</td>
</tr>
<tr>
<td>L</td>
<td>Log Functions</td>
<td>Commands to view and modify logs are displayed.</td>
</tr>
<tr>
<td>F</td>
<td>File Maintenance</td>
<td>Commands to configure file buffering and manage files are displayed.</td>
</tr>
<tr>
<td>P</td>
<td>Port and Session Control Functions</td>
<td>Commands to view port status, port signals, and host session, and to display and modify network parameters are displayed.</td>
</tr>
</tbody>
</table>
Common features included on all menus are title, access level of the user, the commands and the mnemonic for each command. All other ASG Guard/ASG Guard Plus menus are listed, with the letter code that displays them. To display a different menu, enter the command letter assigned to that menu at the ">" prompt.

**NOTE:**
All commands may be entered at the system prompt. The menu does not have to be displayed first.

---

<table>
<thead>
<tr>
<th>MNEMONIC</th>
<th>COMMAND</th>
<th>OTHER MENUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU</td>
<td>List Users</td>
<td>S - System</td>
</tr>
<tr>
<td>AU</td>
<td>Add User</td>
<td>A - Alarm/Event</td>
</tr>
<tr>
<td>XU</td>
<td>Delete User</td>
<td>L - Log</td>
</tr>
<tr>
<td>DU</td>
<td>Display User Record</td>
<td>F - File</td>
</tr>
<tr>
<td>CU</td>
<td>Change User</td>
<td>P Port/Session</td>
</tr>
</tbody>
</table>

**Figure 2-7.** Screen Components
2.10 Editing Modes

The ASG Guard/ASG Guard Plus supports editing in both the TTY and VT-100 modes. VT-100 mode displays all required information and then allows you to move up and down in a screen to edit lines. In TTY mode, the lines are displayed one line at a time. TTY mode is the default mode.

2.10.1 TTY Mode

Information is displayed one line at a time for editing. After the ENTER key is pressed the next line is displayed for editing. In this mode it is impossible to return to already entered lines to modify them. TTY mode is selected in one of two ways. Either by using the SYSOP command VT OFF, which affects the current session only, or by setting the "Terminal Emulation" selection for the port (See "Setting up the ports").

2.10.2 VT-100 Mode

If you have a VT-100 terminal (or your computer is emulating a VT-100 terminal) you can execute SYSOP commands in VT-100 mode. In this mode all of the prompts will be displayed on the screen at once along with the data to be edited. The cursor will initially appear at the beginning of the first field. At this point the arrow keys can be used to move from line to line performing edits in any order. Pressing the ENTER key with the cursor on the last line of the display completes the function. VT-100 mode is selected in one of two ways. Use the SYSOP command VT ON, which only affects the current session, or set the "Terminal Emulation" selection for the port.

NOTE:
Your terminal must support VT-100 mode. If you issue the VT ON command, and your terminal does not support this mode, unpredictable results, such as the appearance of extraneous characters, may occur. If you have a VT-100 terminal (or your computer is emulating a VT-100 terminal) but you have the parameter VT100 On/Off set to Off, TTY mode is used and the configuration screens are displayed one line at a time.
2.11 Using the Editing Keys

Most SYSOP Commands display a series of prompts to allow entry of parameters specific to that command. Default or previously entered information is displayed and can be edited using the techniques described here.

Table 2-1 shows the editing keys that can be used whenever a field is presented for modification.

<table>
<thead>
<tr>
<th>Editing Function</th>
<th>Keys</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move the cursor left, right, up, or down</td>
<td>Left, right, up, or down arrow keys†</td>
</tr>
<tr>
<td>Move cursor to the right</td>
<td>[CTRL] R</td>
</tr>
<tr>
<td>Move Cursor to the Left</td>
<td>[CTRL] L</td>
</tr>
<tr>
<td>Delete the character at the cursor</td>
<td>[CTRL] D</td>
</tr>
<tr>
<td>Toggle overstrike on or off (default is off)</td>
<td>[CTRL] O</td>
</tr>
<tr>
<td>Delete text to the End of Line (EOL)</td>
<td>[CTRL] X</td>
</tr>
<tr>
<td>Move the cursor to the beginning of the line</td>
<td>[CTRL] B</td>
</tr>
<tr>
<td>Move the cursor to the end of the line</td>
<td>[CTRL] E</td>
</tr>
<tr>
<td>Backspace and delete</td>
<td>[← ] (Backspace key)</td>
</tr>
<tr>
<td>Restart field (clears all new data and returns previous data)</td>
<td>[CTRL] Z</td>
</tr>
<tr>
<td>Abort (ends edit and does not change any pre-existing data)</td>
<td>[CTRL] A</td>
</tr>
<tr>
<td>Complete a line and go to next line</td>
<td>[↵ ] (ENTER key)</td>
</tr>
<tr>
<td>Toggle choices (an example of a toggle choice is Yes or No)</td>
<td>SPACE BAR</td>
</tr>
</tbody>
</table>

† = Arrow keys and Delete key only work in the VT-100 mode (see Section 2.10.2)
2.12 Entering Commands

Commands are organized into command group menus. Each menu lists the commands and the corresponding command mnemonics. If you already know the command you wish to use, you may enter the command mnemonic at the system prompt (>). If you are uncertain of the command, you may display the menu by entering the letter assigned to that menu. If [ENTER] only is pressed, the current menu is re-displayed.

To go from one menu to another, enter the command letter assigned to that group at the "->" prompt.

**NOTE:**
*The commands displayed for a particular user is determined by the access class of that user.*

Some commands require that certain parameters be specified. For example, when you type SSP to set system parameters, type SSP and press the ENTER key, the Set System Parameters screen is displayed.

```
site123>ssp
--- Set System Parameters ---
1 = Site Information
2 = Scheduling Params
3 = Modem Action Routine Params

Select Group --> 1
```

**Screen 2-1. Set System Parameters Screen**

Some commands allow you to include additional modifiers that make the command specific. For example, to list only action items beginning with the character .H, type:

```
LA .H (or la .h)
```

and press the ENTER key. The List Action Items screen will be displayed, but only the action items starting with .H are included.

```
site123>LA .H
--- List Action Items ---

<table>
<thead>
<tr>
<th>Alarm:</th>
<th>Routine: Parameters:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>.HOURLY</td>
<td>DOLIST</td>
<td></td>
</tr>
<tr>
<td>.HOURLY.1</td>
<td>LOG</td>
<td></td>
</tr>
<tr>
<td>.HOURLY.2</td>
<td>PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>

-- End of List --
```

**Screen 2-2. List Action Items Screen**
2.12.1 Entering/Selecting Parameters

Parameters are entered or changed by either typing them in or by selecting them from a list of options. The method depends on the command.

For example, to enter a new user name in the User Name field (type U, then the ENTER key) of the Add User (type AU, then press the ENTER key) screen, type the user name:

CHRIS (or Chris)

and then press the ENTER key.

Screen 2-3. Add User Screen

In some cases, the ASG Guard/ASG Guard Plus system provides you with several options. If the option displayed is not appropriate, scroll through the list by pressing the SPACEBAR. When the selection you want appears in the field, press the ENTER key to select that item.

In the Add User screen, for example, the system initially displays ASG Key in the Primary Authentication Method parameter field. To select Password/Callback, press the SPACE BAR once to display Password/Callback in the field and then press the ENTER key.

Screen 2-4. Add User Screen
Page intentionally left blank.
3. Physical Connections and Installation

3.1 What This Chapter Contains

- A description of the LED meanings for the ASG Guard and ASG Guard Plus
- The cables and equipment required to install the ASG Guard/ASG Guard Plus
- The information you must know if you want to install the ASG Guard/ASG Guard Plus on a network
- The steps for installing the ASG Guard/ASG Guard Plus
- How to power-up the ASG Guard/ASG Guard Plus

3.2 LED Displays and Physical Connections

3.2.1 LED Meanings

The following table summarizes the functions of the LEDs on the ASG Guard and ASG Guard Plus.

<table>
<thead>
<tr>
<th>GROUP</th>
<th>LED</th>
<th>FUNCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>AC</td>
<td>Power is being supplied to the unit.</td>
</tr>
<tr>
<td></td>
<td>48VDC</td>
<td>Power is being supplied to the unit from a 48V/DC source.</td>
</tr>
<tr>
<td></td>
<td>Battery</td>
<td>Internal battery is installed and charging.</td>
</tr>
<tr>
<td></td>
<td>Power Fail</td>
<td>Main power has failed and the battery backup is supplying power to the unit.</td>
</tr>
<tr>
<td>System</td>
<td>Pulse</td>
<td>Flashes to indicate that the system is operating correctly.</td>
</tr>
<tr>
<td></td>
<td>green</td>
<td>Alarm - clear</td>
</tr>
<tr>
<td></td>
<td>red</td>
<td>Alarm - pending</td>
</tr>
<tr>
<td></td>
<td>green</td>
<td>Event - clear</td>
</tr>
<tr>
<td></td>
<td>red</td>
<td>Event - pending</td>
</tr>
<tr>
<td></td>
<td>green</td>
<td>File - clear</td>
</tr>
<tr>
<td></td>
<td>red</td>
<td>File - pending</td>
</tr>
<tr>
<td>Ports</td>
<td>Aux</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aux - RX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Aux - DTR</td>
<td></td>
</tr>
<tr>
<td>GROUP</td>
<td>LED</td>
<td>FUNCTION</td>
</tr>
<tr>
<td>-----------</td>
<td>-----</td>
<td>----------</td>
</tr>
<tr>
<td>Host 1</td>
<td>RX</td>
<td>The upper LED (RX) indicates the unit is in the process of receiving data.</td>
</tr>
<tr>
<td></td>
<td>DTR</td>
<td></td>
</tr>
<tr>
<td>Host 2</td>
<td>RX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DTR</td>
<td></td>
</tr>
<tr>
<td>Host 3</td>
<td>RX</td>
<td>The lower LED (DTR) indicates that a device is connected to the port.</td>
</tr>
<tr>
<td></td>
<td>DTR</td>
<td></td>
</tr>
<tr>
<td>Host 4</td>
<td>RX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DTR</td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td>Modem 1</td>
<td>Upper LED (RX) indicates that data is currently being transferred.</td>
</tr>
<tr>
<td></td>
<td>RX</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>Modem 2</td>
<td>RX</td>
<td>Lower LED (CD) indicates that the modem is ready to receive data.</td>
</tr>
<tr>
<td></td>
<td>CD</td>
<td></td>
</tr>
<tr>
<td>Ethernet</td>
<td>RX</td>
<td>Indicate the reception and transmission of network data.</td>
</tr>
<tr>
<td></td>
<td>TX</td>
<td></td>
</tr>
</tbody>
</table>
3.2.2 Connecting a DCE device to a Host Port

All ASG Guard/ASG Guard Plus host ports are configured as Data Communications Equipment (DCE) ports. To connect a data communications device (DCE) to an ASG Guard/ASG Guard Plus host port, you must use a “null host” cable.

Figure 3-1. Null Host 25-Pin to 25-Pin Cable Diagram

Figure 3-2. Null Host 9-Pin to 9-Pin Cable Diagram
3.3 Installation of the ASG Guard/ASG Guard Plus

3.3.1 Cables and Equipment Required

The following cables and equipment are required for installing the ASG Guard/ASG Guard Plus:

- A local terminal or a PC running a terminal emulation program. It will be used to initialize the ASG Guard/ASG Guard Plus and to administer the Aux port (RS-232 9-pin connection). The terminal should have a standard RS-232 (serial) interface for connection to DCE equipment. Use the following terminal settings unless the ASG Guard/ASG Guard Plus has been preconfigured and requires the terminal to have different settings.
  - asynchronous
  - 9600 bps
  - 8 bit character length, one stop bit, no parity
  - XON/XOFF (software) flow control

**NOTE:**
These settings can be changed after the ASG Guard/ASG Guard Plus has been initialized.

- 9-pin male-to-female RS-232C cables (one for each resource to be protected, plus one for the administration terminal)
- Telephone cords with RJ11 connectors (one for each modem)
- Network cable with an AUI or 10base-T connector
- Null modem cables/adapters (as required) if connecting a DCE device to the Host port

3.3.2 Requirements for Network Applications

For network applications, you will also need to assign the ASG Guard/ASG Guard Plus an IP address. Default addresses are provided, but you should obtain addresses that are appropriate for your network from the network administrator.

3.3.3 Install the Unit

The ASG Guard/ASG Guard Plus is installed between the port(s) of a host and/or PBX and the terminal or PC of a remote user who accesses the host(s) and/or PBX via phone line(s). Figure 3-3 shows the cable connections for the unit.

To install the ASG Guard/ASG Guard Plus:

1. Place the ASG Guard/ASG Guard Plus in the location you want.
   
   If you want to rack mount the unit, perform the following steps:
   
   a. Place a wing on each side panel of the ASG Guard/ASG Guard Plus.
   
   b. Bolt the wings in place by inserting and tightening screws in the two holes on the wing front panel and two screws in the bottom wing panel.
   
   c. After the wings are attached, place the ASG Guard/ASG Guard Plus in the rack.
2. Connect the PC or terminal to the Aux port using a standard 9-pin RS-232C serial cable. It will be used to configure the ASG Guard/ASG Guard Plus and may be disconnected after the ASG Guard/ASG Guard Plus is installed.
   a. Connect one end of the serial cable to a serial port on the terminal or computer.
   b. Connect the other end of the serial cable to the Aux Port connector on the ASG Guard/ASG Guard Plus. You may use the Aux port connector on either the rear panel or the front panel.

   **NOTE:**
   Only one Aux port may be active at a time. If both Aux ports are connected to devices, the Aux port on the front panel has priority.

3. Connect each resource to be protected to a Host port on the ASG Guard/ASG Guard Plus. The typical connection from a resource to the ASG Guard/ASG Guard Plus is from a PBX maintenance port to a ASG Guard/ASG Guard Plus host port.
   All ASG Guard/ASG Guard Plus host ports are configured as Data Communications Equipment (DCE) ports. To connect a data communications device (DCE) to the ASG Guard/ASG Guard Plus host port, you must use a null modem cable/adapter.
   a. Connect one end of a standard RS-232C serial cable to the maintenance port of the host or PBX.
   b. Connect the other end to the first HOST connector on ASG Guard/ASG Guard Plus.
   c. Follow a similar procedure to connect each resource to a host port.

4. Connect analog telephone line(s) to the appropriate RJ11 connector(s) on the ASG Guard/ASG Guard Plus internal modem(s). The ASG Guard/ASG Guard Plus will have two PCMCIA modems installed.

   **NOTE:**
   A PCMCIA modem is field-installable only by qualified Lucent personnel.

5. If you are connecting the unit to an Ethernet network, connect the network cable to either the 10-Base-T or AUI connector.

6. Connect the power supply. The ASG Guard/ASG Guard Plus may be connected to a standard 120VAC 60Hz or 220VAC 50Hz power source by using the wall pack. An optional 48V DC power supply may also be used instead of, or in combination with, the AC supply.
   To power the ASG Guard/ASG Guard Plus from a 16V AC power supply:
   a. Connect the 6-pin modular jack on one end of the wall pack cable to the 16 VAC POWER connector located on the rear panel of the ASG Guard/ASG Guard Plus.
   b. Connect the power supply to a standard 120 volt AC power source.
3.3.4 Power up the ASG Guard/ASG Guard Plus

To power up the ASG Guard/ASG Guard Plus, turn the key clockwise to the horizontal position. The red Power LED lights immediately, and the System and Ports LEDs light to indicate the power-up sequence. After about 30 seconds, the LEDs will flash three times. Thirty seconds later, initialization will be complete, and the appropriate LEDs should remain lit to indicate the status of the ASG Guard/ASG Guard Plus. The system status LED labeled pulse (heart icon) will continue to flash periodically, indicating that the system is operating correctly.
The screen with your communication package will show the AUX port information at start-up. It should look similar to the following screen.

---
---
ASG Guard v3.7 (F/W 3.7) ---
--- Copyright 1998, MicroFrame Inc. ---
--- All Rights Reserved ---
---

10/07/98 15:47:49 E5D0 SYSTEM UPGRADE: ASG Guard version 3.7B
10/07/98 15:47:50 25E8 ASG Guard System stopped 10/07/96 at 12:29
10/07/98 15:47:50 ACCA ASG Guard v3.7 (F/W 3.7) - Reset
10/07/98 15:47:50 DBFC Serial Number:
10/07/98 15:47:50 1903 Modem 1 - TDK DF3000 Data/Fax Modem
10/07/98 15:47:50 40C0 Modem 2 - NOT INSTALLED
10/07/98 15:47:56 41C9 [H] Host 1 Idle
10/07/98 15:47:57 1789 [H] Host 2 Idle
10/07/98 15:47:58 D55E [H] Host 3 Idle
10/07/98 15:48:00 AB5B [H] Host 4 Idle

Screen 3-1. AUX Port Information Screen

For more information regarding the front panel and the associated LEDs, refer to "ASG Guard Front Panel," "ASG Guard Plus Front Panel," and "LED Meanings" in Chapter 2.

3.3.5 Verify PSTN Access

To verify the phone lines and the modems in the ASG Guard/ASG Guard Plus, you must dial into the ASG Guard/ASG Guard Plus. Use the communications software package on your PC to dial the phone number of each modem.
Page intentionally left blank.
4. Basic Configuration

4.1 What This Chapter Contains

- How to Add a User Profile
- Description of Network Parameters
- How to Configure the AUX and Host Ports
- Securing the AUX Port
- Reinitializing the ASG Guard/ASG Guard Plus

The ASG Guard/ASG Guard Plus contains a database of authorized users (that is, the User Database). The User Database includes information about each user, including user ID, access level, authentication method and system restrictions. The first user entered into the database should have an access level of master. A master level user can access all the features of the ASG Guard/ASG Guard Plus and can add and delete users from the User Database.

A default system allows Master level access via the local terminal (AUX Port) which can be disabled later.

See Section 2.6 for more information on the User Database and access classes.

4.2 Add the First User Profile

The AU (Add User) command allows you to add an authorized user to the ASG Guard/ASG Guard Plus system. The following procedure should be used to enter the master user.

To add a master user, type AU at the system prompt and press the ENTER key. (You may also type the user name as part of the command.)

For example:

AU CHRIS

In either case, the Add User screen will appear after you enter a user name and press the ENTER key. Note that only one line appears at a time.
--- Add User ---

User Name                          CHRIS
Access Class                       Host One
Block Access                       No
Sessions Allowed (blank=unlimited)
User Expiration Date
Primary Authentication Method      ASG Key
Secondary Authentication Method    None
Auto Execute Command
Comments (1):
(2):
(3):

Screen 4-1. Add User Screen

Field                        Function
User Name
Enter a user name. User names may be up to 15 alpha/numeric characters in length, no spaces are allowed.

NOTE: The ASG Guard/ASG Guard Plus converts all alphabetical characters to upper case.

Access Class
Select CMaster by pressing the SPACE BAR until CMaster is displayed. The CMaster user can modify the user database and can access all ASG Guard/ASG Guard Plus commands including modification of the user database.

NOTE: The first user entered should be a master level user. A CMaster user should be maintained in all systems at all times.

When entering subsequent user profiles, display the Access Classes by pressing the SPACE BAR. Press the ENTER key to select a class.

Block Access
Initially No appears on the screen. Press the SPACE BAR to toggle to Yes.

Select No to allow a user to access the ASG Guard/ASG Guard Plus (that is, do not block access). Select Yes will prevent a user from accessing the ASG Guard/ASG Guard Plus.

Sessions Allowed
Press the ENTER key to allow unlimited sessions.

If the user is to be limited to a finite number of sessions, specify the number of successful sessions allowed for that user by typing in a number from 1 to 999 and pressing the ENTER key.
**User Expiration Date**

Press the ENTER key to NOT have the user’s access privileges expire at a certain date.

If the user privileges are to expire on a specific date, enter the date in the specified month/day/year format and press the ENTER key, which the user will no longer have access to the ASG Guard/ASG Guard Plus. After this date, the user will be denied access.

**NOTE:** If you use a two-digit year format, the years from 00 - 84 will be reported as 2000-2084.

**Primary Authentication Method**

Press the SPACE BAR until the desired choice is displayed: ASG Key, Password/Callback, and Pager. Select the appropriate method by pressing the ENTER key when the desired choice appears.

**NOTE:** Depending on which method of authentication you select, you will be prompted for further information after you complete the main portion of this screen.

**Password/Callback** contains three options: passthru, regular callback and variable callback.

- **Passthru** option requires only that the user enter the correct ID and password to access the ASG Guard/ASG Guard Plus and the equipment it protects.

- **Regular callback** requires the user to have a specific phone number stored in the ASG Guard/ASG Guard Plus database as well as a password. After the user calls the ASG Guard/ASG Guard Plus and enters the correct ID and password, the ASG Guard/ASG Guard Plus will disconnect and call the user back at the stored telephone number. The password is then re-entered.

- **Variable callback** is similar to regular callback, except that the user enters a telephone number during each login. The ASG Guard/ASG Guard Plus will call the user back at the specified telephone number, which may be different from session to session.
ASG Key requires a hand-held device known as a token. During login, the ASG Guard/ASG Guard Plus will send a “challenge” number, which the user enters into the ASG Key unit. The unit then generates a “response” number, which the user sends back to the ASG Guard/ASG Guard Plus. Both units use a DES encryption algorithm associated with a 20 digit “key”.

Pager access requires a user to have the telephone number or PIN of a digital pager stored in the user database. During login, the ASG Guard/ASG Guard Plus will send a one-time numeric password to the user’s pager. The user must enter that password in order to gain access to the ASG Guard/ASG Guard Plus.

**Secondary Authentication Method**
(Optional) Select a second means of access for a user. Use the SPACE BAR to scroll through the following selections: None, ASG Key, Password/Callback and Pager.

**NOTE:** Depending on the authentication method selected, prompts for further information will appear after you complete the main portion of this screen.

**Auto Execute Command**
(Optional) Enter a command that will be executed automatically after the user has been authenticated by the system. This is available only to Sysop users, not Host users.

For example, if you enter LH - the log history will be displayed in reverse order after the user authenticates.

**Comments**
Enter up to 40 alphanumeric characters on the Comments line and press the ENTER key.

### 4.2.1 Password/Callback Authentication Method
If Password/Callback was selected as the primary authentication method, the ASG Guard/ASG Guard Plus will display the following information after the comments field.

|--Password/Callback Details--
Enter Password ************

**Screen 4-2. Password/Callback Details Screen**

Enter a password. The password may be up to 15 alphanumeric characters. Asterisks appear on the screen as you type to prevent your password being displayed on the screen.

**NOTE:**
Passwords are case sensitive.
After you type the password and press the ENTER key, you will then be prompted to verify your password. Retype the password exactly as you entered it the first time, and then press the ENTER key.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Password</td>
<td>Enter Password: **********</td>
</tr>
<tr>
<td>Verify Password</td>
<td>Verify Password: **********</td>
</tr>
<tr>
<td>Access Option</td>
<td>Access Option: Regular Callback</td>
</tr>
<tr>
<td>Phone Number</td>
<td>Phone Number: 19085553435</td>
</tr>
</tbody>
</table>

Screen 4-3. Password/Callback Details Screen

You are next asked to select an access option. Press the SPACE BAR until the desired choice is displayed from these Access Option selections:

- **Regular Callback**: Regular Callback requires the user to have a specific phone number listed in the ASG Guard/ASG Guard Plus user database, in addition to the password. After receiving a phone call followed by the corresponding user name and password, the ASG Guard/ASG Guard Plus disconnects the call, the caller hangs up, and then the ASG Guard/ASG Guard Plus dials the caller back using the number in its database for that user.

  If Regular Callback is selected, you are prompted to enter a phone number.  

  **NOTE**: Enter the phone number as the system needs to dial it. For example, if the ASG Guard/ASG Guard Plus has to dial 9 to get an outside line, or if the number is in a different area code and the ASG Guard/ASG Guard Plus has to dial a 1 first, enter those numbers as well. Dialing instructions common to all users (such as dialing 9 to get an outside line) should be included in the modem dial string by using the Set Modem (SM) command.

- **Passthru**: Passthru requires only the user to enter the correct password after first entering a user name.

- **Variable Callback**: Variable Callback requires a user name and corresponding password. After dialing in to the ASG Guard/ASG Guard Plus and entering the correct user name and password, the user enters a phone number for the ASG Guard/ASG Guard Plus to call back. The ASG Guard/ASG Guard Plus disconnects and the user hangs up. The ASG Guard/ASG Guard Plus then calls the user back at the phone number provided.
4.2.2 ASG Key Authentication Method

If ASG Key was selected as the primary authentication method, the ASG Guard/ASG Guard Plus will display the following information after the comments field.

```
-- ASG Key Details --
Encryption Key Source               Randomly Generated
```

Screen 4-4. ASG Key Details Screen

Encryption Key Source

Use the SPACE BAR to scroll through the following Encryption Key Source selections for the ASG Key authentication method. The choices are listed below:

- Randomly Generated
- Device ID/User Code
- Fixed

Field Function

Randomly Generated

When this source is selected, press the SPACE BAR and the ASG Guard Plus automatically generates the key value and displays the information on the screen.

The information displayed in the Enter These Digits as Key1 or Key2 field is to be entered in to the ASG Key when you initialize the ASG Key. Be sure to note this information carefully. If you make an error in transcribing the information for the ASG Key, use the Change User command to redo the procedure. Follow the instructions supplied with the ASG Key to initialize the ASG Key.

Enter the Test Challenge information displayed on the screen (the test challenge is always "1234567") into your ASG Key per the instructions provided with the ASG Key. If the Reply on your ASG Key matches the one on the screen, you have successfully added this user.

```
-- ASG Key Details --
Encryption Key Source               Randomly Generated

Enter These Digits as Key1 or Key2: 0443 2126 = 3422 1505 = 3160 =
Test Challenge: 1234567 ...Reply: 040-2181

Press <ENTER> to Continue
```

Screen 4-5. ASG Key Details Screen
### Field Function

The *Fixed* selection allows you to enter either 14 hex or 20 octal numbers for your source. The ASG Guard/ASG Guard Plus prompts you for the required information. Hex values include the digits 0 to 9 and the letters A to F. Octal values are digits from 0 to 7. (For example, if you select a hex code, a valid entry would be “003FA876DE45CD”)

This option is provided in case where a ASG Key has been assigned a user from some other system, and the Administrator wants the users to use the same ASG Key with this system.

---

**-- ASG Key Details --**

<table>
<thead>
<tr>
<th>Encryption Key Source</th>
<th>Fixed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fixed Key (14 hex or 20 octal)</td>
<td>003FA876DE45CD</td>
</tr>
<tr>
<td>Enter These Digits as Key1 or Key2:</td>
<td>0443 2126 = 3422 1505 = 3160 =</td>
</tr>
<tr>
<td>Test Challenge:</td>
<td>1234567 ...Reply: 040-2181</td>
</tr>
</tbody>
</table>

Press <ENTER> to Continue

```
```

### Screen 4-6. ASG Key Details Screen

To select the encryption key source, press the ENTER key when the appropriate key source appears on the screen.

The system will then confirm that the user has been added to the database.

Check that the user has been added correctly by typing **DU** (Display user) at the system prompt. If any information is incorrect, type **CU** (Change user) at the system prompt to modify the user information.
4.3 Specify Network Parameters

If the ASG Guard/ASG Guard Plus is part of a network, it is necessary to set both the Ethernet and IP addresses that are appropriate for your system. To display the Set Network Parameters screen, type `S NP` at the system prompt. For a detailed explanation, refer to Section 12.7.1.

```
> s np

--- Set Network Params ---

1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params

Select Group --> 1
Rest ore Factory Defaults ? No
--- Network Initialization Parameters ---
Start Network on Power-up ? No
Ethernet Address (hhhhhhhhhhhh) 08 01 02 00 03 E9
IP Address (nnn.nnn.nnn.nnn) 192.9.200.2
PPP Address (nnn.nnn.nnn.nnn) 192.9.200.3
Default Gateway (nnn.nnn.nnn.nnn)

To start the network type STARTNET

```

**Screen 4-7.** Set Network Params Screen

For a detailed explanation of **Group 1** Network Initialization Params, refer to Section 12.4.

For a detailed explanation of **Group 2** SNMP Manager Params, refer to Section 12.5 and 12.7.

For a detailed explanation of **Group 3** FTP Params, refer to Section 12.11.

To verify that the ASG Guard/ASG Guard Plus can be accessed through the network, start the network module by typing `STARTNET` at the system prompt. Access the ASG Guard/ASG Guard Plus from a terminal on the network using the IP address that you just entered.
4.4 Configure the AUX Port

The next step in setting up the ASG Guard/ASG Guard Plus is to configure the AUX and host ports of the ASG Guard/ASG Guard Plus. When specifying the parameters of these communications ports, remember that they are independent of each other and should be set according to their specific use. For example, each Modem, Host and AUX port can have different speed and parity settings. The ASG Guard/ASG Guard Plus performs all conversions as data passes between ports.

Depending on the application, one or more host ports and/or Modem Ports will require configuration.

The AUX port settings reflect the characteristics of a terminal connected locally to the ASG Guard/ASG Guard Plus AUX port connector. The ASG Guard/ASG Guard Plus includes default values for these parameters. The default settings are listed in Appendix C.

```
site123>sa
--- Set AUX Port Params ---
Restore Factory Defaults ? No
Baud Rate 9600
Char. Length / Parity 8 / None
Terminal Emulation TTY
Default Access Class CMaster
Output While Port Idle Log Data
Sysop Idle Timer None
Host Session Idle Timer None
Host Session Disconnect on Ctrl+A Yes
```

**Screen 4-8. Set AUX Port Params Screen**

To change the settings of the AUX port, type `SA -- Set AUX Port Parameters`. Changes to the AUX Port parameters become effective after the current AUX session is terminated.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Factory Defaults</td>
<td>Initially <strong>No</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>Yes</strong>.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Yes</strong> to restore the settings with which the ASG Guard/ASG Guard Plus was shipped. Select <strong>No</strong> to keep the current settings. The default settings are listed in Appendix C of this manual. Press the ENTER key after desired choice is selected.</td>
</tr>
</tbody>
</table>
Basic Configuration

**Baud Rate**

Speed at which the ASG Guard/ASG Guard Plus transmits data to and receives data from the AUX Port. Press the SPACE BAR until the desired choice is displayed. Press the ENTER key when the desired speed appears.

- 300 bps
- 1200 bps
- 2400 bps
- 4800 bps
- 9600 bps
- 19200 bps
- 38.4 Kbps
- 57.6 Kbps

**Char.Length/Parity**

The character length and parity characteristics the ASG Guard/ASG Guard Plus uses to communicate with the terminal connected to the AUX Port. Press the SPACE BAR until the desired choice is displayed.

**Terminal Emulation**

Specifies the type of terminal that your computer is emulating when it is connected to the ASG Guard/ASG Guard Plus AUX port. Options are TTY and VT-100. Note that your terminal program must support VT-100 emulation. Press the SPACE BAR until the desired choice is displayed.

**Default Access Class**

In addition to the user profiles created with the AU (Add User) command, the ASG Guard/ASG Guard Plus can be configured to permit access through the AUX port without authentication. The Default Access Class defines the type of access granted when a user establishes an AUX port session as the default user. Options include None, CMaster, Sysop1, Sysop2, and Host n, where n is the host port number. Press the SPACE BAR until the desired choice is displayed. These levels are explained in [Section 6.5](#).

Select None to require all users accessing the system via the AUX port to log in.

**Output While Port Idle**

Selects the function of the AUX port while no user sessions active through it. Options are Log Data, host port, PPP Connect, and None. Press the SPACE BAR until the desired choice is displayed.

Log Data prints log information to the AUX port.

PPP Connect attempts to establish a PPP session with the device connected to the AUX port. Host Port prints the output for the specified port.
4.5 Initiate Security on the AUX Port

After the initial setup, you may keep the terminal connected to the Aux Port for system administration purposes. *If the terminal is left connected, security can be implemented by setting the AUX port to restrict log-ins.*

To restrict logins, type `SA` (Set AUX Port) at the system prompt. Press the ENTER key until the cursor is at the *Default Access Class* parameter. Select either a new default access class or select None to require all users accessing the system via the AUX port to log in.
4.6 Configure a Host Port

A host port connects the ASG Guard/ASG Guard Plus to a host device, for example, PBX, router, hub, voice mail, etc. The settings for each host port can be set independently and should be identical to the host device settings. If the Modem port or AUX port is set to a different speed or parity from the host port, the ASG Guard/ASG Guard Plus performs all conversions as data passes between ports.

To set the host port parameters, type SH at the system prompt, and press the ENTER key. Enter host number and press the ENTER key again. Set the parameters for host port communications, then select the desired port. Alternatively, you can enter SH n, where n is the port number, as shown in the following example. The parameters affect how host events are received. Changes to host port parameters become effective immediately upon completion of the command.

```
ASGGUARD1>sh 1
--- Set Host Port Params ---
Restore Factory Defaults ? No
-- Host 0:
  Host Name                             DEFINITY
  Baud Rate Setting                     9600
  Character Length / Parity             8 / None
  Alarm Filter                          Definity
  Force CD/DSR High                     DSR Only
  Flow Control                          None

-- Automatic Buffering --
  Enable Automatic Buffering ? No
  Compress closed buffer files ? No

Auto Switch: (Enter 0 to disable)
  When CURRENT File exceeds ‘n’ KB 50
  Every ‘n’ Hours 24
  - Synchronize at what hour (0-23) 0

-- Alarm Delivery --
  Modem used for Alarm Delivery Modem #1
```

Screen 4-9. Set Host Port Params Screen
Field | Function
--- | ---
Restore Factory Defaults | Initially **No** appears on the screen. Press the SPACE BAR to toggle to **Yes**.

Select **Yes** to restore the settings with which the ASG Guard/ASG Guard Plus was shipped. Select **No** to keep the current settings. Default settings are listed in the appendix at the end of this manual. Press the ENTER key after desired choice is selected.

**Host Name**
The name assigned to the host port in the Set System Parameters screen. Each host port can be named. The name appears when the SH, DH, JS, JSL, CON, or CONL commands are entered. This helps in selecting the appropriate ports. The host port name can be up to 12 characters. The first character must be a letter. No spaces are permitted. The host port name is used to name the directory for the host port if buffering is enabled.

**Baud Rate Setting**
Speed at which the host communicates with the ASG Guard/ASG Guard Plus. Press the SPACE BAR until the desired choice is displayed.

- 300 bps
- 1200 bps
- 2400 bps
- 4800 bps
- 9600 bps
- 19200 bps
- 38.4 Kbps
- 57.6 Kbps

**Character Length/Parity**
The character length and parity characteristics of the Host Port connecting to the host device should match the host device value. Press the SPACE BAR until the desired choice is displayed.

**Alarm Filter**
Type of processing that the ASG Guard/ASG Guard Plus will use to analyze data received by the host port. Standard choices are None, Definity, Intuity, Generic Alarms, Meridian Alarms, and SL100 Alarms. Press the SPACE BAR until the desired choice is displayed. If a custom Host Processing Data Routine has been loaded into the ASG Guard/ASG Guard Plus, it will also be displayed in the list of choices.

**Force CD/DSR High**
Determines the status of CD/DSR signal during host connection. Press the SPACE BAR until the desired choice is displayed and then press the ENTER key.
### Basic Configuration

**Flow Control**
Type of flow control applied to the Host Port. Choices are RTS/CTS (hardware), XON/XOFF (software), None. Press the SPACE BAR until the desired choice is displayed.

The remaining parameters on this screen specify 1.) whether data received by a host port is saved to the ASG Guard/ASG Guard Plus RAMdisk or is discarded, and 2.) the modem used for alarm delivery.

<table>
<thead>
<tr>
<th>--Automatic Buffering--</th>
<th>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Select Yes to store in a file the data received from this host. Select No to discard the data after it has been processed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Automatic Buffering?</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compress closed buffer files?</th>
<th>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Select Yes to compress the buffer files automatically when they are closed. Press the ENTER key when the appropriate selection is displayed. Data is typically compressed at a ratio of 4:1. The ratio, however, varies with the type of data.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Select Yes to compress the buffer files automatically when they are closed. Press the ENTER key when the appropriate selection is displayed. Data is typically compressed at a ratio of 4:1. The ratio, however, varies with the type of data.</td>
</tr>
</tbody>
</table>

**Auto Switch (enter 0 to disable)**

<table>
<thead>
<tr>
<th>When CURRENT File exceeds 'n' KB</th>
<th>Enter the file size (in KB) at which the buffer should be switched.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Every n hours</th>
<th>Enter the number of hours between the switching of buffers.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Synchronize at what hour (0-23)</th>
<th>Indicate the hour at which the buffer switching should be synchronized.</th>
</tr>
</thead>
</table>

The following prompts are based on previous responses to the Automatic Buffering fields:

<table>
<thead>
<tr>
<th>Open Host Buffer Now?</th>
<th>This prompt will only appear when automatic buffering is enabled, but the buffer is currently closed.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Close Host Buffer Now?</th>
<th>This prompt will only appear when automatic buffering is not enabled and the buffer is currently open.</th>
</tr>
</thead>
</table>

Buffers are switched when any of the parameters are met. For a description of Buffer Switching, refer to [Chapter 7](#).
The following prompts are based on previous responses to the Alarm Filter field:

**Modem Used for Alarm Delivery**

This prompt has three options: First Available, Modem 1, and Modem 2. First Available option will use either Modem 1 or Modem 2, whichever one is available. The Modem 1 or Modem 2 option will only attempt to use these phone lines to deliver alarms from the host device.
4.7 Re-Initialize the ASG Guard/ASG Guard Plus via the AUX Port

**WARNING!**:
*This procedure will erase all modifications to the unit including all user files, action routines, logs, and all other settings. Prior to performing this procedure, we recommend that you back up your unit. (See Appendix C.)*

To reset the ASG Guard/ASG Guard Plus to factory settings, follow these steps:

1. Connect a terminal to the AUX port of the ASG Guard/ASG Guard Plus.
2. Using communications software in your computer, set the AUX port of ASG Guard/ASG Guard Plus to 9600 bps.
3. Power-up the ASG Guard Plus.
   - The LED’s light in sequence as each area of software is checked.
   - When the start-up check is complete, the LED’s will flash 3 times, then the pulse (heartbeat) LED lights.
4. At the same time the pulse LED ‘lights’, the ASG Guard/ASG Guard Plus banner will appear. Immediately hit the RETURN key and type (IN CAPS) **INIT**.
5. At the next prompt, press the SPACEBAR to enter YES to reinitialize. (Default is NO.)
5. Modem Port Setup

5.1 What This Chapter Contains

- Overview
- How to display and set modem parameters
- Explanation of each parameter

5.2 Overview

The parameters of each modem port specify the configuration of the port. Modem port parameters must be set correctly in order for you to successfully dial into the ASG Guard/ASG Guard Plus from a remote location and for the ASG Guard/ASG Guard Plus to dial out.

Each unit is shipped with factory defaults for the modems installed in ASG Guard/ASG Guard Plus.

5.3 Modem Port Parameters

5.3.1 Display Modem Port Parameters – DM Command

The DM (Display Modem port parameters) command enables you to view the parameters of the specified modem port.

Type DM at the system prompt to display the modem port parameters. You will be prompted to enter the number of the modem port whose parameters you wish to view. The display will look similar to the one in the SM parameters section. Each parameter is explained in the SM section.
ASGGUARD1>DM

--- Display Modem Port Params ---
Modem Number 1

Baud Rate Settings:
  Modem Control Strings 19200
  User Session CONNECT n
Char. Length / Parity 8 / None
Terminal Emulation TTY
Sysop Idle Timer None
Host Session Idle Timer None
Host Session Disconnect on Ctrl+A Yes

Modem Control Strings (Use '|' for ENTER; '~' for 1 second delay)
Setup                              |~AT &F E0 &C1 &D2 S0=0 S2=38|
Setup (continued)                  |
Answer                             ATA|
Hang Up                             ~&&&~AT|~ATS0=0 H0|
Dial Strings (Use '###' for Phone No., 'MSG' for Pager Message)
  Modem ATDT ###|
  Pager ATDT ### @ MSG ;|

Screen 5-1. Display Modem Port Params Screen

The ASG Guard Plus has the option to add four (4) additional external modems by changing host ports 13 - 16 into modem ports. At the system prompt, type SSP, and at the command line "Number of Expansion Ports reassigned to Modems" type 4, and press the ENTER key.

site123>SSP

--- Set System Parameters ---

1 = Site Information
2 = Scheduling Params
3 = Modem Action Routine Params

Select Group -->1
-- Site Information --
Site Name (USN=Unit Ser. Number) Ser#USN
Unit Phone Number
Host Password for login routine 0000
Number of Expansion Ports Reassigned to Modems 4

Screen 5-2. Set System Parameters Screen

NOTE:
Changes to the Expansion Board Modems will not take effect until the ASG Guard/ASG Guard Plus is restarted.
5.3.2 Set Modem Port Parameters – SM Command

The SM command enables you to display and change the parameters for each modem port. Parameters include baud rate settings, parity, and terminal emulation.

Type SM at the system prompt to display modem port parameters.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Number</td>
<td>Select the modem whose settings you wish to change.</td>
</tr>
<tr>
<td>Restore Factory Defaults?</td>
<td>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Select Yes to restore the settings with which the ASG Guard/ASG Guard Plus was shipped. Select No to keep the current settings. The factory default settings are listed in the appendix.</td>
</tr>
<tr>
<td>Baud Rate Settings:</td>
<td>The speed at which the ASG Guard/ASG Guard Plus transmits data to the modem (internal or external). An AT modem will not usually establish a session with a remote modem at a speed greater than the speed at which it was set up. The actual speed of the user session is a function of the type of connection that is made between the remote modem and the ASG Guard/ASG Guard Plus modem.</td>
</tr>
<tr>
<td>Modem Control Strings:</td>
<td></td>
</tr>
<tr>
<td>Setup ( Use '</td>
<td>' for ENTER; '~' for 1 second delay )</td>
</tr>
<tr>
<td>Modem Control Strings ( Use '</td>
<td>' for ENTER; '~' for 1 second delay )</td>
</tr>
<tr>
<td>Dial Strings ( Use ‘###’ for Phone No., ‘MSG’ for Pager Message)</td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td></td>
</tr>
<tr>
<td>Pager</td>
<td></td>
</tr>
</tbody>
</table>
Press the SPACE BAR until the desired choice is displayed. When the speed you want appears in the field, press the ENTER key to select that speed and advance to the next parameter.

Available baud rates are 300, 1200, 2500, 4800, 9600, 19200, 38400 and 57600.

**User Session**

The speed at which the ASG Guard/ASG Guard Plus communicates with its modem.

When a connection is made to a remote modem, the modems negotiate the appropriate speed for the link. After the speed has been determined, a message is sent to the ASG Guard/ASG Guard Plus modem such as "CONNECT 2400" or "CONNECT 9600". Normally, the modem switches to the speed in the message. Some modems, however, (and most modems at some connect speeds) do not indicate the speed with a CONNECT message. In these instances, the speed must be derived some other way.

Usually an Auto Baud routine is used to sense the speed of the incoming data. Sometimes it is preferable to force the incoming session at a particular speed. CONNECT n sets the speed of the session to the speed in the CONNECT message. If CONNECT n is chosen, and no CONNECT message is sent to the ASG Guard/ASG Guard Plus modem, it reverts to Auto Baud.

Press the SPACE BAR until the desired choice is displayed. When the speed you want appears in the field, press the ENTER key to select that speed. Speeds available are CONNECT n, 57600, 38400, 19200, 9600, 4800, 2400, 1200, 300 and Auto.

**Char. Length/Parity**

Use the SPACE BAR to select the character length and parity characteristics of the Modem Port. Available entries are 7 or 8 data bits, with Even, Odd, Mark, Space or no parity. The Auto entry initiates an auto-parity routine with the user.
### Terminal Emulation
Specify the type of terminal that your computer is emulating when your computer is connected to the Modem Port via a remote modem.
Press the SPACE BAR to toggle between TTY and VT100.

If your computer is emulating a DEC VT-100 terminal, select VT100. If your computer is not emulating a DEC VT-100 terminal, select TTY. After you make your selection, press the ENTER key.

**NOTE: Only Sysop sessions are affected.**

### Sysop Idle Timer
The Sysop idle timer defines the maximum duration of inactivity time during a Sysop session before the call is terminated and the modem is reset.
Press the SPACE BAR until the desired choice is displayed. When your choice appears in the field, press ENTER key to make your selection.

Available selections are 1 min, 5 min, 10 min, 20 min and none.

### Host Session Idle Timer
The Host Session idle timer defines the maximum duration of inactivity time during a Host session before the call is terminated and the modem is reset.
Press the SPACE BAR until the desired choice is displayed. When your choice appears in the field, press the ENTER key to make your selection and advance to the next parameter.

Available selections are 1 min, 5 min, 10 min, 20 min, none.

### Host Session Disconnect on Ctrl + A
Initially **Yes** appears on the screen. Press the SPACE BAR to toggle to **No.**

### Setup
Defines the AT command string used to set up the modem. You may edit this field, depending on your modem requirements.

**NOTE: The factory defaults shown above are specific for the installed modem. If the ASG Guard/ASG Guard Plus includes a modem of a different make or model, a different command string is required. Consult the modem manual to determine the appropriate command string.**

### Answer
Defines the AT Command string used to answer calls. This should be either ATA (answer immediately) or left blank. ATS0=n (answer on the nth ring) can be included in the setup initialization, however, the default ATA is recommended.
Modem Port Setup

**Hangup**

Defines the sequence for hanging up the line

```
~+++~AT|~ATS0=0 H0|
```

where

- `~+++~` escape sequence
- `ATS0=0` disables auto answer
- `ATH` forces modem on-hook hang up

**Dial Strings**

**Modem**

The command string used to initiate a dial-out sequence with the modem. This is typically used as part of a Callback authentication process or to deliver an alarm.

*Example:*  

```
ATDT ### |
```

The default phone number will be substituted for the `###` characters.

**Pager**

This command string specifies the dial string used by the modem to deliver a message to the pager.

*Example:*  

```
ATDT ### @ MSG ; |
```

The default pager number from the System Parameter table will be substituted for the `###` characters and the default pager message will be substituted for `MSG`. Press the ENTER key to confirm your entry.

**NOTE:**

The `|` character represents a carriage return, and allows more than one command to be entered on a single line as though it were being entered on multiple lines. The `~` character forces a one second delay. After editing the field, press the ENTER key.
5.4 Verify the Settings

To ensure that the settings are correct, do the following:

1. Dial into the ASG Guard/ASG Guard Plus to verify that you can access it. Log on as a Master user. If you cannot dial in, check the modem port settings.

2. Check that the ASG Guard/ASG Guard Plus can dial out. Add an Action Item PHONHOME that is issued when a particular event is generated. Generate the event by using the GE command. (See Chapter 8 for more information on Action Tables and Action Items.) Have the ASG Guard/ASG Guard Plus dial a PC running a terminal emulation program. If the connection is successful, the date, time, site name, alarm and event comment is displayed on the screen.
Page intentionally left blank.
6. Modifying the User Database

6.1 What This Chapter Contains

- Overview
- User Maintenance Functions Menu
- How to Add, Delete and Change Information in the User Database
- Description of Access Level and Authentication Methods

6.2 Overview

The ASG Guard/ASG Guard Plus maintains a database of authorized users. Each user who accesses the ASG Guard/ASG Guard Plus or a host(s) through a dial-up port or network connection must have been added to the database. By limiting access through each of the ports, the ASG Guard/ASG Guard Plus provides access security to both the ASG Guard/ASG Guard Plus and protected host devices.

The ASG Guard User Database actually consists of two distinct sets of users: Lucent users and Lucent customer users. The portion of the User Database that specifies the Lucent users is called the Lucent User Table. The portion of the User Database that specifies the Lucent customer users is called the Customer User Table.

The User Database residing in the ASG Guard/ASG Guard Plus contains information about each user, including: the users name, access class, and authentication method. The information included in the database is listed below. The user database can hold information for 75 users.

Each record in the database contains the following information about the user:

- User Name (ID)
- Password or key
- Access Class
- Whether user access is blocked
- User Access Expiration Date
- Number of sessions allowed
- Primary and Secondary Authentication Methods
- Auto Execute Command
- Comments

Each user is assigned an access class that determines his/her access and administrative privileges. Users assigned the access class "Host" can only access host ports and have no administrative privileges on the ASG Guard/ASG Guard Plus. Sysop and Master users can also administer the ASG Guard/ASG Guard Plus, in addition to accessing the host ports.

**NOTE:**

*Only a user with CMaster access privileges can add, delete or modify customer user profiles in the database.*
6.3 Display the User Maintenance Functions Menu

The User Maintenance Functions Menu displays all commands associated with adding, deleting and changing information in the Customer User Table.

To display the User Maintenance Functions Menu, type U at the system prompt and press the ENTER key. All commands associated with maintaining the Customer User Table are shown on this menu.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LU</td>
<td>List Users</td>
</tr>
<tr>
<td>AU</td>
<td>Add User</td>
</tr>
<tr>
<td>XU</td>
<td>Delete User</td>
</tr>
<tr>
<td>LLU</td>
<td>List Lucent Users</td>
</tr>
<tr>
<td>BLU</td>
<td>Block/Unblock Lucent User</td>
</tr>
<tr>
<td>DU</td>
<td>Display User Record</td>
</tr>
<tr>
<td>CU</td>
<td>Change User</td>
</tr>
<tr>
<td>SCK</td>
<td>Set Customer Key</td>
</tr>
<tr>
<td>DLU</td>
<td>Display Lucent User Record</td>
</tr>
<tr>
<td>BLA</td>
<td>Block/Unblock Lucent Asadmin.</td>
</tr>
</tbody>
</table>

Other Menus: S -System  A -Alarm/Event  L -Log  F -File  P -Port/Session

Screen 6-1. User Maintenance Functions Screen
6.4 Command Summary

The Customer User Table contains the records for authorized customer users of the ASG Guard/ASG Guard Plus system.

Table 6-1 lists the commands to administer the Customer User Table. The table includes a brief description of each command and lists the access level that a user must have to successfully issue the command.

**Table 6-1. User Commands**

<table>
<thead>
<tr>
<th>Function</th>
<th>Description</th>
<th>Access Class Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU - Add User</td>
<td>Adds a user profile to be added to the Customer User Table.</td>
<td>CMaster</td>
</tr>
<tr>
<td>CU - Change User</td>
<td>Changes the information associated with a user who has already been entered into the system using the Add User command.</td>
<td>CMaster</td>
</tr>
<tr>
<td>DU - Display User Record</td>
<td>Displays entire record for the user selected.</td>
<td>Sysop 2, CMaster</td>
</tr>
<tr>
<td>LU - List Users</td>
<td>Displays list of all users in the Customer User Table.</td>
<td>Sysop 2, CMaster</td>
</tr>
<tr>
<td>XU - Delete User</td>
<td>Deletes a user and removes all records associated with that user from the ASG Guard/ASG Guard Plus Customer User Table.</td>
<td>CMaster</td>
</tr>
<tr>
<td>SCK – Set Customer Key</td>
<td>Sets an encryption key that is used to encrypt secret user information such as passwords when this information is stored in the ASG Guard/ASG Guard Plus and when the Customer User Table is exported via the Cdump/Cdumpf command.</td>
<td>CMaster</td>
</tr>
<tr>
<td>LLU – List Lucent Users</td>
<td>Displays list of the Lucent Users in the ASG Guard/ASG Guard Plus.</td>
<td>Sysop 2</td>
</tr>
<tr>
<td>BLU – Block/Unblock Lucent User</td>
<td>Prevents a Lucent User from gaining access to the ASG Guard/ASG Guard Plus.</td>
<td>CMaster</td>
</tr>
<tr>
<td>DLU - Display Lucent User</td>
<td>Displays entire record for the selected Lucent User. (Password/Key is not displayed.)</td>
<td>Sysop 2</td>
</tr>
<tr>
<td>BLA – Block/Unblock Lucent Administrator</td>
<td>Provides or removes rights to a Lucent Master to administer Customer Users.</td>
<td>CMaster</td>
</tr>
</tbody>
</table>
6.5 Add a User – AU Command

The AU command allows you to add a user to the ASG Guard/ASG Guard Plus system (that is, add a user to the Customer User Table). To access the system, a password or authentication token is required.

To add a user, type **AU** at the system prompt and press the ENTER key. The Add User information screen is displayed. You may also type the user name as part of the command.

For example:

```
AU CHRIS
```

or **AU** at the User Name prompt

then **CHRIS**

The Add User screen appears after you enter a user name and press the ENTER key. (This assumes you are using VT100 terminal emulation. See section 11.5 to turn VT100 terminal emulation on/off.)

```
Site123>AU

--- Add User ---
User Name                          CHRIS
Access Class                       Host One
Block Access                       No
Sessions Allowed (blank=unlimited)  
User Expiration Date               
Primary Authentication Method      ASG Key
Secondary Authentication Method    None
Auto Execute Command               
Comments (1):                      
(2):                              
(3):                              
```

**Screen 6-2. Add User Screen**
### Field Function

**User Name**  
Enter a user name. User names may be up to 15 alphanumeric characters in length, including spaces.

*NOTE: The ASG Guard/ASG Guard Plus converts alphabetical characters to upper case.*

**Access Class**  
To select the Access Class, press the SPACE BAR until the desired choice is displayed from the following selections:

- **Host “n”** - Allows user access to the host port associated with the host “n” port on the ASG Guard/ASG Guard Plus (number depends on ASG Guard or ASG Guard Plus). The user is not allowed access to any other port ASG Guard/ASG Guard Plus functions.

- **Sysop 1** - Provides access to all host ports and allows the user to view alarm and historical information such as event reports and log history from the ASG Guard/ASG Guard Plus database. The user cannot change any of the information or make any changes to the ASG Guard/ASG Guard Plus database.

- **Sysop 2** - In addition to all Sysop 1 access privileges, the Sysop 2 user can add events to or remove events from the Event Table. The Sysop 2 user can implement all commands associated with the Action and Alarm Functions Menu. A Sysop 2 user cannot make any changes to the user database.

- **CMaster** - In addition to all Sysop 2 access privileges, the Master level of access allows the user to implement all ASG Guard/ASG Guard Plus commands, including modification of the user database.

Select the Access Class by pressing the ENTER key when your choice is displayed. The cursor will then move to the Block Access field.

**Block Access**  
Initially **No** appears on the screen. Press the SPACE BAR to toggle to **Yes**. Select **No** to allow a user to access the ASG Guard/ASG Guard Plus (not to block access). Select **Yes** to prevent a user from accessing the ASG Guard/ASG Guard Plus.

**Sessions Allowed**  
Enter a number from 1 to 999 and press the ENTER key to specify the number of successful sessions allowed for that user in unlimited time frame. To allow unlimited number of sessions, press the ENTER key only (do not enter a number).

**User Expiration Date**  
Enter the date in month/day/year format after which the user is not allowed access. During this time, the user has unlimited access.
Modifying the User Database

Field | Function
---|---
Primary Authentication Method | Press the SPACE BAR until the desired choice is displayed from the following selections: ASG Key, Pager and Password/Callback.

**NOTES:**

> Depending on which method of authentication you select, you are prompted for further information after you complete the main portion of this screen.

Secondary Authentication Method | Select a second means of authentication for a user. Press the SPACE BAR until the desired choice is displayed from the following selections: None: ASG Key, Pager and Password/Callback.

**NOTES:**

> Depending on the authentication method selected, prompts for further information will appear after you complete the main portion of this screen.

Auto Execute Command | (Optional) Enter a command to automatically execute after that user has been authenticated by the system. For example, if you enter LH - the log history will be displayed in reverse order after the user authenticates. This option is available only to users who sign on as a Sysop 1 level or higher.

Comments | Enter up to 40 alphanumeric characters on the Comments line. After you have entered comments in the Comments field, press the ENTER key.

After pressing the ENTER key, you will be prompted for more information about the authentication method that you selected.

### 6.5.1 ASG Key Authentication Method

If ASG Key was selected as the primary authentication method, the ASG Guard/ASG Guard Plus will display the following information.

<table>
<thead>
<tr>
<th><strong>ASG Key Details</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Key Source</td>
</tr>
</tbody>
</table>

Screen 6-3. ASG Key Details Screen
6.5.1.1 Encryption Key Source
Press the SPACE BAR until the desired choice is displayed from the Encryption Key Source selections for the ASG Key authentication method. Each selection is described in subsequent paragraphs. When the appropriate source is displayed, press the ENTER key to select it. After the ENTER key is pressed, the system will confirm that the user has been added to the database.

The three choices are listed below:
- Randomly Generated
- Device ID/User Code
- Fixed

NOTE:
To maintain security, be sure to protect ASG Key seed values and passwords. This information is the key to security on the ASG Guard/ASG Guard Plus.

6.5.1.2 Encryption Key Source: Randomly Generated
Randomly generated means that the ASG Guard/ASG Guard Plus generates the encryption key. When this source is selected, the ASG Guard/ASG Guard Plus generates the key value and displays the information on the screen.

The information displayed in the Enter These Digits as Key1 or Key2 field is to be entered in to the ASG Key when you initialize the ASG Key. Be sure to note this information carefully. If you make an error entering the information for the ASG Key, redo the procedure by using the Change User command. Follow the instructions supplied with the ASG Key to initialize the ASG Key.

Enter the Test Challenge information displayed on the screen (the test challenge is always "1234567") into your ASG Key per the instructions provided with the ASG Key. If the Reply on your ASG Key matches the one on the screen, you have successfully added this user.

<table>
<thead>
<tr>
<th>ASG Key Details</th>
<th>Randomly Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter These Digits as Key1 or Key2: 0443 2126 = 3422 1505 = 3160 =</td>
<td></td>
</tr>
<tr>
<td>Test Challenge: 1234567 ..Reply: 040-2181</td>
<td></td>
</tr>
<tr>
<td>Press &lt;ENTER&gt; to Continue</td>
<td></td>
</tr>
</tbody>
</table>

Screen 6-4. ASG Key Details Screen
6.5.1.3 Encryption Key Source: Device ID/User Code
The ASG Guard/ASG Guard Plus uses the Device ID and the User Code to generate the seed information for the ASG Key authentication method. The ASG Guard/ASG Guard Plus prompts you for the information. Valid values are 1 to 65535 for the Device ID.

<table>
<thead>
<tr>
<th>* ASG Key Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Key Source</td>
</tr>
<tr>
<td>Device ID</td>
</tr>
<tr>
<td>User Code</td>
</tr>
<tr>
<td>Enter These Digits as Key1 or Key2: 5364 4262 = 0646 5515 = 1460 =</td>
</tr>
<tr>
<td>Test Challenge: 1234567 ...Reply: 542-6547</td>
</tr>
<tr>
<td>Press &lt;ENTER&gt; to Continue</td>
</tr>
</tbody>
</table>

Screen 6-5. ASG Key Details Screen

Once the encryption key is generated, enter the information into the ASG Key according to its directions. Enter the Test Challenge information displayed on the screen (the test challenge is always "1234567") into your ASG Key per the instructions provided with the ASG Key. If the Reply on your ASG Key matches the one on the screen, you have successfully added this user.

6.5.1.4 Encryption Key Source: Fixed
The Fixed selection allows you to enter either 14 hex or 20 octal numbers as your source. The ASG Guard/ASG Guard Plus prompts you for the required information. Hex values include the digits 0 to 9 and the letters A to F. Octal values are digits from 0 to 7. (If, for example, you select a hex code, a valid entry would be "003FA876DE45CD.") This option is provided in case the ASG Key has been assigned a fixed key from some other type of system, or the administrator wants to assign a specific key.

<table>
<thead>
<tr>
<th>* ASG Key Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Key Source</td>
</tr>
<tr>
<td>Fixed Key (14 hex or 20 octal)</td>
</tr>
<tr>
<td>Enter These Digits as Key1 or Key2: 0443 2126 = 3422 1505 = 3160 =</td>
</tr>
<tr>
<td>Test Challenge: 1234567 ...Reply: 040-2181</td>
</tr>
</tbody>
</table>

Screen 6-6. ASG Key Details Screen
6.5.2 Password/Callback Authentication Method

If Password/Callback was selected as the primary authentication method, the ASG Guard/ASG Guard Plus will display the following information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Password</td>
<td>The password may be up to 15 alphanumeric characters. Asterisks appear on the screen as you type to prevent your password being displayed on the screen. Press the ENTER key. <strong>NOTE: Passwords are case sensitive.</strong></td>
</tr>
<tr>
<td>Verify Password</td>
<td>Retype the password exactly as you entered it the first time, and then press the ENTER key.</td>
</tr>
<tr>
<td>Access Option</td>
<td>Press the SPACE BAR until the desired choice is displayed for the Access Options. Three options are available: Regular Callback, Passthru and Variable Callback. Each option is discussed in subsequent paragraphs.</td>
</tr>
</tbody>
</table>

When the access option you desire appears on the screen, press the ENTER key to make your selection.

6.5.2.1 Access Option: Regular Callback

Regular Callback requires the user to have a specific phone number listed in the ASG Guard/ASG Guard Plus user database, in addition to the password. After receiving a phone call followed by the corresponding user name and password, the ASG Guard/ASG Guard Plus disconnects the call and the caller hangs up. ASG Guard/ASG Guard Plus then dials the caller back using the number in its database for that user and requests the password. After the password is entered correctly, the user is allowed access.

If Regular Callback is selected, you are prompted to enter a phone number.

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone Number</td>
<td>19085553435</td>
</tr>
</tbody>
</table>
NOTE:
Enter the phone number as the system needs to dial it. For example, if you have to dial 9 to get an outside line, or if the number is in a different area code and you need to dial a 1 first, enter those numbers as well. Dialing instructions common to all users (such as dialing 9 to get an outside line) should be changed in the modem dial string using the Set Modem (SM) command.

6.5.2.2 Access Option: Passthru

Passthru only requires the user to enter a user name and the correct password.

```
| -- Password/Callback Details -- |
|---------|---------|
| Enter Password                          | ***** |
| Verify Password                          | ***** |
| Access Option                           | Passthru |
```

Screen 6-9. Password/Callback Details Screen

6.5.2.3 Access Option: Variable Callback

Variable Callback requires a user name and corresponding password. After dialing into the ASG Guard/ASG Guard Plus and entering the correct user name and password, the user enters a phone number for the ASG Guard/ASG Guard Plus to call back. The ASG Guard/ASG Guard Plus disconnects and the user hangs up. The ASG Guard/ASG Guard Plus then calls the user back at the phone number provided.

```
| -- Password/Callback Details -- |
|---------|---------|
| Enter Password                          | ***** |
| Verify Password                          | ***** |
| Access Option                           | Variable Callback |
```

Screen 6-10. Password/Callback Details Screen

6.5.3 Page Authentication Method

The Pager Authentication method requires an ASG Key and the corresponding password. After the user dials in and enters their user ID, the ASG Guard/ASG Guard Plus sends a password to the user’s pager and then disconnects..

```
Ser#6400434>ATDL
Please Enter User ID ->
Please Enter User ID ->TOM

--- Pager Authentication ---

Sending Password, please enable pager.

Call ASG Guard with password.
```

Screen 6-11. Pager Authentication Screen
The user must dial back into the ASG Guard/ASG Guard Plus. After entering the User ID, the user is prompted to enter the password sent by the ASG Guard/ASG Guard Plus. After entering the password correctly, the user is allowed access.

--- Connected to Site: Ser#6400434 ---
--- ASG Guard - User Authentication ---
Please Enter User ID -> TOM
--- Pager Authentication ---
Enter Password -> ********

**Screen 6-12.** Pager Authentication Screen

**NOTE:**
*To maintain security, be sure to protect ASG Key and Pager seed values and passwords. This information is the key to security on the ASG Guard/ASG Guard Plus.*
6.6 List Users – LU Command

Type **LU** at the system prompt, and press the ENTER key to display the list of users in the Customer User Table. These users are authorized to initiate a Sysop or Host session with the ASG Guard/ASG Guard Plus. The following information is displayed for each user:

- User name
- Access class [Acc. Class]
- Whether user access is specifically blocked [Blk? ]
- Expiration date [Exp. Date]
- Number of sessions allowed [# Ses. Exp? ]
- Primary authentication method [Auth. Mode(s)]
- Secondary authentication method [Auth. Mode(s)]

You cannot change information by using the LU command. To change information, use the Change User (CU) command.

```
site123>LU
--- List Users ---
User Name       Acc.Class   Blk?  Exp.Date  #Ses. Exp?  Auth.Mode(s)
CHUCK           Master                                   PwdCB
JOHN            Master                                   PwdCB
TOM             Sysop 2                                  ASGK  PwdCB
-- End of List --
site123>
```

**Screen 6-13.** List Users Screen
### Field | Function
--- | ---
User Name | List of all users in the Customer User Table authorized to access the ASG Guard/ASG Guard Plus, or other device connected to the ASG Guard/ASG Guard Plus.

Acc. Class | The Access Class defined for that user. Access classes are listed below:

- Host n (number of host ports depends on the ASG Guard or ASG Guard Plus)
- Sysop 1
- Sysop 2
- CMaster

For a description of the access classes, see the Add User information in this chapter.

Blk? | This column shows whether a user’s access has been blocked. “No” means that access is permitted. “Yes” means that access for that user is blocked.

Exp Date | If a date appears in this field, the user will not be allowed access to the ASG Guard/ASG Guard Plus after this date.

# Ses. Exp? | If a number appears in this field, the user will not be allowed access to the ASG Guard/ASG Guard Plus system after he or she has successfully accessed the system the number of times displayed.

This field is blank if the user’s expiration date or number of sessions allowed restriction has not been exceeded. A Yes appears in this field if the expiration date has past or the number of successful sessions has been exceeded.

Auth. Mode(s) | The primary and secondary (if used) methods of authentication for the user are displayed in this column. Authentication methods include:
- ASG Key
- Password/Callback
- Pager

For a description of the authentication methods, see the Add User paragraphs in this chapter.
6.7 Delete a User Profile – XU Command

The Delete User command deletes all records associated with that user from the Customer User Table of the ASG Guard/ASG Guard Plus User Database. After a user profile has been deleted, the user cannot access the ASG Guard/ASG Guard Plus. To reinstate access privileges, a user profile for him/her must be added to the database. (See Section 6.5, Add User command.)

Type XU at the system prompt and press the ENTER key to display the Delete User information screen.

Type in the user name as it appears in the List User display and press the ENTER key. You may also type the user name as part of the command.

For example:

```
> XU or
> XU CHRIS
```

In either case, the Delete User information screen will appear after you enter a user name and press the ENTER key.

| site123>XU |
| --- Delete User --- |
| User Name | CHRIS |
| Access Class | Host One |
| Block Access | No |
| Sessions Allowed (blank=unlimited) | |
| User Expiration Date | |
| Primary Authentication Method | ASG Key |
| Secondary Authentication Method | None |
| Auto Execute Command | |
| Comments | |
| Acc: 0 Fail: 0 Last: 0 | Dur: 00:00 Type: |

```
-- More to Come - Press ENTER (Ctrl+A to quit) --
```

```
-- ASG Key Details—Encryption Key Source | Fixed Test Challenge: 1234567...Reply: 040-2181
Delete Record ? | Yes
```

Screen 6-14. Delete User Screen

The prompt Delete Record ? appears at the bottom of the screen requiring you to confirm that you want to delete that user. Initially No appears on the screen. To delete the user, toggle the field to Yes by pressing the SPACE BAR and then press the ENTER key.

**NOTE:**

To temporarily remove a user from the database, use the block access option in the user profiles. The user will not be allowed access, but all his/her access information will be maintained.
6.8 Display a User Record – DU Command

The Display User Record command displays the entire record for the user selected. The Display User Record command accepts the user name as a parameter on the command line. If the command is entered without a user name, the system will prompt you to enter one.

Type **DU** at the system prompt and press the ENTER key to display the Display User Record information screen.

```
Site123>DU
--- Display User Record ---
User Name
```

**Screen 6-15. Display User Record Screen**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User Name</strong></td>
<td>Enter the user name as it appears in the List User display, and then press the ENTER key. You may also type the user name as part of the command. For example: &gt;DU or &gt;DU CHRIS The User Record information screen for that user will be displayed.</td>
</tr>
</tbody>
</table>

The **Acc:** field displays the number of times the user has accessed the system. The **Fail:** field displays the number of failed access attempts. The **Last:** field displays the date and time of the last successful access. **Dur:** and **Type:** displays the length of time of the last session and the session type, respectively.

For a description of the fields in the Display User Record Screen, refer to Section 6.5.

```
site123>DU HENRY
--- Display User Record ---
User Name                         HENRY
Access Class                      CMaster
Block Access                      No
Sessions Allowed (blank=unlimited) MM/DD/YYYY
User Expiration Date
Primary Authentication Method     ASG Key
Secondary Authentication Method   Password/Callback
Auto Execute Command              OFF SITE
Comments :                      OFF SITE
Acc: 3 Fail: 2 Last: 12/07/98 17:19 Dur: 04:42 Type: AUX-

-- ASG Key Details—Encryption Key Source
Device ID                          12345
Test Challenge: 1234567 ...Reply: 542-6547
```

**Screen 6-16. Display User Record Screen**
6.9 Changing User Information – CU Command

The Change User (CU) command allows you to change the information of a user in the Customer User Table.

Type `CU` and the user name, and then press the ENTER key to display the current information for that user, line-by-line. At each line, you may change the parameter. In some cases, options are displayed by using the SPACE BAR and then selected by pressing the ENTER key. In other cases, you must enter an appropriate value. To advance to the next line without changing the parameter, press the ENTER key.

Each time you change the primary or secondary authentication method, you will need to enter required information for the selected method. For complete information on each parameter, refer to Section 6.5, Add User.

**NOTE:**
If you abort the Change User process, the user profile will be deleted.

```
site123>CU TOM
--- Change User ---
User Name                          TOM
Access Class                       Sysop 2
Block Access                       No
Sessions Allowed (blank=unlimited)
User Expiration Date
Primary Authentication Method      ASG Key
Secondary Authentication Method    Password/Callback
Auto Execute Command
Comments :
-- ASG Key Details—Do You Want to Load ASG Key With New Data ? Yes
Encryption Key Source              Randomly Generated
Enter These Digits as Key1 or Key2: 2021 4204 = 7523 1601 = 0460 =
Test Challenge: 1234567 ...Reply: 276-6303
-- Password/Callback Details—Change Password ?                  No
Access Option                      Passthru

```

Screen 6-17. Change User Screen
### Field: User Name

**Function:** Enter the user name as it appears in the List User display. You may also type the user name as part of the command. For example:

- `>cu`
- `>cu  tom`

### Access Class

**Function:** To change the Access Class, press the SPACE BAR until the desired choice is displayed from the following selections:

- Host n (Number of host ports will vary depending on the ASG Guard or ASG Guard Plus)
- Sysop 1
- Sysop 2
- Cmaster

When the appropriate selection is displayed, press the ENTER key. If you do not wish to change this parameter, press the ENTER key to move the cursor to the next field.

### Block Access

**Function:** Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Select No to allow a user to access the ASG Guard/ASG Guard Plus (not to block access). Select Yes to prevent a user from accessing the ASG Guard/ASG Guard Plus.

### Sessions Allowed

**Function:** Enter a number from 1 to 999 and press the ENTER key to specify the number of successful sessions allowed for that user. To allow unlimited sessions, press the ENTER key only (do not enter a number).

### User Expiration Date

**Function:** Enter a date in month/day/year (mm/dd/yy) format and press the ENTER key after which the user will not be allowed to access the ASG Guard/ASG Guard Plus.

### Primary Authentication Method

**Function:** Press the SPACE BAR until the desired choice is displayed: ASG Key, Pager and Password/Callback.

**NOTES:**

*Depending on which method of authentication you select, you are prompted for further information after you complete the main portion of this screen.*

### Secondary Authentication Method

**Function:** Press the SPACE BAR until the desired choice is displayed: None, ASG Key, Pager, and Password/Callback.

**NOTES:**

*Depending on which method of authentication you select, you are prompted for further information after you complete the main portion of this screen.*
Modifying the User Database

**Auto Execute Command**  (Optional) Enter a command to automatically execute after that user has been authenticated by the system. The user must log on as a Sysop 1 or higher. For example, if you enter LH - the log history will be displayed in reverse order after the user authenticates.

**Comments**  Enter up to 40 alphanumeric characters on each of the three Comments lines. After you have entered comments in each Comments (1) field, press the ENTER key.

**Authentication Methods**  Each authentication method requires additional information to be entered into the system. The prompts for this information appear when you press the ENTER key after the last Comments Line.

**NOTE:**
*If you do not wish to change this parameter, press the ENTER key to move the cursor to the next field.*

For complete information on each of the authentication methods, refer to the [Add User](#) information in this section.
6.10 Set Customer Key – SCK Command

The Set Customer Key command provides a facility to set an Encryption Key (Key). This Key is used to encrypt secret user information such as passwords and Keys. The Key is used to encrypt this data when stored inside the ASG Guard and when the Customer User Table is exported via the Cdump/Cdumpf command.

Type the command **SCK** at the Guard prompt.

```
ASG> SCK

--- Set Customer Key ---
New Customer Key:
```

**Screen 6-18. Set Customer Key Screen**

The Guard requires a 16 hexadecimal entry (that is, ABCDEF0123456789). After entering the new Customer Key press the ENTER key to complete this process. The Guard will confirm that the Customer Key has been changed.

This Customer Key must be replicated in all ASG Guards for successful distribution of User Tables. (See Appendix C.)

**NOTE:**
The ASG Guard is shipped with a default Customer Key. It is important that this default Customer Key is replaced with a new Customer Key for security reasons.
6.11 List Lucent Users – LLU Command

The List Lucent Users command provides a list of the Lucent Users loaded in the ASG Guard. This table output will display the Lucent User I.D., Access Class, Block Status, Expiration Date, # of Sessions before the user Expires & the Authentication Method used. This command is identical in functionality to the LU command except the data relates to the Lucent Users, not Customer users.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Acc.Class</th>
<th>Blk?</th>
<th>Exp.Date</th>
<th>#Ses. Exp?</th>
<th>Auth.Mode(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADAM</td>
<td>Sysop 2</td>
<td>Yes</td>
<td></td>
<td></td>
<td>ASGK</td>
</tr>
<tr>
<td>E</td>
<td>Sysop 1</td>
<td></td>
<td></td>
<td></td>
<td>ASGK</td>
</tr>
<tr>
<td>LUCGUARD</td>
<td>LMaster</td>
<td></td>
<td></td>
<td>5</td>
<td>ASGK</td>
</tr>
<tr>
<td>MARK</td>
<td>LMaster</td>
<td></td>
<td>12/31/1999</td>
<td></td>
<td>ASGK</td>
</tr>
</tbody>
</table>

Screen 6-19. List Lucent Users Screen

6.12 Block/Unblock Lucent User – BLU Command

The Block/Unblock Lucent User command is the only command that allows a Customer Master User to change a Lucent User. This command will Block a Lucent User from gaining access to the ASG Guard. This is a complete blockage from any access to the Guard. To perform this command type BLU followed by the User I.D.

<table>
<thead>
<tr>
<th>User Name</th>
<th>Block Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adam</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Screen 6-20. Block/Unblock Lucent User Screen

The ASG Guard will prompt the user for verification of this change (Yes/No). This command must be performed on every Lucent User should removal of Lucent access to this device be required. There is no way to remove the Lucent Users from ASG Guard.

6.13 Display Lucent User – DLU Command

This command has the same attributes and functions as the Display User command except it reflects data about Lucent Users instead of Customer Users.
6.14 Block/Unblock Lucent Administration – BLA Command

The Block/Unblock Lucent Administration command provides or removes rights to a Lucent Master to administer the Customer Users. This command, when in the Unblock mode, gives the Lucent Master user access to the Add User, Delete User, and Change User command. This command is only available to the Cmaster user. To execute this command type **BLA** at the ASG Guard prompt. The Guard will prompt the user “Block Lucent Administration? (Yes/No)”. Use the SPACE BAR to toggle between Yes and No. The value “Yes” will remove administration rights of the Customer Users from Lucent. The value “No” will give Lucent Master Users access to the AU,CU, and XU commands.

```
Ser#98100221>BLA

--- Block/Unblock Lucent Admin. ---
Block Lucent Administration ?  Yes

```

**Screen 6-21.** Block/Unblock Lucent Admin. Screen

**NOTE:**
The default setting for this command is Unblock giving Lucent Master access to add and modify Customer Users.
Page intentionally left blank.
7. File Buffering

7.1 What This Chapter Contains

- Overview
- RAMdisk organization
- File naming conventions
- RAMdisk protection parameters
- Saving and transferring data received by a host port
- Setting up automatic and manual buffering
- List of RAMdisk events

7.2 Overview

Each host port of the ASG Guard/ASG Guard Plus receives data from the resource to which it is connected. This data may be buffered, or collected in a file, which is temporarily stored on the ASG Guard/ASG Guard Plus RAMdisk. The file may be sent to the administration PC for later review or importation into another software package.

The ASG Guard/ASG Guard Plus offers the option of automatic or manual data buffering from a host port. If automatic buffering is enabled, the system will switch buffer files according to preset parameters. If automatic buffering is not enabled, the administrator must open and switch buffer files manually. Buffer files are stored on the RAMdisk in the subdirectory of the particular host port. The buffer files can be managed using commands that are similar to DOS commands. These commands are listed in the File Management Menu.
### 7.3 File Management Menu

The File Management Menu is organized into two sections: Disk/File Maintenance Functions and Buffer Functions. The Disk/File Maintenance Functions section lists the commands by which the user may edit or manipulate files from the ASG Guard/ASG Guard Plus RAMdisk. The Buffer Functions section lists commands for collecting data into files and for sending to the administration PC. To view the File Management Menu, type `F` at the system prompt and press the ENTER key.

<table>
<thead>
<tr>
<th>--- Disk/File Maintenance Functions ---</th>
<th>--- Buffer Functions ---</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDP</td>
<td>Set Disk Params</td>
</tr>
<tr>
<td>DIR</td>
<td>List Directory</td>
</tr>
<tr>
<td>MD</td>
<td>Make Directory</td>
</tr>
<tr>
<td>COPY</td>
<td>Copy File</td>
</tr>
<tr>
<td>DEL</td>
<td>Delete File</td>
</tr>
<tr>
<td>COMP</td>
<td>Compress file</td>
</tr>
<tr>
<td>SEND</td>
<td>Send File</td>
</tr>
<tr>
<td>RCV</td>
<td>Receive File</td>
</tr>
</tbody>
</table>

Other Menus: S - System  A - Alarm/Event  L - Log  U - User  P - Port/Session

Screen 7-1. Disk/File Maintenance Functions Screen
7.4 RAM Disk Organization

The space available on the RAM disk is 32 MB. Approximately 2 MB is used by the operating system, and the remainder is available for storage. You may create and remove subdirectories, and copy, move, rename and delete files.

The directories listed below are automatically created by the system:

1. A subdirectory is created for each host port that has buffering enabled. The data collected from the host port is stored in this subdirectory. The subdirectory is given the same name as the host port by default. To view the host port directory, type **OPBUFh#** (Where h# is the desired host port number) at the system prompt. You will see a response similar to: ‘--- Open Host Buffer File --- 01/05/96 22:22:36 [AUX] Buffer \HOST1\CURRENT.0 Opened O.K.’ Type **DIR** at the system prompt and the response will be similar to:

```
Site123>DIR
--- List Directory ---
Current Directory: \HOST1
CURRENT.0 0 10/05/98 22:22
Total Bytes on Drive: 30578688 Free: 30486528
Site123>
```

Screen 7-2. List Directory Screen

2. The \SENTFILES is a directory in which is stored a copy of each file sent to the administration PC. These files can be deleted automatically after a preset number of days or when space available on RAMdisk reaches a critical level.

3. The \LOGFILES is a directory, which contains files that are generated each day by the ASG Guard/ASG Guard Plus, to maintain a record of that day’s activities. These files are of two types: Event files, which list the alarms that were processed during one day, and Log files, which contain a copy of one day’s log history.

7.4.1 Host Port Buffer Naming

The user may change the default directory name for each host port. For example, if Host port 1 is being used to monitor a Meridian switch, then directory name may be changed to Meridian. See Section 7.6.1 for more information on changing the directory name.

7.4.2 Buffer File Naming Conventions

Filenames consist of capital letters and numbers and can have a maximum of 12 characters. A period followed by a three-character extension may be used provided the total number of characters does not exceed 12.

Examples: 101296AM.100

REPORT.01

IMPORTANTLOG

Note that in the screen above the default filename is CURRENT.0. The current buffer file for a host port is always named either CURRENT.0 or CURRENT.1. When the buffer is switched, the buffer file is renamed to indicate the host port number from which the data was collected and the date and time the buffer was opened.
Files collected via host port data by the ASG Guard/ASG Guard Plus are stored in the directory of that host port and are assigned sequential names in order to provide the user a means of identifying when and where the data in the file was gathered. The ASG Guard/ASG Guard Plus uses the following naming convention:

\[ \text{Hnyymdd.hhq} \]

Where:
- **H** = the letter H
- \( n \) = host port number \([1-4, \text{ or } 1-16 (1-12 \text{ if ext. mdms), or } 1-28 (1-24 \text{ if ext. mdms})\) Hostports 10-28 are labeled A-T, respectively\]
- \( yy \) = year
- \( mm \) = month
- \( dd \) = day
- \( hh \) = hour
- \( q \) = a letter (starting with ‘A’) used to differentiate multiple files opened during the same hour.

**Example 1: H2981218.14A**

In this example, data is collected from host port 2 on the 18th day of December (12) in 1998 (98) at 2-p.m. (14). The ‘A’ indicates that this is the first file collected in that hour.

**Example 2: HG980709.08D**

In this example, data is collected from host port 16 (H), on the 9th day of July (07) in 1998 (98) at 8-a.m. (08). The ‘D’ indicates that this is the fourth file collected in that hour.

When a buffer is closed, the CURRENT.x file is renamed using the convention described above, and left in the appropriate host port subdirectory.

The Event and Log files that are generated by the ASG Guard/ASG Guard Plus have names of the form listed below:

\[ \text{Evyyymdd.LOG} \quad \text{(for Event files)} \]
\[ \text{Lgyymmd.LOG} \quad \text{(for Log files)} \]

Where:
- \( EV \) = the letters EV
- \( LG \) = the letters LG
- \( yy \) = the last 2 digits of the year
- \( mm \) = the month
- \( dd \) = the day

\[ \text{.LOG} = \text{the letters .LOG} \]

**NOTE:**

This is a sample entry using the ASG Guard/ASG Guard Plus standard date format. The user may select from ten different date formats. See Section 9.4.4 for further details. You may also rename files by using the REN command.
7.5 Set the RAM disk Protection Parameters

You should verify that the RAM disk protection parameters are appropriate for your application. The RAM disk protection feature prevents the disk from running out of room, which could result in the loss of data. Monitoring of available space on the disk by the ASG Guard/ASG Guard Plus is done continuously. You can configure the ASG Guard/ASG Guard Plus to delete files automatically after a specified number of days or when the amount of data on the RAM disk reaches a preset critical level.

Files are not deleted automatically. If you do not specify a critical percentage and the directories from which files are to be deleted, you will have to monitor the disk and delete files when necessary. The ASG Guard/ASG Guard Plus has default values, which may or may not fit your application. Failure to raise the free space above the critical level causes a "DISKCRIT" event to be generated. The event .DISKCRIT can be included in your Action Table along with the specified action to be taken.

The RAM disk protection parameters can be viewed by using the DDP (Display Disk Parameters) command or modified by using the SDP (Set Disk Parameters) command.

```
Site123>SDP
--- Set Disk Params ---
Keep SENT Files for how many days       3
Keep LOG Files for how many days         3
Disk Critical Percent Free              25
Directories to Purge (oldest files first) when Disk is Critical
   - 1.                                SENTFILES
   - 2.                                LOGFILES
   - 3.                                
   - 4.                                
   - 5.                                
   - 6.                                
```

Screen 7-3. Set Disk Params Screen
Field Function

Keep SENT Files for how many days? Enter the number of days that files in the /SENTFILES directory should be kept. Files that have been sent to the administration PC are automatically moved to this directory. Files that have been closed for the specified number of days old will be deleted at midnight. The date of a file (date that the file was closed) is the starting point.

Keep LOG Files for how many days? Enter the number of days that files in the /LOGFILES directory should be kept. System Log and Event files are automatically placed in this directory. Files that are the specified number of days old will be deleted at midnight. The date of a file (date that the file was closed) is the starting point.

Disk Critical Percent Free: Enter the percentage of disk space that must be free. When this percentage is reached, files will be deleted in the order specified by the entry for the Directories to Purge prompt.

Directory Purge sequence While Disk is Critical: Enter the names of the directories that will be purged in sequence. When disk space is critical, files will be deleted from the first directory, oldest files first, followed by the second directory, etc. until disk space is no longer critical.

Purge Host When Critical The Purge feature is set up within the ASG Guard/ASG Guard Plus to prevent all of the memory being used. The setting for “Purge Host Directories when critical” should be set to Yes (the default setting). Host directories will be purged if there are no more “SENTFILES” and “LOGFILES” to be deleted. It is possible to set the purging sequence by using the SDP command.

Initially No appears on the screen. Press the SPACE BAR to toggle to Yes.
7.6 Buffering Data Received by a Host Port

The ASG Guard/ASG Guard Plus provides both automatic and manual control of data buffering from the host ports. If automatic buffering is selected, a buffer file for the specified port will be opened and data collected until either a specified time or file size is reached. The current buffer file is then closed and renamed using the format described in the “File Naming Conventions” section. A new buffer file is opened immediately.

Buffer switching occurs seamlessly, so that no data is lost during the transition between files.

7.6.1 Automatic Buffering

When automatic buffering is enabled for a particular port, data is collected in a buffer file for a preset length of time or until the file reaches a specified size. To enable automatic buffering, enter the SH (Set Host) command.

**NOTE:**
*To disable automatic buffering, use the CLBUF (close buffer) command.*

```
Site123>SH
--- Set Host Port Params ---
Hosts:
1 = HOST1          2 = HOST2          3 = HOST3          4 = HOST4
Host Port Number                   1
Restore Factory Defaults ?        No
-- Host 0:
  Host Name                             HOST1
  Baud Rate Setting                     9600
  Character Length / Parity             8 / None
  Alarm Filter                          None
  Force CD/DSR High                     Yes
  Flow Control                          None
-- Automatic Buffering --
  Enable Automatic Buffering ?          No
  Compress closed buffer files ?        No
  Auto Switch: (Enter 0 to disable)    
    When CURRENT File exceeds ‘n’ KB    50
    Every ‘n’ Hours                     24
    - Synchronize at what hour (0-23)  0

12/02/1998 10:18:42 [H] Host 1 Idle
```

**Screen 7-4.** Set Host Port Params Screen
**Field**

*Enable Automatic Buffering*

Initially **No** appears on the screen. Press the SPACE BAR to toggle to **Yes**. Select **Yes** for automatic buffering. Select **No** to disable it.

*Compress closed buffer files?*

Initially **No** appears on the screen. Press the SPACE BAR to toggle to **Yes**. Select **Yes** to compress buffer files automatically when they are closed.

The compression ratio is typically 4:1, but the ratio may vary because it is dependent on the data.

**Auto Switch (enter 0 to disable)**

*When CURRENT File exceeds ‘n’ KB*

Enter the file size (in KB) at which the buffer should be switched. Note that the CURRENT.x file is renamed using the convention described in this section.

*Every n hours*

Enter 0 to disable this feature. Enter the number of hours between the switching of buffers.

*Synchronize at what hour (0-23)*

Indicate the hour at which the buffer should be switched. If the value is set to 2 and the previous value is set to 8, the buffer will switch at 200, 1000, and 1200 hours.

**NOTE:**

*If both the Current File exceeds ‘n’ KB and the Every n hours parameters are set, the buffer is switched when the first condition is met*
7.6.2 Manual Buffering

Buffers can be opened, closed and switched manually by the Administrator. To do this, use the buffer commands listed in the File Management Menu.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>OPBUF</td>
<td>Open buffer. Opens a buffer for a port. You will be prompted for the port number.</td>
</tr>
<tr>
<td>CLBUF</td>
<td>Close buffer. Closes the buffer file for a particular port. You will be prompted for the port number.</td>
</tr>
<tr>
<td>SWBUF</td>
<td>Switch buffer. Closes the buffer for the specified port and opens a new one. You will be prompted for the port number.</td>
</tr>
<tr>
<td>BST</td>
<td>Buffer status. Displays the status of all open and closed buffer files for a specific host port.</td>
</tr>
<tr>
<td>OBST</td>
<td>Status of open buffers for each host port. Displays the status of all open buffer files. Status includes creation time, file size, and the time and size at which the buffers will be switched (if automatic buffering is enabled).</td>
</tr>
</tbody>
</table>

7.6.3 Displaying the Status of a Buffer

You can check the status of a buffer by using the BST command. The ASG Guard/ASG Guard Plus displays information including the date that the current buffer file was opened, the size and the time at which the buffer will be switched, and the list of closed buffer files that are ready to be transferred to the administration computer.

**NOTE:**
The buffer file is switched either when the maximum buffer size is reached or at the time specified by the user, whichever occurs first.

An example of buffer status is shown below.

Site123>BST

--- Host Buffer Details ---

Hosts: 1=HOST1 2=HOST2 3=HOST3 4=HOST4

Host Port Number 1

(1) HOST1: \HOST1\CURRENT.1
Open Since 00:00 Today - Size: 24 Bytes
Auto Switch at 51200 Bytes - 25% Full
Next Scheduled Auto Switch is Tomorrow at 0:00

-- Buffer Files Ready For Sending --
H1960716.11A 0 07/16/96 11:52

Total Bytes: 24

Site123>

Screen 7-5. Hot Buffer Details Screen
7.6.4 Sending Buffer Files to the Administration PC

A file stored on the ASG Guard/ASG Guard Plus RAM disk can be sent to the administration PC or another device. Typically, the files transferred are closed buffer files from a specified host port and are sent to the administration PC for long term storage, review, or importation into another software package. For instance, CDR information could be sent to a PC and then imported into a call accounting program.

Files can be sent from the ASG Guard/ASG Guard Plus to another device by the following methods:

1. A direct connection to the AUX port may be used to transfer files. Either XMODEM or ASCII protocol may be used.
2. A simple dial-up connection may be used to transfer files. Either XMODEM or ASCII protocol may be selected.
3. Files may be transferred using FTP over an Ethernet or PPP link. (See the NOTE below.)

Notation used: Required parameters are enclosed within angle brackets < >; optional parameters are enclosed within square brackets [ ].

**NOTE:**
To send files using File Transfer Protocol (FTP), see Section 7.6.6 and Section 12.11.

7.6.5 Using a Direct or Dial-up Connection

To send buffer files from a specified host port, follow the steps listed below.

1. Issue the **SEBUF** or **SEND** command.

   SEND sends one file; SEBUF sends all the closed buffer files in the selected host port directory one at a time. You can specify the protocol as either XMODEM or ASCII. If a mode is not specified, XMODEM is used.

   **Command:** SEND
   **Syntax:** SEND <filename>,[mode]
   **Examples:**
   - SEND H1960716.11A or SEND H1960716.11A,X
     sends the file H1960716.11A using XMODEM
   - SEND H1960716.11A,A
     sends the file H1960716.11A using ASCII mode

   To send a file located in another directory, you must specify the path.
   - SEND \host1\ H1960716.11A
     sends the file H1960716.11A in the host1 directory and uses XMODEM protocol

2. From your communication software package, select 'Receive files' and the protocol (XMODEM or ASCII). You will be prompted for a filename.

   **NOTE:**
   The XMODEM setup for the DTE device must be HARDWARE FLOW CONTROL and parity of 8/N/1. Refer to the manual of the receiving device for more information.
3. After the transfer has been completed, the message "Transfer complete" will be displayed and the file(s) moved to the \SENTFILES directory of the RAMdisk.

SEBUF transmits all closed buffer files from the selected host port directory. SEBUF can also transmit files via FTP if the FTP parameters have been set up and FTP has been specified. (See Sections 7.6.6 and 12.11 for FTP instructions)

Command: SEBUF
Syntax: SEBUF <directory>,[mode]
Examples: SEBUF host1,A
         uses ASCII protocol to send all closed buffer files in the host 1 directory.

Buffer files will remain in the \SENTFILES directory until they are deleted, either manually or automatically by the system when their size or age exceeds the values you specified.

7.6.6 Using FTP to Send Files to Another Device

The ASG Guard/ASG Guard Plus supports FTP Client Send commands. Before you can send a file via FTP, the following must have been done.

1. A PPP link or Ethernet connection must be established.
2. Parameters must be set in the Set Network Parameters screen.

After specifying the parameters, you may issue the SEBUF or SEND command with the appropriate parameters.

7.6.6.1 Specify the FTP Parameters

Type SNP to set the Network Parameters, then select 3, FTP Params and press the ENTER key, or type the one line command SNP 3.

<table>
<thead>
<tr>
<th>Screen 7-6.</th>
<th>Set Network Params Screen</th>
</tr>
</thead>
</table>

Site 123>SNP

--- Set Network Params ---

1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params

Select Group -->3

Restore Factory Defaults ? No

--- FTP Parameters ---

PPP link needed for ftp? No
Ftp service type Client only

--- Server 1 (default) ---

IP address (nnn.nnn.nnn.nnn)
User name
Password
Upload Directory

--- Server 2 ---

IP address (nnn.nnn.nnn.nnn)
User name
Password
Upload Directory

Site 123>
**NOTE:**
*User name and password are case-sensitive.*

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Factory Defaults</td>
<td>Initially <strong>No</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>Yes</strong>.</td>
</tr>
<tr>
<td></td>
<td>Select <strong>Yes</strong> to restore original factory settings, or Select <strong>No</strong> to keep the current values.</td>
</tr>
</tbody>
</table>

**NOTE:** *There are two FTP parameters, which have factory default settings. These are:*

- PPP link needed for ftp: **No**
- FTP service type **None**

(To change these values, see below)

**PPP link needed for ftp?**

Initially **No** appears on the screen. Press the SPACE BAR to toggle to **Yes**.

Select this option if the ASG Guard/ASG Guard Plus has been programmed to dial out with a PPP session in order to send files via FTP. (See the [P.PPREQ alarm] and [PHPPP Action Routine] in Chapter 14 of this User's Guide)

**FTP service type**

Select the type of FTP service (None or Client Only). Press the SPACE BAR until the desired choice is displayed.

**Server 1 -- (Default) --**

- **IP address** (nnn.nnn.nnn.nnn)

Enter the IP address of the server. The files transmitted by FTP are sent to this address automatically unless otherwise specified by the user. Consult your Network administrator for FTP system requirements.

**User name**

Enter the name used to logon to the server. This entry is case sensitive.

**Password**

Enter the password for the user named above. This entry is case sensitive

**Upload directory**

Enter the name of the directory that to which the file will be sent.

**-- Server 2 --**

- **IP address** (nnn.nnn.nnn.nnn)

Enter the IP address of the server. The files transmitted by FTP are sent to this address automatically when server 2 is specified.

**Password**

Enter the password for the user named above. This entry is case sensitive.

**Upload directory**

Enter the name of the directory that to which the file will be sent.
7.6.6.2 Sending the File(s) via FTP

Files may be sent using FTP from the ASG Guard/ASG Guard Plus to another device by issuing the SEND or SEBUF command. However, you must set the FTP parameters prior to using these commands.

SEND transmits one file; SEBUF is used to send all the buffer files from the specified host port.

Notation used: As in ASCII and XMODEM protocols, the required parameters are enclosed within angle brackets <>; optional parameters are enclosed within square brackets [].

Command: SEND or SEBUF
Syntax: SEND or SEBUF <filename>,F,<server #>
(uses the IP address, user name and password for the specified server (1or 2). These parameters have been stored in the FTP parameters screen.)

Files are sent from the current directory.

For further details, see Section 12.11.
7.7 Receiving Files

The ASG Guard/ASG Guard Plus can receive files into the current directory from an active port. Either XMODEM, ASCII, or FTP may be specified as the protocol.

The RCV Command to receive files from the active port into an existing directory on the ASG Guard/ASG Guard Plus. Either XMODEM, ASCII, or FTP protocols may be specified.

Command: RCV
Syntax: RCV <filename>, [mode]

where mode is A (ASCII)
    X (XMODEM)
    F (FTP)

Examples:

1. To receive via XMODEM a file named NEW.CFG into the subdirectory HOST1, type the following at the command line:

   RCV \HOST1\NEW.CFG,X

2. To receive the file NEW.CFG using ASCII protocol into the current directory of the ASG Guard/ASG Guard Plus, type the following at the command line:

   RCV NEW.CFG,A

3. To receive the file NEW.CFG using the FTP protocol into the current directory of the ASG Guard/ASG Guard Plus, type the following at the command line:

   RCV NEW.CFG,F

Make sure the FTP server parameters have been set. (See section 12.7.1.3.)

NOTE:
If a mode is not specified, XMODEM is used.
7.8 Managing Files

Most of the commands used to manage files and directories on the RAM disk are the same as those used in DOS. Specifically:

- **CD** - Change Directory
- **MD** - Make Directory
- **RD** - Remove Directory
- **DIR** - List Directory Contents
- **DEL** - Delete File(s)

**NOTE:**
See the Disk/File Maintenance Functions below for a complete listing of user commands.

The following are exceptions in the ASG Guard/ASG Guard Plus to the DOS commands:

- A space must follow the **CD**, **RD**, and **MD** commands. For example, type **CD \** to return to the root directory.
- Wildcards (*) and ?) are permitted for the **DIR** and **DEL** commands only. The asterisk (*) takes the place of zero or more characters, and the question mark (?) takes the place of exactly one character. See the example below.

**Wildcard example:**

Using the command “**DEL H19809??..10??**” will delete all buffer files received by HOST1 from 10AM to 10:59AM throughout the month of September, 1998. In another case, the command “**DEL H3981005. *A**” will delete the first file received each hour by HOST3 on October 5, 1998. (See section 7.4.2 for Buffer Filenaming details)

To display all the File Maintenance functions, type **F** at the system prompt.

```
Site123>F

--- Disk/File Maintenance Functions ---

SDP  Set Disk Params               DDP  Display Disk Params
DIR  List Directory               CD   Change Directory
MD   Make Directory               RD   Remove Directory
COPY Copy File                     MOVE Move File
DEL  Delete File                   REN  Rename File
COMP Compress file                 UCOMP Uncompress file
SEND Send File                     VIEW View File
RCV  Receive File

--- Buffer Functions ---

OPBUF Open Host Buffer File         SWBUF Switch Buffer Files
CLBUF Close Buffer File             SEBUF Send All Buffer Files
BST  Host Buffer Details           OBST Open Buffer Status

Other Menus: S -System  A -Alarm/Event  L -Log  U -User  P -Port/Session

Site123>
```

**Screen 7-7.** Disk/File Maintenance Functions Screen
### 7.9 File Command Summary

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DIR</strong></td>
<td>Displays the files in the current directory. Directories are indicated by <code>&lt;DIR&gt;</code> adjacent to the name, along with their creation date and time.</td>
</tr>
<tr>
<td><strong>MD</strong></td>
<td>Makes a new directory under the current directory.</td>
</tr>
</tbody>
</table>
| MD `<newdirectoryname>` | Example: MD newdir  
Creates a new directory named newdir under the current directory. |
| **CD** | Changes the current directory to a directory specified by the user. Note that a space MUST follow this command. |
| CD | Example:  
CD \ to return to the root directory.  
CD .. to go up one level. |
| **RD** | Removes the specified directory. An error is displayed if the specified directory is not empty. |
| RD `<directoryname>` | Example: RD NEWDIR |
| **COPY** | Copies the specified file to a specified location. The destination directory must exist before the file can be copied. |
| COPY `<source directory>/<filename>` `<destination directory>/<filename>` | Examples:  
COPY `sentfiles\H4961212.2A` `\newdir\H4961212.2A`  
To copy a file from the current directory to a new directory  
COPY H4961212.2A `\newdir\H4961212.2A` |
| **DEL** | Deletes a file from the RAMdisk. |
| DEL `<source directory>/<filename>` | If it not necessary to specify the directory if the file to be deleted is in the current directory. |
| Example:  
DEL `sentfiles\H4961212.2A` |
| **MOVE** | Copies a file to a new directory and then deletes it from the source directory after the file has been copied. |
## Command Function

**MOVE**

MOVE `<source directory>/<filename> <destination directory>/<filename>`

Examples:

MOVE `\sentfiles\H4961212.2A \newdir\H4961212.2A`

To move a file from the current directory to a new directory

MOVE `H4961212.2A \newdir\H4961212.2A`

**RCV**

Command to receive files from the active port into the current directory on the ASG Guard/ASG Guard Plus using XMODEM, ASCII, or FTP transfer. See [Section 7.8](#) for more information.

**REN**

Renames the specified file

REN `<filename> <new filename>`

Example:  

REN `H4961212.2A DAYONE`

The file `H4961212.2A` is renamed as `DAYONE`.

**SEND**

Sends the specified file using either XMODEM, ASCII, or FTP transfer protocol.

**VIEW**

Displays the contents of the specified file, one page at a time. Scroll through the file by pressing <ENTER> to view the next page. <CTRL-A> will return you to the prompt.
7.10 RAM Drive Events

The ASG Guard/ASG Guard Plus, in response to certain RAM drive conditions, will generate events which are part of the standard software/firmware. These standard events are as follows:

- **.BUFREADY**: A buffer file has been closed and is ready to be sent.
- **.DISKCRIT**: The RAM drive has reached the critical level assigned in the Set Disk Parameters screen.
- **.DISKFULL**: The RAM drive is full and all further writes to the disk are suspended.

7.11 Utility Programs

Two utility programs are available: CSUM.EXE and ZPAD.EXE.

7.11.1 CSUM.EXE

CSUM.EXE is a DOS utility that calculates an 8-character hexadecimal checksum of a file

**Syntax**: CSUM <filename>

**Example**:

```
C:\>CSUM UPDATE.CFG  Calculate the checksum of the file
                   UPDATE.CFG
75C2E91A  8-digit hex checksum is printed to screen.
C:\>
```

7.11.2 ZPAD.EXE

When a file is transmitted with the XMODEM protocol, up to 127 extra characters may be appended to it. Therefore, a checksum calculated on the file before it is transmitted will not match a checksum calculated on the received file, because XMODEM changes the file by adding the extra characters. Run ZPAD.EXE to append the extra characters to the file while it is on your PC, preventing XMODEM from altering it during transmission. A checksum is calculated after running ZPAD.EXE and should match the checksum calculated when the file is received via XMODEM.
8. The Action and Event Tables

8.1 What this Chapter Contains

- Definition and Purpose of an Action Table
- Definition of Alarms and Events
- How to Create an Action Table
- Action Table Worksheet
- List of Internal Events and Action Routines

8.2 Overview

The ASG Guard/ASG Guard Plus can monitor and report alarm conditions sent by a PBX or other device connected to a host port of the ASG Guard/ASG Guard Plus. Alarm conditions monitored by the ASG Guard/ASG Guard Plus and the actions to be taken are listed in a database called the Action Table. When the ASG Guard/ASG Guard Plus receives the alarm condition, or event, it compares the alarm with the alarms listed in the Action Table. If a match is found, the associated actions are automatically executed.

Actions taken can include paging, delivery to an alarm catcher and canceling alarms. If the requested action cannot be taken at that time or is scheduled for another time, the event and requested action are listed in the Event Table. The Event Table lists all pending actions. When the action is processed, it is removed from the Event Table.

8.3 Working with Action Tables

To send messages based on alarms generated by a PBX, the Environmental Manager, etc., an Action Table must be created in the ASG Guard/ASG Guard Plus. The ASG Guard/ASG Guard Plus compares all alarm messages against the alarm list in the Action Table. If a match is found, the associated action is taken.

When building an Action Table, you should first consider the following things:

1. The alarms to be monitored.
2. The actions to be taken when an alarm is received.
8.4 Structure of an Action Table

The Action Table consists of a list of alarms, the requested action (Action Routine), parameters associated with the action, and comments.

A typical Action Table is shown below.

```
Site123>LA
--- List Action Items ---

<table>
<thead>
<tr>
<th>Alarm:</th>
<th>Routine:</th>
<th>Parameters:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1)  #NOTIFY-A</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2)  #NOTIFY-B</td>
<td>MGR2000 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3)  #NOTIFY-C</td>
<td>PAGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4)  .DAILY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5)  .DAILY.1</td>
<td>CLKCHECK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6)  .DAILY.2</td>
<td>SETHP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7)  .HOURLY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8)  .HOURLY-A</td>
<td>LOG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9)  .HOURLY-B</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10) DTA005</td>
<td>SCHEDULE 15 PHONHOME</td>
<td>DTI Yellow Alarm</td>
<td></td>
</tr>
<tr>
<td>11) DTA007</td>
<td>CANCEL DTA005^1</td>
<td>Yellow Cleared</td>
<td></td>
</tr>
<tr>
<td>12) DTI024</td>
<td>PHONHOME</td>
<td>DTI No Response</td>
<td></td>
</tr>
<tr>
<td>13) DTI030</td>
<td>PHONHOME</td>
<td>DTI Red Alarm</td>
<td></td>
</tr>
<tr>
<td>14) ERR</td>
<td>LOG</td>
<td>Test</td>
<td></td>
</tr>
<tr>
<td>15) ERR000</td>
<td>PHONHOME</td>
<td>Test</td>
<td></td>
</tr>
</tbody>
</table>
```

Screen 8-1. List Action Items Screen

The Action Table has four components: Alarm, Routine, Parameters, and Comments. Each component is described in the following paragraphs.

**Alarm**

There are four types of alarms/events.

1. Alarms produced by a host (PBX, etc.) can be listed in the Action Table along with a specified action.

2. Alarms (or events) can be generated by the ASG Guard/ASG Guard Plus, by a host user or by a Sysop. Events generated by the ASG Guard/ASG Guard Plus are called internal events. All internal events start with a period (.). Internal events are listed in Chapter 14.

3. Alarms generated by the Environmental Manager. This enables the ASG Guard/ASG Guard Plus to monitor alarms from temperature probes, contact closures, etc.

4. Events generated by user Action Routines. They are especially useful for further processing of alarms.

**Action Routine**

After the ASG Guard/ASG Guard Plus has determined that a match exists between the detected alarm and an entry in the Action Table, it executes the Action Routine listed. The Action Routine specifies what action should be taken when a particular event occurs. Each ASG Guard/ASG Guard Plus includes standard Action Routines (see Chapter 14). In addition to these system Action Routines, custom Action Routines may be written by the user in CCL, the proprietary programming language for the ASG Guard/ASG Guard Plus.
Parameters
Action routines typically have parameters associated with them. A parameter may be a phone number, a pager number, or other information used by the Action Routine.

Comments
The comment may give more information about the alarm. With some Action Routines, when the ASG Guard/ASG Guard Plus processes an alarm, the comment is sent along with it.

8.4.1 Alarm Matching Criteria
When the ASG Guard/ASG Guard Plus receives an alarm, it follows a specific procedure when it searches the Action Table for a match to an alarm (event). Three passes are made.

1. In the first pass, the ASG Guard/ASG Guard Plus attempts to match the alarm from the first character to the first space. That is, if it received an alarm ERR000 Reset, it would try to find ERR000 in the Action Table and then take whatever action is specified.

2. If the first search fails to turn up a match, it searches for a record describing a range of alarms that includes the alarm it received. For example, if it received an alarm ERR004, it might match this to ERR000 - 005, as it appears in the Action Table. Such ranges can be entered into the Action Table to cover a multiple of alarm types.

3. Finally, if there is no match using the first two criteria, it searches for a match to the mnemonic up to the first digit. That is, it drops the digits and just tries to match the mnemonic by itself. For example, if it received the alarm ERR006, but only ERR000, ERR010 - 020, and ERR appear in the Action Table, it matches the ERR in ERR006 to ERR in the Action Table.

In summary, there is a three pass lookup on Action Table:

- Pass 1 - Exact Match (up to first space)
- Pass 2 - Range Match
- Pass 3 - Exact Match (up to first non-alpha)

Following are some examples of the alarm matching procedure.

Sample Action Table:

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.) ERR005</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.) ERR000-030</td>
<td>PHONHOME</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3.) ERR</td>
<td>PAGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4.) .AUTHFAIL</td>
<td>PAGE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.) .AUTHFAIL.1</td>
<td>PAGE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Event:
- ERR000       matches (2)
- ERR005       matches (1)
- ERR040       matches (3)
- .AUTHFAIL    matches (4)
- .AUTHFAIL.1  matches (5)
8.4.2 Multiple Actions on a Single Alarm

In some instances you may want more than one action to occur when a single alarm is detected. For instance, a hacking attempt may be reported to two different people. In that case, the DOLIST command is used. The first line gives the general form of the alarm to be used as the trigger. The following lines have the same mnemonic but with an extension which denotes an order of action. In the example given below, .1 and .2 are added to show two subsequent actions to be taken. When the .AUTHFAIL alarm is detected, the ASG Guard/ASG Guard Plus "phones home" and pages, sending the alarm and the comments.

**NOTE:**
*DOLIST cannot be nested (a DOLIST inside another DOLIST).*

<table>
<thead>
<tr>
<th>ALARM</th>
<th>ACTION</th>
<th>PARAMETER</th>
<th>COMMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>.AUTHFAIL</td>
<td>DOLIST</td>
<td></td>
<td>HACKER ALERT</td>
</tr>
<tr>
<td>.AUTHFAIL.1</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.AUTHFAIL.2</td>
<td>PAGE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NOTE:**
The actions in a DOLIST are dispatched in the order shown in the Action Table, but they are not necessarily executed in that order. For example, the PHONHOME action may be rescheduled if the modem is already in use. In that case, the system will begin to execute the PAGE action without waiting for PHONHOME to complete.

8.5 Planning the Action Table

Before you start to build your Action Table, you should determine which alarm conditions to monitor and decide what action should be taken for each alarm condition.

A worksheet is provided to assist you in planning which alarm/status messages should be monitored by the ASG Guard/ASG Guard Plus, and what actions should be taken by the ASG Guard/ASG Guard Plus when they are received. To help guide you, we have also provided an example of a filled in worksheet at the end of this section.

**NOTE:**
*You must have at least Sysop 2 level access to add, delete or change Action Table items.*

1. **Determine which alarm conditions to monitor.**

Examine the types of alarms to which you or your staff respond on a regular basis and then define them in the worksheet.

In the example worksheet, note that the "SYS000" (System Reload) and "INI000" (System Reload Result) are among the types of messages that are being monitored. Other messages are BSD090 (Power Failure), the Digital Trunking Alarms (DTA and DTI), and the ERR series of alarms.

2. **Decide what action is to be taken when a particular alarm condition is received.**

Based on the action, you should then "match" this action to the alarm you select.

In the worksheet example, the alarm "SYS000" has been "matched" with the Action Routine "SCHEDULE" (which schedules a future action). The SCHEDULE routine requires that you define the action to be taken as well as the time at which that will occur. In the example, the
SCHEDULE routine has the parameter "15 PHONHOME". That means that the ASG Guard/ASG Guard Plus will schedule a PHONHOME action 15 minutes after the alarm occurs.

The reasoning behind this example is that a maintenance center, for instance, will probably want to be alerted to an unsuccessful system reload to check its status. By scheduling the report (PHONHOME) to take place 15 minutes after the event, an unsuccessful reload will be reported because a SYS000 occurs. A successful reload will not be reported because an INI000 occurs when the SYSLOAD is successful.

Also in the example, the routine "DOLIST" (which causes several actions to be performed) is assigned to the alarm "INI000". One of the actions to be performed by DOLIST is CANCEL, which has been given the parameter SYS000. When a successful system reload occurs, the ASG Guard/ASG Guard Plus will CANCEL the alert to the maintenance center. ASG Guard/ASG Guard Plus will, however, create a log entry stating that the "INI000" event occurred.

3. Test the Action Routine.

   Use the GE command to generate the event. Check to see if the desired action occurs.

   Example: Type GE SYS000 and see if the requested action occurs.

### Example ACTION TABLE WORKSHEET

<table>
<thead>
<tr>
<th>Alarm, Message, or Internal Event</th>
<th>Action Routine</th>
<th>Routine Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BATLOW</td>
<td>DOLIST</td>
<td></td>
</tr>
<tr>
<td>.BATLOW-1</td>
<td>PHONHOME</td>
<td>2</td>
</tr>
<tr>
<td>.BATLOW-2</td>
<td>PAGE</td>
<td>5551212,1234</td>
</tr>
<tr>
<td>.DAILY</td>
<td>DOLIST</td>
<td></td>
</tr>
<tr>
<td>.DAILY-1</td>
<td>CLKCHECK</td>
<td></td>
</tr>
<tr>
<td>.DAILY-2</td>
<td>SETHP</td>
<td>3</td>
</tr>
<tr>
<td>.DTRLOW</td>
<td>PHONHOME</td>
<td></td>
</tr>
<tr>
<td>.HOURLY</td>
<td>LOGCHECK</td>
<td>50</td>
</tr>
<tr>
<td>BSD090</td>
<td>PHONHOME</td>
<td></td>
</tr>
<tr>
<td>INI000</td>
<td>DOLIST</td>
<td></td>
</tr>
<tr>
<td>INI000-1</td>
<td>CANCEL</td>
<td>SYS000</td>
</tr>
<tr>
<td>INI000-2</td>
<td>CLKSET</td>
<td></td>
</tr>
<tr>
<td>SYS000</td>
<td>SCHEDULE</td>
<td>15 PHONHOME</td>
</tr>
<tr>
<td>.DTRLOW</td>
<td>PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>
## ACTION TABLE WORKSHEET

<table>
<thead>
<tr>
<th>Alarm, Message, or Internal Event</th>
<th>Action Routine</th>
<th>Routine Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.6 Action Table Commands

The Action and Alarm Functions Menu contains commands for maintaining the Action Table as well as the Event Table.

Type A at the system prompt and press the ENTER key to display the Action and Alarm Functions Menu. All commands associated with action and alarm functions are shown on this menu.

Site123>aa
--- Add Action Item ---
Alarm .DAILY
Action Routine PHONHOME
Routine Parameters 2
Comment Health check

07/17/97 10:21:55 [AUX] .DAILY Action item added

Screen 8-3. Add Action Item Screen

By entering the command mnemonic at the system prompt and pressing the ENTER key, the information screen for that command is displayed.

8.6.1 Adding an item to the Action Table – AA Command

The Add Action Item command is used to add an Action Item to the Action Table.

Type AA at the system prompt and press the ENTER key to display the Add Action Items screen.

Site123>aa
--- Add Action Item ---
Alarm .DAILY
Action Routine PHONHOME
Routine Parameters 2
Comment Health check

Screen 8-3. Add Action Item Screen
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm</td>
<td>Enter the alarm issued by the protected device or an ASG Guard/ASG Guard Plus internal event (internal events are listed at the end of this chapter) and press the ENTER key.</td>
</tr>
<tr>
<td>Action Routine</td>
<td>Enter the name of the Action Routine. The Action Routines included with each ASG Guard/ASG Guard Plus are listed below. Press the SPACE BAR until the desired choice is displayed. In addition, custom Action Routines may be written. A detailed description of each standard Action Routine is included in Chapter 14.</td>
</tr>
<tr>
<td>CANCEL</td>
<td>Cancels a pending Action Routine.</td>
</tr>
<tr>
<td>CLKAHEAD</td>
<td>Advances the ASG Guard/ASG Guard Plus clock by one hour.</td>
</tr>
<tr>
<td>CLKCHECK</td>
<td>Checks if current date is equal to first Sunday in April or last Sunday in October. If so, schedules either a CLKAHEAD (April) or CLKBACK (October) to occur at 2:00 AM.</td>
</tr>
<tr>
<td>DOLIST</td>
<td>Causes a list of Action Routines to be performed.</td>
</tr>
<tr>
<td>LOG</td>
<td>Creates a log entry describing the event.</td>
</tr>
<tr>
<td>LOGCHECK</td>
<td>Checks if the log buffer has reached a specified threshold. If log has exceeded threshold, a .LOGFULL event is generated.</td>
</tr>
<tr>
<td>NOACTION</td>
<td>No action is taken.</td>
</tr>
<tr>
<td>PAGE</td>
<td>Calls a numeric pager and delivers a message.</td>
</tr>
<tr>
<td>PHIRIS</td>
<td>Places a call to IRIS\textsuperscript{SM} and reports the event.</td>
</tr>
<tr>
<td>PHONHOME</td>
<td>Places a call to the maintenance reporting center.</td>
</tr>
<tr>
<td>PHPPP</td>
<td>Initiates a demand-dial PPP link.</td>
</tr>
<tr>
<td>PHSYSOP</td>
<td>Places a call to the maintenance center and initiates a Sysop session with Admin Catcher.</td>
</tr>
<tr>
<td>REMINIT</td>
<td>Performs the remote initialization function.</td>
</tr>
<tr>
<td>RESRELAY</td>
<td>Sets the specified relay(s) to the normally closed (N/C) state.</td>
</tr>
<tr>
<td>SCHEDULE</td>
<td>Schedules an Action Routine to occur at a defined time.</td>
</tr>
<tr>
<td>SETHP</td>
<td>Changes the setting of the Host Processing Flag</td>
</tr>
<tr>
<td>SETRELAY</td>
<td>Sets the specified relay(s) to the normally open (N/O) state (applies only to ASG Guard/ASG Guard Plus units with expansion board)</td>
</tr>
<tr>
<td>SNMPTRAP</td>
<td>Sends an SNMP trap to remote managers through the Ethernet or PPP link.</td>
</tr>
<tr>
<td>Routine Parameters</td>
<td>Enter parameters associated with the Action Routine. Enter values for parameters associated with the specified Action Routine. Parameters must be separated by commas. A comma is not needed at the end of the field. If you want to skip a parameter, place a comma for the parameter and a second one to separate it from the next parameter. For example, to enter the first and third parameters (skip the second parameter), enter two commas in the middle: 1,,3.</td>
</tr>
<tr>
<td>Comments</td>
<td>Type any comments you want attached to the event. Then press the ENTER key.</td>
</tr>
</tbody>
</table>
The system confirms that you have added an action item by displaying a confirming a log entry and displaying the system prompt.

8.6.2 List Action Items – LA Command

The List Action Items command displays the Action Table, which contains the following information:

- Alarms - Trigger (alarm or event) for the Action Routine.
- Routines - Action that will be taken when the alarm is received.
- Parameters - Parameters associated with the Action Routine.
- Comments - Description or explanation of the routine or other information.

The Action Table is updated when changes are made to it using other commands, such as Change Action Item, or Add Action Item, but cannot be changed directly by using the LA command.

Type LA at the system prompt and press the ENTER key to display the List Action Items screen.

To display only part of the Action Table, enter a modifier (for example, LA BSD will display all alarms starting with the letters 'BSD').

To display the complete list, enter LA with no modifiers.

>LA

--- List Action Items ---

<table>
<thead>
<tr>
<th>Alarm:</th>
<th>Routine:</th>
<th>Parameters:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) #NOTIFY-A</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) #NOTIFY-B</td>
<td>MGR2000 2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) #NOTIFY-C</td>
<td>PAGE 4)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7) .DAILY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8) .DAILY.1</td>
<td>CLKCHECK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9) .DAILY.2</td>
<td>SETHP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10) .HOURLY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11) .HOURLY-A</td>
<td>LOG</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12) .HOURLY-B</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13) DTA005</td>
<td>SCHEDULE 15 PHONHOME</td>
<td>DTI Yellow Alarm</td>
<td></td>
</tr>
<tr>
<td>14) DTA007</td>
<td>CANCEL DTA005^1</td>
<td>Yellow Cleared</td>
<td></td>
</tr>
<tr>
<td>15) DTI024</td>
<td>PHONHOME</td>
<td>DTI No Response</td>
<td></td>
</tr>
<tr>
<td>16) DTI030</td>
<td>PHONHOME</td>
<td>DTI Red Alarm</td>
<td></td>
</tr>
<tr>
<td>17) ERR</td>
<td>LOG</td>
<td>Test</td>
<td></td>
</tr>
<tr>
<td>18) ERR000</td>
<td>PHONHOME</td>
<td>Test</td>
<td></td>
</tr>
</tbody>
</table>

Screen 8-4. List Action Items Screen

You can also specify a search string by adding one or more characters after the LA command, separated by a space. For example, to display the action items starting with .H, type:

>LA .H

and press the ENTER key. Only those action items starting with .H are then displayed.
8.6.3 Change Action Item – CA Command

The Change Action Item command allows you to modify an existing action item. Type CA at the system prompt and press the ENTER key to display the Change Action Item screen.

```
Site123>CA
--- Change Action Item ---
  Alarm: Routine: Parameters: Comments:
  1) .DAILY        PHONHOME 2
Alarm           Routine Action Routine
Parameters      PHONHOME               3
Comment
07/17/97 10:36:30 [A] .DAILY Action item added
07/17/97 10:36:30 [A] .DAILY Action item modified
```

Screen 8-5. Change Action Item Screen

When CA is issued with no modifiers, the complete list is displayed. To specify a search string, add one or more characters, separated by a space, after the CA command. For example, to change action items starting with .D, type:

```
>CA .D
```

and press the ENTER key. The system will only display those action items beginning with .D. If the list contains more than 18 action items, you are prompted to press the ENTER key to view additional action items. If the action item you wish to change is not displayed, then press the ENTER key to see more action items.

You are prompted to enter the number corresponding to the action item you wish to change. After you type in a number and press the ENTER key, the system will display that Action Routine and its associated parameters. The Action Table is updated immediately as changes are made to it.

8.6.4 Schedule Action Item – SAI Command

The Schedule Action Item command schedules the occurrence of an Action Item. This command is usually used for remote installation and testing of new Action Routines. It lets you execute an Action Routine when there is no event associated with that action.

To display the Schedule Action Item screen, type SAI at the system prompt and press the ENTER key. Initially the Action Routine field is blank. Use the SPACE BAR to scroll through the list of Action Routines. Select an Action Routine by pressing the ENTER key when the Action Routine you want appears in the field. The cursor will then advance to the Parameters field.

Continue through the fields by typing in your data and pressing the ENTER key. Pressing the ENTER key when the cursor is in the Comment field completes the process.
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameters</td>
<td>Type the parameter, or parameters, that you want to associate with this Action Routine. Press the ENTER key to advance the cursor to the next field.</td>
</tr>
<tr>
<td>Schedule Date</td>
<td>The day on which you want the Action Routine to activate, where:</td>
</tr>
</tbody>
</table>

- today = The Action Routine is scheduled to occur today at the time specified (pressing the ENTER key selects this date).
- mm/dd/yy = Type the month, day, and year that you want the Action Routine to occur and then press the ENTER key.
- nn = Type the number of days from today that you want the Action Routine run and then press the ENTER key. |
| Schedule Time | The time of day (using the 24-hour clock format) at which you want the Action Routine to activate, where: |

- now = The Action Routine will occur immediately (ASAP). Pressing the ENTER key selects this time.
- hh:mm = Type the time of day, in 24-hour clock format (for example, 2:00 PM is given as 14:00) at which you want the routine run and then press the ENTER key.
- nn = Type the number of minutes from now that you want the routine run and then press the ENTER key. |
| Event | If you are simulating a particular Event for testing, type the event here as it would have been received to trigger this action. For example, if you test PHONHOME, this field could be used to signify it is a test. The system defaults to “Sysop Generated”. |
| Comment | Type any comments that you want attached to the Event. |

### 8.6.5 Delete Action Item – XA Command

The Delete Action Item command allows you to remove an action item from the Action Table. Type XA at the system prompt and press the ENTER key to display the Delete Action Item screen.

Depending on the number of action items in the table, you may be prompted to press the ENTER key to view additional action items. If the number corresponding to the action item you wish to delete is higher than 18, press the ENTER key to display the next screen of action items.

The Action Table is updated immediately as changes are made to it. To delete an entry from the table, enter the number corresponding to that entry following the Select # - prompt, then press the ENTER key. The system then displays the line for that action item and asks if you want to delete that record. Initially, a No appears in the field. Press the SPACE BAR to toggle the field to Yes and then press the ENTER key. The system confirms that you have deleted that record.
SITE123>XA

--- Delete Action Item ---

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) .DAILY          PHONHOME 2                    health check</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) .DTA005          SCHEDULE AM PHONHOME          DTI YELLOW ALARM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3) .DTA007          CANCEL   .DTA005              YELLOW ALARM CLEARED</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Select # -> 1  (Ctrl-A to quit)

.DAILY          PHONHOME 2                    health check

Delete Record ?   Yes

07/25/97 09:38:22 [AUX] .DAILY Action item deleted

SITE123>LA

--- List Action Items ---

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) .DTA005          SCHEDULE AM PHONHOME          DTI YELLOW ALARM</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2) .DTA007          CANCEL   .DTA005              YELLOW ALARM CLEARED</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

-- End of List --

Screen 8-6. Delete Action Item Screen

When XA is entered without modifiers, the complete list is displayed. To specify a search string, enter the XA command, followed by a space, and then one or more characters. For example, if you only want to delete action items starting with .H, type: XA .H and press the ENTER key. Only action items beginning with .H will be displayed.
8.7 Alarm/Event Functions Commands

The Alarm/Event Functions allow you to change or delete pending alarms and events. After an alarm is issued, it is placed in the event table for processing. You can list the pending actions contained in the Event Table. In addition, you can generate an alarm or event as if the data had been received on a host port or an internal event had occurred. This is especially useful for testing and demonstration purposes.

8.7.1 List Alarms/Events – LE Command

The List Alarms/Events command allows you to list all pending actions contained in the Event Table (the "event queue").

Type LE at the system prompt and press the ENTER key displays the List Alarms/Events screen.

The complete list is displayed when only LE is entered with no modifiers. A search string can be specified by adding one or more characters after the LE command, separated by a space.

For example, if you only want to display .HOURLY events, type:

```
>LE .H
```

and then press the ENTER key.

```
>LE

--- List Alarms/Events ---

Current Date: 01/10/93   Time: 09:11:29

1) .HOURLY   10/10/93   08:00:01
   PHONHOME (ASAP)
2) .HOURLY   10/10/93   09:00:02
   PAGE (ASAP)

-- End of List --

site123>
```

Screen 8-7. List Alarms/Events Screen

If the list contains more than nine alarms/events, press the ENTER key to view the next nine alarms/events.

8.7.2 Generate Alarm/Event – GE Command

Testing the Action Routine or an alarm is an important part of the process. The SAI command can be used to test an Action Routine. The Generate Alarm/Event command allows you to test any alarm defined in the Action Table. This command generates the Alarm or Event as if the data had been received on the host port or an internal Event had occurred. This command is useful for debugging or modifying Action Tables.
Type **GE** followed by the event that you want the ASG Guard/ASG Guard Plus to generate. For example, type **GE .AUTHFAIL.** to generate the event .AUTHFAIL. You can also generate a "long" event - for example, GE DTA005 1 0020 0031 7.

```
Ser#98100221>GE .AUTHFAIL

--- Generate Alarm/Event ---

02/26/99 10:23:45 9573 [AUX] Event/:.AUTHFAIL
02/26/99 10:23:46 6AD1 SNMPTRAP: .AUTHFAIL
02/26/99 10:23:47 AF35 SNMPTRAP: Rescheduled – Network Down
```

**Screen 8-8.** Generate Alarm/Event Screen

Alternatively, type **GE** and then enter the alarm/event to be generated at the prompt. Note that "Enter alarm/event" limits the number of characters. If you want to generate a "long" event, use the method described above.

```
Ser#98100221>GE .AUTHFAIL

--- Generate Alarm/Event ---
Enter alarm/event .AUTHFAIL

02/26/99 10:23:56 9573 [AUX] Event/:.AUTHFAIL
02/26/99 10:23:59 6AD1 SNMPTRAP: .AUTHFAIL
02/26/99 10:23:59 AF35 SNMPTRAP: Rescheduled – Network Down
```

**Screen 8-9.** Generate Alarm/Event Screen

Type the mnemonic for the alarm or event you want to have performed and press the ENTER key. The system will confirm that the alarm/event was generated.
8.7.3 Delete Alarm/Event – XE Command

The Delete Alarm/Event command allows you to remove a pending action from the Event Table. An access class of Sysop 2 or higher is required.

Type XE at the system prompt and press the ENTER key to display the Delete Alarm/Event screen. The system will then display the parameters for that alarm/event, with the cursor appearing at the first parameter.

```
>XE
--- Delete Alarm/Event ---
Current Date: 10/10/93  Time: 09:15:36
1) .HOURLY    10/10/93 08:00:01
   PHONHOME (ASAP)
2) SYSOP GENERATED 10/10/93 09:00:02
   PHONHOME (ASAP)
3) .CDR_REGIONAL_CALLS,001,0004,Max Call/Hr   10/07/93 09:37:21
   PAGE     (ASAP),9990010004
Select # ->      (ENTER for more, * for all, Ctrl-A to quit)
```

**Screen 8-10. Delete Alarm/Event Screen**

The Event Table is updated immediately as changes are made to it. To delete an entry in the table, enter the number corresponding to that entry at the Select # - prompt, then press the ENTER key.

**NOTE:**
*The entire Event Table may be cleared by typing an asterisk (*) instead of a number.*

The system then displays the line for that action item and asks if you want to delete that record. Initially, a No appears in the field. Press the SPACE BAR to toggle the field to Yes and then press the ENTER key. The system confirms that you have deleted the record.

```
Select # -> 2    (ENTER for more, * for all, Ctrl-A to quit)
            SysOp Generated 10/10/93 09:00:02
            PHONHOME (ASAP)
Delete Record ? Yes
>10/10/93 09:16:12 [M] SysOp Generated Alarm/Event deleted
```

**Screen 8-11. Delete Record Screen**
8.8 Internal Alarms and Events

In addition to the alarms generated by the Host or PBX system, the ASG Guard/ASG Guard Plus supports several internal events. Chapter 14 contains a complete description of each internal event and standard Action Routines and required parameters.

Table 8-1. Internal Events

<table>
<thead>
<tr>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>.AUTHFAIL</td>
<td>Event occurs upon receipt of a failed authentication attempt.</td>
</tr>
<tr>
<td>.BAT48HIGH</td>
<td>Event occurs when battery voltage crosses over from an OK condition to a high voltage condition. Use the SSA command to specify the upper limit.</td>
</tr>
<tr>
<td>.BAT48LOW</td>
<td>Event occurs when battery voltage crosses over from an OK condition to a low voltage condition. Use the SSA command to specify the upper and lower limits.</td>
</tr>
<tr>
<td>.BAT48OK</td>
<td>Event occurs when battery changes from a high or low condition to an OK condition. Use the SSA command to specify the upper and lower limits.</td>
</tr>
<tr>
<td>.BUFREADY</td>
<td>Event occurs when a buffer file has been closed and is ready to be sent.</td>
</tr>
<tr>
<td>.C#CLOSED</td>
<td>Event indicating that the contact closure input has been changed from open to closed, for example, .C3CLOSED.</td>
</tr>
<tr>
<td>.C#OPEN</td>
<td>Event indicating that the contact closure input has been changed from closed to open, for example, .C3OPEN.</td>
</tr>
<tr>
<td>.CLKCHANGE</td>
<td>Event indicating that the internal clock of the ASG Guard/ASG Guard Plus has changed.</td>
</tr>
<tr>
<td>.DISKCRIT</td>
<td>Event occurs when the RAMdrive reaches the critical level assigned by the Set Disk Parameters command.</td>
</tr>
<tr>
<td>.DISKFULL</td>
<td>Event occurs when the RAMdrive is full. All further attempts to write to the disk will be unsuccessful.</td>
</tr>
<tr>
<td>.DTRHIGH.n</td>
<td>Event occurs when the host or PBX asserts DTR (or host cable is connected), e.g DTRHIGH1 indicates the host or PBX on host port number 1 has asserted DTR or the host cable is connected (# indicates host port number).</td>
</tr>
<tr>
<td>.DTRLOW.n</td>
<td>Event occurs when the host or PBX stops asserting DTR or the physical connection is lost between ASG Guard/ASG Guard Plus and the host or PBX (# indicates the host port number).</td>
</tr>
<tr>
<td>.HOURLY</td>
<td>Event occurs at the top of each hour.</td>
</tr>
<tr>
<td>.INTBATLOW</td>
<td>Event occurs when the internal battery status has been changed from OK to Low. A “low” battery status indicates that the voltage is less than 11 volts.</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
</tr>
<tr>
<td>.INTBATOK</td>
<td>Event occurs when the internal battery status has been changed from Low to OK. For the .INTBATOK event to be generated, the voltage must go from &lt;11 volts to above 11.5 volts.</td>
</tr>
<tr>
<td>.LOGFULL</td>
<td>Created by LOGCHECK. Event occurs automatically when the internal Log Buffer is full.</td>
</tr>
<tr>
<td>.MAXRETRY</td>
<td>Generated by PHONHOME, PHIRIS, PHSYSOP, or PAGE according to Max.Retries system parameter.</td>
</tr>
<tr>
<td>.MDMINITERR</td>
<td>Event indicating a modem initialization error.</td>
</tr>
<tr>
<td>.MEMLOW</td>
<td>Event occurs on the hour if fewer than 4 KB are available in the ASG Guard/ASG Guard Plus variable area.</td>
</tr>
<tr>
<td>.MONTHLY</td>
<td>Event occurs once a month.</td>
</tr>
<tr>
<td>.NETDOWN</td>
<td>Event occurs after a preset length of time during which no network activity is detected.</td>
</tr>
<tr>
<td>.NETUP</td>
<td>Event occurs when network activity is detected following a period of inactivity.</td>
</tr>
<tr>
<td>.POWERUP</td>
<td>Event occurs when the system is powered up.</td>
</tr>
<tr>
<td>.PPPREQ</td>
<td>Event to trigger the dial-on-demand PPP link.</td>
</tr>
<tr>
<td>.POWERLOW</td>
<td>Event indicating that the external power supply has changed from OK to low.</td>
</tr>
<tr>
<td>.POWEROK</td>
<td>Event indicating that the external power supply has changed from low to OK.</td>
</tr>
<tr>
<td>.RTSHIGH.n</td>
<td>Event indicating that the RS-232 signal RTS has changed from Low to High. (# indicates host port number)</td>
</tr>
<tr>
<td>.RTSLOW.n</td>
<td>Event indicating that the RS-232 signal RTS has changed from High to Low. (# indicates host port number).</td>
</tr>
<tr>
<td>.S#HIGH</td>
<td>Event indicating that the 5 volt sensor has been changed from OK to High.</td>
</tr>
<tr>
<td>.S#LOW</td>
<td>Event indicating that the 5 volt sensor has been changed from OK to Low.</td>
</tr>
<tr>
<td>.S#OK</td>
<td>Event indicating that the 5 volt sensor has been changed from Low or High to OK.</td>
</tr>
<tr>
<td>.TEMPHIGH</td>
<td>Event occurs when temperature crosses over from an OK condition to a high temperature condition.</td>
</tr>
<tr>
<td>.TEMPLOW</td>
<td>Event occurs when temperature crosses over from an OK condition to a low temperature condition.</td>
</tr>
<tr>
<td>Event</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-------------------------------------------------------------</td>
</tr>
<tr>
<td>.TEMPOK</td>
<td>Event occurs when temperature changes from a high or low condition to an OK condition.</td>
</tr>
<tr>
<td>.WEEKLY</td>
<td>Event occurs once a week, each Sunday at midnight.</td>
</tr>
</tbody>
</table>
8.9 Action Routines

The ASG Guard/ASG Guard Plus is pre-programmed with a number of Action Routines that can be used when alarms or internal events occur. These Action Routines are summarized in Table 8-2 and described fully in Chapter 14.

Table 8-2. Action Routines

<table>
<thead>
<tr>
<th>Action Routine</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CANCEL</td>
<td>Cancels a pending action.</td>
</tr>
<tr>
<td>CLKAHEAD/CLKBACK</td>
<td>Advances (or sets back) the time setting in ASG Guard/ASG Guard Plus by 1 hour and schedules CLKSET for immediate execution.</td>
</tr>
<tr>
<td>CLKCHECK</td>
<td>Checks if current date is the first Sunday in April or last Sunday in October. If it is, schedules either a CLKAHEAD or CLKBACK to occur at 2:00 am.</td>
</tr>
<tr>
<td>DOLIST</td>
<td>Causes a list of Action Routines to be performed.</td>
</tr>
<tr>
<td>LOG</td>
<td>Creates a log entry that describes the event.</td>
</tr>
<tr>
<td>LOGCHECK</td>
<td>Checks to see if the Log buffer has reached a specified threshold. If log has exceeded the threshold, a .LOGFULL event is generated.</td>
</tr>
<tr>
<td>NOACTION</td>
<td>Creates &quot;Event: &quot; Log entry.</td>
</tr>
<tr>
<td>PAGE</td>
<td>Calls a pager number and delivers a message.</td>
</tr>
<tr>
<td>PHIRIS</td>
<td>Delivers an alarm message to IRIS®.</td>
</tr>
<tr>
<td>PHONHOME</td>
<td>Places a call to the maintenance reporting center.</td>
</tr>
<tr>
<td>PHPPPP</td>
<td>Initiates a demand-dial PPP link</td>
</tr>
<tr>
<td>PHSYSOP</td>
<td>Places a call to the maintenance center and starts a Sysop session.</td>
</tr>
<tr>
<td>REMINIT</td>
<td>Performs the Remote Initialization function.</td>
</tr>
<tr>
<td>RESRELAY#*</td>
<td>Resets the specified relay so that attached device is turned off.</td>
</tr>
<tr>
<td>SCHEDULE</td>
<td>Schedules an action for a later time.</td>
</tr>
<tr>
<td>SETHP</td>
<td>Changes the setting of the Host Processing Flag. (see SHP system function command).</td>
</tr>
<tr>
<td>SETRELAY#*</td>
<td>Sets the specified relay so that attached device is turned on.</td>
</tr>
<tr>
<td>SNMPTRAP</td>
<td>Sends an SNMP trap to remote managers through the Ethernet or PPP link.</td>
</tr>
</tbody>
</table>

* Applies only to ASG Guard.
Page intentionally left blank.
9. System Functions

9.1 What This Chapter Contains

- Overview
- Site Information Parameters
- Scheduling Parameters
- Modem Action Routine Parameters
- Software Upgrade Information

9.2 Overview

The System Functions Menu provides commands for setting and displaying system and environmental manager functions. The System Parameters are used primarily for information purposes. For example, the site name and the phone number of the unit are specified by these parameters. When the unit pages or phones home, this information may be sent along with the alarm and any message. The system parameters also specify scheduling information. For example, the start of the overnight period is set by these parameters.

9.3 Systems Functions Menu

Type S at the system prompt and press the ENTER key to display the System Functions Menu.

```
-- -- -- SYSTEM FUNCTIONS ( CMaster ) -- -- --

--- System Parameters Functions ---
DSP   Display System Parameters     SSP   Set System Parameters
SHP   Set Host Proc. Flag           SDT   Set Date and Time

--- Environmental Control Functions ---
SSA   Set Sensor Alarms             DSA   Display Sensor Alarms
DSI   Display Sensor Inputs         DCC   Display Contact Inputs
SRLY  Set Relays                    RRLY  Reset Relays

--- Device Management Functions ---
UPG   Upgrade ASG Guard Software     BOOT  Reboot Unit
DUMP  Dump Config. Details          DUMPF Dump Config. Details to File
CDUMP Dump Customer Users           CDUMPF Dump Customer Users to File

Other Menus: A -Alarm/Event  U -User  L -Log  F -File  P -Port/Session
```

Screen 9-1. System Functions Screen
The System Parameters Functions menu has three functional groups: System Parameters Functions, Environmental Control Functions and Device Management Functions.

**System Parameters Functions**

The commands in this functional group enable you to set and display system parameters including the host processing flag and the date and time of the ASG Guard/ASG Guard Plus.

**Environmental Control Functions**

The commands in this function group enable you to set and display sensor and contact inputs and alarms. Descriptions of Environmental Manager functions are included in [Chapter 10](#), Environmental Manager.

**Device Management Functions**

The commands in this function group enable you to upgrade the ASG Guard/ASG Guard Plus software, reboot the ASG Guard/ASG Guard Plus, and back up and restore configuration data and the Customer User Table.
9.4 System Parameter Functions

The commands in this functional group enable you to set and display system parameters including the host processing flag and the date and time of the ASG Guard/ASG Guard Plus.

9.4.1 Set System Parameters – SSP Command

The Set System Parameters (SSP) command enables you to set site information, scheduling parameters and default telephone numbers.

Type SSP to select which parameter group you want to be displayed. The following screen appears.

```
site123>SSP

--- Set System Parameters ---

1 = Site Information
2 = Scheduling Params
3 = Modem Action Routine Params

Select Group -->1
```

Screen 9-2. Set System Parameters Screen

9.4.1.1 Site Information

Type 1 to set Site Information. Site information includes site name, ASG Guard/ASG Guard Plus phone number and the host password. When the ASG Guard/ASG Guard Plus pages or phones in response to a particular alarm or event, it sends its site name and unit phone number along with the error message and other information that enables the receiver to contact the correct ASG Guard/ASG Guard Plus.

```
site123>SSP

--- Set System Parameters ---

1 = Site Information
2 = Scheduling Params
3 = Modem Action Routine Params

Select Group -->1

-- Site Information --
Site Name (USN=Unit Ser. Number)   Ser#USN
Unit Phone Number
Host Password for login routine    0000
Number of Expansion Ports
Reassigned to Modems                0
```

Screen 9-3. Set System Parameters Screen
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>Descriptive name of the ASG Guard/ASG Guard Plus location. When information is sent to another device, the site name is included automatically. Additionally, the site name is shown at the prompt. The site name may have a maximum of 30 alphanumeric characters. Only the first 15 characters appear at the prompt. The default site name is the unit's serial number. If you have more than one ASG Guard/ASG Guard Plus at a site, using the serial number as the site name is useful. If a site name is not entered, only the command prompt is displayed.</td>
</tr>
<tr>
<td>Unit Phone Number</td>
<td>Enter the phone number of the ASG Guard/ASG Guard Plus. This number is sent by the PHONHOME Action Routine.</td>
</tr>
<tr>
<td>Host Password for login routine</td>
<td>Enter the password for the host system for automatic login. The password may have a maximum of 16 alphanumeric characters.</td>
</tr>
<tr>
<td>Number of Expansion Ports Reassigned to Modems (ASG Guard Plus only)</td>
<td>The last four host ports on a host port expansion board can be converted to inbound modem ports. Press the SPACE BAR until the desired choice is displayed (0 and 4). Note that all four host ports must be converted. Sets host ports 13-16 or 25-28 as external Modem ports. After reconfiguring, the system must be rebooted for the change to take affect. <strong>NOTE: If modems are connected, cross-over (null host) cables must be used.</strong></td>
</tr>
</tbody>
</table>
9.4.1.2 Scheduling Parameters

After entering SSP, type 2 to set the Scheduling Parameters and press the ENTER key. In this section, the start of the overnight or P.M. period, the time of the A.M. report, and the number of times the ASG Guard/ASG Guard Plus will try to execute a rescheduled event, such as paging, are set.

<table>
<thead>
<tr>
<th>Start of Overnight Period</th>
<th>18:00</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time for AM Report</td>
<td>06:00</td>
</tr>
<tr>
<td>Max. Retries</td>
<td>5</td>
</tr>
<tr>
<td>Minutes Between Retries</td>
<td>3</td>
</tr>
<tr>
<td>... After Retries Expired</td>
<td>60</td>
</tr>
</tbody>
</table>

Screen 9-4. Set System Parameters Screen

**Field** | **Function**
--- | ---
Start of Overnight Period | Enter the time that the overnight period starts. This defines the end of the working day. All alarms (non-critical) assigned to Action Routines scheduled for AM execution collected after the specified time and before the “Time for AM Report” will be scheduled for delivery at the beginning of the A.M. period.

Time for AM Report | Enter the time at which the alarms scheduled for AM execution will be sent. This defines the start of the working day.

Max. Retries | The number of times a scheduled event will attempt to execute before it will reschedule according to the time delay defined by the “After Retries Expired”. See Chapter 14.

Minutes Between Retries | The number of minutes between attempts to execute a scheduled event.

... After Retries Expired | “After Retries Expired” is the number of minutes the ASG Guard/ASG Guard Plus will wait before retrying to send the report after the number set by “Max. Retries” has been reached.
### 9.4.1.3 Modem Action Routine Parameters

Type 3 to set the modem Action Routine parameters and press the ENTER key.

```
>ssp
--- Set System Parameters ---

1 = Site Information  
2 = Scheduling Params  
3 = Modem Action Routine Params

Select Group -->3

-- Modem Action Routine Parameters --
Home Phone Number 1 (Default)
Home Phone Number 2
Home Phone Number 3
Delay Before Transmit (sec)        5
Report Multiple Alarms ?           Yes
Default Pager Number
Default Pager Message
Default Action Routine Modem       Modem #1
```

**Screen 9-5. Set System Parameters Screen**

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home Phone Number 1 (Default)</td>
<td>Default phone number to be used by Action Routines such as the PHONHOME Action Routine. (If no parameter is specified in the Action Table, the Action Routine will use Home Phone Number 1.) To use Home Phone Number 2, specify 2 in the parameter field.</td>
</tr>
<tr>
<td>Home Phone Number 2</td>
<td>The length of time, in seconds, that the modem will wait before transmitting data after a connection has been established. This is useful in MNP connections.</td>
</tr>
<tr>
<td>Home Phone Number 3</td>
<td></td>
</tr>
</tbody>
</table>

**Delay Before Transmit (sec)**

Initially **No** appears on the screen. Press the SPACE BAR to toggle to **Yes**. Select **Yes** to have all scheduled alarms to the same location reported when the ASG Guard/ASG Guard Plus calls in to report the first alarm. Select **No** to have the ASG Guard/ASG Guard Plus report alarms on an individual basis.

**Report Multiple Alarms?**

**Default Pager Number**

The number used by PAGE Action Routine to dial a remote pager if a number has not specified in the parameters of the PAGE Action Routine.

**Default Pager Message**

Default message delivered to the remote pager when dialed by the PAGE Action Routine. If a message is included with the PAGE Action Routine parameters, the default message will not be used.
**Default Action Routine Modem**

The modem that is used by Action Routines unless a different modem is specified. Press the SPACE BAR until the appropriate choice is displayed.

### 9.4.2 Display System Parameters – DSP Command

The Display System Parameters (DSP) and Set System Parameters (SSP) commands enable you to view or set site information, scheduling parameters and default telephone numbers.

To see the current system settings for these parameters, type **DSP** at the system prompt. The following screen appears.

```
Site123>DSP

--- Display System Parameters ---

-- Site Information --

Site Name (USN=Unit Ser. Number) Site123
Unit Phone Number
Host Password for login routine 0000
Use Log Message Authentication Codes? Yes
Number of Expansion Ports
Reassigned to Modems 0

-- Scheduling Parameters --

Start of Overnight Period
Time for AM Report
Max. Retries
Minutes Between Retries
.. After Retries Expired

-- Modem Action Routine Parameters --

Home Phone Number 1 (Default)
Home Phone Number 2
Home Phone Number 3
Delay Before Transmit (sec)
Report Multiple Alarms? No
Default Pager Number
Default Pager Message
Default Action Routine Modem Modem #1

Site123>
```

**Screen 9-6.** Display System Parameters Screen
To change any of these settings, type **SSP** at the system prompt. The following screen appears.

--- Set System Parameters ---

1 = Site Information  
2 = Scheduling Params  
3 = Modem Action Routine Params

Select Group -> 1

**Screen 9-7. Set System Parameters Screen**

Type the number (1, 2 or 3) of the category in which you would like to change the setting, then press the ENTER key. If you are familiar with the ASG Guard/ASG Guard Plus, you can go directly to the desired category by using a one-line command.

**Example:**

Site123>SSP 1

This command puts the user directly to the Site Information parameters.

(The screen example is shown in Section 9.4.1.)

**9.4.3 Set Host Processor Flag – SHP Command**

The set host processing command allows the user four options for processing information relative to action routines. Typing **SHP** at the system prompt displays these options:

--- Set Host Proc. Flag ---

Choices Are:  
1 - All Action Routines Enabled  
2 - Modem/Host Action Routines Disabled  
3 - All Action Routines Disabled  
5 - All Action Routines Disabled, Ignore Host Data

--> 1

**Screen 9-8. Set Host Proc. Flag Screen**

By default, all action routines are enabled. However, the user may choose to disable only modem and host action routines, disable all action routines while still monitoring host data, or disable all action routines and ignoring host data.
9.4.4 Set Date and Time – SDT Command

The Set Date and Time command (SDT) allows the user to set the date format to one of ten options and to set the actual date and time. Type SDT at the system prompt and you will see (one line at a time):

```
Site123> SDT
--- Set Date and Time ---
Date Format                        YY/MM/DD
Current Date                       98/12/08
Current Time                       18:42
```

Screen 9-9. Set Date and Time Screen

The default date format is shown above. By using the SPACE BAR, the user may change the format to one of ten date formats. All areas within the ASG Guard/ASG Guard Plus will reflect the change in format. As an example, if an action item is scheduled to occur (in the default format) on 07/09/98, and the user changes the format to a four-digit year, the Action Item date will contain a four-digit year. The ten options available in the ASG Guard/ASG Guard Plus are:

- MM/DD/YY
- MM/DD/YYYY
- YYYY/MM/DD
- YY/MM/DD
- DD/MM/YYYY
- MM-DD-YY
- MM-DD-YYYY
- YYYY-MM-DD
- YY-MM-DD
- DD-MM-YYYY

Scroll through the options with the SPACE BAR until the desired format is viewed and press enter. Following the format just set, enter the current date and press enter. Enter the current time using the 24 hour (Military) time format and press enter. You will receive a response similar to:

```
98/12/08 18:41:23 54B6 [AUX] .CLKCHANGE
98/12/08 18:41:23 32BF [AUX] Set Date and Time - O.K.
Site123>
```

Screen 9-10. Set Date and Time Screen
9.5 Device Management Functions

The commands in this function group enable you to upgrade the ASG Guard/ASG Guard Plus software, reboot the ASG Guard/ASG Guard Plus, and back up and restore configuration data and the Customer User Table.

9.5.1 Check the Software Version – VER Command

The VER command can be issued to display configuration information. Issue the VER command at the system prompt. An example of the type of information displayed by the VER command is shown below.

```
ver
--- Version Information ---
ASG Guard v3.72 /r /l (F/W 3.71)
FLASH Version: 2.2
Memory (DRAM) Size: 32 MB
Host ports: 4
Modem ports: 2
Telnet ports: 3
Real-World Expansion: Detected
Modem 1: TDK DF5600 Data-Fax Modem
Modem 2: TDK DF5600 Data-Fax Modem
Site Name: Ser#98100221
Unit Serial Number: 982H10022118
System Date/Time: 12/02/1998 10:10:53
```

Screen 9-11. Version Information Screen

If a host port expansion board is installed, it will be listed in the VER command response.

The VER command result consists of the following components:

- **ASG Guard Version**: Current version of software and firmware loaded in the ASG Guard. The "/r" signifies the Real World Interface (capable of using contact closures and temperature sensors). The "/l" signifies the Guard contains Lucent code. "F/W" identifies the CCL Interpreter revision level.
- **Flash Version**: Operating system revision level.
- **Memory (DRAM) Size**: The amount of RAM within the ASG Guard.
- **Host ports**: The quantity of host ports.
- **Modem ports**: The amount of modem ports available.
- **Telnet ports**: The amount of Telnet ports.
- **Real-World Expansion**: Identifies whether the ASG Guard has RWI available on the Mother Board. The ASG Guard Plus requires a RWI expansion board.
- **Modem 1**: Identifies the modem installed in ASG Guard.
- **Modem 2**: Identifies the modem installed in ASG Guard.
• Site Name: The site name which can be changed using the SSP command.
• Unit Serial Number: The unit serial number.
• System Date/Time: Current date and time.

9.5.2 Upgrade the Software – UPG Command

The Secure ASG Guard/ASG Guard Plus software (Option 1), CCL interpreter (Option 2), and flash memory (E-PROM, Option 3) of the ASG Guard/ASG Guard Plus can be upgraded by copying the files to the appropriate area and using the UPG command. The files can be transferred from another device to the ASG Guard/ASG Guard Plus by using a communications package such as ProComm Plus. The files must reside in the current directory before attempting to upgrade procedure.

To upgrade the software, download the files by using ProComm or other communication package to the RAM disk of the ASG Guard/ASG Guard Plus. Type the UPG command and press the ENTER key, and then select the area you wish to upgrade. Enter the appropriate *.DAT file located in the current directory of the ASG Guard/ASG Guard RAM disk. The file is then copied to the non-volatile appropriate memory area of the ASG Guard/ASG Guard Plus.

--- Upgrade ASG Guard Software ---

1 = Secure ASG Guard
2 = CCL Interpreter
3 = Flash Memory

Select Area to Upgrade --> 1

Screen 9-12. Upgrade ASG Guard Software Screen

9.5.3 Restart the ASG Guard/ASG Guard Plus – BOOT Command

The ASG Guard/ASG Guard Plus can be soft booted from a SYSOP (at the system prompt). A soft boot will re-initialize all ports. This feature was added in order to restart the unit but NOT lose any stored files. A hard boot (power-cycling the unit) will clear the RAM disk, and ALL FILES WILL BE DELETED! Perform one of the following steps:

To soft boot the unit, type BOOT at the command prompt. You will see:

Site123>BOOT

--- Reboot Unit ---
All operations will be cancelled and all ports reinitialized
Are You Sure (Y/N)? No

Screen 9-13. Reboot Unit Screen

The default value is NO. Press the SPACE BAR once to change it to YES, then press the ENTER key. The ASG Guard/ASG Guard Plus will re-start and initialize all ports.

NOTE: Power Cycling the ASG Guard/ASG Guard Plus will cancel all running Action Routines and delete all buffers!
9.5.4 View or Save Configuration Data on Remote Device - DUMP Command

The DUMP command allows the user to either view or save the ASG Guard/ASG Guard Plus configuration. The entire configuration or any portions thereof can be viewed or saved in a file on an administrative personal computer. Appendix C provides the procedures for using the DUMP command.

9.5.5 Save Configuration Data on RAM Disk File - DUMPF Command

The DUMPF command allows the user to save the ASG Guard/ASG Guard Plus configuration in a file on the ASG Guard/ASG Guard Plus RAM disk. The entire configuration or any portions thereof can be saved in a file. Appendix C provides the procedures for using the DUMPF command.

9.5.6 Put Customer User Table on Remote Device – CDUMP Command

The CDUMP command allows the user to either view or save the Customer User Table in a file on an administrative personal computer. Appendix C provides the procedures for using the CDUMP command.

9.5.7 Put Customer User Table on RAM Disk File – CDUMPF Command

The CDUMPF command allows the user to save the Customer User Table in a file on the ASG Guard/ASG Guard Plus RAM disk. Appendix C provides the procedures for using the CDUMPF command.

9.5.8 Load a Configuration File – CONFIG Command

The CONFIG command allows the user to import a configuration file (i.e., load the configuration data) from an administrative personal computer or from the ASG Guard/ASG Guard Plus RAM disk. Appendix C provides the procedures for using the CONFIG command.

9.5.9 Load a Customer User Table – CCONFIG Command

The CCONFIG command allows the user to import a Customer User Table (i.e., load the Customer User Table data) from an administrative personal computer or from the ASG Guard/ASG Guard Plus RAM disk. Appendix C provides the procedures for using the CCONFIG command.
10. Environmental Manager

10.1 What This Chapter Contains

- Overview
- Environmental Manager Menu
- How to Monitor Conditions by Using the Environmental Manager
- Defining Threshold Limits

10.2 Overview

The Environmental Manager uses analog sensors to monitor conditions such as temperature, humidity, and battery voltage. In addition, the Environmental Manager can also monitor change of state activities such as contact closures. External devices like auxiliary fans or alarms can be controlled by the ASG Guard’s two solid state relays in conjunction with external power relays.

The ASG Guard/ASG Guard Plus converts analog input signals to digital signals used to generate internal events. For information on how to associate internal events with Action Routines, refer to Chapter 14.

10.3 ASG Guard/ASG Guard Plus Series Environmental Manager Options

Below is an outline of the Environmental Manager Options for the ASG Guard/ASG Guard Plus product line. Along with the differences listed here, there is also a difference in the interface cable between the ASG Guard Plus and ASG Guard. The ASG Guard Plus uses an Amphenol connector to access all environmental functions. The ASG Guard uses standard RJ45 connections for the 2 temperature probes and the 0-5 volt analog input. The solid state relays use a 6 pin Euroblock connection, while the contact closures use a 10 pin Euroblock connection.

ASG Guard Plus (Base Unit) inputs to the Environmental Manager are listed below:

- 48-Volt Battery Monitor available with or without the optional 48V DC-DC converter.
- One temperature Sensor: requires temperature probes required
- Three 0-5 VDC analog inputs
- Eight contact closures inputs

ASG Guard inputs to the Environmental Manager are listed below:

- 48 volt battery monitor available with or without the optional 48V DC-DC converter
- Two temperature sensors; temperature probes required
- One 0-5 VDC analog inputs
- Five contact closure inputs
- Two Solid State Relays (Relay #1 latching, #2 non-latching)
10.4 Environmental Manager Functions and Commands

Environmental functions are included in the system menu. To display the menu, type `S` at the system prompt and press the ENTER key.

The System menu has three functional groups: System Parameters Functions, Environmental Control Functions, and Device Management Functions.

The commands for the ASG Guard and ASG Guard Plus are below:

| --- System Parameters Functions --- |
| DSP | Display System Parameters | SSP | Set System Parameters |
| SHP | Set Host Proc. Flag | SDT | Set Date and Time |

| --- Environmental Control Functions --- |
| SSA | Set Sensor Alarms | DSA | Display Sensor Alarms |
| DSI | Display Sensor Inputs | DCC | Display Contact Inputs |
| SLRY | Set Relays | RRLY | Reset Relays |

| --- Device Management Functions --- |
| UPG | Upgrade ASG Guard Software | BOOT | Reboot Unit |
| DUMP | Dump Config. Details | DUMPF | Dump Config. Details to File |
| CDUMP | Dump Customer Users | CDUMPF | Dump Customer Users to File |

Other Menus: A -Alarm/Event U -User L -Log F -File P -Port/Session

Screen 10-1. System Functions Screen

10.4.1 Set Sensor Alarms – SSA Command

The Set Sensor Alarms is used to set the alarming values used with the sensor inputs to determine what are valid alarm conditions on the sensor. See Section 10.7 for details of the SSA command.

For example: Temperature alarm is set to trip if the temperature falls below 65 degrees or above 85 degrees.

10.4.2 Display Sensor Alarms – DSA Command

Display Sensor Alarms command displays the values defined for the Sensor Alarms.

10.4.3 Display Sensor Inputs – DSI Command

This command is used to display the onboard sensor readings for such things as; battery voltage, wall power, temperature, etc. See Section 10.10 for more details.

No prompts are displayed only the values repeat until a keystroke is pressed to stop the reading.

10.4.4 Display Contact Inputs – DCC Commands

Display Contact Closures command is used to display the open/closed state of up to 5 dry contact closures on ASG Guard and up to 8 dry contact closures on the basic ASG Guard Plus. See Section 10.11 for more details.

No prompts are displayed only the values repeat until a keystroke is pressed to stop the reading.
10.4.5 Set Relays – SRLY Command

The command for setting relays, SRLY, applies to the ASG Guard. The ASG Guard has two solid state relays: one latching (selection 1) relay and one non-latching (selection 2) relay. Latching relays are open by default. Once activated, they close and then remain closed until the RRLY command is issued. If in the CLOSED position, the SRLY command will not change the state. Non-latching relays are also open by default, and after issuing the SRLY command they quickly close and then immediately re-open.

```
ASGGUARD1>srl
--- Set Relays ---
Enter relay number (1-2): 1

02/08/99 16:54:06 2683 [AUX] Relay 1 SET

Screen 10-2. Set Relays Screen
```

10.4.6 Reset Relays – RRLY Command

The command for re-setting relays, RRLY, applies to the ASG Guard. The ASG Guard has two solid state relays: one latching (selection 1) relay and one non-latching (selection 2) relay. Issuing the RRLY command opens latching relays, which are closed. Non-latching relays or latching relays in the open position are not affected by the RRLY command.

```
ASGGUARD1>rrly 1
--- Reset Relays ---

02/08/99 16:54:26 13A1 [AUX] Relay 1 RESET

Screen 10-3. Reset Relays Screen
```
10.5 The Environmental Manager

As mentioned in the previous section, the interface for the ASG Guard Plus Environmental Manager is a 50-pin Amphenol connector located on the back panel. See Figure 10-1 and Table 10-1.

The ASG Guard uses the Euroblock connections for accessing the relay outputs and contact closure inputs, as well as RJ45 connections for the two temperature probes and the 0-5 volt analog input. See Figure 10-3, Table 10-2 and Table 10-3 in Section 10.5.2.

10.5.1 The Environmental Interface of the ASG Guard Plus

The interface for the ASG Guard Plus is shown in Figure 10-1 and Table 10-1 below.

Make the appropriate connections. For example, to monitor temperature you need to connect the temperature probe to the sensor input, +5 V and ground. To do this, connect the temperature sensor to pins 7, 8 and 2 respectively of the Environmental Manager interface on the ASG Guard Plus rear panel.

Enable alarms and define the upper and lower threshold limits. When a monitored input is outside the limits, the ASG Guard Plus issues an alarm. Type SSA to set threshold limits. For more information, see Section 10.5.2.

Decide what action is to be taken when an alarm is received. Update your Action Table to include the alarm and the requested action. Chapter 14 lists internal events and standard Action Routines. For example, by using the SCHEDULE and CANCEL Action Routines, you can SCHEDULE an action to be taken a few minutes after an alarm is received. If the condition returns to normal before the action is taken, the ASG Guard Plus can CANCEL the alarm. The events are recorded in the log history.

Figure 10-1. Environmental Manager Connector of the ASG Guard Plus
### Table 10-1. Pin out of the ASG Guard Plus Environmental Manager

<table>
<thead>
<tr>
<th>PIN NUMBER</th>
<th>Telco Color Code*</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WH/BLUE</td>
<td>Sensor #1</td>
</tr>
<tr>
<td>26</td>
<td>BLUE/WH</td>
<td>Ground</td>
</tr>
<tr>
<td>2</td>
<td>WH/ORN</td>
<td>PLUS 5 V</td>
</tr>
<tr>
<td>27</td>
<td>ORN/WH</td>
<td>GROUND</td>
</tr>
<tr>
<td>3</td>
<td>WH/GRN</td>
<td>SENSOR #2</td>
</tr>
<tr>
<td>28</td>
<td>GRN/WH</td>
<td>GROUND</td>
</tr>
<tr>
<td>4</td>
<td>WH/BRN</td>
<td>PLUS 5 V</td>
</tr>
<tr>
<td>29</td>
<td>BRN/WH</td>
<td>GROUND</td>
</tr>
<tr>
<td>5</td>
<td>WH/SLT</td>
<td>SENSOR #3</td>
</tr>
<tr>
<td>30</td>
<td>SLT/WH</td>
<td>GROUND</td>
</tr>
<tr>
<td>6</td>
<td>RE/BLUE</td>
<td>PLUS 6 V</td>
</tr>
<tr>
<td>31</td>
<td>BLUE/RE</td>
<td>GROUND</td>
</tr>
<tr>
<td>7</td>
<td>RE/ORN</td>
<td>TEMPERATURE SENSOR</td>
</tr>
<tr>
<td>32</td>
<td>ORN/RE</td>
<td>GROUND</td>
</tr>
<tr>
<td>8</td>
<td>RE/GRN</td>
<td>PLUS 5 V</td>
</tr>
<tr>
<td>33</td>
<td>GRN/RE</td>
<td>GROUND</td>
</tr>
<tr>
<td>9</td>
<td>RE/BRN</td>
<td>PBX BATTERY +</td>
</tr>
<tr>
<td>34</td>
<td>BRN/RE</td>
<td>PBX BATTERY -</td>
</tr>
<tr>
<td>10</td>
<td>RE/SLT</td>
<td>PLUS 5V</td>
</tr>
<tr>
<td>35</td>
<td>SLT/RE</td>
<td>GROUND</td>
</tr>
<tr>
<td>11</td>
<td>BLK/BLUE</td>
<td>NOT USED</td>
</tr>
<tr>
<td>36</td>
<td>BLUE/BLK</td>
<td>NOT USED</td>
</tr>
<tr>
<td>12</td>
<td>BLK/ORN</td>
<td>NOT USED</td>
</tr>
<tr>
<td>37</td>
<td>ORN/BLK</td>
<td>NOT USED</td>
</tr>
<tr>
<td>13</td>
<td>RE/GRN</td>
<td>CONTACT CLOSURE #1</td>
</tr>
<tr>
<td>38</td>
<td>GRN/RE</td>
<td>CONTACT CLOSURE #1</td>
</tr>
<tr>
<td>14</td>
<td>RE/BRN</td>
<td>CONTACT CLOSURE #2</td>
</tr>
<tr>
<td>39</td>
<td>BRN/RE</td>
<td>CONTACT CLOSURE #2</td>
</tr>
<tr>
<td>15</td>
<td>RE/SLT</td>
<td>CONTACT CLOSURE #3</td>
</tr>
<tr>
<td>40</td>
<td>SLT/RE</td>
<td>CONTACT CLOSURE #3</td>
</tr>
<tr>
<td>16</td>
<td>YL/BLUE</td>
<td>CONTACT CLOSURE #4</td>
</tr>
</tbody>
</table>
### Environmental Manager

<table>
<thead>
<tr>
<th>PIN NUMBER</th>
<th>Telco Color Code*</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>41</td>
<td>BLUE/YL</td>
<td>CONTACT CLOSURE #4</td>
</tr>
<tr>
<td>17</td>
<td>YL/ORN</td>
<td>CONTACT CLOSURE #5</td>
</tr>
<tr>
<td>42</td>
<td>ORN/YL</td>
<td>CONTACT CLOSURE #5</td>
</tr>
<tr>
<td>18</td>
<td>GRN/YL</td>
<td>CONTACT CLOSURE #6</td>
</tr>
<tr>
<td>43</td>
<td>YL/GRN</td>
<td>CONTACT CLOSURE #6</td>
</tr>
<tr>
<td>19</td>
<td>BRN/YL</td>
<td>CONTACT CLOSURE #7</td>
</tr>
<tr>
<td>44</td>
<td>YL/BRN</td>
<td>CONTACT CLOSURE #7</td>
</tr>
<tr>
<td>20</td>
<td>SLT/YL</td>
<td>CONTACT CLOSURE #8</td>
</tr>
<tr>
<td>45</td>
<td>YL/SLT</td>
<td>CONTACT CLOSURE #8</td>
</tr>
<tr>
<td>21, 22, 23, 24, 25</td>
<td>Not used</td>
<td></td>
</tr>
<tr>
<td>46, 47, 48, 49, 50</td>
<td>Not used</td>
<td></td>
</tr>
</tbody>
</table>

*Key*

**Most Significant Color** | **Least Significant Color**
---|---
WH=White | BL=Blue
RD=Red | OR=Orange
BK=Black | GR=Green
YL=Yellow | BN=Brown
VI=Violet | SL=Slate (i.e. gray)

### 10.5.2 The Environmental Interface of the ASG Guard

The interface to the Environmental Manager of the ASG Guard is an industry standard 5.08 mm "Euroblock" connectors (for relays), or RJ45 connectors (temperature, 0-5V GP) located on the back panel. One 6 pin Euro-block connector is used for the relay outputs; a 10 pin Euroblock connector is used for the contact inputs. Two RJ45 plugs are provided for connecting temperature probes. A third RJ45 plug allows for connection to the 0-5V general purpose input. (All connection points are clearly marked on the back panel.)
**Figure 10-2.** Back panel of the ASG Guard

**Table 10-2.** Pin out of the ASG Guard 10 Pin Euroblock (Contact Closures)

<table>
<thead>
<tr>
<th>PIN NUMBER</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>CONTACT CLOSURE #1</td>
</tr>
<tr>
<td>2</td>
<td>GROUND</td>
</tr>
<tr>
<td>3</td>
<td>CONTACT CLOSURE #2</td>
</tr>
<tr>
<td>4</td>
<td>GROUND</td>
</tr>
<tr>
<td>5</td>
<td>CONTACT CLOSURE #3</td>
</tr>
<tr>
<td>6</td>
<td>GROUND</td>
</tr>
<tr>
<td>7</td>
<td>CONTACT CLOSURE #4</td>
</tr>
<tr>
<td>8</td>
<td>GROUND</td>
</tr>
<tr>
<td>9</td>
<td>CONTACT CLOSURE #5</td>
</tr>
<tr>
<td>10</td>
<td>GROUND</td>
</tr>
</tbody>
</table>

**Table 10-3.** Pin out of the ASG Guard 6 Pin Euroblock (Relay Outputs)

<table>
<thead>
<tr>
<th>PIN NUMBER</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>NC1</td>
</tr>
<tr>
<td>2</td>
<td>COM1</td>
</tr>
<tr>
<td>3</td>
<td>NO1</td>
</tr>
<tr>
<td>4</td>
<td>NC2</td>
</tr>
<tr>
<td>5</td>
<td>COM2</td>
</tr>
<tr>
<td>6</td>
<td>NO2</td>
</tr>
</tbody>
</table>
10.6 Relays on the ASG Guard

For the ASG Guard, the No. 1 relay is latching and No. 2 is non-latching.

10.7 Defining Threshold Limits – SSA Command

In order for the ASG Guard Plus to monitor inputs and issue alarms, you must enable the alarms and set threshold limits. Type SSA and press the ENTER key.

```
Site123>SSA

--- Set Sensor Alarms ---
Restore Factory Defaults ?        No
-- Internal Battery --
  Alarms Enabled                  Yes
-- Temperature --
  Alarms Enabled                  Yes
    .. Normal Range (nn-nn Deg. F) 60-90
-- 48 Volt Input --
  Alarms Enabled                  Yes
    .. Normal Range (nn.n-nn.n V) 45-53
-- General Purpose 0-5 Volt (maximum) Sensor Inputs --
  (S1) Alarms Enabled             No
    .. Normal Range (nn.nn-n.nn V) 1-4
  (S2) Alarms Enabled             No
    .. Normal Range (nn.nn-n.nn V) 1-4
  (S3) Alarms Enabled             No
    .. Normal Range (nn.nn-n.nn V) 1-4

Site123>
```

Screen 10-4. Set Sensor Alarms Screen for ASG Guard Plus

For the ASG Guard, the screen will look similar to:

```
JR #1>SSA

--- Set Sensor Alarms ---
Restore Factory Defaults ?        No
-- Internal Battery --
  Alarms Enabled                  Yes
-- Temperature --
  (T1) Alarms Enabled             Yes
    .. Normal Range (nn-nn Deg. F) 60-90
  (T2) Alarms Enabled             Yes
    .. Normal Range (nn-nn Deg. F) 60-90
-- 48 Volt Input --
  Alarms Enabled                  Yes
    .. Normal Range (nn.n-nn.n V) 45-53
-- General Purpose 0-5 Volt (maximum) Sensor Input --
  (S1) Alarms Enabled             No
    .. Normal Range (nn.nn-n.nn V) 1-4

Site123>
```

Screen 10-5. Set Sensor Alarms Screen for ASG Guard
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore Factory Defaults?</strong></td>
<td>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes.</td>
</tr>
<tr>
<td><strong>--Internal Battery--</strong></td>
<td>Select Yes to restore factory defaults. Select No to keep the current changes.</td>
</tr>
<tr>
<td><strong>Alarms Enabled</strong></td>
<td>Select Yes to enable alarms. Select No to disable them.</td>
</tr>
<tr>
<td><strong>--Temperature--</strong></td>
<td>Select Yes to enable the alarm.</td>
</tr>
<tr>
<td><strong>Alarms Enabled</strong></td>
<td>Enter the upper and lower limits of temperature beyond which an alarm is issued.</td>
</tr>
<tr>
<td><strong>Normal Range (nn-nn Deg. F)</strong></td>
<td>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes.</td>
</tr>
<tr>
<td><strong>--48V Input--</strong></td>
<td>Select Yes to enable the alarm,</td>
</tr>
<tr>
<td><strong>Alarms Enabled</strong></td>
<td>Enter the upper and lower limits of the normal voltage range. An alarm will be issued when the voltage falls outside this range.</td>
</tr>
<tr>
<td><strong>Normal Range (nn.n-nn.n )?</strong></td>
<td>For each general purpose sensor input:</td>
</tr>
<tr>
<td><strong>--General Purpose 0-5 Volt (maximum) Sensor Inputs--</strong></td>
<td>Select Yes to enable the alarm. Select No disable it.</td>
</tr>
<tr>
<td><strong>(S1) Alarm Enabled</strong></td>
<td>Enter the upper and lower limits of voltages. If the voltage does not fall within this range, an alarm is issued.</td>
</tr>
<tr>
<td><strong>Normal Range (nn.n-nn.n V )</strong></td>
<td>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes.</td>
</tr>
<tr>
<td><strong>(S2) Alarm Enabled</strong></td>
<td>Select Yes to enable the alarm. Select No disable it.</td>
</tr>
<tr>
<td><strong>Normal Range (nn.n-nn.n V )</strong></td>
<td>Enter the upper and lower limits of voltages. If the voltage does not fall within this range, an alarm is issued.</td>
</tr>
</tbody>
</table>
10.8 Analog Sensors

Analog sensors are used to monitor temperature, 0-5 volts, and 48-volt PBX battery backup. These sensors are connected to the Environmental Manager Interface on the rear panel of the ASG Guard Plus. (See previous Section for the ASG Guard.)

10.8.1 48-Volt Battery

To monitor the 48-volt PBX battery backup voltage, connect the leads from the PBX battery to the terminals on the Environmental Manager connector located on the rear panel of the ASG Guard/ASG Guard Plus. The ASG Guard/ASG Guard Plus can then monitor the input voltage and initiate an action when the voltage level falls outside the high and low thresholds defined by the user. The voltage range that this input sensor can monitor is from 1 to 100 Volts DC. The ASG Guard is 20-60VDC.

10.8.2 Temperature

The temperature sensor input to the ASG Guard Plus is via an external sensor. The sensor is housed in a standard RJ45 connector to facilitate remote measurement. The sensor may be located up to 200 feet from the ASG Guard Plus. This sensor can be used to monitor room temperature or the ambient temperature of an enclosure.

The far end of the temperature sensor should be secured with tape or Velcro at the location where the temperature is to be measured.

The ASG Guard Plus can then be programmed to initiate an action should the temperature fall outside the range of a high or low threshold defined by the user.

10.8.3 Voltage Inputs

The voltage-based sensors are used to monitor various conditions and issue an alarm if the voltage-based signal exceeds the preset limits. Any sensor that reports its signal in the range of 0-5VDC can be attached to the Environmental Manager.
10.9 Contact Closure Inputs

The contact closures can be used to control external devices. If a contact closure changes state, an alarm is issued. Each ASG Guard Plus includes eight contact closures.

The ASG Guard has 5 contact closure inputs.

10.10 Displaying Analog Sensor Inputs – DSI Command

Type DSI and press the ENTER key to display the sensor inputs of sensors that are connected. The ASG Guard Plus updates the display to show the condition of each sensor every 1-2 seconds. In addition to the sensor reading, OK, HI, LO markings show the present recording in relationship to the alarm range.

Screen 10-6. Display Sensor Inputs Screen

Note that both the ASG Guard Plus and ASG Guard display similar information when the DSI command is issued.

Screen 10-7. Display Sensor Inputs Screen
10.11 Displaying the Status of Contact Inputs

The state of each contact closure can be displayed. For the ASG Guard Plus base unit, type **DCC** and press the ENTER key to display the state of each contact closure. Note that the states of eight closures are displayed at a time. The ASG Guard Plus updates the display of the status of each closure every 0.5 seconds.

**Screen 10-8.** Display Contact Inputs Screen for ASG Guard Plus

For the **ASG Guard**, the display has only 5 contact closures.

**Screen 10-9.** Display Contact Inputs Screen for ASG Guard
11. User Connectivity

11.1 What This Chapter Contains

- How to initiate a dial-up session
- How to authenticate using Password/Callback, ASG Key, and Pager
- How to access the ASG Guard/ASG Guard Plus or a host system using auto-baud and auto-parity
- How to join in and view host sessions in progress
- How to determine port control parameters and status

11.2 Overview

The primary means of remotely accessing the ASG Guard/ASG Guard Plus is through a modem connection. The ASG Guard and ASG Guard Plus have two internal modem ports (Modems 1 and 2) which can be used for the dial-up operation. In addition, an ASG Guard Plus with one or two host expansion boards can be configured with four additional external modems attached to the last four host ports (Refer to Chapter 5 for more details).

In order to authenticate into the ASG Guard/ASG Guard Plus via a modem connection, the authorized user must exist or the ASG Guard/ASG Guard Plus will not allow the user access. The user can be setup with a password to immediately gain access. The callback option provides an even higher level of security. It is used when the ASG Guard/ASG Guard Plus is to be accessed from either a pre-defined telephone number (regular callback) or from whichever telephone number the user is dialing in from (variable callback). There is also an encrypted code that can be assigned to the user, which requires the use of an ASG Key.

Once access is gained, the user can establish or join an existing session on one of the ASG Guard/ASG Guard Plus ports, or the user can view a session dialog for an existing session on one of the ASG Guard/ASG Guard Plus ports. Up to three users can be linked into the same session in this manner.

11.3 Dial-up Preparations

Verify that the ASG Guard/ASG Guard Plus communications ports are configured and the user is added according to the instructions provided in Chapters 3, 4, and 5.

If the modem Baud Rate and Char. Length/Parity parameters of the ASG Guard/ASG Guard Plus are set to auto, the ASG Guard/ASG Guard Plus modem will match whatever speed and parity at which you connect. You must follow the procedure outlined below in order for the ASG Guard/ASG Guard Plus to determine the speed and parity.

Auto-Baud

When the internal modem Baud Rate parameter is set to Auto, you must press the ENTER key several times after the modems connect and before you continue the dial in session. This enables the ASG Guard/ASG Guard Plus internal modem to determine the speed at which your modem is operating. Once the ASG Guard/ASG Guard Plus internal modem learns your modem’s speed, it will begin to place the character “p” on the screen.
Auto-Parity
For the ASG Guard/ASG Guard Plus internal modem to determine the parity of your modem, enter characters that have opposite parity. (Half the characters on your keyboard are even and half are odd parity). Entering P and O first is recommended. If these do not result in the terminal displaying the ASG Guard/ASG Guard Plus "greeting" message, continue entering different characters. Once it establishes the speed and parity of your modem, the modem will display the initial greeting message. The default messages '--- ASG Guard - User Authentication ---' and 'Please Enter User ID ->' will appear on the screen. You can then authenticate into the ASG Guard/ASG Guard Plus and continue with the dial-up session.

11.4 Initiate a Dial-up Session
Before a dial-up user can access the ASG Guard/ASG Guard Plus (and the connected resource), the user must authenticate. Authentication is the verification of the identity of the dial-in user. Each user in the ASG Guard/ASG Guard Plus User Database can be assigned a primary and secondary authentication method. Authentication methods available include password/callback, ASG Key, and Pager. ASG Key requires a handheld token (that is, the ASG Key). The method of authentication is set when the user is added to the ASG Guard/ASG Guard Plus user database.

11.4.1 Password/Callback
The Password/Callback authentication method allows for three different types of user authentication.

- Passthru
- Regular Callback
- Variable Callback

To dial in to the ASG Guard/ASG Guard Plus using the Password/Callback Passthru authentication method:

1. From your terminal, or terminal emulator, initialize your modem, and type in the ASG Guard/ASG Guard Plus telephone number, and then press the ENTER key.

   The ASG Guard/ASG Guard Plus responds by requesting that you enter your User ID. From your User ID, the ASG Guard/ASG Guard Plus will determine that you are using the Passthru method of access.

   --- ASG Guard - User Authentication ---
   Please Enter User ID -> CHUCK

   --- Password/Callback Authentication ---
   Enter Password ->******

   --- Authentication Complete ---


Screen 11-1. User Authentication Screen

2. At the ASG Guard/ASG Guard Plus system prompt, type your User ID and then press the ENTER key. The ASG Guard/ASG Guard Plus then requests that you enter your password.
3. Type your password at the system prompt and then press the ENTER key. The password is case sensitive.

**NOTE:**
*As you type your password, the ASG Guard Plus displays asterisks (*) for security purposes.*

If the password is correct, you will either be connected to the ASG Guard/ASG Guard Plus or to a host port, depending on your Access Class:

- If you are connected to the ASG Guard/ASG Guard Plus (Sysop Session), you can perform all of the operations permitted by your Access Class.
- If you are connected to the host port (Host Session), you will have a direct connection to the host device. You may be required to perform all of the normal host login procedures.

If you entered your password incorrectly, the ASG Guard/ASG Guard Plus allows you to re-enter the correct password. Retype your password at the system prompt and then press the ENTER key.

You are permitted three attempts at entering your User ID and three attempts at entering your password. If the third response is incorrect, the connection is dropped. If you know that you should have access, and that you have entered your password correctly, contact your System Administrator for assistance.

**NOTE:**
The Passthru user authentication method should be used only during the evaluation period to allow ease of use in a non-secure environment. We discourage this use in a "live" environment. Passthru requires only that the user enter the correct ID and password to access the host or PBX through the ASG Guard/ASG Guard Plus.

### 11.4.2 Regular Callback

To dial in to the ASG Guard/ASG Guard Plus using the Password/Callback - Regular Callback authentication method:

1. From your terminal, or terminal emulator, initialize your modem, and type in the ASG Guard/ASG Guard Plus telephone number, and then press the ENTER key.

   The ASG Guard/ASG Guard Plus responds by requesting that you enter your User ID. From your User ID, the ASG Guard/ASG Guard Plus will determine that you are using the Regular Callback method of access.

2. At the ASG Guard/ASG Guard Plus system prompt, type your User ID and then press the ENTER key. The ASG Guard/ASG Guard Plus then requests that you enter your password.

3. Type your password at the system prompt and then press the ENTER key. The ASG Guard/ASG Guard Plus then disconnects.

   **NOTE:**
   *As you type your password, the ASG Guard/ASG Guard Plus displays asterisks (*) for security purposes.*

   The ASG Guard/ASG Guard Plus will now call you back at the number in its database. Make certain that your modem is in auto-answer mode or that you are prepared to answer the call via modem commands.
4. After handshaking has been completed, the ASG Guard/ASG Guard Plus will again request your password. Enter your password at the system prompt. If your password is correct, you will either be connected to the ASG Guard/ASG Guard Plus or to the host port, depending on your Access Class:

- If you are connected to the ASG Guard/ASG Guard Plus (Sysop session), you can perform all of the operations to which your Access Class entitles you.
- If you are connected to the host port (Host Session), you will have a direct connection to the host device. If required, you will have to perform all of the normal host login procedures.

If you entered your password incorrectly, the ASG Guard/ASG Guard Plus will give you a second chance to enter the correct password. Retype your password at the system prompt and then press the ENTER key.

You are permitted three attempts at entering your User ID and three attempts at entering your password. If the third response is incorrect, the connection is dropped. If you know you should have access, and that you entered your password correctly, contact your System Administrator for assistance.

--- ASG Guard - User Authentication ---
Please Enter User ID -->BILL

--- Password/Callback Authentication ---
Enter Password -->******

--- Please Awaits Callback ---

NO CARRIER
RING
CARRIER: 1200
PROTOCOL: ALT
COMPRESSION: CLASS 5
CONNECT 9600

--- ASG Guard - Returning Call ---
Enter Password -->******

--- Authentication Complete ---


Screen 11-2. Password/Callback Authentication Screen
11.4.3 Using Variable Callback

When you use the Variable Callback authentication method, the ASG Guard/ASG Guard Plus will call you back at whatever number you enter. This authentication method is not as secure as Fixed Callback. To dial in to the ASG Guard/ASG Guard Plus using the Password/Callback Variable Callback authentication method:

1. From your terminal, or terminal emulator, type the proper modem commands followed by the ASG Guard/ASG Guard Plus telephone number, and then press the ENTER key.

   The ASG Guard/ASG Guard Plus responds by requesting that you enter your User ID. From your User ID, the ASG Guard/ASG Guard Plus will determine that you are using the Variable Callback method of access.

2. At the ASG Guard/ASG Guard Plus system prompt, type your User ID and then press the ENTER key. Type your password at the system prompt and then press the ENTER key.

   **NOTE:**
   
   As you type your password, the ASG Guard/ASG Guard Plus displays asterisks (*) for security purposes.

3. The ASG Guard/ASG Guard Plus will then ask for the number at which to call you back. At the system prompt, type the number the ASG Guard/ASG Guard Plus is to use to call you back, and then press the ENTER key. The ASG Guard/ASG Guard Plus then disconnects.

   The ASG Guard/ASG Guard Plus will now call you back at the number you gave it. Make certain that your modem is in auto-answer mode or that you are prepared to answer the call using modem commands.

4. After handshaking has been completed, the ASG Guard/ASG Guard Plus will again request your password. Enter your password at the system prompt. If your password is correct, you will either be connected to the ASG Guard/ASG Guard Plus or to the host, depending on your Access Class:

   - If you are connected to the ASG Guard/ASG Guard Plus (Sysop session), you can perform all of the operations to which your Access Class entitles you.
   - If you are connected to the host port (Host Session), you will have to perform all of the normal host login procedures.

   If you entered your password incorrectly, the ASG Guard/ASG Guard Plus will give you a second chance to enter the correct password. Retype your password and then press the ENTER key.

   You are permitted three attempts at entering your User ID and three attempts at entering your password. If the third response is incorrect, the connection is dropped. If you know you should have access, and that you entered your password correctly, contact your System Administrator for assistance.
--- ASG Guard - User Authentication ---
Please Enter User ID ->JOHN

--- Password/Callback Authentication ---
Enter Password ->******
Phone Number to be Called Back at ->2015551212

--- Please Await Callback ---

NO CARRIER
RING
CARRIER 2400
PROTOCOL: ALT
COMPRESSION: CLASS 5
CONNECT 9600

--- ASG Guard - Returning Call ---
Enter Password ->******

--- Authentication Complete ---

>

Screen 11-3. Password/Callback Authentication Screen

11.4.4 Using ASG Key

To dial into the ASG Guard/ASG Guard Plus using the ASG Key authentication method, follow the procedure outlined below.

**NOTE:**
If your ASG Key has not been initialized, see Appendix A for initialization instructions.

1. From your terminal, or terminal emulator, type the proper modem commands followed by the ASG Guard/ASG Guard Plus telephone number, and then press the ENTER key.

   The ASG Guard/ASG Guard Plus responds by requesting that you enter your User ID. From your User ID, the ASG Guard/ASG Guard Plus will determine that you are using the ASG Key method of access.

2. At the ASG Guard/ASG Guard Plus system prompt, type your User ID and then press the ENTER key. The ASG Guard/ASG Guard Plus then presents you with the seven-digit challenge.
--- ASG Guard - User Authentication ---
Please Enter User ID --> TOM

--- ASG Key Authentication ---
Challenge = 853-2446
Response -->

Screen 11-4. ASG Key Authentication Screen

3. Turn on your ASG Key by pressing the ON/C button. A zero (0) appears in the display window.
4. Press the red button on your ASG Key. ENTER PIN is displayed in the window.
5. Enter your PIN into the ASG Key and then press the equal (=) button.
6. Enter the seven-digit challenge number displayed on your terminal into the ASG Key and then press the equal button.

**NOTE:**
*Do not include the hyphen (-) in the challenge.*

The ASG Key will then display a response number in the window.

7. Enter the response displayed in the ASG Key window into your terminal and press the ENTER key. If the response is correct, the ASG Guard/ASG Guard Plus will signify that the authentication has been successfully completed and you will either be connected to the ASG Guard/ASG Guard Plus or to the host, depending on your Access Class:
   - If you are connected to the ASG Guard/ASG Guard Plus (Sysop session), you can perform all of the operations to which your Access Class entitles you.
   - If you are connected to the host port (Host Session), you will have to perform all of the normal host login procedures.

--- ASG Guard - User Authentication ---
Please Enter User ID --> TOM

--- ASG Key Authentication ---
Challenge = 853-2446
Response --> 1829782

--- Authentication Complete ---

09/21/93 10:19:17 [M] User: TOM - Connected to Sysop
>

Screen 11-5. ASG Key Authentication Screen

If you entered the response incorrectly, the ASG Guard/ASG Guard Plus sends a second challenge, giving you another opportunity to enter the correct response. Enter your PIN again, and then the second challenge in to the ASG Key and press the equal button.
Enter the response displayed in the ASG Key window into your terminal and press the ENTER key.

You are permitted three attempts at entering your User ID and three attempts at entering your response. If the third response is incorrect, the connection is dropped. If you know that you should have access, and that you entered the response correctly, check that the ASG Key initialization was done correctly (see Section 4.1.3). For more assistance, contact your System Administrator.

11.4.5 Using Pager Authentication Method

To dial in to the ASG Guard/ASG Guard Plus using the Pager authentication method:

1. From your computer, type the proper modem commands followed by the ASG Guard/ASG Guard Plus telephone number, and then press the ENTER key.

   The ASG Guard/ASG Guard Plus responds by requesting that you enter your User ID. From your User ID, the ASG Guard/ASG Guard Plus will determine that you are using the Pager method of access.

2. At the ASG Guard/ASG Guard Plus system prompt, type your user ID and then press the ENTER key.

   With a dual modem setup, the ASG Guard/ASG Guard Plus will dial out to the pager service on the second modem. It will deliver a unique 7-digit "password" to your pager preceded by 999 to distinguish it from a phone number. For example, 999 1234567.

3. At the ASG Guard/ASG Guard Plus prompt, enter the number displayed on the pager. If the number matches the number sent (with or without the '999'), the authentication process is complete.

   For a single modem system, the ASG Guard/ASG Guard Plus will disconnect and then call the pager service to deliver the numeric password. You then dial back into the ASG Guard/ASG Guard Plus and enter the password at the prompt. If the proper value is entered, the authentication process is complete.

--- ASG Guard - User Authentication ---
Please Enter User ID ->TOM

--- Pager Authentication ---
Sending Password, please enable pager.
Call ASG Guard with password.

Screen 11-6. Pager Authentication Screen
11.5 Session Control Functions and Commands
The ASG Guard/ASG Guard Plus allows a user to participate in or view a host session from a terminal connected to the ASG Guard/ASG Guard Plus. These commands are particularly useful when troubleshooting configuration problems. At the prompt, type P to display the port and session control options, then press the ENTER key.

```
Site123>p
-- -- - Port and Session Control Functions (CMaster) -- -- -

--- Session Control Functions ---
VS View Host Session       JS Join Host Session
CON Connect to Host        DIS Disconnect
VT VT100 On/Off

--- Port Control Functions ----
PST Port Status             DPS Display Port Signals
RES Reset Port             DNS Display Network Status
SNP Set Network Params      DNP Display Network Params
PING Query Remote Node      PPP Start PPP Session
STARTNET Startup Network
DA/DM/DH/DT - Display AUX/Modem/Host/Telnet Port Params
SA/SM/SH/ST - Set AUX/Modem/Host/Telnet Port Params

Other Menus: S -System  A -Alarm/Event  U -User  L -Log  F -File

Screen 11-7. Port and Session Control Functions (CMaster) Screen

11.5.1 Join Lucent Host – JSL Command
The JSL command allows a sysop or CMaster level user to interactively join in a host session with a Lucent host device. This access can be either from a remote terminal through a PPP link, an Ethernet connection, a modem port, or from a local terminal connected to an AUX port. Up to three users can communicate simultaneously through a join Lucent session to a specific host.

After you type JSL, you will be prompted for the number of the host port. At the prompt, enter the host port number. You may also enter the host port number as part of the command. For example, to join session with host port 2, type

```
> JSL 2
```

To end the session, press CTRL+E (press E while holding down the control key).

11.5.2 Join Host Session – JS Command
The JS command allows a sysop or CMaster level user to interactively join in a host session. This access can be either from a remote terminal through a PPP link or Ethernet connection, a modem port or from a local terminal connected to an AUX port. Up to three users can communicate simultaneously through a join session to a specific host.

After you type JS, you will be prompted for the number of the host port. At the prompt, enter the host port number. You may also enter the host port number as part of the command. For example, to join session with host port 2, type

```
> JS 2
```

To end the session, press CTRL+E (press E while holding down the CONTROL key).
11.5.3 View Session – VS Command
The VS command enables a sysop or CMaster level user to view, but not join in, a host session in progress. After you type `VS`, you will be prompted for the number of the host port. At the prompt, enter the host port number. You may also enter the host port number as part of the command. For example, to view a session with host port 3, type

```
>VS 3
```

Press any key to end the session.

11.5.4 Connect to Lucent Host – CONL Command
The Lucent Connect to Host command (CONL) allows a sysop or CMaster level user to access a Lucent host device connected to an ASG Guard/ASG Guard Plus Host Port. The access can be either from a remote terminal via a modem port, from a remote terminal through a PPP link or Ethernet connection, or from a local terminal connected to the AUX Port.

Type `CONL` at the system prompt and press the ENTER key to display the Connect to Host screen. You may also enter the host port number as part of the command. For example, to connect to host port 3, type

```
>CONL 1 or >CONL H1
```

The ASG Guard/ASG Guard Plus will default to the host port if no alphabet indicator is used.

You can end the session by typing CTRL+E if your login port parameters have "Host Session Disconnect on CTRL+E" set to Yes. Otherwise, you must break your connection to the ASG Guard/ASG Guard Plus by either hanging up your modem or disconnecting your terminal from the AUX Port.

11.5.5 Connect to Host – CON Command
The Connect to Host command (CON) allows a sysop or CMaster level user to access a host connected to an ASG Guard/ASG Guard Plus Host Port or a modem port (internal or external). The access can be either from a remote terminal via a modem port, from a remote terminal through a PPP link or Ethernet connection, or from a local terminal connected to the AUX Port.

Type `CON` at the system prompt and press the ENTER key to display the Connect to Host screen. You may also enter the host port number as part of the command. For example, to connect to host port 3, type

```
>CON 3 or >CON H3
```

The ASG Guard/ASG Guard Plus will default to the host port if no alphabet indicator is used.

You can end the session by typing Ctrl+A if your login port parameters have "Host Session Disconnect on Ctrl+A" set to Yes. Otherwise, you must break your connection to the ASG Guard/ASG Guard Plus by either hanging up your modem or disconnecting your terminal from the AUX Port.

11.5.6 Disconnect – DIS Command
The Disconnect command disconnects an active call on the modem port if the command is issued from a terminal connected to the ASG Guard/ASG Guard Plus via a modem port. If the command is issued from a terminal connected to the AUX port, the session on the AUX port is terminated.

Type `DIS` at the system prompt and press the ENTER key. If you decide not to terminate the communications session, press the SPACE BAR to toggle the field to No and then press the ENTER key. If you are sure that you want to end this communications session, press the ENTER key when Yes appears in this field.
11.5.7 Terminal Mode – VT Command
The VT100 command is used to turn on and off VT100 terminal mode.
While VT100 is on, all editing commands are displayed on the screen, with all associated prompts. The user may move the cursor to the line to be edited and perform operations there. With VT100 off, the commands are presented in a single prompt format (that is, TTY mode).
Type VT at the system prompt and press the ENTER key. The display of the current status will appear. Type VT off at the system prompt to turn off VT mode, or type VT on at the system prompt to turn on VT mode.

11.6 Port Control Commands
This section provides the commands for checking the status and resetting ports.

11.6.1 Port Status – PST Command
The PST command displays the Port ID and Admin. Port Status.
Type PST at the system prompt and press the ENTER key. The status of each network device is listed individually.

<table>
<thead>
<tr>
<th>Port ID</th>
<th>Admin. Port Status</th>
<th>User Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUX</td>
<td>Sysop</td>
<td>AUX_Default</td>
</tr>
<tr>
<td>Modem 1</td>
<td>Idle</td>
<td></td>
</tr>
<tr>
<td>Modem 2</td>
<td>Not Available</td>
<td></td>
</tr>
<tr>
<td>Telnet 1</td>
<td>Host1</td>
<td>MARK</td>
</tr>
<tr>
<td>Telnet 2</td>
<td>Available</td>
<td></td>
</tr>
<tr>
<td>Telnet 3</td>
<td>Available</td>
<td></td>
</tr>
</tbody>
</table>

Screen 11-8. Administration Port Status Screen

The Port Status screen displays the status of every access point (modem, telnet/network, and Aux. Port) into the ASG Guard/ASG Guard Plus.
If a port is in use, the status will indicate the access class (Host or Sysop) and user ID. If access is via the Aux. Port using the default user, no user ID is provided. An Idle status indicates that the port is available but currently not in use.
11.6.2 Display Port Signals – DPS Command

The DPS command displays the current status of the control signal for each of the ports.

Type **DPS** at the system prompt and press the ENTER key. If the command is executed with ’VT ON’, the command will loop until a key is pressed. A state of ’1’ equals a high, a state of ’0’ equals a low.

```
Site123>DPS
--- Display Port Signals ---
-- Port Signals --

<table>
<thead>
<tr>
<th>Port ID</th>
<th>DTR</th>
<th>RTS</th>
<th>CTS</th>
<th>DCD</th>
<th>DSR</th>
<th>RI</th>
</tr>
</thead>
<tbody>
<tr>
<td>AUX</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Modem 1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Modem 2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Host 1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Host 2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Host 3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Host 4</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**Screen 11-9.** Display Port Signals Screen

11.6.3 Reset Port – RES Command

The RES command is used to reset any of the ports, real (AUX, modem, host) or virtual (Telnet) and the Host Action Routine. There are special custom routines that interrogate a host device. By default, the ASG Guard/ASG Guard Plus has no “Host Action Routines.”

Type **RES** at the system prompt and press the ENTER key. A list of formats will scroll on screen and the system prompt will return.

```
Site123>RES
--- Reset Port ---
*** Format is RES A for Aux Port, RES Mn for Modem, RES Hn for Host Port, RES HA for Host Action Routine, RES Tn for Telnet Session.
```

**Screen 11-10.** Reset Port Screen

The user is required to explicitly indicate what port to reset. With the Host Expansion Board, there are 12 (1 Board) or 24 (2 Boards) additional ports and several options are available. For example, to reset host port 7, type

```
>RES H7
```
The screen will look similar to:

```
Site123>RES H7
--- Reset Port ---
01/04/96 05:40:27 1223 [AIX] Reset Port: H7 - O.K.
01/04/96 05:40:29 78D0 [H] Host 7 Idle
Site123>
```

**Screen 11-11.** Reset Port Screen
Page intentionally left blank.
12. Network Functions

12.1 What This Chapter Contains

- Overview of network capabilities
- Setting network parameters
- SNMP overview
- Establishing a PPP link
- Initiating a Telnet session
- Setting up FTP
- Determining network status

12.2 Overview of Supported Network Functions

The ASG Guard/ASG Guard Plus may be connected to your TCP/IP network through either an Ethernet connection or a Point-to-Point Protocol (PPP) link.

An Ethernet connection physically connects the ASG Guard/ASG Guard Plus to a network. PPP allows a network connection to a remote device via a modem connection. After a PPP link has been established, you can perform network functions, such as Telnet or FTP, to the ASG Guard/ASG Guard Plus or to specific devices on the network. To establish a PPP link or to initiate a Telnet session, you must have the appropriate commercial software package installed and setup on the remote PC. Connection to a TCP/IP network provides for the following services:

- Ping
- Telnet communication
  - Network access to the ASG Guard/ASG Guard Plus for unit administration
  - Network access to the devices connected to the host ports
  - Network access to other devices on the network, using the ASG Guard/ASG Guard Plus as a security server
- SNMP trap delivery
  - Delivery of SNMP traps for errors detected in the ASG Guard/ASG Guard Plus
  - Delivery of SNMP traps for alarms conditions detected in the devices connected to the host ports
- FTP file delivery (client support)
  - Delivery of buffer files from the ASG Guard/ASG Guard Plus to a network file server

In order to use these features, you must correctly set the network parameters of the ASG Guard/ASG Guard Plus.
NOTE: For specific information on how to establish a PPP link using your TCP/IP communications package, refer to its manual.

12.3 Overview of Telnet Support by ASG Guard/ASG Guard Plus

The ASG Guard supports the Telnet protocol. The following Telnet communication is provided:

1. Telnet access to the ASG Guard/ASG Guard Plus for administration of the unit.
2. Telnet access to the ASG Guard/ASG Guard Plus for connection to the host ports.
3. Telnet access to the other network devices, using the ASG Guard/ASG Guard Plus as a security server.

There are three Telnet sessions available on the ASG Guard that allow the user access to a Sysop session. The ASG Guard Plus with one or two Expansion Boards has the three Sysop level Telnet sessions available, but also has an additional 12 Telnet sessions available at the Host access level.

12.4 Overview of SNMP Support by ASG Guard/ASG Guard Plus

SNMP (Simple Network Management Protocol) is a TCP/IP protocol for network management. It allows compliant devices to be configured and/or to send error messages to Network Management software packages such as HP Openview, Cabletron Spectrum, Castle Rock SNMPc, etc.

The ASG Guard/ASG Guard Plus can send SNMP traps based on alarm conditions detected in host devices or in the ASG Guard/ASG Guard Plus itself. Any alarm condition that can be listed in the Action Table can be sent to a management system via an SNMP Trap. Thus, the ASG Guard/ASG Guard Plus acts as an SNMP trap proxy agent for devices that deliver alarms via asynchronous RS-232 communication, via contact closures, or other non-network mechanisms.

The ASG Guard/ASG Guard Plus will respond to any of a multitude of "alarms" (such as an error condition on a PBX) by performing an appropriate user-defined action. A typical action might be connecting to a remote computer over a modem link and sending error information from the PBX to that computer. SNMP, the Simple Network Management Protocol, provides a standard way for the ASG Guard/ASG Guard Plus to report alarms to one or more computers that are connected via network. You can configure the ASG Guard/ASG Guard Plus to send a message, or "SNMP trap," to one or more supervisor computers, which are called SNMP managers, in response to alarm conditions. These parameters are set using the SNMP command to set the Group 2 network parameters (that is, SNMP Manager Parameters).

12.4.1 MIBs

SNMP uses a data structure known as Management Information Base, or MIB, to store information. Each piece of information, or object, in the MIB has a unique Object Identifier. Object identifiers are indices based on a tree structure. The information is held in a "node" at the end of a "branch" in the tree. The Object Identifier shows the path by listing each branch needed to reach the node.

The identifier serves to name or reference the object. MIBs for specific companies are allocated to the MIB branch known as enterprise. Thus, each company branches from the general branch known as enterprise. From that point on in the MIB, the company developing the MIB controls the information and Object Identifier used to reference the data. This information is required to coordinate the sending and receiving of data between an SNMP-compliant device and an SNMP-based network management system.
When both the SNMP Agent and SNMP Management system have the same MIB structure, data can be easily transferred and used. SNMP data packets, each containing an object identifier and information associated with that object, are passed between the device and management system to populate the appropriate fields in the receiver’s MIB. Both the Agent and Management System can then reference the object and process the data as needed.

12.4.2 ASG Guard/ASG Guard Plus MIB

The ASG Guard/ASG Guard Plus has a general MIB as well as proprietary MIBs for companies that use the ASG Guard/ASG Guard Plus as an SNMP trap proxy. (For more information regarding proprietary MIBs contact Lucent Technologies.) The ASG Guard/ASG Guard Plus MIB is under enterprise number 1476 branch ASG Guard/ASG Guard Plus (1), branch mfTrap (1).

Table 12-1 shows the basic set-up of a MIB and shows information about:

- Object Identifiers- The index used to identify the information in the MIB.
- Object Data- The information contained in the referenced data node.
- Object Source- The field in the ASG Guard/ASG Guard Plus where the information is located.

Table 12-1. Basic Setup of a MIB

<table>
<thead>
<tr>
<th>Object Identifier</th>
<th>Object Data</th>
<th>Object Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.3.6.4.1.1476.1.1.1</td>
<td>trapId</td>
<td>Alarm Severity. Placed in the Action Table Parameter Field. The value can be from 1 to 10.</td>
</tr>
<tr>
<td>1.3.6.4.1.1476.1.1.2</td>
<td>trapSiteDesc</td>
<td>Site name in System Parameter.</td>
</tr>
<tr>
<td>1.3.6.4.1.1476.1.1.3</td>
<td>trapSource</td>
<td>SNMP Agent.</td>
</tr>
<tr>
<td>1.3.6.4.1.1476.1.1.4</td>
<td>trapDesc</td>
<td>Alarm or error code. This is the alarm as delivered by the host device or ASG Guard/ASG Guard Plus system. It includes all parameters.</td>
</tr>
<tr>
<td>1.3.6.4.1.1476.1.1.5</td>
<td>trapComment</td>
<td>Comment Field in Action Table. The date and time of alarm are also included in this field.</td>
</tr>
<tr>
<td>1.3.6.4.1.1476.1.1.6</td>
<td>trapExtraInfo</td>
<td>Extra information associated with this message. Assigned by custom Action Routine.</td>
</tr>
<tr>
<td>1.3.6.4.1.1476.1.1.7</td>
<td>trapExpertData</td>
<td>May contain up to 161 characters, and provides additional data to the technician that helps in the isolation or correction of the problem.</td>
</tr>
</tbody>
</table>

With the information in Table 12-1, the SNMP Management System can be configured to receive and use SNMP traps sent by the ASG Guard/ASG Guard Plus.

NOTE:

Configuration of the SNMP Management System may require the assistance of your LAN Administrator. Please contact him/her to determine how to compile the appropriate MIB for your particular system.
12.4.3 Delivery of SNMP Traps

The ASG Guard/ASG Guard Plus can send SNMP traps via two mechanisms. If the network manager is on the same LAN or WAN as the ASG Guard/ASG Guard Plus, the trap can be sent with the SNMPTRAP Action Routine. This uses the Ethernet connection.

If the Network Manager is not on the same LAN or WAN, the ASG Guard/ASG Guard Plus can establish a PPP link via modem and then deliver the SNMP Trap.

12.4.3.1 SNMP Traps Via Ethernet (Network)

Set all required network information using the SNP command. In the Action Table, place an entry similar to the following:

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Action Routine</th>
<th>Parameter</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR123</td>
<td>SNMPTRAP</td>
<td>1</td>
<td>This is a major alarm</td>
</tr>
</tbody>
</table>

When the ERR123 alarm is detected, an SNMP trap is sent to the management system(s) identified in the network parameters. All information in the fields listed in Table 12-1 is sent automatically. The parameter for the SNMPTRAP routines sets the trap level (1-10). This parameter is the enterprise specific trap ID and depends on the trap format.

12.4.3.2 SNMP Traps Via PPP

To denote that an SNMP trap is to be delivered via a PPP link, set the appropriate field in the SNP command. When an SNMP trap is to be delivered via a dial up PPP link, the ASG Guard/ASG Guard Plus generates a .PPPREQ event. In the Action Table, include entries similar to the following:

<table>
<thead>
<tr>
<th>Alarm</th>
<th>Action Routine</th>
<th>Parameter</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR001</td>
<td>SNMPTRAP</td>
<td>2</td>
<td>This is a minor alarm</td>
</tr>
<tr>
<td>.PPPREQ</td>
<td>PHPPP</td>
<td>5551212</td>
<td>Create the PPP link</td>
</tr>
</tbody>
</table>

The telephone number can be specified directly, or any of the default telephone numbers specified in the system parameters can be referenced. PHPPP assumes that there is no firewall or security on the remote access device.

12.5 Overview of FTP Support by ASG Guard/ASG Guard Plus

The ASG Guard/ASG Guard Plus supports FTP Client Send and Receive commands.

Files can be sent from the ASG Guard/ASG Guard Plus to an FTP server using the FTP protocol. You may use the SEBUF or SEND commands described in Chapter 7 to accomplish this file transfer. Files can be sent from the FTP server to an ASG Guard/ASG Guard Plus using the FTP protocol. You may use the RCV command described in Chapter 7 to accomplish this file transfer.
12.6 Overview of PPP Support by ASG Guard/ASG Guard Plus

PPP is Point-to-Point Protocol, which provides a dial-up connection the ability to emulate a TCP/IP network connection. Using this protocol, a dial-up session can be used to send SNMP alarms or Telnet to a Host Port on the ASG Guard/ASG Guard Plus.

The PPP link can be initiated in the ASG Guard/ASG Guard Plus in one of two ways. The user can either designate a specific port as a dedicated PPP port, or the user may initiate a PPP connection on demand. See [Section 12.11](#) for details on setting up PPP connections.

12.7 Network Parameters

If the ASG Guard/ASG Guard Plus is part of a network, it is necessary to set the Network Initialization Parameters prior to starting the network module of the ASG Guard/ASG Guard Plus. Changes made to the Network Initialization Parameters will only take effect if the network has not yet been started, or by restarting the ASG Guard/ASG Guard Plus. You can restart the ASG Guard/ASG Guard Plus by issuing the BOOT command from the command prompt to perform a 'soft' boot.

Before connecting the ASG Guard/ASG Guard Plus to your network, contact your network administrator and obtain the following information:

- IP address to be assigned to the ASG Guard/ASG Guard Plus
- IP address to be used for PPP connections
- Subnet mask for the network segment to which the ASG Guard/ASG Guard Plus will be connected
- IP address of the default gateway to be used by the ASG Guard/ASG Guard Plus

The ASG Guard/ASG Guard Plus allows a user to establish a PPP connection to one of its modems. This connection allows a Telnet session to either the ASG Guard/ASG Guard Plus or another device on the network attached to the ASG Guard/ASG Guard Plus. In the latter case the ASG Guard/ASG Guard Plus acts as a dial up security server.

When a remote user attempts to access other network devices via a PPP session, those devices must know how to direct their responses back to the user. The simplest way to accomplish this is with a router that supports RIP, the standard Router Information Protocol. The strategy is to make the devices on the network direct their responses to the router, and then have the router forward the data to the ASG Guard/ASG Guard Plus. To do this, ensure that a RIP-enabled router is on the network, and then configure the other devices to use it as their default gateway. Then, when a PPP link is established with the ASG Guard/ASG Guard Plus, the ASG Guard/ASG Guard Plus will automatically use RIP to tell the router how to forward data addressed to the remote user.

**NOTE:**

The network number (the first set of numbers) for the PPP connection in the ASG Guard/ASG Guard Plus should be different than the network number used for the network IP address. Thus, if the network address of the ASG Guard/ASG Guard Plus is 193.1.1.1 then the PPP address of the network should be something like 192.1.1.1.
12.7.1 Set Network Parameters – SNP Command

To set network parameters, type **SNP** at the system prompt and press the ENTER key. The SNP command is used to set three groups of network parameters:

- Group 1 – Network Initialization Parameters
- Group 2 – SNMP Manager Parameters
- Group 3 – FTP Parameters

For a detailed explanation of Group 1 Network Initialization Params, refer to Section 12.7.1.1.

For a detailed explanation of Group 2 SNMP Manager Params, refer to Section 12.7.1.2.

For a detailed explanation of Group 3 FTP Params, refer to Section 12.7.1.3.

12.7.1.1 Network Initialization Parameters

The Network Initialization Parameters are set using the SNP 1 command:

```
Site123>SNP 1
--- Set Network Params ---
Restore Factory Defaults?         No
- Network Initialization Parameters -
Start Network on Power-up?        No
IP Address (nnn.nnn.nnn.nnn)       192.9.200.2
PPP Address (nnn.nnn.nnn.nnn)      192.9.200.3
Subnet Mask (nnn.nnn.nnn.nnn)      255.255.255.0
Default Gateway (nnn.nnn.nnn.nnn)  
Enable RIP?      Yes
Network-Loss Alarm Delay Time      60

To start the network type STARTNET
```


Screen 12-1. Set Network Params Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Factory Defaults?</td>
<td>Initially <strong>No</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>Yes</strong>. Select <strong>Yes</strong> to reload the values set at the factory. Use the SPACE BAR to toggle between Yes and No.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>--Network Initialization Parameters--</td>
<td>Initially <strong>No</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>Yes</strong>. <strong>Yes</strong> will start the network module on unit power-up using the parameters defined with the SNP command.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address (nnn.nnn.nnn.nnn)</td>
<td>Enter the IP address of the ASG Guard/ASG Guard Plus. Each device on the network must have its own unique IP address. The IP address assigned to the ASG Guard/ASG Guard Plus at the factory may not be appropriate for your network.</td>
</tr>
<tr>
<td>Field</td>
<td>Function</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>THE IP ADDRESS MUST BE SET BEFORE THE NETWORK MODULE OF THE ASG GUARD/ASG GUARD PLUS IS STARTED. Once the Network has been started, changes to this parameter will take effect only after the ASG Guard/ASG Guard Plus is rebooted.</td>
</tr>
<tr>
<td><strong>PPP Address (nnn.nnn.nnn.nnn)</strong></td>
<td>Enter the PPP address of the ASG Guard/ASG Guard Plus. This is the IP address that is used to identify the ASG Guard/ASG Guard Plus over a PPP link. The network portion of the PPP address must be different from the IP address used above.</td>
</tr>
<tr>
<td><strong>Subnet Mask (nnn.nnn.nnn.nnn)</strong></td>
<td>The subnet mask determines which part of the ASG Guard/ASG Guard Plus’s IP address represents its network number and which part represents its node number. Obtain an appropriate value from your network administrator.</td>
</tr>
<tr>
<td><strong>Default Gateway (nnn.nnn.nnn.nnn)</strong></td>
<td>The default gateway is the IP address of the router or other equipment on the local network segment that is used to direct traffic to and from the segment. Obtain an appropriate value from your network administrator.</td>
</tr>
<tr>
<td><strong>Enable RIP?</strong></td>
<td>Initially <strong>Yes</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>No</strong>. <strong>Yes</strong> allows the ASG Guard/ASG Guard Plus to direct routers on the local network segment to use it as the gateway to devices connected to the ASG Guard/ASG Guard Plus via PPP.</td>
</tr>
<tr>
<td><strong>Network-Loss Alarm Delay Time</strong></td>
<td>Enter a time in seconds, from 0 to 255. If no network activity is detected for longer than the specified amount of time, the ASG Guard/ASG Guard Plus will generate a .NETDOWN alarm.</td>
</tr>
</tbody>
</table>
12.7.1.2  SNMP Manager Parameters

The following is a description of how to set the SNMP Manager parameters. Type `S NP 2` at the ASG Guard/ASG Guard Plus command prompt.

```
Site123>SNP 2
--- Set Network Params ---
Restore Factory Defaults?  No

-- SNMP Manager Parameters --
PPP link needed for trap?  No
SNMP Community Name  SNMP_trap

-- IP Addresses for SNMP Managers (nnn.nnn.nnn.nnn) --
Manager 1  192.9.200.6
Manager 2
Manager 3
Manager 4
Manager 5

```

Screen 12-2.  Set Network Params Screen

<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restore Factory Defaults?</strong></td>
<td>Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Select Yes to reload the values set at the factory. Use the SPACE BAR to toggle between Yes and No.</td>
</tr>
<tr>
<td><strong>--SNMP Manager Parameters--</strong></td>
<td>If the ASG Guard/ASG Guard Plus is not connected to the same network as its SNMP Manager, it can reach the manager over a modem link by using the “Point-to-Point Protocol” (PPP). Initially No appears on the screen. Press the SPACE BAR to toggle to Yes. Set this option to Yes to establish a modem link to ONLY ONE SNMP manager. Additional steps may be necessary to configure the dial-out process. Refer the SNMP Manager Manual for more information. Select No if the trap will be sent via the network connection. Use the SPACE BAR to toggle between Yes and No.</td>
</tr>
<tr>
<td><strong>PPP link needed for trap?</strong></td>
<td>This option selects one of the active MIBs to format the SNMP Trap. Two formats are available: Standard and Nortel. Press the SPACE BAR until the desired choice is displayed.</td>
</tr>
<tr>
<td><strong>Trap format</strong></td>
<td>This option selects one of the active MIBs to format the SNMP Trap. Two formats are available: Standard and Nortel. Press the SPACE BAR until the desired choice is displayed.</td>
</tr>
</tbody>
</table>
Network Functions

Field: **SNMP Community Name**

**Function:** Enter the SNMP community name (up to 20 characters can be used as a name).

---IP Addresses for SNMP Manager---
- Manager 1
- Manager 2
- Manager 3
- Manager 4
- Manager 5

A maximum of five IP addresses can be entered as SNMP Managers to accept SNMP traps. If the IP address is not on the ASG Guard/ASG Guard Plus's network segment, make sure the default gateway is set and all routers have been programmed with the proper routes.

### 12.7.1.3 FTP Parameters

To specify the FTP parameters, type **SNP 3** to display the Network Parameters menu, FTP Parameters option.

```
Site123>sn 3

-- FTP Parameters --
Restore Factory Defaults ?   No
PPP link needed for ftp?    No
Ftp service type             Client only
-- Server 1 (default) --
  IP address (nnn.nnn.nnn.nnn)
  User name
  Password
  Upload Directory .
-- Server 2 --
  IP address (nnn.nnn.nnn.nnn)
  User name
  Password
  Upload Directory .
```

**Screen 12-3. FTP Parameters Screen**

**NOTE:**
In setting the user name and password, remember that they are case-sensitive.

Field: **Restore Factory Defaults**

**Function:** Press the SPACE BAR until the desired choice is displayed. Select “Yes” to restore original factory settings. Select ‘No’ to keep the current values.

**PPP link needed for ftp?**

**Function:** Select this option if the ASG Guard/ASG Guard Plus needs to dial out with a PPP session to send files via FTP. (See the .PPPREQ alarm and PHPPP Action Routine in Section 14 of the ASG Guard/ASG Guard Plus User’s Guide)
### Field Function

**FTP service type**

There are two Server Types: NONE and CLIENT ONLY. Use the CLIENT ONLY setting to allow FTP file transfers.

**Server 1 (default) —**

**IP address (nnn.nnn.nnn.nnn)**

Enter the IP address of the server. The files transmitted by FTP are sent to this address automatically unless specified otherwise.

**User name**

Enter the name used to logon onto the server. This entry is case-sensitive.

**Password**

Enter the password for the user named above. This entry is case sensitive.

**Upload directory**

Enter the name of the directory that should receive the file.

---

**Server 2**

**IP address (nnn.nnn.nnn.nnn)**

Enter the IP address of the server. The files transmitted by FTP are sent to this address automatically when server 2 is specified.

**User name**

Enter the name used to logon onto the server. This entry is case-sensitive.

**Password**

Enter the password for the user named above. This entry is case sensitive.

**Upload directory**

Enter the name of the directory that should receive the file. A period denotes the root directory.
12.7.2 Display Network Parameters – DNP Command

The DNP command displays network initialization parameters previously set.

Type **DNP** at the system prompt and press the ENTER key. Parameter settings will scroll down the screen as follows:

```
Site123> --- Display Network Params ---
-- Network Initialization Parameters --
Start Network on Power-up?        No
IP Address (nnn.nnn.nnn.nnn)       192.9.200.2
PPP Address (nnn.nnn.nnn.nnn)      192.9.200.3
Subnet Mask (nnn.nnn.nnn.nnn)      255.255.255.0
Default Gateway (nnn.nnn.nnn.nnn)  
Enable RIP?                        Yes
Network-Loss Alarm Delay Time      60
Ethernet Address (hhhhhhhhhhhh)    00 E0 89 00 00 00
-- SNMP Manager Parameters --
PPP link needed for trap?          No
Trap format                        Standard
SNMP Community Name                SNMP_trap
-- IP Addresses for SNMP Managers (nnn.nnn.nnn.nnn) --
Manager 1
Manager 2
Manager 3
Manager 4
Manager 5
-- FTP Parameters --
PPP link needed for ftp?           No
Ftp service type                   None
-- Server 1 (default) --
IP address (nnn.nnn.nnn.nnn)       
User name                         
Password                          
Upload Directory                  .
-- Server 2 --
IP address (nnn.nnn.nnn.nnn)       
User name                         
Password                          
Upload Directory                  .
```

*Screen 12-4. Display Network Params Screen*
12.8 Network Startup and Status

Commands are provided to start the network interface of the ASG Guard/ASG Guard Plus as well as to display the network status.

12.8.1 Startup Network – STARTNET Command

The STARTNET command allows the user a one step method for connecting the ASG Guard/ASG Guard Plus to a systems network. The default value for the ASG Guard/ASG Guard Plus at startup has the network connection disabled.

Type STARTNET at the system prompt, and press the ENTER key. If you are already on the network, the following messages appear:

--- Start up Network ---
The network is already running.
To restart the network connection you must reboot.

If the network has not been started, the following messages appear:

--- Start up Network --- M

12.8.2 Display Network Status – DNS Command

The DNS command displays the status of the network.

Type DNS at the system prompt and press the ENTER key. If the network has not been started, the following messages will appear:

--- Display Network Status ---
The network has not been started

If the network has been started on the ASG Guard/ASG Guard Plus but no activity is seen, the following messages will appear:

--- Display Network Status ---
The network has been down since this ASG Guard Plus was started

If the network was up and then went down while the ASG Guard/ASG Guard Plus was on the network, the amount of time the network has been down will appear.

If the network has been started on the ASG Guard/ASG Guard Plus and is currently “up,” the following messages will appear:

--- Display Network Status ---
The network has been running since 09/28/98 16:20:26

Two alarms are available which allow the network status to be determined. The .NETDOWN alarm is issued after a preset length of time during which no network activity is detected. When network activity is detected, the .NETUP alarm is issued.

The determination of network up and down is based on detected traffic on the Ethernet. The time interval for non activity ranges from 1 to 255 seconds, and can be selected by the user.

To enter the time interval, type SNP 1 at the prompt. At the Network-Loss Alarm Delay Time, enter the time allowed between non-activity on the network.
A network quiet time longer than the Network-Loss Alarm Delay Time will trigger the alarm .NETDOWN.

### 12.9 Querying Remote Nodes – PING Command

The Port and Session Control Functions menu includes the PING command. The PING command is issued to query another device (IP address) on a network.

**Syntax:**

```
PING <Ipaddr>.
```

Where `<Ipaddr>` is the IP address of the device

If successful, the reply shows the length of time it took to reach the device. If the ping is unsuccessful, the message is "Device not Reachable".

### 12.10 Telnet Port Parameters

#### 12.10.1 Setting Telnet Port Parameters – ST Command

If you plan to Telnet to the ASG Guard/ASG Guard Plus, you must set up the ASG Guard/ASG Guard Plus Telnet port parameters. To set these parameters, type `ST` at the system prompt and press the ENTER key.

```bash
Site123>ST
--- Set Telnet Port Params ---
Restore Factory Defaults? No
Terminal Emulation TTY
Sysop Idle Timer None
Host Session Idle Timer None
Host Session Disconnect on Ctrl+A Yes

```

Screen 12-6. Set Telnet Port Params Screen
<table>
<thead>
<tr>
<th>Field</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore Factory Defaults?</td>
<td>Initially <strong>No</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>Yes</strong>. Select <strong>Yes</strong> to reload the values set at the factory.</td>
</tr>
<tr>
<td>Termination Emulation</td>
<td>Select either TTY or VT100 (if supported by your terminal). Press the SPACE BAR until the desired choice is displayed.</td>
</tr>
<tr>
<td></td>
<td>If TTY is selected, prompts appear one at a time. When VT-100 is selected, a list of prompts for a particular task screen appears; the cursor is located at the first prompt. In TTY mode, each prompt appears after the ENTER key is pressed. Note that this option affects SYSOP sessions only. Host sessions are &quot;transparent.&quot;</td>
</tr>
<tr>
<td>Sysop Idle Timer</td>
<td>Select the maximum duration of inactivity during a Sysop session after which the session terminates and the port resets. Press the SPACE BAR until the desired choice is displayed.</td>
</tr>
<tr>
<td>Host Session Idle Timer</td>
<td>Select the length of idle time (no commands are received) after which the Sysop session is disconnected. Press the SPACE BAR until the desired choice is displayed.</td>
</tr>
<tr>
<td>Host Session Disconnect on Ctrl+A</td>
<td>Initially <strong>No</strong> appears on the screen. Press the SPACE BAR to toggle to <strong>Yes</strong>. Select <strong>Yes</strong> to disconnect from the host when the key sequence Ctrl+A is pressed.</td>
</tr>
</tbody>
</table>

To verify that the ASG Guard/ASG Guard Plus can be accessed through the network, start the ASG Guard/ASG Guard Plus network module by typing STARTNET at the system prompt. Next, add a user to the ASG Guard/ASG Guard Plus user database. Access the ASG Guard/ASG Guard Plus from a Telnet terminal on the network. To access the system, enter the ASG Guard/ASG Guard Plus's IP address. If you are prompted for a user name, you have reached the ASG Guard/ASG Guard Plus. Once you respond to the authentication challenge, you will be connected to the ASG Guard/ASG Guard Plus.
12.10.2 Display Telnet Port Parameters – DT Command

The DT command displays parameter settings for the Telnet ports.

Type **DT** at the system prompt and press the ENTER key. Telnet parameter fields will be displayed.

```
Site123>DT

--- Display Telnet Port Params ---
Restore Factory Defaults? No
Terminal Emulation TTY
Sysop Idle Timer None
Host Session Idle Timer None
Host Session Disconnect on Ctrl+A Yes

Site123>
```

**Screen 12-7.** Display Telnet Port Params

The parameter values apply to all Telnet sessions.
12.11 Initiate a PPP Link – PPP Command

The PPP link can be initiated in the ASG Guard/ASG Guard Plus in one of two ways. The user can either designate a specific port as a dedicated PPP port, or you may initiate a PPP connection on-demand.

12.11.1 Designate a Port as a PPP Port

Designate a specific port as a PPP port. After it has been designated as a PPP port, the port is available only for a PPP connection. This ensures that a port is always available for a PPP session. After authenticating and accessing the command prompt, issue the PPP command with the appropriate parameters.

Command: PPP

Syntax: PPP active/passive flag, Host port ID

Example: To have Host port 4 as a designated PPP port, type:

PPP A,4

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>active/passive flag</td>
<td>Indicates the state of the PPP link when it is initially opened. Active links will send out broadcast packets to initiate a PPP link. If a passive link has been established, broadcast packets will NOT be sent out. Instead, the port will remain in PPP mode until it receives a broadcast packet to initiate the PPP session. Enter A for active link, P for passive link.</td>
</tr>
<tr>
<td>hostport ID</td>
<td>Specifies to the ASG Guard/ASG Guard Plus which port is to become the dedicated PPP host port. Valid port ID’s are H1, H2, H3, and H4.</td>
</tr>
</tbody>
</table>

At this point, the port will be available for PPP connections. When the port responds to the incoming call, the user will be prompted to authenticate. To return the port to its normal state (remove PPP designation), reset the port by using the RES command.

12.11.2 Initiate a PPP Connection On-Demand

The ASG Guard Plus can support a Point to Point Protocol (PPP) connection via its modem port. ASG Guard Plus can be used as a secured gateway into a TCP/IP network by implementing the PPP connection. This also allows the user to use TCP/IP based protocols in support of the ASG Guard Plus. These protocols include SNMP, Telnet, and FTP.
12.11.2.1 ASG Guard/ASG Guard Plus Setup
Before an ASG Guard/ASG Guard Plus can support a PPP connection, it must be configured for network operation. To do this, use the Set Network Parameters command and select Option 1 (SNP 1). The following set of options will be presented.

**IP Address** - This is the IP address of the TCP/IP network to which the ASG Guard Plus is attached via the 10BaseT connection. Consult your Network Administrator for this address.

**PPP IP Address** - This is the IP address that will be referenced when connecting to the ASG Guard/ASG Guard Plus via the PPP connection. The entered address should indicate a network other than the one for the 10BaseT network. It should also be different than any other network that can be accessed via the 10BaseT LAN.

**Default Gateway** - This should be the default gateway that is used by the ASG Guard/ASG Guard Plus for its 10baseT connection. The ASG Guard/ASG Guard Plus will act as the default gateway for the PPP connection.

**RIP Enabled** - This should be set to Yes. Router Information Protocol (RIP) allows routers on the network to know how to send packets to destination IP addresses. For example, if you dial into the ASG Guard/ASG Guard Plus from a remote site and establish a PPP connection with RIP enabled, the ASG Guard/ASG Guard Plus will broadcast (every 30 seconds) to the network that this connection exists. Routers in the network then "know" packets destined for the remote site should be sent to the ASG Guard/ASG Guard Plus (The 'default gateway' for the remote site).

*NOTE:*
*If you are using protocols such as Telnet or FTP for devices other than the ASG Guard/ASG Guard Plus, they must also support RIP.*

When all the settings have been entered, either start the network or reboot the ASG Guard/ASG Guard Plus so that the settings take effect.

12.11.2.2 Setup for PPP Client using "Dial-Up Networking" – New Connection
The following outlines the procedure for establishing a remote PPP link to the ASG Guard/ASG Guard Plus using Microsoft's "Dial-Up Networking" package (with the Windows 95 operating system) for a new connection. If your system has already been set-up, refer to Section 12.11.2.3.

1. From the "Start menu, select "Programs", "Accessories" and scroll down to Dial-Up Networking.

2. Open Dial-Up Networking, and double-click on "Make New Connection" icon. Press the "Next>" button to continue.

   *NOTE:*
   *Since this is a first time installation, the make new connection wizard will appear. Press the "Next>" button to continue.*

3. Enter a name for the ASG Guard/ASG Guard Plus and select the modem to be used for the dial out connection.

4. Next, press the Configure button.

5. Select the Option tab, then select "Bring up terminal window after dialing". This will allow you to authenticate into the ASG Guard/ASG Guard Plus.
6. Press the OK button. The original "Make New Connection" screen will appear. Press the "Next->" button.

7. Set up the phone number (and country code, if applicable). When the data is entered, press the "Next->" button. You are now ready to establish a remote connection.

12.11.2.3 Setup for PPP Client using "Dial-Up Networking" – Remote Connection

1. In the Dial-Up Networking group, click once to highlight the icon for the ASG Guard/ASG Guard Plus (from above) and press the right mouse button. From the "Menu" bar, select "Properties".

2. Select the Server Types. Select the "PPP" option from the drop down menu a (as a minimum) click the box next to the TCP/IP selection.

3. Next, press the TCP/IP "Settings" button and select "Specify and IP Address". Enter the ASG Guard/ASG Guard Plus's IP address and press the OK button.

The PC is ready to start a PPP connection to the ASG Guard/ASG Guard Plus.

12.11.2.4 Establishing a PPP Connection

1. From the Dial up Networking group, open the Profile entered for the dial up PPP connection to the ASG Guard/ASG Guard Plus. The 'User Name' and 'Password Fields' are NOT used by the ASG Guard/ASG Guard Plus for authentication. Consequently, the fields can be left blank.

2. To start the connection, press the Connect button. This will begin the dial out process.

3. When the connection to the modem is made, a pop up terminal window will appear. Use this window to authenticate yourself into the ASG Guard/ASG Guard Plus.

4. When authentication is completed, type PPP at the system prompt and hit return.

5. A string of characters will appear. Press the F7 key. This will complete the PPP connection between the ASG Guard/ASG Guard Plus and the client PC. At this point any TCP/IP protocol can be used over the connection.
12.12 Initiating a Telnet Session

The ASG Guard Plus supports Telnet sessions over its 10base T connection.

12.12.1 Initiating a Telnet Session: Direct Connect

The following outlines the steps to take to initiate a direct connect Telnet session using a PC (Windows 95/98 or Windows NT client) on an Ethernet connection to the network:

1. Set up the ASG Guard/ASG Guard Plus to set the IP Address, PPP Address, Default Gateway and enable RIP. Before an ASG Guard/ASG Guard Plus can support a Telnet session, it must be configured for network operation. To do this, use the Set Network Parameters command and select Option 1 (SNP 1). The following set of options will be presented.
   - **IP Address** - This is the IP address of the TCP/IP network to which the ASG Guard Plus is attached via the 10BaseT connection. Consult your Network Administrator for this address.
   - **PPP IP Address** - This is the IP address that will be referenced when connecting to the ASG Guard/ASG Guard Plus via the PPP connection. The entered address should indicate a network other than the one for the 10BaseT network. It should also be different than any other network that can be accessed via the 10BaseT LAN.
   - **Default Gateway** - This should be the default gateway that is used by the ASG Guard/ASG Guard Plus for its 10baseT connection. The ASG Guard/ASG Guard Plus will act as the default gateway for the PPP connection.
   - **RIP Enabled** - This should be set to **Yes**. Router Information Protocol (RIP) allows routers on the network to know how to send packets to destination IP addresses. For example, if you dial into the ASG Guard/ASG Guard Plus from a remote site and establish a PPP connection with RIP enabled, the ASG Guard/ASG Guard Plus will broadcast (every 30 seconds) to the network that this connection exists. Routers in the network then "know" packets destined for the remote site should be sent to the ASG Guard/ASG Guard Plus (The ‘default gateway’ for the remote site).

   **NOTE:**
   *If you are using protocols such as Telnet or FTP for devices other than the ASG Guard/ASG Guard Plus, they must also support RIP.*

2. When all the settings have been entered, start the network using the STARTNET command. If the network is already running and network settings were changed, you MUST reboot the system. The remote connection will be lost and you will have to reconnect.

3. From the Windows Start button, click on "Run".

4. When the "RUN" window appears, type **TELNET** and the IP address of the ASG Guard/ASG Guard Plus to be accessed. Click the OK button.

   When the connection is made, you will be prompted to authenticate yourself into the ASG Guard/ASG Guard Plus.

   If using another communication package (such as Procomm, HyperTerminal, etc.) see the section in the respective package on establishing a Telnet session.
12.12.2 Telnet Session via PPP through a ASG Guard/ASG Guard Plus

It is possible to use the ASG Guard Plus as a security server into a TCP/IP network. In this scenario, the remote users dial into the ASG Guard/ASG Guard Plus, establish a PPP link, then Telnet to a another device on the network. When using the ASG Guard/ASG Guard Plus as a security server, make sure that RIP is enabled in the ASG Guard/ASG Guard Plus and that both the ASG Guard/ASG Guard Plus and the device being accessed are using the same default Gateway. To establish this telnet link:

1. Establish a dial-up connection (see Section 12.11.2.2) to the ASG Guard/ASG Guard Plus.
2. When authentication is completed, type PPP at the system prompt (see Section 12.11.2.2).
3. Establish a Telnet session (see Section 12.12.1).
13. Log Functions

13.1 What This Chapter Contains

- Overview
- Description of each log maintained by the ASG Guard/ASG Guard Plus
- How to display and clear logs

13.2 Overview

The ASG Guard Plus product line contains information about the specific history of the product. In total, there are four areas where this information is stored:

**Access History Log** - Contains information about attempts to access the ASG Guard/ASG Guard Plus. Users with Sysop 1, Sysop 2, or CMaster level access can view the log.

**Error Log** - Contains a history of CCL system errors or exceptions that have occurred. Users with Sysop 1, Sysop 2, or CMaster level access can view this log.

**Failure History** - Contains a list of failed access attempts and the reasons for the failure. Users with Sysop 1, Sysop 2, or CMaster level access can view this log.

**Log History** - Contains a list of activity of the ASG Guard/ASG Guard Plus. These include phoning home, user profile changes, and modem accessed. Users with Sysop 1, Sysop 2, or CMaster level access can view this log.
13.3 The Log Functions Menu

The Log Functions Menu provides commands that display records of activity on the ASG Guard/ASG Guard Plus. To display the Log Functions menu, type **L** at the prompt and press the ENTER key. The commands to display each log type are listed.

```
Site123>l
--- LOG FUNCTIONS ( CMaster ) ---
--- Log Functions ---
AH    Access History                FH    Failure History
LH    Log History                   DER   Display Error Log
Other Menus: S -System  A -Alarm/Event  U -User  F -File  P -Port/Session
```

Screen 13-1. Log Functions (CMaster) Screen

13.3.1 Access History – AH Command

The ASG Guard/ASG Guard Plus maintains a log of each access attempt. The log includes the date, time, MAC, User ID, duration and session type.

Type **AH** to display the Access History. Access attempts, starting with the oldest, will be listed.

The following options may be entered to display a selected part of the log history.

**NOTE:**
*Be sure to type a space between the command and option in the command line. Use a comma to separate options.*

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AH</strong></td>
<td>The Access History log is displayed in chronological order, from the oldest at the beginning to the most recent record at the end.</td>
</tr>
<tr>
<td><strong>AH-</strong></td>
<td>The Access History log is displayed in chronological order, from the most recent record at the beginning to the oldest record at the end.</td>
</tr>
<tr>
<td><strong>AH n</strong></td>
<td>Entering a value <strong>n</strong> causes only <strong>n</strong> lines of the Access History to be displayed, starting with oldest entry.</td>
</tr>
<tr>
<td><strong>AH -n</strong></td>
<td>Enter a value for <strong>-n</strong> and only <strong>n</strong> lines of the Access History are displayed, starting with oldest record.</td>
</tr>
<tr>
<td><strong>AH all</strong></td>
<td>Lists the entire Access History, without page breaks, starting with the oldest record.</td>
</tr>
<tr>
<td><strong>AH -all</strong></td>
<td>Lists the entire Access History, without page breaks, starting with the most recent record.</td>
</tr>
<tr>
<td><strong>AH ,matchstring</strong></td>
<td>Enter a character string for the User ID. The Access History log will be searched and the User IDs containing that character string are displayed. This parameter is case sensitive.</td>
</tr>
</tbody>
</table>
Each entry in the access history log contains the date, time, MAC, User ID, duration, and session type.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The month/day/year of the log event.</td>
</tr>
<tr>
<td>Time</td>
<td>The time of day, in hours:minutes at which the event occurred.</td>
</tr>
<tr>
<td>User ID</td>
<td>The User ID of the person who accessed the ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>Duration</td>
<td>The total number of minutes:seconds the user accessed the ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>Session Type</td>
<td>The Session Type lists the Port used to access the ASG Guard/ASG Guard Plus and the Access Class of that user. Port types are Aux., Host, and Modem. Access Class types are CMaster, Sysop2, Sysop1, and Host.</td>
</tr>
</tbody>
</table>
--- Access History ---

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>MAC</th>
<th>User ID</th>
<th>Duration</th>
<th>Session Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/21/98</td>
<td>10:08</td>
<td>7EA3</td>
<td>AUX_Default</td>
<td>06:43</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:25</td>
<td>F129</td>
<td>GREGG</td>
<td>00:18</td>
<td>TELNET-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:25</td>
<td>1CE8</td>
<td>HENRY</td>
<td>01:49</td>
<td>TELNET-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:24</td>
<td>4901</td>
<td>AUX_Default</td>
<td>11:24</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:52</td>
<td>1986</td>
<td>AUX_Default</td>
<td>00:10</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:53</td>
<td>0052</td>
<td>LUCGUARD</td>
<td>00:13</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:53</td>
<td>AEB6</td>
<td>AUX_Default</td>
<td>00:29</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>10:54</td>
<td>0D59</td>
<td>LUCGUARD</td>
<td>06:09</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>11:00</td>
<td>FFC4</td>
<td>AUX_Default</td>
<td>01:15</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/21/98</td>
<td>11:02</td>
<td>5AE2</td>
<td>AUX_Default</td>
<td>03:16</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/23/98</td>
<td>11:34</td>
<td>AB02</td>
<td>AUX_Default</td>
<td>01:08</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/23/98</td>
<td>15:40</td>
<td>3E7B</td>
<td>AUX_Default</td>
<td>02:21</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/24/98</td>
<td>08:55</td>
<td>CFF4</td>
<td>AUX_Default</td>
<td>51:57</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/24/98</td>
<td>15:00</td>
<td>FA45</td>
<td>AUX_Default</td>
<td>01:04</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/24/98</td>
<td>17:11</td>
<td>E656</td>
<td>AUX_Default</td>
<td>08:41</td>
<td>AUX-&gt;Sysop</td>
</tr>
<tr>
<td>11/24/98</td>
<td>17:12</td>
<td>E008</td>
<td>HENRY</td>
<td>07:22</td>
<td>TELNET-&gt;Sysop</td>
</tr>
<tr>
<td>11/25/98</td>
<td>14:57</td>
<td>D25D</td>
<td>HENRY</td>
<td>04:42</td>
<td>TELNET-&gt;Sysop</td>
</tr>
<tr>
<td>11/25/98</td>
<td>15:02</td>
<td>73C2</td>
<td>HENRY</td>
<td>01:59</td>
<td>TELNET-&gt;Sysop</td>
</tr>
<tr>
<td>11/25/98</td>
<td>15:07</td>
<td>669F</td>
<td>HENRY</td>
<td>01:00</td>
<td>TELNET-&gt;Sysop</td>
</tr>
<tr>
<td>11/25/98</td>
<td>15:03</td>
<td>C2EB</td>
<td>HENRY</td>
<td>04:46</td>
<td>TELNET-&gt;Sysop</td>
</tr>
</tbody>
</table>

Screen 13-2. Access History Screen

13.3.2 Log History – LH Command

Type LH to display the log history and press the ENTER key. The LH command lists the oldest record first.

The Log History file contains a list of activity of the ASG Guard/ASG Guard Plus. These activities are events that take place within the Guard such as alarms, changes to the configuration and User Access. The purpose of this log is to assist an administrator in viewing activities that take place in the Guard. This is a very useful tool when trying to look at recent history to pinpoint a problem with a host device or the ASG Guard.

The following options can be entered to display a selected part of the log history.

**NOTE:**

*Be sure to type a space between the command and option in the command line. Use a comma between options.*

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>LH</td>
<td>The entries in the Log History are displayed in chronological order, from the oldest record to the most recent record.</td>
</tr>
<tr>
<td>LH -</td>
<td>The entries in the Log History are displayed in chronological order, from the most recent record to the oldest record.</td>
</tr>
<tr>
<td>LH n</td>
<td>Enter a value n to cause only n lines of the Log History to be displayed, starting with oldest entry.</td>
</tr>
<tr>
<td>LH -n</td>
<td>Enter a value for -n and only n lines of the Log History are displayed, starting with the most recent record.</td>
</tr>
</tbody>
</table>
LH all  Lists the entire Log History, without page breaks, starting with the oldest record.

LH -all  Lists the entire Log History, without page breaks, starting with the most recent record.

LH ,matchstring  Enter the character string of the Port ID for which the ASG Guard/ASG Guard Plus will search the Log History. The log entries containing the Port ID that matches the entered character string are displayed. This parameter is case sensitive

Each entry in the log history log contains the date, time, MAC, User with event description.

Command  Function
Date     The month/day/year of the log event.
Time     The time of day, in hours:minutes at which the event occurred.
Port     The port type on which the event occurred. Port types are AUX, Host, and Modem.
User with description  The user ID of the person or function that triggered the event. The event description gives a brief dialog of what occurred to trigger this event.

Ser#98100221>LH

--- Log History ---

Screen 13-3. Log History Screen
13.3.3 Failure History – FH Command

Type FH and press the ENTER key to display a log of failed attempts to access the ASG Guard/ASG Guard Plus.

NOTE: Be sure to type a space between the command and option in the command line. Use a comma to separate options.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>FH</td>
<td>The entries in the Failure History log are displayed in chronological order, from the oldest record at the beginning to the most recent record at the end.</td>
</tr>
<tr>
<td>FH -</td>
<td>The entries in the Failure History log are displayed in chronological order, from the most recent record at the beginning to the oldest record at the end.</td>
</tr>
<tr>
<td>FH n</td>
<td>Entering a value n causes only n lines of the Failure History to be displayed, starting with oldest entry.</td>
</tr>
<tr>
<td>FH -n</td>
<td>Enter a value for -n and only n lines of the Failure History are displayed, starting with the most recent record.</td>
</tr>
<tr>
<td>FH all</td>
<td>Lists the entire Failure History, without page breaks, starting with the oldest record.</td>
</tr>
<tr>
<td>FH -all</td>
<td>Lists the entire Failure History, without page breaks, starting with the most recent record.</td>
</tr>
<tr>
<td>FH ,matchstring</td>
<td>Enter a character string for the Port ID or User ID. The log entries containing the specified Port ID or User ID are displayed. This parameter is case sensitive. For example, to display only the failure history records for the user with the User ID “CHRIS” type:</td>
</tr>
</tbody>
</table>

```
> FH ,CHRIS
```

Each entry in the failure history log contains the date, time, MAC, User ID, Port, and Reason.

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The month/day/year of the failed access attempt.</td>
</tr>
<tr>
<td>Time</td>
<td>The time of day, in hours:minutes at which the attempt was initiated.</td>
</tr>
<tr>
<td>User ID</td>
<td>The User ID of the person who attempted access. If the caller is unknown, question marks (?) are displayed.</td>
</tr>
</tbody>
</table>
Log Functions

Port
The port type that the caller attempted to access. Port types are AUX, Host and Modem.

Reason
The reason that the access attempt failed. Reasons include:
- Invalid User ID
- Blocked/Expired
- ASG Key Invalid Response
- ASG Key Error
- Password Invalid
- Callback Error
- Time Out
- User Disconnected
- Host Busy

NOTE:
Callback error codes that appear in these messages can help Lucent Technologies Technical Support to identify and resolve Callback errors.

Ser#98100221>fh

--- Failure History ---

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Ser#</th>
<th>Name</th>
<th>Port</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/21/98</td>
<td>10:08</td>
<td>6251</td>
<td>DJKFALD</td>
<td>AUX</td>
<td>Invalid User ID</td>
</tr>
<tr>
<td>11/24/1998</td>
<td>17:11</td>
<td>EFE7</td>
<td>HENRY</td>
<td>TELNET</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>11/24/1998</td>
<td>17:12</td>
<td>54FE</td>
<td>GREGG</td>
<td>TELNET</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>11/24/1998</td>
<td>17:11</td>
<td>9C09</td>
<td>TOM</td>
<td>TELNET</td>
<td>User Disconnected</td>
</tr>
<tr>
<td>11/25/1998</td>
<td>15:07</td>
<td>4BCC</td>
<td>GREGG</td>
<td>TELNET</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>12/01/1998</td>
<td>13:07</td>
<td>E16E</td>
<td>HENRY</td>
<td>TELNET</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>12/01/1998</td>
<td>13:08</td>
<td>F3F4</td>
<td>HENRY</td>
<td>TELNET</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>12/01/1998</td>
<td>13:16</td>
<td>8500</td>
<td>LUGUARD</td>
<td>TELNET</td>
<td>User Disconnected</td>
</tr>
<tr>
<td>12/07/1998</td>
<td>16:02</td>
<td>FCDC</td>
<td>HENRY</td>
<td>AUX</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>12/07/1998</td>
<td>17:17</td>
<td>0BC4</td>
<td>HENRY</td>
<td>AUX</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>12/07/1998</td>
<td>17:19</td>
<td>5922</td>
<td>HENRY</td>
<td>AUX</td>
<td>Password Invalid</td>
</tr>
<tr>
<td>12/24/98</td>
<td>11:43</td>
<td>0BAA</td>
<td>1234</td>
<td>AUX</td>
<td>Invalid User ID</td>
</tr>
<tr>
<td>12/24/98</td>
<td>11:43</td>
<td>5080</td>
<td>HENRY</td>
<td>AUX</td>
<td>Password Invalid</td>
</tr>
</tbody>
</table>

-- End of List --

Screen 13-4. Failure History Screen
13.3.4 Display Error Log – DER Command

Type **DER** to display the Error Log screen and press the ENTER key.

**NOTE:**
*Be sure to type a space between the command and the option in the command line. Use a comma between options.*

<table>
<thead>
<tr>
<th>Command</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>DER</td>
<td>The Display Error Log is displayed in chronological order, from the most oldest record at the beginning to the most recent record at the end.</td>
</tr>
<tr>
<td>DER -</td>
<td>The Display Error Log is displayed in chronological order, from the most recent record at the beginning to the oldest record at the end.</td>
</tr>
<tr>
<td>DER n</td>
<td>Entering a value n causes only n lines of the Display Error Log to be displayed, starting with oldest entry.</td>
</tr>
<tr>
<td>DER -n</td>
<td>Enter a value for -n and only n lines of the Display Error Log are displayed, starting with the most recent record.</td>
</tr>
<tr>
<td>DER all</td>
<td>Lists the entire Display Error Log, without page breaks, starting with the oldest record.</td>
</tr>
<tr>
<td>DER -all</td>
<td>Lists the entire Display Error Log, without page breaks, starting with the most recent record.</td>
</tr>
</tbody>
</table>

```
Site123>DER
--- Display Error Log ---
09/17/98 14:18:23 ** RESTART 00 P2:20094E53 TA
?en
09/19/98 22:58:05 ** RESTART 00 P2:20094E53 TA
?en
09/21/98 14:26:13 ** RESTART 00 P2:20094E53 TA
?en
09/21/98 14:29:33 ** RESTART 00 P2:20094E53 TA
?en
09/21/98 14:32:15 ** RESTART 00 P2:20094E53 TA
?en
09/21/98 15:35:45 ** RESTART 00 P2:20094E53 TA
?en
09/22/98 09:38:49 ** RESTART 00 P2:20094E53 TA
?en
09/28/98 12:13:39 ** RESTART 00 P2:20094E53 TA
?en
09/28/98 16:02:25 ** RESTART 00 P2:20094E53 TA
?en
-- End of List --
```

**Screen 13-5.** Display Error Log Screen
13.3.5 Clear Log History – CLH Command

The Clear Log History command clears the system log that contains a record of activity of the ASG Guard/ASG Guard Plus and devices connected to it.

Type **CLH** at the system prompt and press the ENTER key to display the Clear Log History screen.

```
Site123>CLH
--- Clear Log History ---
Are You Sure ?                     Yes
>
```

**Screen 13-6. Clear Log History Screen**

Initially No appears at the “Are You Sure?” prompt. If you do not want to clear the log history, press the ENTER key. If you want to clear the log history, press the SPACE BAR to toggle the field to Yes and then press the ENTER key. The system will confirm that the log history has been cleared.

13.3.6 Clear Error Log – CER Command

The Clear Error Log command clears all entries in the CCL Error Log.

Type **CER** at the system prompt and press the ENTER key to display the Clear Error Log screen to be displayed.

```
Site123>CER
--- Clear Error Log ---
Are You Sure ?                     No
```

**Screen 13-7. Clear Error Log Screen**

To clear the error log, press the SPACE BAR to toggle the field to Yes and then press the ENTER key. The system confirms that the error log as been cleared.

If you do not want to clear the error log, press the ENTER key when No is displayed.
14. Events and Action Routines

14.1 What This Chapter Contains

- Overview
- Description of Events
- Description of Action Routines

14.2 Overview

The ASG Guard/ASG Guard Plus can be programmed to respond to a particular event or trigger. There are two types of events: Internal and External. An internal event is generated by the ASG Guard/ASG Guard Plus automatically in response to a particular condition, such as a failed authentication attempt or a low battery. An external event is an alarm received from a device connected to the ASG Guard/ASG Guard Plus. Internal events are listed in this chapter.

The action that the ASG Guard/ASG Guard Plus initiates in response to an event is specified by the Action Routine associated with that event in the Action Table. A set of Action Routines is included with the ASG Guard/ASG Guard Plus. A description and an example of each Action Routine are included in this chapter. Note that customized Action Routines may be written in CCL, the communications control language for the ASG Guard/ASG Guard Plus.

14.3 Internal Events

This section describes internal events that can be generated by the ASG Guard/ASG Guard Plus.

14.3.1 .AUTHFAIL Internal Event

The .AUTHFAIL internal event occurs each time there is a failed attempt at authentication during a user logon. The format of this internal event is:

.AUTHFAIL Parameter 1 Parameter 2 Parameter 3

Where:

- Parameter 1 - authentication failure code (typically used as a parameter associated with the PAGE Action Routine.) The codes for this parameter are listed in Table 14-1.
- Parameter 2 - User ID
- Parameter 3 - text description of the reason for the authentication failure.
Table 14-1. Authentication Failure Codes

<table>
<thead>
<tr>
<th>Code</th>
<th>Description</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0010</td>
<td>Invalid User ID</td>
<td>0050</td>
<td>Invalid password #1</td>
</tr>
<tr>
<td>0011</td>
<td>Blocked user</td>
<td>0053</td>
<td>Call Back unsuccessful</td>
</tr>
<tr>
<td>0012</td>
<td>Wrong time</td>
<td>0054</td>
<td>Invalid password #2</td>
</tr>
<tr>
<td>0032</td>
<td>Invalid ASG Key response</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

14.3.2 .BAT48HIGH Internal Event
The .BAT48HIGH event occurs when the 48V battery being monitored crosses over from an OK threshold to a high voltage threshold. These thresholds are set using the Set Sensor Alarms (SSA) command (see Section 10.7).

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BAT48HIGH</td>
<td>SCHEDULE</td>
<td>15 PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>

This example activates a call to the maintenance reporting center 15 minutes after the .BAT46HIGH condition occurs.

14.3.3 .BAT48LOW Internal Event
The .BAT48LOW event occurs when the battery being monitored crosses over from an OK threshold to a low voltage threshold. These thresholds are set using the Set Sensor Alarms (SSA) command (see Section 10.7).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BAT48LOW</td>
<td>SCHEDULE</td>
<td>15 PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>

In this example, the maintenance center is called 15 minutes after the .BAT48LOW condition occurs.
14.3.4 .BAT48OK Internal Event

The .BAT48OK event occurs when the battery being monitored crosses over from a low voltage or high voltage threshold to an OK threshold. These thresholds are set using the Set Sensor Alarms (SSA) command (see Section 10.7).

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BAT48OK</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.BAT48OK.1</td>
<td>CANCEL</td>
<td>.BAT48HIGH</td>
<td></td>
</tr>
<tr>
<td>.BAT48OK.2</td>
<td>CANCEL</td>
<td>.BAT48LOW</td>
<td></td>
</tr>
</tbody>
</table>

This example cancels the .BAT48HIGH and .BAT48LOW alarms when .BAT48OK event is received.

14.3.5 .BUFREADY Internal Event

This alarm is sent when a buffer file is closed and is ready to be sent.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BUFREADY</td>
<td>PAGE</td>
<td>5551212,1234</td>
<td>File ready</td>
</tr>
</tbody>
</table>

14.3.6 .C#CLOSED Internal Event

This alarm is sent when the contact closure (number) on the main board has been closed.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.C2CLOSED</td>
<td>PHONHOME</td>
<td>4944440</td>
<td>Contact #2 closed</td>
</tr>
</tbody>
</table>

14.3.7 .C#OPEN Internal Event

This alarm is sent when the contact closure (number) on the main board has been opened.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.C2OPEN</td>
<td>PHONHOME</td>
<td>4944440</td>
<td>Contact #2 open</td>
</tr>
</tbody>
</table>
14.3.8 .CCLERROR Internal Event

The .CCLERROR event occurs automatically if the ASG Guard/ASG Guard Plus detects an error in its internal program, or in a user-written Action Routine. Upon generation of a .CCLERROR event, an entry is made in the Error Log. This can be extracted later using the Display Error Log (DER) command (see Section 13.3). Although this event is not expected to occur regularly (especially if Action Routines are properly tested), the occurrence of the .CCLERROR event might indicate that the ASG Guard/ASG Guard Plus is not performing properly and should, therefore, be investigated. To insure proper processing of this event, associate it with a well-tested Action Routine.

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.CCLERROR</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example uses the default phone number to call the maintenance reporting center.

14.3.9 .CLKCHANGE Internal Event

The .CLKCHANGE alarm is generated when the internal clock of the ASG Guard/ASG Guard Plus has been changed. This alarm could be the result of changing the clock for Daylight Saving Time using the Set Date and Time (SDT) command (see Section 10.4.1).

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.CLKCHANGE</td>
<td>SNMPTRAP</td>
<td>1</td>
<td>Clock Reset</td>
</tr>
</tbody>
</table>

14.3.10 .DAILY Internal Event

This event occurs automatically each day at midnight. This event can also be used to schedule an action for some point later in the day.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DAILY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.DAILY-1</td>
<td>SCHEDULE</td>
<td>08:00 PHONHOME</td>
<td></td>
</tr>
<tr>
<td>.DAILY-2</td>
<td>CLKCHECK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this example, the routine associated with .DAILY-1 performs a daily "check-in" with the maintenance center at 8 AM. Units that do not "check-in" may have a problem that affects their ability to report alarms.

Additionally, the CLKCHECK routine associated with .DAILY-2 checks for a change from standard to daylight savings time at midnight, or vice-versa.
14.3.11 .DISKCRIT Internal Event

The RAMDISK has reached a critical level assigned in the Set Disk Parameters (SDP) menu. (See Section 7.10.)

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DISKCRIT</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.DISKCRIT-1</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.DISKCRIT-2</td>
<td>SCHEDULE 30</td>
<td>PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>

In the example above, the .DISKCRIT alarm results in the a call to the default phone number specified in the system parameters. If the alarm is not canceled, the phone number will be called again in 30 minutes.

14.3.12 .DISKFULL Internal Event

This alarm is generated when the RAMdisk is full. No additional information can be stored on the disk. If this occurs, data from host ports stored in buffer files will be lost.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DISKFULL</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.DISKFULL-1</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.DISKFULL-2</td>
<td>SCHEDULE 30</td>
<td>PAGE</td>
<td></td>
</tr>
</tbody>
</table>

In this example, the .DISKFULL alarm results in a call to the phone number set in the System Parameters (SSP) menu (see Section 9.4.2). If the alarm is not canceled with 30 minutes, a page is sent to the default pager number.

14.3.13 .DTRHIGH, .DTRLOW, .DTRHIGH.n, and .DTRLOW.n Internal Events

The .DTRLOW event occurs automatically on the high to low transition of the DTR signal on a Host port. The .n indicates the port number. This may be caused by a cable being removed from a port or by the attached equipment being switched off.

The .DTRHIGH event occurs automatically on the low to high transition of this same signal. This can be caused by attaching a cable to a port.

These events can be used to detect if the PBX or host has lost power, or if the ASG Guard/ASG Guard Plus has been disconnected from the maintenance port.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DTRLOW</td>
<td>SCHEDULE 2</td>
<td>PHONHOME</td>
<td></td>
</tr>
<tr>
<td>.DTRHIGH</td>
<td>CANCEL .DTRLOW</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
This example schedules a PHONHOME to report the alarm two minutes after DTR is lost (transitions from high to low). If DTR is re-established (DTR goes high), the .DTRHIGH alarm occurs and cancels the action PHONHOME Action Routine. Since no port number is specified, this event will occur when DTR is lost on any port.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DTRLOW.1</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example initiates a PHONHOME if the Data Terminal Ready (DTR) signal is lost only on host port 1.

**14.3.14 .HOURLY Internal Event**

This event occurs automatically at the beginning of each hour (that is, 1:00, 2:00, 3:00, etc.). Actions assigned to this event are performed every hour on the hour.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.HOURLY</td>
<td>LOGCHECK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example checks if the log buffer is approaching its limit. If that is the case, the internal event .LOGFULL is generated.

**14.3.15 .INTBATLOW Internal Event**

The status of the internal battery has changed from OK to low.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.INTBATLOW</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this example, the PHONHOME Action Routine is initiated when the internal battery is low. After the alarm is received, a technician may be sent to the site.

**14.3.16 .INTBATOK Internal Event**

The .INTBATOK alarm is generated when the status of the internal battery changes from low to OK. This indicates that the internal battery has been recharged or replaced.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.INTBATOK</td>
<td>CANCEL</td>
<td>.INTBATLOW</td>
<td></td>
</tr>
</tbody>
</table>

In the above example, the status of the internal battery has changed from low to OK, resulting in the canceling of the phone call to the maintenance center for the battery low alarm.
14.3.17 .LOGFULL Internal Event

This event is a result of the LOGCHECK Action Routine when it detects that the LOG has passed a specified capacity threshold. In order for the .LOGFULL event to occur, the LOGCHECK routine must be associated with some regularly occurring event (such as .DAILY or .HOURLY).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.LOGFULL</td>
<td>PHSYSOP</td>
<td>555-4321,3</td>
<td></td>
</tr>
</tbody>
</table>

This example initiates a call to 555-4321 and then establishes an access class 3 Sysop session. The computer at 555-4321 could be programmed to receive the Site ID, extract the LOG from the ASG Guard/ASG Guard Plus, and then issue the Clear Log History (CLH) command (see Section 13.3).

14.3.18 .MAXRETRY Internal Event

This event is generated by PHONHOME, PHIRIS, PHSYSOP, or PAGE. It will occur after the value entered for the Max. Retries system parameter is surpassed.

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MAXRETRY</td>
<td>PHONHOME</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

This example initiates a PHONHOME to Home Phone Number 2, as defined in the System Parameter table, when the maximum retry counter has been exceeded.

14.3.19 .MDMINITERR Internal Event

This alarm is generated when a modem initialization error occurs.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MDMINITERR</td>
<td>SNMPTRAP</td>
<td>1</td>
<td>Modem error</td>
</tr>
</tbody>
</table>

14.3.20 .MEMLOW Internal Event

The alarm .MEMLOW is generated on the hour if fewer than 4KB (4096 bytes) are available on the ASG Guard/ASG Guard Plus variable area.

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MEMLOW</td>
<td>PHONHOME</td>
<td></td>
<td>Memory low</td>
</tr>
</tbody>
</table>
In this example, the ASG Guard/ASG Guard Plus will call the default number specified in the System Parameters screen when the remaining space on the ASG Guard/ASG Guard Plus variable area is 4 KB or less.

**NOTE:**
*MEMLOW does not detect low memory on the RAMDISK.*

### 14.3.21 .MONTHLY Internal Event

This event occurs automatically every month at the designated time.

**Example:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MONTHLY</td>
<td>PHSYSOP</td>
<td>555-1234</td>
<td>1</td>
</tr>
</tbody>
</table>

In the example the ASG Guard/ASG Guard Plus will, once a month, phone the number specified in the parameters field and initiate an access class 1 Sysop session. The computer at 555-1234 could be programmed to receive the Site ID, request a host session and download the current configuration of the PBX to ensure that maintenance records are up to date.

### 14.3.22 .NETDOWN and .NETUP Internal Event

The .NETDOWN alarm is issued after a preset length of time during which no network activity is detected. When network activity is detected, the .NETUP alarm is issued. The determination of network up and down is based on detected traffic on the Ethernet. The time interval for non-activity ranges from 1 to 255 seconds, and can be selected by the user. To do this, enter the SNP command and select option 1 (see Section 12.3). At the Network Loss Alarm Delay Time, enter the length of time during which no network activity is detected.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.NETDOWN</td>
<td>SCHEDULE</td>
<td>5 PHONHOME</td>
<td></td>
</tr>
<tr>
<td>.NETUP</td>
<td>CANCEL</td>
<td>.NETDOWN</td>
<td></td>
</tr>
</tbody>
</table>

In this example, the alarm .NETDOWN is generated, the default number specified by the PHONHOME parameter will be called 15 minutes after the .NETDOWN alarm is received. If a .NETUP alarm occurs, the .NETDOWN alarm will be canceled.

### 14.3.23 .POWERLOW Internal Event

The .POWERLOW event is generated when the extern power connection has changed from OK to low. In the example below, the .POWERLOW event results in a call to the maintenance center.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.POWERLOW</td>
<td>PHONHOME</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>
14.3.24 .POWEROK Internal Event

The .POWEROK event is generated when the external power connection of the ASG Guard/ASG Guard Plus has changed from low to OK. This event can be generated when the power cable to the ASG Guard/ASG Guard Plus has been reconnected.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.POWERLOW</td>
<td>PHONHOME</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>.POWEROK-1</td>
<td>CANCEL</td>
<td>.POWERLOW</td>
<td></td>
</tr>
</tbody>
</table>

In the example above, the .POWEROK event results in the canceling the call to the maintenance center.

14.3.25 .POWERUP Internal Event

The .POWERUP event occurs automatically whenever the ASG Guard/ASG Guard Plus is powered up. This might indicate a new installation, recovery from a power loss, or that the unit was moved to a new location.

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.POWERUP</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example causes the ASG Guard/ASG Guard Plus to report to the maintenance center that the unit has been reset. If desired, someone can then investigate the reason for the .POWERUP event.

14.3.26 .PPPREQ Internal Event

This event is triggered when a PPP link is needed to send an SNMP trap or to send a file via FTP. It is usually associated with the phone PPP (PHPPP) Action Routine.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.PPPREQ</td>
<td>PHPPP</td>
<td>5551212</td>
<td>Create the PPP link.</td>
</tr>
</tbody>
</table>

The telephone number can be specified directly, or any of the default telephone numbers specified in the system parameters can be referenced. PHPPP assumes that there is no firewall or security on the remote access device.
14.3.27 .RTSLOW.n and .RTSHIGH.n Internal Events

The .RTSHIGH event is generated when the RS-232 RTS signal has changed from low to high. The .RTSLOW event occurs from the RS-232 RTS signal has changed from high to low. The .n indicates the port number.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.RTSLOW</td>
<td>SCHEDULE</td>
<td>2 PHONHOME</td>
<td></td>
</tr>
<tr>
<td>.RTSHIGH</td>
<td>CANCEL</td>
<td>.RTSLOW</td>
<td></td>
</tr>
</tbody>
</table>

This example schedules a PHONHOME to report the alarm two minutes after RTS is lost (transitions from high to low). If RTS is re-established (RTS goes high), the .RTSHIGH alarm occurs and cancels the action PHONHOME Action Routine. Since no port number is specified, this event will occur when RTS is lost on any port.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.RTSLOW.2</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example initiates a PHONHOME if the Ready to Transmit signal (RTS) is lost only on host port 2.

14.3.28 .S#HIGH, .S#LOW, or .S#OK Internal Event

The .S#HIGH event is generated when the 5V sensor# has changed from OK to high based on the parameters set with SSA command (see Section 10.7). The .S1LOW event is generated when the 5V sensor1 has changed from OK to low. The .S1OK event is generated when the 5V sensor1 has changed from either low or high to OK.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.S1HIGH</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.S1LOW</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.S1OK</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.S1OK-1</td>
<td>CANCEL</td>
<td>.S1LOW</td>
<td></td>
</tr>
<tr>
<td>.S1OK-2</td>
<td>CANCEL</td>
<td>.S1HIGH</td>
<td></td>
</tr>
</tbody>
</table>

In the example above, a .S1OK event cancels .S1LOW and the .S1HIGH events and all actions associated with them.
14.3.29 .TEMPHIGH

The .TEMPHIGH event occurs when the temperature being monitored crosses over from an OK threshold to a high temperature threshold. These thresholds are set by using the Set Sensor Alarms (SSA) command (see Section 10.7).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.TEMPHIGH</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.TEMPHIGH-1</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.TEMPHIGH-2</td>
<td>SCHEDULE 10 PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example activates a call to the maintenance reporting center when the .TEMPHIGH condition occurs. Unless the alarm is canceled, the maintenance center is called again in 10 minutes.

14.3.30 .TEMPLOW Internal Events

The .TEMPLOW event occurs when the temperature being monitored crosses over from an OK threshold to a low temperature threshold. These thresholds are set using the Set Sensor Alarms (SSA) command (see Section 10.7).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.TEMPLOW</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example activates a call to the maintenance reporting center when the .TEMPLOW condition occurs.

14.3.31 .TEMPOK Internal Events

The .TEMPOK event occurs when the temperature being monitored crosses over from a low temperature or high temperature threshold to an OK threshold. These thresholds are set using the Set Sensor Alarms (SSA) command (see Section 10.7).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.TEMPOK</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.TEMPOK-1</td>
<td>CANCEL .TEMPHIGH</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.TEMPOK-2</td>
<td>CANCEL .TEMPLOW</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Since the .TEMPOK can be rectified from either a high or low state, this one DOLIST will cover both situations.

14.3.32 .WEEKLY Internal Event

This event occurs automatically every week on Sunday evening at midnight.

Examples:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.WEEKLY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
<tr>
<td>.WEEKLY.2</td>
<td>SCHEDULE</td>
<td>1 08:00 PHONHOME</td>
<td></td>
</tr>
<tr>
<td>.WEEKLY.3</td>
<td>SCHEDULE</td>
<td>5 08:00 PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>

This example schedules a "check-in" with the maintenance center on Monday, and Friday of each week at 8:00 AM.
14.4 ACTION ROUTINES

14.4.1 AUXCC Action Routine
This Action Routine determines which AUX contact closure was closed when assigned to the event .RTSHIGH. It will generate .AUXCC1 if CTS is looped to RTS and .AUXCC2 if DSR is looped to RTS.

Format: AUXCC
Resource Required: None
Parameters: None

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.RTSHIGH</td>
<td>AUXCC</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NOTE: The action table MUST HAVE ENTRIES for the .AUXCC1 and .AUXCC2 events OR THEY WILL BE IGNORED!

14.4.2 CANCEL Action Routine
This Action Routine cancels a scheduled action corresponding to a particular event containing particular parameters. When multiple pending events can be canceled, the one first into the queue is canceled.

Format: CANCEL
Resource Required: None
Parameters:

ASSOCIATED EVENT, 1st Match Parameter, 2nd Match Parameter,...Nth Match parameter

Associated Event: Event mnemonic of the event to be canceled.

Parameters to be matched against Event: As many parameters as necessary may be specified. The position of a parameter represents the position in the event to be matched. Blank parameters are "wild cards". Parameters are separated by commas.

Examples:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DTRLOW</td>
<td>CANCEL</td>
<td>.DTRHIGH</td>
<td></td>
</tr>
</tbody>
</table>
This example will cancel the action associated with the event .DTRLOW.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTA007</td>
<td>CANCEL</td>
<td>DTA005, ^2</td>
<td></td>
</tr>
</tbody>
</table>

This example will cancel the action associated with event DTA005 if the second parameter in the DTA007 message is equal to the second parameter in the message associated with this action.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTA007</td>
<td>CANCEL</td>
<td>DTA005, , 87</td>
<td></td>
</tr>
</tbody>
</table>

This example will cancel the action associated with event "DTA007" if the third parameter in the DTA007 message equals 87.

14.4.3 CLKAHEAD and CLKBACK Action Routines

The CLKAHEAD Action Routine advances the ASG Guard/ASG Guard Plus time by one hour.

The CLKBACK Action Routine sets the ASG Guard/ASG Guard Plus time back by one hour.

**NOTE:**
The CLKAHEAD and CLKBACK routines also generate the internal event .CLKCHANGE. These routines are generally executed as a result of CLKCHECK and are not called directly.

14.4.4 CLKCHECK Action Routine

The CLKCHECK Action Routine checks to see if the current date is equal to the first Sunday in April or the last Sunday in October. If it is case, the ASG Guard/ASG Guard Plus will schedule a CLKAHEAD or CLKBACK routine for 2 am.

Attaching this Action Routine to the event .DAILY will take care of standard-to-daylight and daylight-to-standard conversion.

**Format:**
CLKCHECK

**Resource Required:** None

**Parameters:** None

**Example:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DAILY</td>
<td>CLKCHECK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
14.4.5 DOLIST Action Routine

The DOLIST Action Routine causes a list of actions to be performed. The ASG Guard/ASG Guard Plus scans the Action Table looking for event mnemonics that match or partially match parameter one.

**Format:**

DOLIST Name of list

**Parameters:**

name of list

The parameter is an alarm match string that is used as a criterion to search the action table for actions to be performed. If it is omitted, then the instigating event, itself, is used as the match criterion.

**Examples:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.WEEKLY</td>
<td>DOLIST</td>
<td>.OOPS</td>
<td></td>
</tr>
</tbody>
</table>

This example, on a weekly basis, performs all actions relating to events that begin with the event .OOPS.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DAILY</td>
<td>DOLIST</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example performs all actions whose events match the instigating event. In the example, if the Action Table contains entries for .DAILY-1 ((.DAILY-XX, then the actions associated with those events will be performed.

14.4.6 LOG Action Routine

The LOG Action Routine creates a log entry describing the event. The ASG Guard/ASG Guard Plus takes no further action.

**Format:**

LOG

**Resource Required:**

None

**Parameters:**

None

**Example:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.CDR AREA1</td>
<td>LOG</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example logs the event .CDR AREA1 into the ASG Guard/ASG Guard Plus log history file.
14.4.7 LOGCHECK Action Routine

The LOGCHECK Action Routine checks to see if the log buffer has reached a specified threshold. If the log has exceeded this threshold then the event .LOGFULL is generated.

**Format:**

LOGCHECK

**Parameters:**

Percent full threshold (Default is 80)

**Examples:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DAILY</td>
<td>LOGCHECK</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

In this example, the log buffer is checked to see if its threshold of 80% has been exceeded.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.DAILY</td>
<td>LOGCHECK</td>
<td>50</td>
<td></td>
</tr>
</tbody>
</table>

This example checks if the log buffer has exceeded a threshold of 50%.

**NOTE:**

*The event itself (.DAILY in this example) will generate log data, thereby tending to fill the log.*

14.4.8 NOACTION Action Routine

The NOACTION Action Routine creates an "Event: " log entry, but otherwise does nothing.

**Example:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.LOGI</td>
<td>NOACTION</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
14.4.9 PAGE Action Routine

The PAGE Action Routine calls a numeric pager (beeper) and delivers a numeric message.

Format: 

```
PAGE PAGER PHONE NUMBER, Message
```

Resource Required: 

Modem

Parameters: 

- **Pager Phone Number** - Phone number of pager (optional)
- **Message** - Message to be delivered (optional)

If either parameter is omitted, the default value (system parameter) will be used. Refer to the Set System Parameters (SSP) Command in Chapter 9, Systems Functions. Pager dialing and message delivery are controlled via the Pager Dial String (modem parameter). Refer to the Set Modem Port Parameters (SM) Command (Section 5.3).

**NOTE:**

"@" waits for 5 seconds of silence before transmitting. If your pager system will not support this, modify the string to use commas (fixed delay period) instead. When setting up for the "PAGE" action routine or setting up a user for pager authentication, the ASG Guard/ASG Guard Plus uses the modem pager template in the modem parameters section. Issue a "SM command" and change the Pager command. The correct settings depend on the pager type and the delays from that particular site. Some specific examples:

**Straight numeric pager**

```
ATDT ### @ MSG ;|
```

or

```
ATDT ###,,,,, MSG ;|
```

**Skytel pager with direct 1800 number access:**

```
ATDT ###,,,,1#,MSG##;|
```

**Skytel digital pager without direct 1800 access:**

```
ATDT 18007597243,,,,#,MSG## ;|
```

**Skytel text pager with direct 1800 access, but need a 9 to get an outside line:**

```
ATDT 9,###,,,,,1#,MSG## ;|
```

The way to determine the correct number of commas needed is to dial the number manually. Count how many seconds it takes for the pager service to answer, and how many seconds until the pager system drops the call if nothing is entered. Split the difference and figure the correct number of commas when the comma is set to 2 second intervals. For example, if the counts are 7 seconds, and 12 seconds respectively, set the commas for 9.5 seconds, round up to 10 seconds, and divide by 2 seconds/comma = 5 (five commas).
Examples:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.AUTHFAIL</td>
<td>PAGE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example calls a pager at the default number, when an authorization failure occurs, and delivers the default message to the pager.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BAT48LOW</td>
<td>PAGE</td>
<td>5551324,9990001</td>
<td></td>
</tr>
</tbody>
</table>

This example calls a pager at the number 555-1324 and delivers the message "9990001" when the battery voltage falls below the set limit.

14.4.10 PHIRIS Action Routine

The PHIRIS Action Routine places a call to the IRISSM alarm collection package and delivers the alarm condition.

Format: PHIRIS

Resource Required: Modem

Parameters:

- phone number
  - 1 to 3 - For home phone number 1, 2, or 3 (from system parameters)
  - or
  - Phone Number - Phone number to dial (optional)

Examples:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERR005</td>
<td>PHIRIS</td>
<td></td>
<td>C\ERR005</td>
</tr>
</tbody>
</table>

This example places a call to IRIS at Home Phone Number 1 (default) when the external event ERR005 occurs.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BAT48LOW</td>
<td>PHIRIS</td>
<td>2</td>
<td>C\BATTERY LOW</td>
</tr>
</tbody>
</table>

This example places a call to IRIS at Home Phone Number 2 when the .BAT48LOW event occurs.
### Events and Action Routines

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTA005</td>
<td>PHIRIS</td>
<td>xxxxxxxxx</td>
<td>C'digit trunk</td>
</tr>
</tbody>
</table>

This example telephones IRIS at phone number xxx-xxx-xxxx (where x is a valid digit) when the event external event DTA005 occurs.

The PHIRIS Action Routine requires a comment entry starting with either C\ or M\ which represents the criticality of the alarm. The remainder of the field is the alarm comment.

### 14.4.11 PHONHOME Action Routine

The PHONHOME Action Routine places a call to a specified number and delivers a ASG Guard/ASG Guard Plus alarm message when the call is complete.

**Format:** PHONHOME

**Resource Required:** Modem

**Parameters:**
- **phone number**
  - **1 to 3** - For home phone number 1, 2, or 3 (from system parameters)
  - or
  - **Phone Number to call** - Phone number to call. If omitted, Home Phone Number 1 is used.

**Examples:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.HOURLY-2</td>
<td>PHONHOME</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This example calls Home Phone Number 1 (default) when the .HOURLY-2 internal event occurs.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTI030</td>
<td>PHONHOME</td>
<td>xxxxxxxxx</td>
<td>TRUNK DOWN</td>
</tr>
</tbody>
</table>

This example places a call to phone number xxxxxxxxx (where x is a valid digit) when the external event DTI030 occurs.
14.4.12 PHPPP Action Routine

The PHPPP Action Routine initiates a demand-dial PPP link.

Format: PHPPP
Resource required: Modem
Parameters: phone number

1 - Phone number to dial (1, 2, or 3 are home numbers).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.PPPREQ</td>
<td>PHPPP</td>
<td>5551212</td>
<td></td>
</tr>
</tbody>
</table>

The PHPPP establishes a PPP link to a remote network. The TCP/IP applications can then be executed.

14.4.13 PHSYSOP Action Routine

The PHSYSOP Action Routine is the same as PHONHOME except at the end of the report, the remote terminal is placed in a Sysop session as user MDM_Default.

Format: PHYSOP PHONE NUMBER TO CALL
Resource Required: Modem
Parameters: phone number, access class

1 to 3 - For home phone number 1, 2, or 3 (from system parameters)
or
Phone Number to call - Phone number to call. If omitted, Home Phone Number 1 is used.
Access class of Sysop session - Defaults to 3 (Sysop3). May be specified as 1 (Sysop 1), 2 (Sysop 2), 3 (Sysop 3), or 4 (Master).

Examples:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.MAXRETRY</td>
<td>PHSYSOP</td>
<td>5551212, 2</td>
<td></td>
</tr>
</tbody>
</table>

This example telephones the Sysop at 555-1212 and places the terminal in a Level 2 Sysop session when the .MAXRETRY internal event occurs.
Alarm/Event | Action Routine | Parameters | Comments
--- | --- | --- | ---
DTI030 | PHSYSOP | 3,1 | 

This example phones the Sysop at Phone Home Number 3 and places the terminal in a Level 1 Sysop session when the DTI030 external event occurs.

### 14.4.14 REMINIT Action Routine

The REMINIT Action Routine performs the Remote Initialization function. REMINIT is usually performed as the result of the Schedule Action Item (SAI) command or a SIT inserted into the TAG port at power up. Prior to phoning home for initialization, the Comment field, up to @, is put into the Site ID, and the Comment field, after @), is put into the Unit Phone number field in the system parameters. If the Site ID and Phone number are not to be updated, then the comment field must be left blank.

REMINIT also schedules a repeat execution five minutes after the first to ensure that a retry is performed if the initialization transfer is aborted before completion.

**Format:**

REMINIT

**Resource Required:**

Modem

**Parameters:**

- phone number
  - 1 to 3 - For home phone number 1, 2, or 3 (from system parameters)
  - or
  - **Phone Number** - Phone number to call. If omitted, Home Phone Number 1 is used.

**Example:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>POWERUP</td>
<td>REMINIT</td>
<td>5551212,4 .SITE442@6667854</td>
<td></td>
</tr>
</tbody>
</table>

This example performs a remote initialization of the ASG Guard/ASG Guard Plus located by using phone number 555-1212. The ASG Guard/ASG Guard Plus calls in as a master level access class. Included in the header of the call are a site ID (SITE442) and a site phone number (6667854).
14.4.15 RESRELAY Action Routine

This Action Routine is used to reset the specified relay, thereby turning off the external device attached to the N/O contact and/or turning on the device attached to the N/C contact.

When this Action Routine occurs, the common terminal is switched from the normally open contact (N/O) on the relay(s) specified to the normally closed (N/C) contact.

![Diagram of relay contacts (N/O, N/C, COMMON, CONTROL)]

Figure 14-1. Environmental Manager (RESRELAY Condition)

Format: RESRELAY

Resource Required: None

Parameters: relay number

- 1 - Resets Relay 1 (This relay is always reset on power-up.)
- 2 - Resets Relay 2
- ALL - Resets relays

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.TEMPLOW</td>
<td>RESRELAY</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

This example sets the contacts of Relay 2 to the N/C condition when the internal event .TEMPLOW occurs.
14.4.16 SCHEDULE Action Routine

The SCHEDULE Action Routine schedules another Action Routine to be performed now, or at some later date or time.

**Format:** SCHEDULE

**Resource Required:** None

**Parameters:**

- **Date or "AM"** (optional) - Either a date in the format mm/dd/yy, or a number of days from today. If specified as a number of days, the Time parameter must also be included.

  *If "AM" is specified, and the current time is greater than the "Start of Overnight Period" in the system parameters, the call is scheduled for the "AM Report Time." If the current time is between the AM Report Time and the Start of Overnight Period, then the action is scheduled for now.*

  - If "AM" is specified, omit the Time parameter.
  - If Date is omitted, action is scheduled for this day.

- **Time** (optional)

  *Either a time in the format hh:mm, or a number of minutes from the current time.*

**Event associated with action to be scheduled:** - Name of Action Routine to be scheduled.

**Action Routine Parameters:** - Parameters to be passed to scheduled Action Routine.

**Examples:**

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CED063</td>
<td>SCHEDULE</td>
<td>AM PHONHOME</td>
<td></td>
</tr>
</tbody>
</table>

This example schedules a PHONHOME for now or the next AM report when the external event CED063 occurs.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CED063</td>
<td>SCHEDULE</td>
<td>15 PHONHOME 5551212</td>
<td></td>
</tr>
</tbody>
</table>

This example schedules a PHONHOME to telephone number 555-1212 for 15 minutes from now.

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>CED063</td>
<td>SCHEDULE</td>
<td>23:00 SETHP 3</td>
<td></td>
</tr>
</tbody>
</table>

This example sets the Host Processing Flag to 3 at 11 PM tonight.
### Events and Action Routines

**Alarm/Event | Action Routine | Parameters | Comments**
---|---|---|---|
CED063 | SCHEDULE | 20 PHYSYSOP 2,3 |  

This example schedules a PHONHOME for this time two days from now using Phone Home Number 2, and then establishes a Level 3 Sysop session.

**Alarm/Event | Action Routine | Parameters | Comments**
---|---|---|---|
CED063 | SCHEDULE | 07/01/96 12:00 PHONHOME |  

This example schedules a PHONHOME for 12:00 on July 1, 1996.

**Alarm/Event | Action Routine | Parameters | Comments**
---|---|---|---|
CED063 | SCHEDULE | 1 18:00 DOLIST.SPECIAL |  

This example schedules a DOLIST for 6 PM tomorrow.

### 14.4.17 SETHP Action Routine

The SETHP Action Routine changes the setting of the Host Processing Flag (see the SHP System Functions command, [Section 10.4.1](#)).

**Format:**
SETHP PROCESSING FLAG VALUE

**Resource Required:** None

**Parameters:** Host Processing Flag Value - 1, 2, 3, or 5

**Example:**

**Alarm/Event | Action Routine | Parameters | Comments**
---|---|---|---|
.CCLERROR | SETHP | 3 |  

This example disables all Action Routines, including those of the ASG Guard/ASG Guard Plus.
14.4.18 SETRELAY Action Routine

This Action Routine is used to set the specified relay, thereby turning on the external device attached to the N/O contact and/or turning off the device attached to the N/C contact.

When this Action Routine occurs, the common terminal is switched from the normally closed contact (N/C) on the relay(s) specified to the normally open (N/O) contact,

Format: \( \text{SETRELAY RELAY NUMBER} \)

Resource Required: None

![Diagram of relay contacts](image)

Figure 14-2. Environmental Manager Relay (SETRELAY Condition)

Parameters:

1 - Sets Relay 1 (This relay is always reset on power-up.)
2 - Sets Relay 2
ALL - Sets both relays

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>.BATOK</td>
<td>SETRELAY</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

This example sets the contacts of Relay 2 to the N/O condition when the internal event .BATOK occurs.
14.4.19 SNMPTRAP
Sends an SNMP trap to remote managers through the Ethernet or PPP link.

Parameters:

1 - Sets trap level (1-10) This parameter is the enterprise specific trap ID and depends on the trap format (Nortel or Standard).

Example:

<table>
<thead>
<tr>
<th>Alarm/Event</th>
<th>Action Routine</th>
<th>Parameters</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>ERRORA21</td>
<td>SNMPTRAP</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
A. ASG Key User’s Guide

A.1 Overview

The Access Security Gateway (ASG) Key is a hand-held hardware device that enables you to log into a Lucent Technologies’ system (such as DEFINITY® Enterprise Communications Server and INTUITY® system) that is protected by the Access Security Gateway family of security products. Even though you have a valid login for the Lucent system, you will be unable to access the system without using the ASG Key.

![Access Security Gateway Key](image)

The ASG system that protects the Lucent system provides a random seven-digit “Challenge” every time you attempt to access the system. The ASG system expects you to enter the corresponding “Response” to the Challenge. The ASG Key provides the Response that the ASG system expects. To receive the valid Response, you must first enter your PIN, and then enter the seven-digit Challenge into the ASG Key and press the ON button. The ASG Key displays the Response that the ASG system expects. Provided that you used a valid login ID for the Lucent system, entered the Challenge correctly into the ASG Key, and entered the corresponding Response correctly into the Lucent system, you will gain access to the Lucent system.

To use the ASG Key to enter the ASG system and access a Lucent system, you must know a valid login ID for the Lucent system and your Personal Identification Number (PIN) for the ASG Key. The Lucent system login ID identifies you to the Lucent system as a user. The PIN is your private number for use with the ASG Key. The ASG Key, in conjunction with your PIN and a valid Lucent system login ID, enables you to identify yourself as an authorized user of the Lucent system.
A.2 Security Alert

The ASG Key must be kept secure at all times. You must take all safeguards against losing the ASG Key.

You are fully responsible and accountable for the:

- Whereabouts of your ASG Key
- Appropriate use of your ASG Key
- Return of your ASG Key when you no longer need it

In case you lose or misplace your ASG Key, it is extremely important to notify your ASG Key Distribution Coordinator as soon as possible.

For security reasons, never give your PIN to anyone. Memorize the number. Do not record the number in any place that can be easily accessed. It is recommended that your PIN contain the maximum allowable digits. Change your PIN regularly and do not recycle old ones.

Your PIN should be hard to guess and should not contain:

- All the same numbers (for example, 8888)
- Sequential numbers (for example, 4321)
- Digit strings associated with you, including names, birthdays, telephone numbers, or social security number

Use a well distributed PIN (for example, 1840 or 0517).

You must not share your ASG Key with anybody else unless approved by your ASG Key Distribution Coordinator (that is, the person from whom you received your ASG Key).

Note that if you forget your PIN, the ASG Key cannot be used or reprogrammed. You must exchange it for a new key. Contact your ASG Key Distribution Coordinator.

A.3 Setting Up the ASG Key

You must perform this procedure before you can start using the ASG Key. You will only need to perform this procedure once unless the secret key in the product is changed. Then, you must repeat this procedure.

Before performing this procedure, you must know the 20-digit secret key. To get the secret key, contact the System Administrator in your company who is responsible for entering the secret key into the ASG Guard.

To set up the ASG Key:

1. Press the ON button on the ASG Key.
2. Enter the default PIN (1234) and press the ON button.
3. Enter any seven-digit number (for example, 1234567) and press the ON button.
   A new seven-digit number is displayed.
4. Press the Menu button three times.
   The ASG Key displays INIT KEYS.
5. Press the ON button.
   The ASG Key displays DATA 2.
6. Enter the first eight digits of the secret key and press the ON button.
   The ASG Key displays **DATA 3**.
7. Enter the second eight digits of the secret key and press the ON button.
   The ASG Key displays **DATA 4**.
8. Enter the last four digits of the secret key and press the ON button.
   The ASG Key displays **COMPLETE**.
9. Change the default PIN by performing the procedures in "Changing Your Pin."

### A.4 Using the ASG Key

**To use the ASG Key:**

1. Connect to the Lucent system (such as a DEFINITY or INTUITY system) you want to access via the appropriate interface (for example, your PC or laptop).
2. At the **LOGIN:** prompt from the Lucent system, enter a valid login ID for the Lucent system.
   The system verifies your login ID and then displays the **CHALLENGE:** prompt and a seven-digit Challenge.
3. Press the ON button on the ASG Key.
4. Enter your PIN and press the ON button.
5. Enter the seven-digit Challenge into the ASG Key and press the ON button.
   The ASG Key displays a seven-digit Response.
6. Enter the seven-digit Response into the Lucent system.
   If you entered the PIN, Challenge, and Response correctly, you will gain access to the Lucent system. The ASG Key will turn off automatically in 30 seconds.
   If you entered an incorrect or invalid PIN, the ASG Key displays **ERROR**. If you entered the Challenge or the Response incorrectly, the Lucent system displays **INCORRECT LOGIN**.

### A.5 Changing Your PIN

The PIN is a four-digit to eight-digit code that you must enter to use the ASG Key. If you enter an incorrect PIN, you will be unable to generate correct Responses to any Challenges issued by the ASG system.

**To change your PIN:**

1. Press the ON button on the ASG Key.
2. Enter your PIN and press the ON button. The default PIN is 1234.
3. Enter any seven-digit number (for example, 1234567) and press the ON button.
4. Press the Menu button.
   The ASG Key displays **CHANGE PIN**.
5. Press the ON button.
   The ASG Key displays **NEW PIN**.
6. Enter your new PIN and press the ON button. (If you do not want to change the PIN, press the Menu button to exit the Change PIN procedure.)

The ASG Key displays **CONFIRM**.

7. Re-enter the new PIN and press the ON button.

The ASG Key displays **COMPLETE**. The ASG Key will turn off automatically in 30 seconds.

### A.6 Viewing the Serial Number of the ASG Key

Each ASG Key has a unique serial number. To view the serial number for your ASG Key:

1. Press the ON button on the ASG Key.
2. Enter your PIN and press the ON button.
3. Enter any seven-digit number (for example, 1234567) and press the ON button.
4. Press the Menu button two times.

The ASG Key displays **VIEW SN**.

5. Press the ON button.

The ASG Key displays its serial number.

### A.7 Replacing the Battery

When the battery in the ASG Key needs to be replaced, the ASG Key display will not turn on or the low battery icon will appear in the upper right-hand corner of the display:

![Low Battery Icon]

The ASG Key requires a single Sony CR2025 3 Volt Lithium coin cell battery.

To replace the battery:

1. Make sure the ASG Key is off.
2. Locate the battery compartment on the back of the ASG Key. The battery compartment cover is fastened by a single screw.
3. Remove the cover of the battery compartment.
4. Remove the old battery.
5. Insert the new battery into the holder with the positive (+) side facing the front (display side) of the ASG Key.
6. Place the battery compartment into the ASG Key, and then fasten the battery compartment with the screw.
7. Press the ON button on the ASG Key to make sure the ASG Key works properly.
## B. Port Default Settings

### B.1 Modem Port Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modem Number</td>
<td>1</td>
</tr>
<tr>
<td>Baud Rate Settings:</td>
<td></td>
</tr>
<tr>
<td>Modem Control Strings</td>
<td>19200</td>
</tr>
<tr>
<td>User Session</td>
<td>CONNECT n</td>
</tr>
<tr>
<td>Char. Length / Parity</td>
<td>8 / None</td>
</tr>
<tr>
<td>Terminal Emulation</td>
<td>TTY</td>
</tr>
<tr>
<td>Sysop Idle Timer</td>
<td>None</td>
</tr>
<tr>
<td>Host Session Idle Timer</td>
<td>None</td>
</tr>
<tr>
<td>Host Session Disconnect on Ctrl+A</td>
<td>Yes</td>
</tr>
<tr>
<td>Modem Control Strings (Use '</td>
<td>' for ENTER; '~' for 1 second delay)</td>
</tr>
<tr>
<td>Setup</td>
<td>~AT &amp;F E0 &amp;C1 &amp;D2 S0=0 S2=38</td>
</tr>
<tr>
<td>Setup (continued)</td>
<td></td>
</tr>
<tr>
<td>Answer</td>
<td>ATA</td>
</tr>
<tr>
<td>Hang Up</td>
<td>~+++<del>AT</del>ATS0=0 H0</td>
</tr>
<tr>
<td>Dial Strings (Use '###' for Phone No., 'MSG' for Pager Message)</td>
<td></td>
</tr>
<tr>
<td>Modem</td>
<td>ATDT ###</td>
</tr>
<tr>
<td>Pager</td>
<td>ATDT ### @ MSG ;</td>
</tr>
</tbody>
</table>


B.2 AUX Port Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baud Rate</td>
<td>9600</td>
</tr>
<tr>
<td>Char. Length / Parity</td>
<td>8 / None</td>
</tr>
<tr>
<td>Terminal Emulation</td>
<td>TTY</td>
</tr>
<tr>
<td>Default Access Class</td>
<td>CMaster</td>
</tr>
<tr>
<td>Output While Port Idle</td>
<td>Log Data</td>
</tr>
<tr>
<td>Sysop Idle Timer</td>
<td>None</td>
</tr>
<tr>
<td>Host Session Idle Timer</td>
<td>None</td>
</tr>
<tr>
<td>Host Session Disconnect on Ctrl+A</td>
<td>Yes</td>
</tr>
</tbody>
</table>

B.3 Host Port Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Port Number</td>
<td>1</td>
</tr>
<tr>
<td>Restore Factory Defaults ?</td>
<td>No</td>
</tr>
<tr>
<td>-- Host 1:</td>
<td></td>
</tr>
<tr>
<td>Host Name</td>
<td>HOST1</td>
</tr>
<tr>
<td>Baud Rate Setting</td>
<td>9600</td>
</tr>
<tr>
<td>Character Length / Parity</td>
<td>8 / None</td>
</tr>
<tr>
<td>Alarm Filter</td>
<td>None</td>
</tr>
<tr>
<td>Force CD/DSR High</td>
<td>Yes</td>
</tr>
<tr>
<td>Flow Control</td>
<td>None</td>
</tr>
<tr>
<td>-- Automatic Buffering --</td>
<td></td>
</tr>
<tr>
<td>Enable Automatic Buffering?</td>
<td>No</td>
</tr>
<tr>
<td>Compress closed buffer files?</td>
<td>No</td>
</tr>
<tr>
<td>Auto Switch: (Enter 0 to disable)</td>
<td></td>
</tr>
<tr>
<td>When CURRENT File exceeds 'n' KB</td>
<td>50</td>
</tr>
<tr>
<td>Every 'n' Hours</td>
<td>24</td>
</tr>
<tr>
<td>Synchronize at what hour (0-23)</td>
<td>0</td>
</tr>
</tbody>
</table>
### B.4 Network Initialization Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Group</td>
<td>--&gt;1</td>
</tr>
<tr>
<td>Restore Factory Defaults?</td>
<td>No</td>
</tr>
<tr>
<td>Start Network on Power-up?</td>
<td>No</td>
</tr>
<tr>
<td>IP Address (nnn.nnn.nnn.nnn)</td>
<td>192.9.200.2</td>
</tr>
<tr>
<td>PPP Address (nnn.nnn.nnn.nnn)</td>
<td>192.9.200.3</td>
</tr>
<tr>
<td>Subnet Mask (nnn.nnn.nnn.nnn)</td>
<td>255.255.255.0</td>
</tr>
<tr>
<td>Default Gateway (nnn.nnn.nnn.nnn)</td>
<td></td>
</tr>
<tr>
<td>Enable RIP?</td>
<td>Yes</td>
</tr>
<tr>
<td>Network-Loss Alarm Delay Time</td>
<td>60</td>
</tr>
</tbody>
</table>

### B.5 SNMP Manager Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP link needed for trap?</td>
<td>No</td>
</tr>
<tr>
<td>Trap format</td>
<td>Standard</td>
</tr>
<tr>
<td>SNMP Community Name</td>
<td>SNMP_trap</td>
</tr>
<tr>
<td>Manager 1</td>
<td></td>
</tr>
<tr>
<td>Manager 2</td>
<td></td>
</tr>
<tr>
<td>Manager 3</td>
<td></td>
</tr>
<tr>
<td>Manager 4</td>
<td></td>
</tr>
<tr>
<td>Manager 5</td>
<td></td>
</tr>
</tbody>
</table>
B.6 FTP Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPP link needed for ftp?</td>
<td>No</td>
</tr>
<tr>
<td>Ftp service type</td>
<td>None</td>
</tr>
<tr>
<td>-- Server 1 (default) --</td>
<td></td>
</tr>
<tr>
<td>IP address (nnn.nnn.nnn.nnn)</td>
<td></td>
</tr>
<tr>
<td>User name</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Upload Directory</td>
<td>.</td>
</tr>
<tr>
<td>-- Server 2 --</td>
<td></td>
</tr>
<tr>
<td>User name</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td></td>
</tr>
<tr>
<td>Upload Directory</td>
<td>.</td>
</tr>
</tbody>
</table>
C. Configuration Files

C.1 Overview

Each ASG Guard/ASG Guard Plus has a configuration file that specifies the parameters of the ASG Guard/ASG Guard Plus and determines how the unit operates. A configuration file includes the Action Table; User Action Routines; System Parameters; Parameters of the Aux, Modem, and Host Ports; and Text Pager Messages. Configuration files can be created on the ASG Guard/ASG Guard Plus or off-line on an administrative Personal Computer (PC). Typically in ASCII format, a configuration file can be transferred between the administration PC and the ASG Guard/ASG Guard Plus. This procedure can be used to replicate a configuration across multiple ASG Guards. A configuration file can be loaded (that is, configured) into the ASG Guard/ASG Guard Plus with the CONFIG command described in Sections C.2 and C.3 of this Appendix. Once an ASG Guard/ASG Guard Plus has the parameters set, they can be saved in a file on a remote Administrative PC, on the RAM disk of the ASG Guard/ASG Guard Plus, or printed to the screen. The capabilities to save the configuration data to a file or print to a screen are provided via the DUMP and DUMPF commands and the procedures for using these commands are described in Sections C.4 and C.5 of this Appendix.

A Customer Key is used to encrypt the Customer User Table when it is stored inside the ASG Guard/ASG Guard Plus and when the Customer User Table is exported. Section C.6 describes the procedure for changing the Customer Key.

The ASG Guard/ASG Guard Plus provides capabilities to import and export the Customer User Table. These capabilities are provided via the CCONFIG, CDUMP, and CDUMPF commands and the procedures for using these commands are described in Section C.7.

Since the ASG Guard/ASG Guard Plus configuration file and the Customer User Table are stored in an ASCII file format, programs such as Notepad or Wordpad can be used to edit or create these files. When using a Word-processing program such as Microsoft Word the configuration file must be saved in text only file format.

Prior to using the commands in this section, the user should understand how to use a PC communication package to send and receive files using the XMODEM and ASCII file transfer protocols.
C.2 CONFIG Procedure With a Remote Configuration File

C.2.1 Overview

A configuration file may be sent to the ASG Guard/ASG Guard Plus from a PC or to a PC from the ASG Guard/ASG Guard Plus. The CONFIG command is used to import the file (that is, load the configuration data), and the DUMP and DUMPF commands are used to create a configuration file. The CONFIG command allows a user to import a configuration into an ASG Guard/ASG Guard Plus from a file on the local RAM disk, over a direct connection to the Aux port, over phone lines, or via the network. The procedure in this section describes how to import a configuration from a configuration file on a remote PC using ASCII file transfer.

IMPORTANT NOTE: The most reliable way to configure an ASG Guard/ASG Guard Plus is to use an error-correcting file transfer protocol (such as XMODEM or ftp) to transfer the CONFIG file to the RAM disk of the ASG Guard/ASG Guard Plus. Once the file is on the RAM disk, follow the procedure in Section C.3.3 to CONFIG the ASG Guard/ASG Guard Plus.

C.2.2 Materials

- PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
- Communication Package (such as Procomm Plus or HyperTerminal)

C.2.3 CONFIG Procedure With ASCII File Transfer

1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. Type in the command CONFIG and press the ENTER key.
   At this point the message --- Upload Configuration Details --- will appear.
3. Use the ASCII or text file transfer procedure in your communication package to send the configuration file to the ASG Guard/ASG Guard Plus.
   
   NOTE: Set flow control to software (XON/XOFF)! Configurations can be corrupted if flow control is set incorrectly. If you encounter difficulties, follow the procedure for a stored CONFIG in Section C.3.3.
4. At the end of the CONFIG process, the ASG Guard/ASG Guard Plus will respond with the message:
   
   Upload Configuration Details - O.K. (Refer to the following screen.)

```
Site123> CONFIG

--- Upload Configuration Details ---

; Action Routines

Begin ACTROUT
End ACTROUT

10/05/98 11:35:12 [AUX] Upload Configuration Details - O.K.
Site123>
```

Screen C-1. CONFIG Command
C.3 CONFIG Procedure With a Configuration File on the Local RAM Disk

C.3.1 Overview
A configuration file may be sent to the ASG Guard/ASG Guard Plus from a PC or to a PC from the ASG Guard/ASG Guard Plus. The CONFIG command is used to import the file (that is, load the configuration data), and the DUMP and DUMPF commands are used to create a configuration file. The CONFIG command allows a user to import a configuration into an ASG Guard/ASG Guard Plus from a file on the local RAM disk, over a direct connection to the Aux port, over phone lines, or via the network. The procedure in this section describes how to import a configuration file that is stored on the local RAM disk.

C.3.2 Materials
- PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
- Communication Package (Procomm Plus or CrossTalk)

C.3.3 CONFIG Procedure
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. If the configuration file is not stored on the local RAM disk, transfer the configuration file from the PC to the RAM disk using the RCV command (refer to Section 7.7 for more details on this procedure).
3. To configure the ASG Guard/ASG Guard Plus, type `CONFIG filename` at the system prompt and press the ENTER key. The path where the file is saved must be included in the command string or the disk pointer must be in the subdirectory where the file is saved for successful execution of the CONFIG command.

```plaintext
> RCV TEST.CFG
--- Receive File ---
Receiving XMODEM - File: \TEST.CFG
CCCC
--- Receive Complete ---
03/01/99 11:51:16 E2E3 [AUX] \TEST.CFG: Receive Complete
Ser123>CONFIG TEST.CFG
--- Upload Configuration Details ---
Begin SYSPARS
End SYSPARS
; Disk Parameters
Begin SYSPARS
End SYSPARS
Begin ACTROUT
End ACTROUT
03/01/99 11:51:41 8601 [AUX] Upload Configuration Details - O.K.
```

Screen C-2. CONFIG Command from the RAM Disk
C.4 DUMP Procedures

C.4.1 Overview
The DUMP command allows the user to view or back up the configuration of an ASG Guard/ASG Guard Plus with a direct connection via the AUX port, over phone lines, or via the network port. This section describes a procedure for viewing the configuration on a terminal and a procedure for creating a configuration file on a PC.

C.4.2 Materials
- PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
- Communication Package (such as Procomm Plus or Telnet session)

C.4.3 DUMP Procedure for Viewing the Configuration at the Terminal Screen
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. Type in the command DUMP and press the ENTER key.
   At this point the banner "--- Dump Config Details ---" will appear, and a list of system tables and system parameters will be displayed. To view a subset of the system tables/parameters, press the Control (CTRL) key and the letter "X" at the same time to delete the entire list. Type in those sections desired and press the ENTER key.
3. The banner 'Press ENTER when ready to receive Configuration Dump (CTRL+A to Abort)' will appear. Pressing the ENTER key will then "DUMP" the selected configuration to the screen for viewing.

Site123> DUMP

--- Dump Configuration Details ---
Dump List ATAB

Press ENTER when ready to receive Configuration Dump (CTRL+A to Abort)

; Action Table
ACTIONTAB
////
END

03/01/99 12:04:41 A4EA [AUX] DUMP: ATAB
03/01/99 12:04:47 E54C [AUX] DUMP: Complete
Site123>

Screen C-3. DUMP Command for viewing the configuration at the PC terminal window.
C.4.4 DUMP Procedure for Saving the Configuration to a File on a PC

1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.

2. Type in the command DUMP and press the ENTER key.

   At this point the banner --- Dump Config Details --- will appear, and a list of system tables and system parameters will be displayed. To save a subset of the system tables and parameters, press the Control (CTRL) key and the letter "X" at the same time to delete the entire list. Types in those sections desired and press the ENTER key.

3. The banner 'Press ENTER when ready to receive Configuration Dump (CTRL+A to Abort)' will appear. DO NOT PRESS THE ENTER KEY. Instead, use the ASCII transfer procedure in the communication program to receive the configuration file from the ASG Guard/ASG Guard Plus. If required by your communications package, initiate the transfer by sending an ENTER.

4. When the DUMP is complete, terminate the ASCII transfer from the communication program, if necessary. Press ENTER at the terminal window to get back to the system prompt.

5. To verify that the file was saved correctly, open the file with a text editor such as “Notepad” or “Wordpad.” The file should appear to have appropriate programming structure (look for extraneous characters) and be terminated with the word “END.”

```
Site123>DUMP

--- Dump Config. Details ---
Dump List        ATAB

Press ENTER when ready to receive Configuration Dump (CTRL+A to Abort)

03/01/99 12:49:10 48AG [AUX] DUMP: ATAB
03/01/99 12:49:26 49FC [AUX] DUMP: Complete
Site123>
```

Screen C-4. DUMP Command for Saving the Configuration to a File on a PC
C.5 DUMPF Procedure

C.5.1 Overview
The DUMPF command is similar to the DUMP command in that it creates a configuration file. However, the DUMPF command copies the configuration to a local file on the RAM disk of an ASG Guard or ASG Guard Plus.

C.5.2 Materials
- PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
- Communication Package (such as Procomm Plus or Telnet session)

C.5.3 Procedure
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. Type in the command DUMPF and press the ENTER key. At this point the banner ‘--- Dump Config Details to File ---’ and the prompt ‘File name:’ will appear.
3. Enter a file name at the “File Name” prompt and press the ENTER key to see a list of the system tables and system parameters. To save a subset of the system tables and parameters, press the Control (CTRL) key and the letter “X” at the same time to delete the entire list. Types in those sections desired and press the ENTER key to save the file to the RAM disk.
4. The transfer will take only a few seconds. To verify the transfer was successful, type ‘VIEW filename’ at the system prompt.

| >DUMPF |
| --- Dump Config. Details to File --- |
| File name: ASG.CFG |
| Dump List ATAB |
| ; Action Table |
| 7 record(s) DUMPed to file ASG.CFG. |
| 03/01/99 12:55:25 E9D8 [AUX] DUMP: ATAB |
| 03/01/99 12:55:25 7C30 [AUX] DUMP: Complete |

Screen C-5. DUMPF Command for saving a file on the RAM disk

Now it is possible to XMODEM or FTP the information to your PC by using the SEND command to transfer the configuration file. (Refer to the ASG Guard/ASG Guard Plus User’s Guide Section 7.6.6 for detailed information about using the SEND command.) After transferring the file to a PC, use a word processor program such as Microsoft Word to view the file. To Edit the file first save the file as a text file in Microsoft Word. Then edit the file using Notepad or Wordpad. Notepad and Wordpad will not properly display the raw file (as it comes for the ASG Guard/ASG Guard Plus) since these programs do not recognize the carriage returns without line feeds in the document.
C.6  Set Customer Key – SCK Command

C.6.1  Overview
The Set Customer Key (SCK) command provides a facility to change the Customer Key. The Customer Key is used to encrypt secret user information such as passwords. The Customer Key is used to encrypt this data when stored inside the ASG Guard/ASG Guard Plus and when the Customer User Table is exported via the DUMP/DUMPF command.

NOTE:
The ASG Guard/ASG Guard Plus is shipped from the factory with a Default Customer Key. For security purposes, it is important that this key be changed.

C.6.2  Materials
• PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
• Communication Package (such as Procomm Plus or Telnet session)

C.6.3  Procedure for Setting the Customer Encryption Key
1. Type the command **SCK** at the ASG Guard/ASG Guard Plus prompt. The ASG Guard/ASG Guard Plus requires a 16-digit hexadecimal entry (for example, ABCDEF0123456789).
2. Enter the new Customer Key and press the ENTER key to complete this process. The ASG Guard/ASG Guard Plus will confirm that the Customer Key has been changed.

```
>SCK
--- Set Customer Key ---
New Customer Key: ABCDEF0123456789
03/01/99 14:54:22 0D05 [AUX] Customer Encryption Key Value Loaded
```

Screen C-6.  Set Customer Key (SCK) Command
C.7 Procedures for Importing and Exporting Customer User Tables

C.7.1 Overview
This section describes the commands that allow for securely importing and exporting the Customer User Table. The `CDUMP`, `CDUMPF` and `CCONFIG` commands parallel the commands described earlier in this appendix. These commands, however, are used to ‘dump’ and ‘config’ (respectively) Customer User Table information. Since the Customer User Table contains secret information, such as a user passwords and keys, some of this data must be encrypted. Prior to importing/exporting this data, an encryption key must be set in the ASG Guard/ASG Guard Plus as detailed in Section C.6. To successfully export (CDUMP/CDUMPF) a Customer User Table from one ASG Guard/ASG Guard Plus and import (CCONFIG) to another ASG Guard/ASG Guard Plus, both units must have the same encryption key.

C.7.2 CDUMP Procedures

C.7.2.1 Overview
This section provides a procedure for saving a Customer User Table to a text file on a PC. The `CDUMP` command allows the user to back up the configuration of an ASG Guard/ASG Guard Plus with a direct connection via the AUX port, over phone lines, or via the network port.

C.7.2.2 Materials
- PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
- Communication Package (such as Procomm Plus or Telnet session)

C.7.2.3 CDUMP Procedure for Viewing the Customer User Table at the Terminal Screen
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. Type in the command `CDUMP` and press the ENTER key. At this point a banner beginning with `--- Dump Customer Users ---` will appear.
3. To view the encrypted Customer User Table, press the ENTER key. Pressing the ENTER key again will return the system prompt.
Screen C-7. CDUMP for Viewing the Customer User Table

C.7.2.4 CDUMP Procedure for Saving the Configuration to a File on a PC

1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.

2. Type in the command CDUMP and press the ENTER key. At this point a banner beginning with "--- Dump Customer Users ---" will appear. DO NOT PRESS THE ENTER KEY.

3. To save the User Table to a file on the PC, use the ASCII transfer procedure in the communication program to receive the configuration file from the ASG Guard/ASG Guard Plus. Initiate the transfer by sending an ENTER based on how your communications package operates. When the DUMP is complete, terminate the ASCII transfer from the communication program, if necessary. Press ENTER at the terminal window to get back to the system prompt.

4. To verify that the file was saved correctly, open the file with a text editor such as "Notepad" or "Wordpad". The file should appear to have appropriate programming structure (Look for extraneous characters) and be terminated with the word "END".

Screen C-8. CDUMP for Saving the Customer User Table to the PC
C.7.3 CDUMPF Procedure

C.7.3.1 Overview
The CDUMPF command allows the user to copy the Customer User Table to the RAM disk of an
ASG Guard/ASG Guard Plus.

C.7.3.2 Materials
• PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
• Communication Package (such as Procomm Plus or Telnet session)

C.7.3.3 Procedure for Saving the User Table to the RAM Disk
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. Type in the command CDUMPF and press the ENTER key. You will see the banner '---
   Dump Customer Users to File ---' and the prompt 'File Name: '
3. Enter a file name at the “File Name” prompt and press the ENTER key to save the file to the
   RAM disk.
4. The transfer will take only a few seconds. To verify the transfer was successful, type ‘VIEW
   filename’ at the system prompt.

Site123>CDUMPF
--- Dump Customer Users to File ---
File Name: USERTAB ; Customer User Table 10
03/02/99 11:26:13 B11B [AUX] CDUMPF Starting
03/02/99 11:26:13 BD3B [AUX] CDUMPF Completed by User: AUX_Default
Site123>

Screen C-9. CDUMPF Command for Saving the User Table as a file on the RAM Disk

Now it is possible to XMODEM or FTP the information to your PC by using the SEND command
to transfer the configuration file. (Refer to the ASG Guard/ASG Guard Plus User’s Guide Section
7.6.6 for detailed information about using the SEND command.) After transferring the file to a
PC, use a word processor program such as Microsoft Word to view the file. To edit the file, first
save the file as a text file in Microsoft Word. Then edit the file using Notepad or Wordpad.
Notepad and Wordpad will not properly display the raw file (as it comes for the ASG Guard/ASG
Guard Plus) since these programs do not recognize the carriage returns without line feeds in the
document.
C.7.4 CCONFIG Procedure With a Remote Customer User Table

C.7.4.1 Overview
A Customer User Table file may be sent to the ASG Guard/ASG Guard Plus from a PC or from a PC to the ASG Guard/ASG Guard Plus. The CCONFIG command is used to import the Customer User Table file (that is, load the Customer User Table data). The CCONFIG command allows a user to import a Customer User Table into an ASG Guard/ASG Guard Plus from a file on the local RAM disk, over a direct connection to the Aux port, over phone lines, or via the network. The procedure in this section describes how to import a Customer User Table from a Customer User Table file on a remote PC using ASCII file transfer.

C.7.4.2 Materials
- PC connected to the ASG Guard/ASG Guard Plus via network, Aux, or Modem port.
- Communication Package (such as Procomm Plus or Telnet session)

C.7.4.3 CCONFIG Procedure With ASCII File Transfer
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. Type in the command CCONFIG and press the ENTER key. The message --- Config Customer Keys --- will appear.
3. Use the communications program ASCII or text file transfer process to send the configuration file to the ASG Guard/ASG Guard Plus.

   NOTE: Set flow control to software (XON/XOFF)! Configurations can be corrupted if flow control is set incorrectly. If you encounter difficulties, follow the procedure for a stored CONFIG.

```plaintext
> CCONFIG

--- Config Customer Keys ---
; Customer User Table

Begin USERTAB
End USERTAB

03/02/99 11:43:01 19DC [AUX] CCONFIG Completed by User: AUX_Default

Screen C-10. CCONFIG Command from the PC
```
C.7.5 CCONFIG Procedure With a Customer User Table on the Local RAM Disk

C.7.5.1 Overview
A Customer User Table file may be sent to the ASG Guard/ASG Guard Plus from a PC or from a PC to the ASG Guard/ASG Guard Plus. The CCONFIG command is used to import the Customer User Table file (that is, load the Customer User Table data). The CCONFIG command allows a user to import a Customer User Table into an ASG Guard/ASG Guard Plus from a file on the local RAM disk, over a direct connection to the Aux port, over phone lines, or via the network. The procedure in this section describes how to import a Customer User Table from a Customer User Table file that is stored on the RAM disk.

C.7.5.2 Materials
• PC connected to the ASG Guard/ASG Guard Plus via Aux or Modem port.
• Communication Package (such as Procomm Plus)

C.7.5.3 Procedure for Configuring the Customer User Table from the RAM Disk
1. Log onto the ASG Guard or ASG Guard Plus as a CMaster User.
2. If the Customer User Table is not stored on the local RAM disk, download the Customer User Table file to the RAM Disk (refer to section 7.7 for more detail on this process).
3. To configure the ASG Guard/ASG Guard Plus, type CCONFIG filename at the system prompt and press the ENTER key.

```
> RCV USERTAB

--- Receive File ---
Receiving XMODEM - File: \USERTAB
CCCC
--- Receive Complete ---
03/02/99 11:53:26 24FF [AUX] File \USERTAB: Receive Complete
ASGTEST>CCONFIG USERTAB

--- Config Customer Keys ---
; Customer User Table

Begin USERTAB
End USERTAB

03/02/99 11:53:39 D4E4 [AUX] CCONFIG Completed by User: AUX_Default
```

Screen C-11. CCONFIG Command from the PC
D. Troubleshooting

D.1 Troubleshooting the Installation

If you have a problem installing the ASG Guard/ASG Guard Plus or it does not seem to be functioning properly, check the table below to see if the symptoms are listed.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Cause</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>No lights or power light only on</td>
<td>Battery dead</td>
<td>Connect AC power or 48 V power and restart ASG Guard/ASG Guard Plus.</td>
</tr>
<tr>
<td>No data on local terminal or can’t type on local terminal.</td>
<td>Bad cable, Terminal not set for 9600, 8/None.</td>
<td>Check cable and terminal program.</td>
</tr>
<tr>
<td>Unable to access the network.</td>
<td>Parameters set incorrectly.</td>
<td>Verify that the Ethernet and IP addresses are correct; check cable connections.</td>
</tr>
<tr>
<td></td>
<td>Cables not connected.</td>
<td>Verify that “Yes” has been selected for “Start Network on Powerup”. If the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>network module of the ASG Guard/ASG Guard Plus has not been started, type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>startnet to start it.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connect cable.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Power cycle the system.</td>
</tr>
<tr>
<td>Unable to access the user database and/or perform user maintenance</td>
<td>Check user’s access class. Only Master users can access the user</td>
<td>The system must have at least one user with the access level of Master. Log on</td>
</tr>
<tr>
<td>functions</td>
<td>database.</td>
<td>as a CMaster user.</td>
</tr>
<tr>
<td>ASG Guard/ASG Guard Plus is not operating correctly</td>
<td>Not connected correctly.</td>
<td>Check cable connections.</td>
</tr>
<tr>
<td></td>
<td>Software configuration not correct</td>
<td>Call System Administrator or Lucent Technologies Technical Support.</td>
</tr>
</tbody>
</table>

If the problem has not been resolved, call Lucent Technologies Technical Support at 1-800-242-2121. To solve the problem as quickly as possible, describe the problem, the status of the LEDs on the front panel, and the steps that you have taken to resolve it.
E. Internal Battery Replacement

E.1 Introduction

This guide is intended to instruct a trained technician in the process of removal and re-installation of the internal battery within the Access Security Gateway (ASG) Guard and Access Security Gateway (ASG) Guard Plus devices.

E.2 General Safety Warnings

Before replacing the internal battery, it is highly recommended that you back up to an administrative personal computer any files stored on the RAM disk. These files, which include history files, buffer files, etc. will be lost when power to the ASG Guard/ASG Guard Plus is turned off. The operating system software and Customer User Table will not be affected when power is turned off. If you have a Service Agreement with Lucent Technologies for products connected to host ports on the ASG Guard/ASG Guard Plus, please inform the Lucent Technical Service Center (800-242-2121) before replacing the internal battery. Whether or not you have a Service Agreement, Lucent can replace the internal battery for a fee. If you replace the battery, it is your responsibility to back up files that are stored on the RAM disk.

It is recommended that before attempting to remove the internal battery from the ASG Guard/ASG Guard Plus device, the unit key switch should be turned to the OFF position, the key removed from keyhole and all power supplies (16V AC, 48V DC, AC adapter) be unplugged. The proper safety precautions detailed in this guide must be followed to ensure the safety of the technician and the continual successful operation of the device.

- The internal battery for the **Access Security Gateway (ASG) Guard Plus** can be removed and replaced through the front panel of the device. (Refer to Figure E-1.)

- To remove and replace the internal battery for the **Access Security Gateway (ASG) Guard**, the outer casing will need to be removed from the unit and the internal hardware connections handled with extreme caution. (Refer to Figure E-8.)

It is extremely important that maintenance to any of the ASG devices be performed in a static free environment, on a flat stable surface that is clear and clean of all debris or loose items that could fall into the unit.

**NOTE:**

*Please Read All Instructions Thoroughly Before Attempting to Remove the Internal Battery from the Access Security Gateway (ASG) Guard and Access Security Gateway (ASG) Guard Plus devices.*
E.3 Pre-Installation

The following tools will be required to properly change the internal battery in the Access Security Gateway (ASG) Guard and Access Security Gateway (ASG) Guard Plus devices*:

- Phillips head screwdriver*
- 3/16" Hex driver*
- 5/16" Hex driver or 5/16 Socket*
- Diagonal Cutter (small) or Scissors*
- Needle nose pliers (optional)

E.4 Access Security Gateway (ASG) Guard Plus device

This section of the instruction guide describes the removal of the internal battery from the Access Security Gateway (ASG) Guard Plus device.

Figure E-1. Front View of the Access Security Gateway (ASG) Guard Plus

E.4.1 Preparation

Once it has been determined that the battery will need to be changed, make sure no electrical current is flowing. The unit’s key switch should be turned to the OFF position, the key removed from keyhole and so no electrical current is flowing, all power supplies (16V AC, 48V DC, AC adapter) should be unplugged. The area should be clear of all debris in which screws, washers or bolts could become misplaced.
E.4.2 Installation Procedures

1. The internal battery is located behind the small bolted plate on the lower right side of the front panel of the Access Security Gateway (ASG) Guard Plus device. Carefully unfasten the two screws from the plate and set aside. The screws are captive so after loosening them, the screws, springs and plate can be removed as one piece.

![Figure E-2. Remove Front Plate for ASG Guard Plus](image1)

2. The removal of the plate will expose a white tab fastened to the front of the battery. Firmly hold down the case and pull the tab up and out to free battery from the case. The battery should be pulled out of the casing completely and in a smooth motion. If the battery hesitates or becomes stuck, the wires may be caught on the casing. Gently move the battery side to side to release a possible snag.

![Figure E-3. Pull Out Battery for ASG Guard Plus](image2)
3. After the battery has been completely removed from housing, disconnect the red wire from (+) positive terminal and black wire from (-) negative terminal. Do not pull on the wires but slightly tug on the plastic tabs connected to the metal terminals, using a side-to-side rocking motion. A pair of needle nose pliers may be used to tug gently on the plastic tabs and not the wires.

Figure E-4. Disconnect Wires from Battery for ASG Guard Plus

4. Connect the red wire to (+) positive terminal and black wire to (-) negative terminal of the replacement battery. Battery metal terminals should be flattened and wires should be to the left of battery, to avoid hang-ups on internal bracket.

Figure E-5. Connect Wires to Replacement Battery for ASG Guard Plus
5. Slide the new battery into the internal bracket. (Battery will fit only one way, with the red wire towards the back and the tabs towards the center of the unit.) Tuck wires carefully into internal bracket, so they do not snag on the bracket and disconnect tabs from the battery.

![Image](image1)

**Figure E-6.** Insert New Battery for ASG Guard Plus

6. When the battery is completely returned to the case, insert the key and turn to ON position to confirm proper connection and re-installation of the battery.

![Image](image2)

**Figure E-7.** Confirm Proper Connection and Re-Installation of the Battery for ASG Guard Plus
NOTE:
If the Access Security Gateway (ASG) Guard Plus does not Power-up (no lights appear on panel), then retry the above steps. The wire and tab connections may have become disconnected while sliding the battery into the casing.

If the Access Security Gateway (ASG) Guard Plus does Power-up (the red PWR FAIL light will be ON, indicating that the internal battery is operable), then replace the bolted panel, and reconnect all power supplies (16V AC, 48V DC, AC adapter).

E.5 Access Security Gateway (ASG) Guard device

This section of the instruction guide describes the removal of the internal battery from the Access Security Gateway (ASG) Guard device.

NOTE:
Please Read All Instructions Thoroughly Before Attempting to Remove the Internal Battery from the Access Security Gateway (ASG) Guard device.

Figure E-8. Front View of Access Security Gateway (ASG) Guard

E.5.1 Preparation

Once it has been determined that the battery will need to be changed, make sure no electrical current is flowing. The unit’s key switch should be turned to the OFF position, the key removed from keyhole and all power supplies (16V AC, 48V DC, AC adapter) should be unplugged. The area should be clear of all debris in which event, the screws, washers or bolts could become misplaced and/or falling objects that may hinder the future operation of the unit.

E.5.2 Installation Procedures

The internal battery is located amongst the internal hardware of Access Security Gateway (ASG) Guard device in which the outer housing must be removed to gain access.
E.5.2.1 Removal of the Outer Housing

1. Unfasten all the outside housing screws (2 from the top, 2 from each side, 3 from the bottom, and two 3/16” Hex screws on the front panel next to the AUX port).

2. Gently slide top portion of housing forward and lift to clear the AUX port.

Figure E-9. Remove Top Portion of ASG Guard Housing

3. Lay top portion of housing adjacent to base chassis.

Figure E-10. View of Open ASG Guard
4. Reach in and gently lift up the 3 black retaining hooks and pull the white connector, this will disconnect the 3-prong connector key switch. Then remove the top housing completely and place on a flat surface.

![Figure E-11. Key Switch and 3-Prong Connector of ASG Guard](image)

**Description:** The internal battery is located on the right side of internal hardware. The red wire (positive) and black wire (negative) are on the left of the battery.
E.5.2.2 Hardware Interaction

1. Carefully cut the plastic zip tie that constrains the black modem wires in front of the battery bracket. For access to the bracket screws, re-position the black modem wires to opposite sides of the bracket. Gently lift up the 2 black retaining hooks and pull the white connector to disconnect 2-prong connector next to the battery.

Figure E-12. 2-Prong Connector and Modem Wires for ASG Guard
2. Detach the red wire from (+) positive terminal and black wire from (-) negative terminal on the ends of the battery. It is important that you do not pull on the wires but gently tug on the plastic tabs connected to metal terminals.

**NOTE:**
*DO NOT remove the zip tie from the battery wires.*

![Image of battery wires](image1)

**Figure E-13.** Detach Wires from the Battery for ASG Guard

3. Unfasten the two 5/16" nuts that are mounted at each end of the battery bracket. Remove the bracket from the top of battery and then remove the battery.

![Image of battery bracket nuts](image2)

**Figure E-14.** Front and Rear Bracket Nuts for ASG Guard
Battery bracket removed

Figure E-15. Remove Battery from ASG Guard

Battery removal complete

Figure E-16. Battery Removal Complete for ASG Guard
4. Connect plastic tabs on the red wire to (+) positive terminal and black wire to (-) negative terminal on the replacement battery. Place battery in base of casing; metal terminals should be flattened and wires should be to the left of battery.

5. Reconnect the white connector to the 2-prong connector located to the left of the battery.
6. Gently reconnect the white connector to the 3-prong connector for the key switch. (The white connector’s angular protrusion (crest) will clip under the black retaining hooks).

![Figure E-19. Connect 3-Prong Connector for ASG Guard](image)

**VERY IMPORTANT!** White connector MUST have angular protrusion (crest) on top, before connecting to prong. An incorrect connection will result in permanent damage to the Access Security Gateway (ASG) Guard device.

7. To test the battery connection, re-insert the key and turn the key switch to the ON position. Observe whether or not the red PWR FAIL light is ON (this light indicates that the internal battery is operable).

![Figure E-20. Test Battery Connection for ASG Guard](image)

**NOTE:**
*If the Access Security Gateway (ASG) Guard does not Power-up (no lights appear on panel), check and re-secure all connections.*

*If the Access Security Gateway (ASG) Guard does Power-up (the red PWR FAIL light is ON, indicating that the internal battery is operable), proceed with the following steps.*
8. Turn key switch to OFF position and remove from keyhole. Replace battery bracket on top of battery. Fasten the two 5/16" nuts to each end of the battery bracket. Place the black modem wires in channel located on the right side of the battery. Wrap around in front of the casing and secure with a new zip tie.

![Figure E-21. Replace Battery Bracket and Secure Modem Wires for ASG Guard](image)

9. Replace the outer housing on top of unit and tighten all the outside housings screws on all sides of the unit. Do not over torque, this may cause the screw threads to strip.

10. Reconnect all power supplies (16V AC, 48V DC, AC adapter).
E.6 Help/Troubleshooting

E.6.1 Access Security Gateway (ASG) Guard Plus device
1. Unbolt front panel plate, pull the white tab up and out to release internal battery and make sure plastic tabs on the red wire are fitted to (+) positive terminal and black wire to (-) negative terminal. DO NOT OPEN OR REMOVE THE EXTERNAL HOUSING FROM THE ASG GUARD PLUS DEVICE.
2. If the unit will not Power-up after checking the connections, report the trouble to the Lucent Technical Service Center (800-242-2121).

E.6.2 Access Security Gateway (ASG) Guard device
1. Unfasten all screws on external housing, lift cover of unit carefully and check that all connections have been properly made.
2. If the unit will not Power-up after checking the connections, report the trouble to the Lucent Technical Service Center (800-242-2121).
# F. Glossary of Command References

## F.1 Action and Alarm Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Add action item</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>CA</td>
<td>Change action item</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>GE</td>
<td>Generate event</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>LA</td>
<td>List action items</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>LE</td>
<td>List events</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>SAI</td>
<td>Schedule action item</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>XA</td>
<td>Delete action item</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>XE</td>
<td>Delete event</td>
<td>CMaster, Sysop 2</td>
</tr>
</tbody>
</table>

## F.2 System Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCC</td>
<td>Display contact inputs</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DSA</td>
<td>Display sensor alarms</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DSI</td>
<td>Display sensor inputs</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DSP</td>
<td>Display system parameters</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>RRLY</td>
<td>Reset relays</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SDT</td>
<td>Set date and time</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SHP</td>
<td>Set host processing flag</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SRLY</td>
<td>Set relays</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SSA</td>
<td>Set sensor alarms</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SSP</td>
<td>Set system parameters</td>
<td>CMaster, Sysop 2</td>
</tr>
</tbody>
</table>
### F.3 User Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>AU</td>
<td>Add users</td>
<td>CMaster</td>
</tr>
<tr>
<td>BLA</td>
<td>Block/unblock Lucent administration</td>
<td>CMaster</td>
</tr>
<tr>
<td>BLU</td>
<td>Block/unblock Lucent users</td>
<td>CMaster</td>
</tr>
<tr>
<td>CU</td>
<td>Change users</td>
<td>CMaster</td>
</tr>
<tr>
<td>DLU</td>
<td>Display Lucent users</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>DU</td>
<td>Display users</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>LLU</td>
<td>List Lucent users</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>LU</td>
<td>List users</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SCK</td>
<td>Set an encryption key</td>
<td>CMaster</td>
</tr>
<tr>
<td>XU</td>
<td>Delete users</td>
<td>CMaster</td>
</tr>
</tbody>
</table>

### F.4 Log Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>AH</td>
<td>Access history</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>CER</td>
<td>Clear error log</td>
<td>CMaster</td>
</tr>
<tr>
<td>CLH</td>
<td>Clear log history</td>
<td>CMaster</td>
</tr>
<tr>
<td>DER</td>
<td>Display error log</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>FH</td>
<td>Display failure history</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>LH</td>
<td>Display log history</td>
<td>All Sysop levels</td>
</tr>
</tbody>
</table>
## F.5 File Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>CD</td>
<td>Change directory</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>COMP</td>
<td>Compress a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>COPY</td>
<td>Copy a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>DDP</td>
<td>Display disk parameters</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>DEL</td>
<td>Delete a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>DIR</td>
<td>List files in directory</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>MD</td>
<td>Make a directory</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>MOVE</td>
<td>Move a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>RCV</td>
<td>Receive a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>RD</td>
<td>Remove a directory</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>REN</td>
<td>Rename a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SDP</td>
<td>Set disk parameters</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SEND</td>
<td>Sends a file to another device</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>UCOMP</td>
<td>Uncompress a file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>VIEW</td>
<td>View a file</td>
<td>CMaster, Sysop 2</td>
</tr>
</tbody>
</table>

## F.6 Buffer Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>BST</td>
<td>Display host buffer details</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>CLBUF</td>
<td>Close buffer file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>OBST</td>
<td>Open buffer status</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>OPBUF</td>
<td>Open host buffer file</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SEBUF</td>
<td>Send all buffer files to another device</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SWBUF</td>
<td>Switch buffer files</td>
<td>CMaster, Sysop 2</td>
</tr>
</tbody>
</table>
### F.7 Session Control Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>CON</td>
<td>Connect to port</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>CONL</td>
<td>Connect to Lucent device</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DIS</td>
<td>Disconnect from unit</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>JS</td>
<td>Join host session</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>JSL</td>
<td>Join host session with Lucent device</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>VS</td>
<td>View session</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>VT</td>
<td>VT100 on and off</td>
<td>All Sysop levels</td>
</tr>
</tbody>
</table>

### F.8 Port Control Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>DA/DM/DH/DT</td>
<td>Display Aux/Modem/Host/Telnet port parameters</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DNP</td>
<td>Display network parameters</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DNS</td>
<td>Display network status</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>DPS</td>
<td>Display port signals</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>PING</td>
<td>Query remote device</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>PPP</td>
<td>Start PPP session</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>PST</td>
<td>Port status</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>RES</td>
<td>Reset port</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>SA/SM/SH/ST</td>
<td>Set Aux/Modem/Host/Telnet port parameters</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>SNP</td>
<td>Set network parameters</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>STARTNET</td>
<td>Start up the network</td>
<td>CMaster, Sysop 2</td>
</tr>
</tbody>
</table>
## F.9 Device Management Functions

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Access Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>BOOT</td>
<td>Restart system</td>
<td>CMaster, Sysop 2</td>
</tr>
<tr>
<td>CDUMP</td>
<td>View or save the User Table information to a file on the host PC</td>
<td>CMaster</td>
</tr>
<tr>
<td>CDUMPF</td>
<td>Save the User Table information to a file on the RAM disk</td>
<td>CMaster</td>
</tr>
<tr>
<td>CCONFIG</td>
<td>Upload a custom encrypted User Table to the unit</td>
<td>CMaster</td>
</tr>
<tr>
<td>CONFIG</td>
<td>Upload a custom configuration file to the unit</td>
<td>CMaster</td>
</tr>
<tr>
<td>DUMP</td>
<td>View or save the system configuration to a file on the host PC</td>
<td>CMaster</td>
</tr>
<tr>
<td>DUMPF</td>
<td>Save the system configuration to a file on the RAM disk</td>
<td>CMaster</td>
</tr>
<tr>
<td>VER</td>
<td>Display system information about the ASG Guard/ASG Guard Plus</td>
<td>All Sysop levels</td>
</tr>
<tr>
<td>UPG</td>
<td>Upgrade the ASG Guard/ASG Guard Plus</td>
<td>CMaster</td>
</tr>
</tbody>
</table>
Index


AA command | Access Classes | Access History command (AH) | Action Routines | AUXCC | CANCEL | CLKAHEAD | CLKBACK | CLKCHECK | DOLIST | LOG | LOGCHECK | NOACTION | PAGE | PHIRIS | PHONHOME | PHPPP | PHSYSOP | REMINIT | RESRELAY | SCHEDULE | SETHP | SETRELAY | SNMPTRAP | Action Table commands | overview | planning | structure | using | Add Action Item command (AA) | Add User command (AU) | Administration | block/unblock Lucent users | AH command | Alarm Management | Alarm Processing | Alarm/Event Functions command | Alarms | matching criteria | multiple actions | Analog Sensors |
<table>
<thead>
<tr>
<th>Index</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASG Guard</strong></td>
<td></td>
</tr>
<tr>
<td>add user profile</td>
<td>25</td>
</tr>
<tr>
<td>configuration</td>
<td>4</td>
</tr>
<tr>
<td>configure</td>
<td>120</td>
</tr>
<tr>
<td>configure AUX port</td>
<td>33</td>
</tr>
<tr>
<td>configure Host port</td>
<td>36</td>
</tr>
<tr>
<td>connect DCE device</td>
<td>19</td>
</tr>
<tr>
<td>Environmental Manager interface</td>
<td>126</td>
</tr>
<tr>
<td>Environmental Manager relays</td>
<td>128</td>
</tr>
<tr>
<td>Events and Action Routines</td>
<td>177</td>
</tr>
<tr>
<td>front panel</td>
<td>4</td>
</tr>
<tr>
<td>functional overview</td>
<td>7</td>
</tr>
<tr>
<td>installation</td>
<td>20</td>
</tr>
<tr>
<td>Internal Events</td>
<td>177</td>
</tr>
<tr>
<td>log functions</td>
<td>167</td>
</tr>
<tr>
<td>network applications requirements</td>
<td>20</td>
</tr>
<tr>
<td>power up</td>
<td>22</td>
</tr>
<tr>
<td>rear panel</td>
<td>5</td>
</tr>
<tr>
<td>re-initialize</td>
<td>40</td>
</tr>
<tr>
<td>relays</td>
<td>128</td>
</tr>
<tr>
<td>required cables and equipment</td>
<td>20</td>
</tr>
<tr>
<td>restart</td>
<td>119</td>
</tr>
<tr>
<td>secure AUX port</td>
<td>35</td>
</tr>
<tr>
<td>upgrade the software</td>
<td>119</td>
</tr>
<tr>
<td>user database</td>
<td>49</td>
</tr>
<tr>
<td>verify PSTN access</td>
<td>23</td>
</tr>
<tr>
<td><strong>ASG Guard Plus</strong></td>
<td></td>
</tr>
<tr>
<td>add user profile</td>
<td>25</td>
</tr>
<tr>
<td>configuration</td>
<td>4</td>
</tr>
<tr>
<td>configure</td>
<td>120</td>
</tr>
<tr>
<td>configure AUX port</td>
<td>33</td>
</tr>
<tr>
<td>configure Host port</td>
<td>36</td>
</tr>
<tr>
<td>connect DCE device</td>
<td>19</td>
</tr>
<tr>
<td>Environmental Manager interface</td>
<td>124</td>
</tr>
<tr>
<td>Environmental Manager relays</td>
<td>128</td>
</tr>
<tr>
<td>Events and Action Routines</td>
<td>177</td>
</tr>
<tr>
<td>front panel</td>
<td>5</td>
</tr>
<tr>
<td>functional overview</td>
<td>7</td>
</tr>
<tr>
<td>installation</td>
<td>20</td>
</tr>
<tr>
<td>Internal Events</td>
<td>177</td>
</tr>
<tr>
<td>log functions</td>
<td>167</td>
</tr>
<tr>
<td>network applications requirements</td>
<td>20</td>
</tr>
<tr>
<td>power up</td>
<td>22</td>
</tr>
<tr>
<td>rear panel</td>
<td>6</td>
</tr>
<tr>
<td>re-initialize</td>
<td>40</td>
</tr>
<tr>
<td>required cables and equipment</td>
<td>20</td>
</tr>
<tr>
<td>restart</td>
<td>119</td>
</tr>
<tr>
<td>secure AUX port</td>
<td>35</td>
</tr>
<tr>
<td>upgrade the software</td>
<td>119</td>
</tr>
<tr>
<td>user database</td>
<td>49</td>
</tr>
<tr>
<td>verify PSTN access</td>
<td>23</td>
</tr>
<tr>
<td><strong>ASG Key</strong></td>
<td>28</td>
</tr>
<tr>
<td>set</td>
<td>67</td>
</tr>
<tr>
<td>user's guide</td>
<td>203</td>
</tr>
<tr>
<td>ASG Key Authentication</td>
<td>30, 54, 138</td>
</tr>
<tr>
<td>Encryption Key Source</td>
<td>30</td>
</tr>
<tr>
<td>AU command</td>
<td>25, 52</td>
</tr>
<tr>
<td><strong>Authentication</strong></td>
<td></td>
</tr>
<tr>
<td>ASG Key</td>
<td>30, 54, 138</td>
</tr>
<tr>
<td>pager</td>
<td>58</td>
</tr>
<tr>
<td>Pager</td>
<td>140</td>
</tr>
<tr>
<td>Password/Callback</td>
<td>28, 57, 134</td>
</tr>
<tr>
<td>Regular Callback</td>
<td>135</td>
</tr>
<tr>
<td>Variable Callback</td>
<td>137</td>
</tr>
<tr>
<td>Auto-Baud</td>
<td>133</td>
</tr>
<tr>
<td>Auto-Parity</td>
<td>134</td>
</tr>
<tr>
<td>AUX Port</td>
<td></td>
</tr>
<tr>
<td>configure</td>
<td>33</td>
</tr>
<tr>
<td>initiate security</td>
<td>35</td>
</tr>
<tr>
<td>parameters</td>
<td>208</td>
</tr>
<tr>
<td>AUXCC Action Routine</td>
<td>189</td>
</tr>
</tbody>
</table>

### B

| **Battery** | 130, 225 |
| **BLA command** | 69 |
| **Block/Unblock Lucent Administration command (BLA)** | 69 |
| **Block/Unblock Lucent Users command (BLU)** | 68 |
| **BLU command** | 68 |
| **BOOT command** | 119 |
| **BST command** | 79 |
| **Buffer File Naming** |  |
| conventions | 73 |
| overview | 73 |
| **Buffer Files** | 77 |
| host port subdirectory | 73 |
| **Buffering Data** |  |
| automatically | 77 |
| display buffer status | 79 |
| manually | 79 |
| overview | 77 |
| send buffer files to administration PC | 80 |
| send buffer files via a dial-up connection | 80 |
| send buffer files via a direct connection | 80 |

### C

| **CA command** | 98 |
| **Cables and Equipment** | 20 |
| **CANCEL Action Routine** | 189 |
| **CCONFIG command** | 120, 220 |
| **CD command** | 85, 86 |
| **CDUMP command** | 120, 218 |
| **CDUMPF command** | 120, 219 |
| **CER command** | 175 |
| **CLKAHEAD Action Routine** | 98 |
| **Change Action Item command (CA)** | 98 |
| **Change User command (CU)** | 64 |
| **Check the Software Version command (VER)** | 118 |
| **Clear Error Log command (CER)** | 175 |
| **Clear Log History command (CLH)** | 175 |
| **CLH command** | 175 |
| **CLKAHEAD Action Routine** | 190 |
| **CLKBACK Action Routine** | 190 |
| **CLKCHECK Action Routine** | 190 |
Index

Commands: 241

AA command 95
Access History command (AH) 168
action table commands 95
Add Action Item command (AA) 95
Add User command (AU) 52
add users (AU) 25
AH command 168
Alarm/Event Functions 101
AU command 25, 52
BLA command 69
Block/Unblock Lucent Administration command (BLA) 69
Block/Unblock Lucent Users command (BLU) 68
BLU command 68
BOOT command 119
BST command 79
CA command 98
CCONFIG command 120
CD command 85
CDUMP command 120, 218
CDUMPF command 120, 219
CER command 175
Change Action Item command (CA) 98
Change User command (CU) 64
Check the Software Version command (VER) 118
Clear Error Log command (CER) 175
Clear Log History command (CLH) 175
CLH command 175
CON command 142
CONFIG command 120
configure AUX port 33
Configure the Unit command (CONFIG) 120, 220
CONL command 142
Connect to Host command (CON) 142
Connect to Lucent Host command (CONL) 142
CU command 64
Customer User Table 51
DCC command 122, 132
DDP command 75
DEL command 85
Delete Action Item command (XA) 99
Delete Alarm/Event command (XE) 103
Delete User command (XU) 62
DER command 174
DIR command 85
DIS command 142
Disconnect command (DIS) 142
Display Analog Sensor Inputs command (DSI) 131
Display Contact Inputs command (DCC) 122
Display Error Log command (DER) 174
Display Lucent Users command (DLU) 68
Display Modern Port Parameters command (DM) 41
Display Network Parameters command (DNP) 157
Display Network Status (DNS) 158
Display Port Signals command (DPS) 144
Display Sensor Alarms command (DSA) 122
Display Sensor Inputs command (DSI) 122
Display Status of Contact Inputs command (DCC) 132
Display System Parameters command (DSP) 115
Display Telnet Port Parameters command (DT) 161
Display User Record command (DU) 63
DLU command 168
DM command 141
DNP command 157
DNS command 158
DPS command 144
DSA command 122
DSI command 122, 131
DSP command 115
DT command 161
DU command 63
DUMP command 120
DUMPF command 120
edit keys 13
entering 14
Failure History command (FH) 172
FH command 172
FTP Parameters 155
GE command 101
Generate Alarm/Event command (GE) 101
INIT command 40
initiate PPP Link command (PPP) 162
Join Host Session command (JS) 141
Join Lucent Host command (JSL) 141
JS command 141
JSL command 141
LA command 97
LE command 101
LH command 170
List Action Items command (LA) 97
List Alarms/Events command (LE) 101
List Lucent Users command (LLU) 68
List User command (LU) 60
LLU command 168
Log History command (LH) 170
LU command 60
MD command 85
Network Initialization Parameters 152
PING command 159
Port Control commands 143
Port Status command (PST) 143
PPP command 162
PST command 143
Put Configuration Data on RAM Disk command (DUMPF) 120
Put Configuration Data on Remote Device command (DUMP) 120
Put User Table on RAM Disk command (CDUMPF) 120
Put User Table on Remote Device command (CDUMP) 120
Query Remote Nodes command (PING) 159
RCV command 184
RD command 85
RES command 144
Reset Port command (RES) 144
Reset Relays command (RRLY) 123
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart command (BOOT)</td>
<td>119</td>
</tr>
<tr>
<td>RRLY command</td>
<td>123</td>
</tr>
<tr>
<td>SA command</td>
<td>33</td>
</tr>
<tr>
<td>SAI command</td>
<td>98</td>
</tr>
<tr>
<td>Schedule Action Item command (SAI)</td>
<td>98</td>
</tr>
<tr>
<td>SCK command</td>
<td>67</td>
</tr>
<tr>
<td>SDP command</td>
<td>75</td>
</tr>
<tr>
<td>SDT command</td>
<td>117</td>
</tr>
<tr>
<td>SEBUF command</td>
<td>80,83</td>
</tr>
<tr>
<td>SEND command</td>
<td>83</td>
</tr>
<tr>
<td>Set Customer Key command (SCK)</td>
<td>67</td>
</tr>
<tr>
<td>Set Date and Time command (SDT)</td>
<td>117</td>
</tr>
<tr>
<td>Set Host command (SH)</td>
<td>77</td>
</tr>
<tr>
<td>Set Host Processor Flag command (SHP)</td>
<td>116</td>
</tr>
<tr>
<td>Set Modern Port Parameters command (SM)</td>
<td>43</td>
</tr>
<tr>
<td>Set Network Parameters command (SNP)</td>
<td>152</td>
</tr>
<tr>
<td>Set Relays command (SRLY)</td>
<td>123</td>
</tr>
<tr>
<td>Set Sensor Alarms command (SSA)</td>
<td>122</td>
</tr>
<tr>
<td>Set System Parameters command (SSP)</td>
<td>111</td>
</tr>
<tr>
<td>Set Telnet Port Parameters command (ST)</td>
<td>159</td>
</tr>
<tr>
<td>Set Threshold Limits command (SSA)</td>
<td>128</td>
</tr>
<tr>
<td>SH command</td>
<td>36,77</td>
</tr>
<tr>
<td>SHP command</td>
<td>116</td>
</tr>
<tr>
<td>SM command</td>
<td>43</td>
</tr>
<tr>
<td>SNMP Parameters</td>
<td>154</td>
</tr>
<tr>
<td>SNMP command</td>
<td>32, 81,152</td>
</tr>
<tr>
<td>SRLY command</td>
<td>123</td>
</tr>
<tr>
<td>SSA command</td>
<td>122,128</td>
</tr>
<tr>
<td>SSP command</td>
<td>111</td>
</tr>
<tr>
<td>ST command</td>
<td>159</td>
</tr>
<tr>
<td>STARTNET command</td>
<td>158</td>
</tr>
<tr>
<td>Terminal Mode command (VT)</td>
<td>143</td>
</tr>
<tr>
<td>UPG command</td>
<td>119</td>
</tr>
<tr>
<td>Upgrade the Software command (UPG)</td>
<td>119</td>
</tr>
<tr>
<td>VER command</td>
<td>118</td>
</tr>
<tr>
<td>View Session command (VS)</td>
<td>142</td>
</tr>
<tr>
<td>VS command</td>
<td>142</td>
</tr>
<tr>
<td>VT command</td>
<td>143</td>
</tr>
<tr>
<td>XA command</td>
<td>99</td>
</tr>
<tr>
<td>XE command</td>
<td>103</td>
</tr>
<tr>
<td>XU command</td>
<td>62</td>
</tr>
<tr>
<td>Comments (Action Routine)</td>
<td>96</td>
</tr>
<tr>
<td>Comments (User Maintenance)</td>
<td>28,54,66</td>
</tr>
<tr>
<td>Communications Ports</td>
<td></td>
</tr>
<tr>
<td>configure the Aux Port</td>
<td>33</td>
</tr>
<tr>
<td>CON command</td>
<td>142</td>
</tr>
<tr>
<td>CONFIG command</td>
<td>120,212</td>
</tr>
<tr>
<td>Configure the Communications Ports</td>
<td></td>
</tr>
<tr>
<td>configure a Host Port</td>
<td>36</td>
</tr>
<tr>
<td>CONL command</td>
<td>142</td>
</tr>
<tr>
<td>Connect to Host command (CON)</td>
<td>142</td>
</tr>
<tr>
<td>Connect to Lucent Host command (CONL)</td>
<td>142</td>
</tr>
<tr>
<td>Contact Closure Inputs</td>
<td>131</td>
</tr>
<tr>
<td>COPY command</td>
<td>86</td>
</tr>
<tr>
<td>CSUM.EXE Program</td>
<td>88</td>
</tr>
<tr>
<td>CU command</td>
<td>64</td>
</tr>
<tr>
<td>Customer User Table commands</td>
<td>51,218</td>
</tr>
</tbody>
</table>

**D**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data buffering</td>
<td>7</td>
</tr>
<tr>
<td>Date and Time</td>
<td>117</td>
</tr>
<tr>
<td>DCC command</td>
<td>122,132</td>
</tr>
<tr>
<td>DCE Device connecting</td>
<td>19</td>
</tr>
<tr>
<td>DDP command</td>
<td>75</td>
</tr>
<tr>
<td>DEL command</td>
<td>85,86</td>
</tr>
<tr>
<td>Delete Action Item command (XA)</td>
<td>99</td>
</tr>
<tr>
<td>Delete Alarm/Event command (XE)</td>
<td>103</td>
</tr>
<tr>
<td>Delete User command (XU)</td>
<td>62</td>
</tr>
<tr>
<td>DER command</td>
<td>174</td>
</tr>
<tr>
<td>Device ID/User Code Encryption Key Source</td>
<td>56</td>
</tr>
<tr>
<td>Device Management Functions</td>
<td></td>
</tr>
<tr>
<td>documentation overview</td>
<td>118</td>
</tr>
<tr>
<td>Dial-Up Preparations</td>
<td>133</td>
</tr>
<tr>
<td>Dial-Up Session</td>
<td>134</td>
</tr>
<tr>
<td>DIR command</td>
<td>85,86</td>
</tr>
<tr>
<td>DIS command</td>
<td>142</td>
</tr>
<tr>
<td>Disconnect command (DIS)</td>
<td>142</td>
</tr>
<tr>
<td>Display Analog Sensor Inputs command (DSI)</td>
<td>131</td>
</tr>
<tr>
<td>Display Contact Inputs command (DCC)</td>
<td>122</td>
</tr>
<tr>
<td>Display Error Log command (DER)</td>
<td>174</td>
</tr>
<tr>
<td>Display Lucent Users command (DLU)</td>
<td>68</td>
</tr>
<tr>
<td>Display Modern Port Parameters command (DM)</td>
<td>41</td>
</tr>
<tr>
<td>Display Network Parameters command (DNP)</td>
<td>157</td>
</tr>
<tr>
<td>Display Network Status command (DNS)</td>
<td>158</td>
</tr>
<tr>
<td>Display Port Signals command (DPS)</td>
<td>144</td>
</tr>
<tr>
<td>Display Sensor Alarms command (DSA)</td>
<td>122</td>
</tr>
<tr>
<td>Display Sensor Inputs command (DSI)</td>
<td>122</td>
</tr>
<tr>
<td>Display Status of Contact Inputs</td>
<td></td>
</tr>
<tr>
<td>command (DCC)</td>
<td>132</td>
</tr>
<tr>
<td>Display System Parameters command (SSP)</td>
<td>115</td>
</tr>
<tr>
<td>Display Telnet Port Parameters command (DT)</td>
<td>161</td>
</tr>
<tr>
<td>Display User Record command (DUR)</td>
<td>63</td>
</tr>
<tr>
<td>DLU command</td>
<td>68</td>
</tr>
<tr>
<td>DM command</td>
<td>41</td>
</tr>
<tr>
<td>DNP command</td>
<td>157</td>
</tr>
<tr>
<td>DNS command</td>
<td>158</td>
</tr>
<tr>
<td>Documentation Conventions</td>
<td></td>
</tr>
<tr>
<td>DOLIST Action Routine</td>
<td>191</td>
</tr>
<tr>
<td>DPS command</td>
<td>144</td>
</tr>
<tr>
<td>DSA command</td>
<td>122</td>
</tr>
<tr>
<td>DSI command</td>
<td>122,131</td>
</tr>
<tr>
<td>DSP command</td>
<td>115</td>
</tr>
<tr>
<td>DT command</td>
<td>161</td>
</tr>
<tr>
<td>DU command</td>
<td>63</td>
</tr>
<tr>
<td>DUMP command</td>
<td>120,214,218</td>
</tr>
<tr>
<td>DUMPF command</td>
<td>120,216,219</td>
</tr>
</tbody>
</table>
### E

| Editing Keys | 13 |
| Editing Modes |   |
|   |   |
|   | editing keys | 13 |
|   | overview | 12 |
|   | TTY mode | 12 |
|   | VT-100 mode | 12 |
| Encryption Key Source | 30 |
|   | device ID/user code | 56 |
|   | fixed | 31, 56 |
|   | overview | 55 |
|   | randomly generated | 30, 55 |
| Environmental Manager |   |
|   | 48-volt battery | 130 |
|   | analog sensors | 130 |
|   | connections | 124 |
|   | contact closure inputs | 131 |
|   | functions and commands | 122 |
|   | interface | 124, 126 |
|   | options | 121 |
|   | overview | 121 |
|   | pinout | 126 |
|   | relays | 128 |
|   | temperature sensor input | 130 |
|   | voltage inputs | 130 |
| Event Table |   |
|   | overview | 89 |
| Events | 104 |
| Events and Action Routines |   |
|   | overview | 177 |

### F

| Failure History command (FH) | 172 |
| File Buffering |   |
|   | overview | 71 |
| File Command Summary | 86 |
| File Management Menu | 72 |
| Files |   |
|   | manage | 85 |
| Fixed Encryption Key Source | 56 |
| FTP |   |
|   | overview | 81 |
|   | parameters | 81, 155 |
|   | support | 150 |

### G

| GE command | 101 |
| Generate Alarm/Event command (GE) | 101 |

### H

| Host Port |   |
|   | buffer naming | 73 |
|   | buffering data automatically | 77 |
|   | buffering data manually | 79 |
|   | configure | 36 |
|   | display buffer status | 79 |
|   | parameters | 208 |
|   | send buffer file to administration PC | 80 |
|   | send buffer files via a dial-up connection | 80 |
|   | send buffer files via a direct connection | 80 |

### I

| INIT command | 40 |
| Installation | 20 |
| Internal Alarms and Events | 104 |
| Internal Events | 177 |
|   | .AUTHFAIL Internal Event | 177 |
|   | .BAT48HIGH Internal Event | 178 |
|   | .BAT48LOW Internal Event | 178 |
|   | .BAT48OK Internal Event | 179 |
|   | .BUFREADY Internal Event | 179 |
|   | .C#CLOSED Internal Event | 179 |
|   | .C#OPEN Internal Event | 179 |
|   | .CCLERROR Internal Event | 180 |
|   | .CLKCHANGE Internal Event | 180 |
|   | .DAILY Internal Event | 180 |
|   | .DISKCRIT Internal Event | 181 |
|   | .DISKFULL Internal Event | 181 |
|   | .DTRHIGH Internal Event | 181 |
|   | .DTRLOW Internal Event | 181 |
|   | .HOURLY Internal Event | 182 |
|   | .INTBATLOW Internal Event | 182 |
|   | .INTBATOK Internal Event | 182 |
|   | .LOGFULL Internal Event | 183 |
|   | .MAXRETRY Internal Event | 183 |
|   | .MDMINITERR Internal Event | 183 |
|   | .MEMLOW Internal Event | 183 |
|   | .MONTHLY Internal Event | 184 |
|   | .NETDOWN Internal Event | 184 |
|   | .NETUP Internal Event | 184 |
|   | .POWERLOW Internal Event | 184 |
|   | .POWEROK Internal Event | 185 |
|   | .POWERUP Internal Event | 185 |
|   | .PPPREQ Internal Event | 185 |
|   | .RTSHIGH Internal Event | 186 |
|   | .RTSLOW Internal Event | 186 |
|   | .S#HIGH Internal Event | 186 |
|   | .S#LOW Internal Event | 186 |
|   | .S#OK Internal Event | 186 |
|   | .TEMPHIGH Internal Event | 187 |
|   | .TEMPLOW Internal Event | 187 |
|   | .TEMPOK Internal Event | 187 |
|   | .WEEKLY Internal Event | 188 |
| IP Address | 32 |
**Index**

**R**
- RAM disk
  - events generated
  - files
  - organization
  - put configuration data on RAM disk file
  - put customer user table on RAM disk file
  - set protection parameters
- Randomly Generated Encryption Key Source
- RCV command
- RD command
- Receive Files
- Regular Callback Authentication
- Regular Callback Password/Callback Authentication
- Re-Initialize the ASG Guard
- Re-Initialize the ASG Guard Plus
- REMINIT Action Routine
- REN command
- RES command
- RESRELAY Action Routine
- Restart command (BOOT)
- Routine Parameters
- RRLY command

**S**
- SA command
- SAI - Schedule Action Item command
  - Event
  - Schedule Time
- SAI command
- Schedule Action Item command (SAI)
- SCHEDULE Action Routine
- Scheduling Parameters
- SCK command
- SDP command
- SDT command
- SEBUF command
- Security
  - ASG Key
  - authentication
  - block access
  - initiate security on the AUX port
  - limiting the number of sessions
  - overview
  - password
  - user expiration date
- Security Management
  - access classes
  - overview
  - user database
- SEND command
- Send Files
  - FTP
- Session Control Functions and commands
- Set Customer Key command (SCK)
- Set Date and Time command (SDT)
- Set Host command (SH)
- Set Host Processor Flag command (SHP)
- Set Modem Port Parameters command (SM)
- Set Network Parameters command (SNP)
- Set Relays command (SRLY)
- Set Sensor Alarms command (SSA)
- Set System Parameters command (SSP)
- modem action routine parameters
- scheduling parameters
- Site Information
- Set Telnet Port Parameters command (ST)
- Set Threshold Limits command (SSA)
- SETHP Action Routine
- SETRELAY Action Routine
- SH command
- SHP command
- Site Information
- Site name
- SM - Set Modem Port Parameters command
  - Baud Rate Settings
- Software upgrade
- SRLY command
- SSA command
- SSP command
- ST command
- STARTNET command
- Startup Network command (STARTNET)
- System Functions
  - overview
- System Functions Menu
- System Parameter Functions
  - overview

**T**
- Telnet
  - initiate a direct connect session
  - initiate a PPP session
  - Port Parameters
- Temperature Sensor Input
- Terminal Mode command (VT)
- Terminology
- Troubleshooting
- TTY Mode
Index

**U**

UPG command 119
Upgrade
  ASG Guard Plus software 119
  ASG Guard software 119
Upgrade the Software command (UPG) 119
User
  connectivity 133
User Connectivity
    authentication 134
    auto-baud 134
    auto-parity 134
    dial-up 133
    initiate a dial-up session 134
    overview 133
Session Control Functions and Commands 141
User Database 8
User Database 49
User Maintenance Functions Menu 50
Users
  add 25, 52
  block/unblock Lucent users 68
  change information 64
  delete 62
  display Lucent users 68
  display record 63
  list 60
  list Lucent users 68
Utility Programs
  CSUM.EXE 88
  overview 88
  ZPAD.EXE 88

**V**

Variable Callback Authentication 137
Variable Callback Password/Callback Authentication 58
VER command 118
VIEW command 87
View Session command (VS) 142
Voltage Inputs 130
VT command 143
VT100 command (VT) 143
VT-100 Mode 12

**X**

XA command 99
XE command 103
XU command 62

**Z**

ZPAD.EXE Program 88