

# T/MonXM Software

## User Manual



4955 East Yale Avenue  
Fresno, California 93727

(559) 454-1600  
Fax (559) 454-1688

support@dpstele.com  
www.dpstele.com

**CHANGE  
NOTICE**

This manual has been updated for version 6.8 and later. See the appropriate Quick Start guide for your software version for further details.

Retail price \$79.

Copies of this manual are available on CD-ROM.

The material in this manual is for information purposes and is subject to change without notice. DPS Telecom shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

This document contains proprietary information which is protected by copyright. All rights are reserved. No part of this document may be photocopied without prior written consent of DPS Telecom.

© Copyright 2012, DPS Telecom

---

## Warranty

DPS Telecom warrants, to the original purchaser only, that its products a) substantially conform to DPS' published specifications and b) are substantially free from defects in material and workmanship. This warranty expires two years from the date of product delivery with respect to hardware and ninety days from the date of product delivery with respect to software. If the purchaser discovers within these periods a failure of the product to substantially conform to specifications or that the product is not substantially free from defects in material and workmanship, the purchaser must promptly notify DPS. Within a reasonable time after notification, DPS will endeavor to correct any substantial non-conformance with the specifications or substantial defects in material and workmanship, with new or used replacement parts. All warranty service will be performed at the company's office in Fresno, California, at no charge to the purchaser, other than the cost of shipping to and from DPS, which shall be the responsibility of the purchaser. If DPS is unable to repair the product to conform to the warranty, DPS will provide at its option one of the following: a replacement product or a refund of the purchase price for the non-conforming product. These remedies are the purchaser's only remedies for breach of warranty. Prior to initial use the purchaser shall have determined the suitability of the product for its intended use.

DPS does not warrant a) any product, components or parts not manufactured by DPS, b) defects caused by the purchaser's failure to provide a suitable installation environment for the product, c) damage caused by use of the product for purposes other than those for which it was designed, d) damage caused by disasters such as fire, flood, wind or lightning unless and to the extent that the product specification provides for resistance to a defined disaster, e) damage caused by unauthorized attachments or modifications, f) damage during shipment from the purchaser to DPS, or g) any abuse or misuse by the purchaser.

THE FOREGOING WARRANTIES ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

In no event will DPS be liable for any special, incidental, or consequential damages based on breach of warranty, breach of contract, negligence, strict tort, or any other legal theory. Damages that DPS will not be responsible for include but are not limited to: loss of profits; loss of savings or revenue; loss of use of the product or any associated equipment; cost of capital; cost of any substitute equipment, facilities or services; downtime; claims of third parties, including customers; and injury to property.

The purchaser shall fill out the requested information on the Product Warranty Card and mail the card to DPS. This card provides information that helps DPS make product improvements and develop new products.

For an additional fee DPS may, at its option, make available by written agreement only an extended warranty providing an additional period of time for the applicability of the standard warranty.

---

## Technical Support

If a purchaser believes that a product is not operating in substantial conformance with DPS' published specifications or there appear to be defects in material and workmanship, the purchaser should contact our technical support representatives. If the problem cannot be corrected over the telephone and the product and problem are covered by the warranty, the technical support representative will authorize the return of the product for service and provide shipping information. If the product is out of warranty, repair charges will be quoted. All non-warranty repairs receive a 90-day warranty.





# Supported Systems

**T/Mon LNX**

---



**T/Mon NOC**

---



**T/Mon LT**

---



**T/Mon SLIM**

---



**IAM-5**

---



**IAM**

---



**T/MonXM Workstation**

---



# Quick Reference Table of Contents

## Section:

1	-	T/Mon NOC/LNX Hardware Installation Guide .....	1-1
2	-	Starting T/MonXM Software .....	2-1
3	-	Network Setup .....	3-1
4	-	T/MonXM Interface .....	4-1
5	-	Configuring Remote Access .....	5-1
6	-	Define Windows .....	6-1
7	-	Managing System Users .....	7-1
8	-	Configure Pager and Email Alarm Notification .....	8-1
9	-	Define Remote Ports and Virtual/LAN Jobs .....	9-1
10	-	Point Definition Tutorial .....	10-1
11	-	Display Mapping Reference Guide .....	11-1
12	-	Configure Controls .....	12-1
13	-	Define Building Status Unit Controls .....	13-1
14	-	Defining Internal Alarms .....	14-1
15	-	Configuring Root Groups .....	15-1
16	-	Define Miscellaneous Parameters .....	16-1
17	-	Monitor Mode Tutorial .....	17-1
18	-	Web Browser Interface .....	18-1
19	-	Managing System Files .....	19-1
20	-	Managing Reports .....	20-1
21	-	Configure Redundant Dual T/Mon Back-up .....	21-1
22	-	DNS .....	22-1

## Software Module Section:

M1	-	DCP(F) Interrogators and Responders.....	M1-1
M2	-	TRIP Dial-up.....	M2-1
M3	-	Standard Dial-up Remotes .....	M3-1
M4	-	Badger Interrogator.....	M4-1
M5	-	Larse Interrogator.....	M5-1
M6	-	ASCII Interrogator .....	M6-1
M7	-	E2A Interrogators and Responders.....	M7-1
M8	-	DCM Interrogator .....	M8-1
M9	-	TBOS Interrogators and Responders .....	M9-1
M10	-	FX 8800 Interrogators.....	M10-1
M11	-	Integrated SNMP Agent.....	M11-1
M12	-	SNMP Trap Processor.....	M12-1
M13	-	TL1 Responder.....	M13-1
M14	-	TABS Responder .....	M14-1
M15	-	FTP Server .....	M15-1
M16	-	Pulsecom Datalok Interrogator .....	M16-1
M17	-	DTMF On-Call.....	M17-1
M18	-	NEC 21SV Interrogator .....	M18-1
M19	-	Modbus Interrogator .....	M19-1
M20	-	8 Port Teltrac MUX Interrogator.....	M20-1
M21	-	8 Port ASCII MUX Interrogators and Responders.....	M21-1
M22	-	Building Access System .....	M22-1
M23	-	Alarm Message Forwarding.....	M23-1
M24	-	T/Mon SQL.....	M24-1
M25	-	Hard Drive Mirroring.....	M25-1
M26	-	ASCII Query Language (AQL) .....	M26-1
M27	-	TAP Interrogator .....	M27-1
M28	-	DNP3 Interrogator.....	M28-1
M29	-	ASCII Gateway.....	M29-1

M30	–	Modbus Responder .....	M30-1
M31	–	DNP3 Responder.....	M31-1
M32	–	SiteDialer for T/Mon.....	M32-1

## Appendix:

A	–	ASCII Tutorial .....	A-1
B	–	Define Controller Cards .....	B-1
C	–	Configuring a X.25 Port Card .....	C-1
D	–	Ethernet Card Installation .....	D-1
E	–	Diagnostics .....	E-1
F	–	Disk Files .....	F-1
G	–	Uninterruptible Power System .....	G-1
H	–	Troubleshooting .....	H-1
I	–	Quick Reference Tables .....	I-1
J	–	Modem Initialization Strings .....	J-1
K	–	LED Display Bar .....	K-1
L	–	Frequently Asked Questions .....	L-1
M	–	Hardware Installation Quick Reference .....	M-1
N	–	Text/Message Definition .....	N-1

# Table of Contents

About This Manual .....	1
-------------------------	---

## Section 1 - T/Mon NOC/LNX Hardware Installation Guide ..... 1-1

Slide Rack Mounting .....	1-1
Back Panel Connections .....	1-4
Slide Rack Mounting .....	1-5
Network Connections .....	1-7
Serial Port Pinouts .....	1-8
Changing Port Interface Cartridges .....	1-10
LCD Display .....	1-13

## Section 2 - Starting T/MonXM Software ..... 2-1

W/Shell .....	2-1
Run T/MonXM from W/Shell.....	2-2
Upgrading The Software from a CD.....	2-2
Upgrading The Software from Floppy Disks.....	2-6
Remove Software .....	2-10
History Command Keys.....	2-11
Installation History .....	2-11
T/Link .....	2-12
Quit .....	2-12
T/Link File Transfer .....	2-14
System Time .....	2-15
Format Floppy Disk.....	2-15
Workstation Info Menu .....	2-16
Automatic Backup .....	2-17

## Section 3 - Network Setup..... 3-1

Ethernet I/O .....	3-1
Step One: Network Setup for NOC, SLIM, and IAM.....	3-1
Step One: Network Setup for LNX.....	3-3
Step Two: Port 28 .....	3-5

Step Three: TCP Ports.....	3-6
Assigning a Data Connection .....	3-7
Define the TCP port .....	3-8
Define the port usage .....	3-9
Assign the data connection .....	3-6
<b>Section 4 - T/MonXM Interface .....</b>	<b>4-1</b>
T/MonXM Interface Menus .....	4-1
Function Hot Key Commands.....	4-2
Common Key Commands .....	4-2
Menu List Box.....	4-3
Hot Key Edit Commands .....	4-4
Standard Database Field Editing .....	4-5
<b>Section 5 - Configuring Remote Access .....</b>	<b>5-1</b>
Port Usage .....	5-1
Serial Format (Physical ports only) .....	5-1
Terminal Type.....	5-1
Modem Config .....	5-2
Fast Answer.....	5-2
Printer Logging .....	5-2
Auto Login Inits.....	5-2
Remote Access Audible Options.....	5-3
Remote Access Server.....	5-4
Log On/Off .....	5-8
Remote Terminal Control Keys .....	5-9
Terminal Driver Query.....	5-9
Help Screen .....	5-9
Refreshing the Terminal Display .....	5-9
Changing Terminal Drivers.....	5-9
Selecting Function Keys on Remotes.....	5-10
Selecting Shift Function Keys.....	5-10
Selecting Function Keys .....	5-10
Selecting Alternate Function Keys .....	5-10
Selecting Control Function Keys .....	5-10
Selecting Special Keys on Remotes .....	5-10
Alarm Printer Logging .....	5-11
Cursor Movement Keys.....	5-11
Remote Users over LAN .....	5-12
<b>Section 6 - Define Windows .....</b>	<b>6-1</b>
Windows Screen.....	6-1
Window Definition .....	6-3
<b>Section 7 - Managing System Users .....</b>	<b>7-1</b>
System User Access Overview .....	7-1
Define System Users .....	7-2
Security Help Screen .....	7-4
Copy System User Attributes .....	7-5
<b>Section 8 - Configure Pager and Email Alarm Notification.....</b>	<b>8-1</b>
Introduction.....	8-1
Pager and Email Alarm Notification Setup Overview .....	8-2
Pager and Email Field Options Relationships .....	8-3
System Security.....	8-4
Parameters .....	8-4

Pager Profiles .....	8-4
Operators .....	8-5
Pager Carrier .....	8-5
Pager Scheduling.....	8-5
Pager Alarm Notification Port Setup.....	8-6
Setup Procedure Overview.....	8-6
Setup Procedure Detail.....	8-6
SNPP Alarm Notification Port Setup .....	8-8
Setup Procedure Overview.....	8-8
Setup Procedure Detail.....	8-8
Email Alarm Notification Port Setup .....	8-10
Setup Procedure Overview.....	8-10
Setup Procedure Detail.....	8-10
Pager Carriers .....	8-13
Entering Email Addresses .....	8-15
Weekly Operator Schedules .....	8-17
Schedule Exceptions.....	8-19
Alphanumeric Pager Formats .....	8-20
Pager Profiles.....	8-24
Entering Pager Profiles .....	8-27
Groups.....	8-28
<b>Section 9 - Define Remote Ports and Virtual/LAN Jobs .....</b>	<b>9-1</b>
Remote Port Definition.....	9-2
Remote Port Parameter Defaults .....	9-3
Ping Interrogator.....	9-4
Craft Interface.....	9-7
Network Time (NTP) .....	9-9
Time Service.....	9-11
<b>Section 10 - Point Definition Tutorial .....</b>	<b>10-1</b>
Introduction.....	10-1
1.0 Suggested Routines .....	10-1
1.1. Develop a Generic display .....	10-1
1.2. Create the Generic display .....	10-1
2.0 Point Editing.....	10-2
Point Definition Commands.....	10-3
Address Defaults .....	10-8
3.0. Editing Shortcuts .....	10-9
3.4. Vertical Editing.....	10-10
4.0. Point (Line) Editing.....	10-11
5.0. Point (Line) Copying.....	10-11
6.0. Column (Attribute) Entry .....	10-13
7.0 Description Modification.....	10-14
8.0. Windows Modification .....	10-19
9.0. Message Translation.....	10-20
10.0. Cloning Entire Displays or Sites .....	10-21
11.0. Cloning Part of a Display .....	10-22
12.0 Device Templates .....	10-24
<b>Section 11 - DPS Display Mapping Guide.....</b>	<b>11-1</b>
Introduction.....	11-1
NetGuardian 832A/NetMediator .....	11-1
NetGuardian 216.....	11-2

NetGuardian- Q8 .....	11-3
KDA Remotes.....	11-4
TBOS Protocol .....	11-9
Modular Alarm System .....	11-10
Protection Switch.....	11-11
NetMediator T2S .....	11-11
<b>Section 12 - Configure Controls .....</b>	<b>12-1</b>
Site Controls .....	12-1
Labeled Controls Definition .....	12-6
Derived Alarms/ Controls.....	12-10
How an Equation is Evaluated.....	12-14
Creating Derived Alarms for Events That Don't Happen.....	12-15
<b>Section 13 - Define Building Status Unit Controls .....</b>	<b>13-1</b>
Introduction .....	13-1
BSU Activation Overview .....	13-1
Assign Controls .....	13-2
Configure Sanity Frequency .....	13-4
<b>Section 14 - Define Internal Alarms .....</b>	<b>14-1</b>
Internal Alarms Point Definition Screen .....	14-3
Standard Internal Alarms.....	14-3
Address 0 Display 1 Alarms.....	14-6
Address 0 Display 2 Alarms.....	14-10
Address 13 Display 1 Alarms.....	14-11
Internal Alarms Assignments .....	14-11
User Defined Internal Alarms .....	14-13
How To Create User Defined Internal Alarms .....	14-14
<b>Section 15 - Configuring Root Groups .....</b>	<b>15-1</b>
Root Groups.....	15-1
<b>Section 16 - Define Miscellaneous Parameters .....</b>	<b>16-1</b>
Define Miscellaneous Parameters .....	16-1
<b>Section 17 - Monitor Mode Tutorial.....</b>	<b>17-1</b>
Monitor Mode Overview .....	17-1
Alarm Summary Screen .....	17-3
Alarm Summary Window.....	17-4
Page Index Window .....	17-6
Summary Legend Window.....	17-8
Monitor Sub-Mode Descriptions.....	17-10
Monitor Alarm Point Descriptions .....	17-11
Monitor Mode Operation Notes .....	17-12
Automatic History Purging .....	17-12
Standing Alarm Virtual Mode.....	17-12
Automatic Alarm Acknowledging.....	17-12
Initialization.....	17-13
Core Prep.....	17-14
Alarm Formatting .....	17-15
Level and Status Attributes .....	17-19
Level and Status Matrix .....	17-20
Alarm Message Forwarding .....	17-21
Basic Operation and Setup .....	17-21

Alarm Forward Parameters.....	17-22
Alarm Summary Colors.....	17-23
Change Of State (COS) Alarms .....	17-25
First Column Descriptions .....	17-26
ACK Alarms .....	17-27
Standing Alarms .....	17-28
Root Alarm Filter Status.....	17-30
TAG Alarms .....	17-31
Silence Alarms/Windows .....	17-31
Performance/Statistics Mode.....	17-32
Site Controls .....	17-35
Site Controls Point Selection.....	17-37
Individual Point Operation .....	17-37
Batch Point Operation .....	17-39
Alarm Indicator Control .....	17-40
English Analyzer Mode/English Filter .....	17-43
Report Mode .....	17-45
Protocol Analyzer .....	17-47
Channel Summary .....	17-49
Dialup Site Monitor .....	17-50
System Information .....	17-52
Craft Mode.....	17-54
Labeled Controls Mode .....	17-56
Labeled Controls Point Selection .....	17-58
Individual Point Operation .....	17-58
Batch Point Operation .....	17-60
Pager Status in Monitor Mode .....	17-61
Lock Function .....	17-61
Flush Pager Queue .....	17-62
Sending Pager Messages .....	17-62
Site Statistics.....	17-63
View Analogs .....	17-66
Exit Monitor Mode (Log Off/On) .....	17-67
<b>Section 18 - Web Browser Interface .....</b>	<b>18-1</b>
Features Overview .....	18-1
Browser Compatibility .....	18-1
Set Up Procedure Overview .....	18-1
TCP and UDP Procedure Detail.....	18-2
Connecting via Web Browser.....	18-6
Using the Classic Web Browser Interface.....	18-7
Preferences.....	18-11
Using the Web 2.0 Browser Interface .....	18-12
Using the Mobile Web Interface (T/Mon LNX Only) .....	18-16
<b>Section 19 - Managing System Files.....</b>	<b>19-1</b>
Utilities Menu .....	19-1
Back Up Data Files .....	19-1
Restore Data Files .....	19-3
History File Purge .....	19-4
Trouble Log Purge .....	19-5
Compress History.....	19-6
Disk Information .....	19-7
Compress Points.....	19-7
Report Maintenance .....	19-8
Rebuild Key Files.....	19-9

Delete System Log .....	19-11
Delete Live Files .....	19-12
Preventive Maintenance .....	19-13
Import Alarm Definitions .....	19-13
File Preparation .....	19-13
Importing a File .....	19-14
MIB File Manager .....	19-15
Import MIB .....	19-15
View Logs .....	19-16
Compile MIBs .....	19-16
Delete MIB .....	19-17
Import/Export ASCII Rules .....	19-17
Export ASCII Rules .....	19-18
Import ASCII Rules .....	19-19
T/MonXM Disk Files .....	19-20
Program Files .....	19-20
Database Files .....	19-20
<b>Section 20 - Managing Reports .....</b>	<b>20-1</b>
Running Reports from T/RemoteW and T/Windows .....	20-5
History Report .....	20-5
Standard History .....	20-6
Export History .....	20-9
Duration Summary (Time) .....	20-10
Duration History .....	20-10
Duration History (Incident) .....	20-12
Duration Summary (Incident) .....	20-13
Duration Detail (Incident) .....	20-14
Dial-Up History Report .....	20-15
Alarm Database Report .....	20-17
1. Remote Ports .....	20-19
2. Windows .....	20-20
3. Text/Messages .....	20-20
7. Derived .....	20-21
4, 5, 6. ASCII Rules, Tables and Actions .....	20-21
8. VDMs .....	20-22
9. Site Reports .....	20-22
10. BSU .....	20-25
11. Cards .....	20-25
12. Dial-Up Sites .....	20-26
13. KDA Shelves .....	20-28
14. Export Alarms .....	20-28
Labeled Controls Report .....	20-30
Site Controls Report .....	20-31
LED Bars Report .....	20-31
Users Report .....	20-32
Building Access .....	20-32
Pager .....	20-33
View Report File .....	20-37
Report Mode in Monitor Mode .....	20-38
Hard Copy .....	20-40
Trouble Log Mode in Monitor Mode .....	20-42
Trouble Log Print Mode .....	20-45
Compile Trouble Log Reports .....	20-45
View compiled Trouble Log reports .....	20-47
Related Trouble Log Sections .....	20-48



<b>Section 21 - Configure Redundant Dual T/Mon Backup .....</b>	<b>21-1</b>
Overview.....	21-1
TMonNET.....	21-2
Port .....	21-3
TMonNET Address.....	21-5
Node Definition.....	21-6
TMonNET Transfer.....	21-9
Other Parameters .....	21-10
Databasing .....	21-11
TMonNET Alt. Path.....	21-11
Databasing Requirements .....	21-12
English Messages .....	21-13
Housekeeping Alarms .....	21-14
TMONNET ALT. PATH FAILED .....	21-14
Testing the Alternate Communication Path.....	21-15
<b>Section 22 - DNS .....</b>	<b>22-1</b>
Overview.....	22-1
DNS Operation .....	22-2
<b>Software Module 1 DCP(F) Interrogators and Responders.....</b>	<b>M1-1</b>
DCP(F) Interrogator .....	M1-1
Define a Virtual (IP) Port for DCP(F) Interrogators .....	M1-3
Create a Data Connection .....	M1-3
DCP(F) Device Definition.....	M1-4
Defining an Address.....	M1-5
Point Definition (F1) .....	M1-7
Analog Point Definition (F5) .....	M1-8
Analog Display Worksheet.....	M1-9
Device Failures/Offlines (F3).....	M1-10
Control Relays .....	M1-10
DCP(F) Database Transfer .....	M1-11
TMonNET Port .....	M1-11
TMonNET Address.....	M1-12
TMonNET Nodes.....	M1-13
DCP(F) Network Status (Monitor Mode) .....	M1-15
Manual NRI sync .....	M1-15
Address Statistics (Monitor Mode) .....	M1-16
View Analogs .....	M1-18
DCP(F) Responder .....	M1-19
Remote Device Definition.....	M1-20
Responder Definition .....	M1-21
LAN-Based Remotes —NetGuardian .....	M1-22
Define a job port for DCP(F) Interrogator.....	M1-22
Create a Data Connection .....	M1-23
Define the NetGuardian .....	M1-24
NetGuardian Device Definition .....	M1-26
Define Points.....	M1-27
Define Analog Points (Optional) .....	M1-28
Analog Display Worksheet .....	M1-29
Define Internal Alarms.....	M1-30
Define Control Relays (Optional) .....	M1-30
Global Options .....	M1-31
Expansion Module — NetMediator 4-Port TBOS/TABS.....	M1-32

Define a Remote Port for the DCP(F) Interrogator .....	M1-33
Create a Data Connection .....	M1-33
Define DCP1 Remotest — Harris™ DS5000 .....	M1-33
Define your DCP1 devices.....	M1-34
Define Alarm Points.....	M1-35
Define Analog Points (Optional) .....	M1-35
Define Internal alarm (Optional).....	M1-35
Define Control Relays (Optional) .....	M1-36
Provision the Accumulator Timer .....	M1-36
Ring Polling Application .....	M1-37
Alt Path Switch.....	M1-39
Define the Remote Port.....	M1-39
Define the Remote Device Definition.....	M1-40
Provision the Unit .....	M1-41
Configure Alarm Points. ....	M1-42
Configure Controls.....	M1-43
Define Site Control Categories.....	M1-43
Issue Site Controls .....	M1-46
Download Configuration to the Alt Path Switch.....	M1-47
Protection Switch.....	M1-49
MAT (400) and Dial-Up MAT (400).....	M1-51
DCP(F) Dial-Up .....	M1-53
<b>Software Module 2 TRIP Dial-Up.....</b>	<b>M2-1</b>
<b>Software Module 3 Standard Dial-Up Remotes .....</b>	<b>M3-1</b>
Dial-Up Networks.....	M3-1
DPM Sites .....	M3-2
AlphaMax 82A and 82S Sites.....	M3-3
KDA 864 and KDA 832-T8 Sites.....	M3-4
Options and Model Numbers .....	M3-5
KDA-TS Sites .....	M3-5
KDA 832-T8 Sites .....	M3-5
Datalok 10D Sites .....	M3-5
MAS Sites .....	M3-6
ASCII Sites.....	M3-6
KDA Shelves .....	M3-7
Centrally Administered Configuration.....	M3-7
Provisioning Expansion Cards - 16 Channel Analog.....	M3-21
Provisioning Expansion Cards - LR-24 Relay Card .....	M3-24
8 Analog and 4 TBOS Expansion Card .....	M3-25
Downloading the Provisioning File.....	M3-27
Virtual Port Type Assignment .....	M3-27
Dial-Up Remotes .....	M3-28
DPM Sites .....	M3-28
AlphaMax 82A Sites.....	M3-28
DPM 216 Sites .....	M3-28
KDA 864, KDA-TS, KDA 832-T8 Sites.....	M3-28
Datalok 10D Sites .....	M3-29
ASCII Sites.....	M3-29
MAS Sites .....	M3-29
Defining a Remote DPM, AlphaMax, or Net Dog .....	M3-30
Site Definition .....	M3-31
Device Definition .....	M3-32

Point Definition .....	M3-34
DPM and AlphaMax Provisioning .....	M3-35
Pager Assignments .....	M3-35
Alarm Provisioning .....	M3-37
Relay Provisioning .....	M3-39
Advanced Provisioning .....	M3-40
Derived Controls .....	M3-41
<b>Software Module 4 Badger Interrogator .....</b>	<b>M4-1</b>
Install or Upgrade the Software .....	M4-1
Configure the Badger Interrogator .....	M4-1
Define the Remote Port .....	M4-1
Define Badger Remote Devices .....	M4-2
Define Alarm Points .....	M4-4
Define Analog Points .....	M4-6
Analog Display Worksheet .....	M4-7
Define Internal Alarms .....	M4-8
Define Control Relays .....	M4-9
<b>Software Module 5 Larse Interrogator .....</b>	<b>M5-1</b>
Software Installation .....	M5-1
Configuration .....	M5-1
Define the Remote Port .....	M5-1
Define Larse/Badger Remote Devices .....	M5-2
Provision the Larse/Badger Remote Unit .....	M5-4
Define T/MonXM Analog Alarm Thresholds .....	M5-7
Analog Display Worksheet .....	M5-8
Note on Analog Alarms .....	M5-9
Define Alarm Points .....	M5-10
Define Internal Alarms .....	M5-10
Define Control Relays .....	M5-11
<b>Software Module 6 ASCII Interrogator .....</b>	<b>M6-1</b>
Introduction .....	M6-1
How to Use this Section .....	M6-2
ASCII Terms/Glossary .....	M6-3
Basic Concepts .....	M6-5
Message Processing .....	M6-6
Navigating the ASCII Device Rules screens .....	M6-7
ASCII Connectivity Test .....	M6-10
Numbered Rules .....	M6-11
ASCII Processing Language .....	M6-14
Match commands .....	M6-17
Positioning Commands .....	M6-19
Slot Commands .....	M6-21
Loop Commands .....	M6-28
While Loops .....	M6-28
Repeat Loops .....	M6-28
While Line Loops .....	M6-30
Detailed Logging .....	M6-35
ASCII Tables .....	M6-37
ASCII Parameters .....	M6-36
ASCII Scripts .....	M6-37
ASCII Debug .....	M6-38
Debug Slot Contents .....	M6-42
Alarm Processing — Overview .....	M6-44

Remote Ports, ASCII Dial-Up.....	M6-45
Properties to be Databased Overview .....	M6-45
Incoming Call Device Type Identification.....	M6-47
Selecting the Device Type Using the \KDlit Command.....	M6-49
ASCII Dial-Up Definition .....	M6-50
Remote Ports, Dedicated ASCII.....	M6-54
ASCII Point Definitions .....	M6-58
ASCII Action Definitions.....	M6-61
ASCII Templates .....	M6-63
Build a Template.....	M6-63
Template Site Definition .....	M6-64
Attach a Template to a Site.....	M6-64
ASCII Analyzer Display Modes .....	M6-65
ASCII Analyzer .....	M6-65
Port and Rule Selection.....	M6-65
Logging .....	M6-66
Auto-Databasing ASCII .....	M6-71
Overview .....	M6-71
Slots and Keys.....	M6-72
Key Mapping.....	M6-74
Alarm Status.....	M6-75
Alarm Level.....	M6-77
Text Message.....	M6-78
Pager Profile.....	M6-79
Categories (Windows).....	M6-80
Screen Log.....	M6-81
Alarm History.....	M6-82
Alarm Qualification.....	M6-83
Alarm Counter.....	M6-84
The \!AUTO Command .....	M6-85
Remote Port Definition .....	M6-87
ASCII Input Device Definition .....	M6-87
Clear All.....	M6-87
ASCII Action Definitions .....	M6-88
Auto-ASCII Site Definition .....	M6-89
Point Definition .....	M6-91
Conclusion .....	M6-91
<b>Software Module 7 E2A Interrogators and Responders .....</b>	<b>M7-1</b>
E2A Interrogators .....	M7-1
Remote Device Definition.....	M7-4
Point Definition.....	M7-5
Internal Alarms.....	M7-6
E2A Responders .....	M7-7
Remote Device Definition.....	M7-8
Responder Definition .....	M7-9
Miscellaneous Interrogator/ Responder Notes .....	M7-10
<b>Software Module 8 DCM Interrogator.....</b>	<b>M8-1</b>
DCM Interrogator Remote Port Definition .....	M8-1
Remote Device Definition.....	M8-3
Point Definition .....	M8-5
Internal Alarms.....	M8-6
<b>Software Module 9 TBOS Interrogators and Responders .....</b>	<b>M9-1</b>
TBOS Interrogator.....	M9-1

TBOS Remote Device Definition .....	M9-2
Internal Alarms.....	M9-5
TBOS Responder.....	M9-6
TBOS Responder Remote Device Definition .....	M9-7
TBOS Responder Definition.....	M9-8
<b>Software Module 10 FX 8800 Interrogator.....</b>	<b>M10-1</b>
FX 8800 Interrogator.....	M10-1
Remote Device Definition.....	M10-2
Point Definition.....	M10-4
FX 8800 Alarm Output Mapping.....	M10-5
Internal Alarms.....	M10-7
<b>Software Module 11 Integrated SNMP Agent.....</b>	<b>M11-1</b>
SNMP Agent Configuration.....	M11-1
Performance/Stats.....	M11-4
SNMP Manager Display.....	M11-5
<b>Software Module 12 SNMP Trap Processor.....</b>	<b>M12-1</b>
Introduction.....	M12-1
Install or Upgrade the Software.....	M12-1
Configuration .....	M12-1
Shortcut Commands .....	M12-24
Copy, Next, and Previous .....	M12-24
Translate Command .....	M12-24
<b>Software Module 13 TL1 Responder.....</b>	<b>M13-1</b>
TL1 Tutorial .....	M13-1
TL1 Responder .....	M13-1
Transaction Language 1 (TL1) .....	M13-1
SIDs and AIDs .....	M13-2
TL1 Responder Setup Procedure.....	M13-4
Defining TL1 Source Interrogators .....	M13-5
SID Definition Screen.....	M13-6
Defining TL1 Alarm Points.....	M13-7
Alarm Point Definition Keys .....	M13-7
TL1 Alarm Point Attributes .....	M13-8
Alarm Definition Commands .....	M13-9
Defining TL1 Control Points.....	M13-13
Command: OPR-EXT-CONT.....	M13-14
Command: RLS-EXT-CONT .....	M13-14
Command: RTRV-ATTR-CONT .....	M13-14
Command: SET-ATTR-CONT .....	M13-14
Defining TL1 Responders .....	M13-15
Remote Device Definition.....	M13-16
Responder Definition.....	M13-18
TL1 User Input Command Errors .....	M13-19
IISP - Input, Invalid Syntax or Punctuation.....	M13-19
ICNV - Input, Command Not Valid .....	M13-19
IDNV - Input, Data Not Valid .....	M13-19
TL1 Messages .....	M13-20
TL1 Commands, Messages and Codes.....	M13-20
TL1 Commands .....	M13-20
Error Codes and Meanings.....	M13-20
IITA - Input, Invalid Target identifier.....	M13-21
IIAC - Input, Invalid ACcess Identifier.....	M13-21

IICT - Input, Invalid Correlation Tag.....	M13-21
SROF - Status, Request Operation Failed .....	M13-21
Configuration Tables .....	M13-22
TL1 Glossary .....	M13-23
TL1 Command Overview.....	M13-24
Notations .....	M13-24
General Command Syntax .....	M13-24
Mod .....	M13-24
TID .....	M13-25
AID.....	M13-25
CTAG.....	M13-25
ATAG.....	M13-25
Data parameters.....	M13-25
; (semi colon).....	M13-26
Short cuts.....	M13-26
TL1 Command Definitions.....	M13-27
<b>Software Module 14 TABS Responder.....</b>	<b>M14-1</b>
Protocol Mediation Steps .....	M14-1
TABS Responder Setup.....	M14-1
Defining the Remote Port .....	M14-1
Defining the TABS Master .....	M14-2
Mapping Devices to the TABS Display .....	M14-3
<b>Software Module 15 FTP Server.....</b>	<b>M15-1</b>
Set up a FTP Server.....	M15-2
Setup a FTP Server Job.....	M15-2
Setup a FTP Data Transfer Job .....	M15-4
Test the FTP Connection.....	M15-6
<b>Software Module 16 Pulsecom Datalok Interrogator .....</b>	<b>M16-1</b>
Overview.....	M16-1
Network Design.....	M16-1
Datalok Operational Summary .....	M16-1
Provisioning 10A Units .....	M16-2
Remote Device Definition.....	M16-3
Point Definition .....	M16-5
Device Internal Alarm Assignment.....	M16-7
D10 Alarm Point Definition.....	M16-8
D10 Control Point Definition.....	M16-9
D10 Analog Point Definition .....	M16-10
Analog Display Worksheet .....	M16-11
Move Address .....	M16-12
Define Points for TL1 Alarm Reporting.....	M16-12
Define Remote Parameters.....	M16-13
Provisioning 10D Units .....	M16-13
D10 Site Definition .....	M16-14
Datalok 10D Device Definition .....	M16-15
D10 Analog Point Definition .....	M16-17
D10 Control Point Definition.....	M16-17
D10 Alarm Point Definition.....	M16-17
Internal Alarms Definition .....	M16-17
Point Definition.....	M16-17
D10 Modem Point Definition .....	M16-18
Define Points for TL1 Alarm Reporting.....	M16-19

Labeled Controls .....	M16-19
Internal Device Failures .....	M16-19
10A Statistic Explanations .....	M16-19
10D Dialup Stats.....	M16-19
Monitor Mode Options .....	M16-19
Configuration Tables .....	M16-22
Point Display Mapping .....	M16-22
Datalok Alarm Points to T/MonXM Display Conversion.....	M16-22
Datalok Housekeeping Mapping.....	M16-24
Control Point Mapping.....	M16-25
Expansion Cards 2 and 3 Analog Point Mapping.....	M16-26
<b>Software Module 17 DTMF On-Call .....</b>	<b>M17-1</b>
Setup .....	M17-1
Barge-In Feature (Bypass Automated Menu Prompts).....	M17-2
Pager Carrier Response Options .....	M17-2
Operation - How to Ack/Tag Alarms.....	M17-3
Problem Message Numbers.....	M17-4
<b>Software Module 18 21SV Interrogator .....</b>	<b>M18-1</b>
21SV Interrogator Setup.....	M18-1
Defining the Remote Port .....	M18-1
Defining 21SV Remote Devices .....	M18-2
Define Alarm Points.....	M18-4
Point Mapping.....	M18-4
Provision the NEC 21SV Device.....	M18-5
Monitor Points Provision .....	M18-6
Provision Control Points .....	M18-7
Define Controls for the 21SV/RA or 21SV/EXP 32 DO .....	M18-8
<b>Software Module 19 Modbus Interrogator .....</b>	<b>M19-1</b>
Install or Upgrade the Software .....	M19-1
Configure the Modbus Interrogator .....	M19-1
Define the Remote Port .....	M19-1
Create a Data Connection (Virtual Port Jobs).....	M19-2
Define Modbus Remote Device .....	M19-5
Define Alarm Points .....	M19-6
Define Internal Alarms (Optional) .....	M19-7
Define Modbus Addressing.....	M19-7
Define Analog Points (Optional).....	M19-11
Import/Export Modbus Templates.....	M19-12
<b>Software Module 20 8 Port Teltrac MUX Interrogator .....</b>	<b>M20-1</b>
Define a Remote Port.....	M20-1
Remote Device Definition.....	M20-3
Define a Virtual Port Job .....	M20-4
Remote Device Definition (Virtual Port).....	M20-5
Create a Data Connection .....	M20-7
<b>Software Module 21 ASCII MUX Interrogators and Responders .....</b>	<b>M21-1</b>
Prepare ASCII Rules.....	M21-1
Define a Remote Port.....	M21-1
Remote Device Definition.....	M21-1
Define a Virtual Port Job .....	M21-2

Create a Data Connection .....	M21-4
<b>Software Module 22 Building Access System .....</b>	<b>M22-1</b>
BAS for NetGuardian .....	M22-2
BAS Global.....	M22-11
Site Log In Status .....	M22-12
BAS for KDA .....	M22-13
DTMF Access.....	M22-16
Building Access Unit (BAU) .....	M22-23
Site Report .....	M22-31
Frequently Asked Questions.....	M22-32
<b>Software Module 23 Alarm Message Forwarding.....</b>	<b>M23-1</b>
Basic Operation and Setup.....	M23-1
Alarm Forward Parameters .....	M23-2
<b>Software Module 24 T/Mon SQL.....</b>	<b>M24-1</b>
I. Configure T/Mon SQL Agent .....	M24-1
I.A Application Options.....	M24-3
I.B Debug Mode.....	M24-4
Data Dictionary .....	M24-5
II. Configure Settings for the T/Mon SQL Agent .....	M24-7
II.A Remote Parameters Settings .....	M24-7
II.C Define the Remote Device.....	M24-9
II.B Setup a Data Connection .....	M24-9
II.F Performance/Stats in Monitor Mode.....	M24-10
II.D Internal Alarms .....	M24-10
<b>Software Module 25 T/Mon Hard Drive Mirroring.....</b>	<b>M25-1</b>
Hard Drive Recovery Program.....	M25-2
Hard Drive Recovery Status Messages.....	M25-3
Abnormal Hard Drive Recovery .....	M25-3
<b>Software Module 26 ASCII Query Language.....</b>	<b>M26-1</b>
ASCII Query Language.....	M26-2
Remote Parameters Settings.....	M26-3
Command Syntax Summary .....	M26-5
<b>Software Module 27 TAP Interrogator .....</b>	<b>M27-1</b>
TAP Interrogator Remote Parameter Screen.....	M27-2
TAP Interrogator Job Setup .....	M27-3
<b>Software Module 28 DNP3 Interrogator .....</b>	<b>M28-1</b>
Remote Parameters Field Descriptions.....	M28-2
DNP3 Device Definition .....	M28-4
Defining an Address .....	M28-4
Address Default. ....	M28-6
DNP3 Interrogator Display Map .....	M28-7
Point Definition.....	M28-8
Analog Display Worksheet .....	M28-11
Device Failures/OfflinesAddress Statistics (Monitor Mode) .....	M28-12
View Analogs .....	M28-15



<b>Software Module 29 ASCII Gateway.....</b>	<b>M29-1</b>
Define the ASCII Gateway Connection on T/Mon.....	M29-1
Define the ASCII Gateway Subconnections.....	M29-3
Modify/Create ASCII Input Jobs That Will Use These Connections.....	M29-3
Configure the T/Mon ASCII Gateway Agent.....	M29-4
 <b>Software Module 30 Modbus Responder .....</b>	 <b>M30-1</b>
Install or Upgrade the Software.....	M30-1
Configure the Modbus Responder.....	M30-1
Define the Modbus Responder Remote Device.....	M30-3
Define the Modbus Responder.....	M30-4
Mapping for Modbus Function Code 0x02 (Read Discrete Inputs).....	M30-5
Mapping for Modbus Function Code 0x04 (Read Input Registers).....	M30-5
Assigning Analog Channels.....	M30-6
Mapping for Modbus Function Code 0x05 (Write Single Coil).....	M30-7
Mapping for Modbus Function Code 0x0 (Read Coil Status).....	M30-7
 <b>Software Module 31 DNP3 Responder .....</b>	 <b>M31-1</b>
Remote Device Definition.....	M31-2
Responder Definition.....	M31-3
DNP3 Databasing Notes.....	M31-4
 <b>Software Module 32 SiteDialer for T/Mon.....</b>	 <b>M32-1</b>
Configuring the SiteDialer.....	M32-1
 <b>Appendix A - ASCII Tutorial.....</b>	 <b>A-1</b>
Introduction: How To Use This Tutorial.....	A-1
Overview: ASCII Messages.....	A-2
Overview: How the ASCII Processor (Message Processing) Works.....	A-3
Overview: How the ASCII Processor (the Alarm Processor) Works .....	A-4
Recognizing Patterns In Messages .....	A-5
Lines, Columns, Fields and Separators .....	A-7
Example 1: Using Separators.....	A-8
Example 2: A Typical Multi-line Input Message .....	A-10
Pattern Recognition.....	A-11
Action Extraction .....	A-11
Slot Contents .....	A-12
Example 3: Exercise .....	A-13
Example 4: Using ASCII Tables .....	A-14
Pattern Recognition Rules.....	A-14
Action Extraction Rules .....	A-14
ASCII Table SCU .....	A-15
Example 5: While Loops .....	A-16
Pattern Recognition Rules.....	A-16
Action Extraction Rules .....	A-16
Example 6: While Line Loops.....	A-17
Pattern Recognition Rules.....	A-17
Action Extraction Rules .....	A-17
Example 7: ASCII Auto-Databasing .....	A-18
Pattern Recognition Rules.....	A-18
Action Extraction Rules .....	A-18
ASCII Tables used with Example 7.....	A-20
Pattern Recognition Rules.....	A-20
Action Extraction Rules .....	A-20
Key Mapping.....	A-22

Alarm Status.....	A-23
Alarm Level .....	A-23
Text Message .....	A-23
Pager Profile.....	A-23
Category 1-6.....	A-24
Testing the Auto Databasing process.....	A-24
Example 8: TL1 Auto-Databasing.....	A-25
Field Separators.....	A-25
Pattern Recognition Rules.....	A-26
Action Extraction Rules .....	A-26
Automatic Key Mapping.....	A-27
Key Mapping.....	A-27
Alarm Status.....	A-27
Alarm Level .....	A-27
Category 1 .....	A-27
Clearing Multiple ASCII Alarms with a Single Message.....	A-29
How To Generate An Alarm Notification When A Scheduled Event Doesn't Happen.....	A-33
<b>Appendix B Define Controller Cards .....</b>	<b>B-1</b>
Card Definition .....	B-1
Changing Port Interface Cartridges .....	B-3
<b>Appendix C Configuring a X.25 Port Card .....</b>	<b>C-1</b>
Hardware Connections .....	C-1
Port Definition/X.25 TL1 Responder .....	C-2
Software Configuration .....	C-2
Device Definition screen.....	C-4
Device Definition screen.....	C-4
LCN Definition - TL1 Port .....	C-5
Port Definition/X.25 I/O.....	C-6
PVC Definition - X.25 I/O Port.....	C-7
SVC Definition - X.25 I/O Port.....	C-8
Job Ports.....	C-9
Data Connection.....	C-11
Card Definition .....	C-12
X25 Provisioning.....	C-14
<b>Appendix D Ethernet Card Installation .....</b>	<b>D-1</b>
Overview.....	D-1
Installation .....	D-2
Software Installation.....	D-5
<b>Appendix E Diagnostics .....</b>	<b>E-1</b>
Remote Access Cards .....	E-2
Remote Access Card Test Screen .....	E-2
Tune Modems .....	E-4
Tuning procedures.....	E-4
108 Relay Card (Aud/Vid) .....	E-7
Relays .....	E-8
Cut Off Switches .....	E-9
Sound.....	E-9
Quit.....	E-9
102 Relay Card (local) .....	E-10
Relays .....	E-10
Cut Off Switches .....	E-11
Sound.....	E-11

Quit.....	E-11
Printer Test .....	E-12
File Info .....	E-13
TASK Files.....	E-13
System Log.....	E-14
TACCESS.ERR .....	E-15
DTMF Greeting File .....	E-15
Installable Modules.....	E-16
Installation Status .....	E-16
Module Information .....	E-17
Front Panel Test.....	E-18
LCD Buttons .....	E-19
LCD Screen .....	E-19
Fuse Alarm .....	E-20
Audio .....	E-20
T/Link .....	E-21
Hard Drive Info .....	E-21
Ethernet.....	E-22
Maintenance Reset.....	E-22
<b>Appendix F Disk Files .....</b>	<b>F-1</b>
Program Files.....	F-1
Database Files.....	F-1
<b>Appendix G Uninterruptible Power System .....</b>	<b>G-1</b>
<b>Appendix H Troubleshooting .....</b>	<b>H-1</b>
Run-Time Errors .....	H-1
Security Errors .....	H-2
<b>Appendix I Quick Reference Tables .....</b>	<b>I-1</b>
Alarm Summary Mode Quick Reference.....	I-1
Alphabetic Listing of Key Commands .....	I-1
COS Mode Quick Reference.....	I-3
Alphabetic Listing of Key Commands .....	I-3
Standing Alarms Quick Reference.....	I-5
Alphabetic Listing of Key Commands .....	I-5
<b>Appendix J Modem Initialization Strings .....</b>	<b>J-1</b>
<b>Appendix K LED Display Bar .....</b>	<b>K-1</b>
Basic Operation and Setup .....	K-1
LED Bar Remote Parameters .....	K-1
LED Bar Address Definition.....	K-3
LED Alarm Color Definition .....	K-4
LED Alarm Format.....	K-5
<b>Appendix L Frequently Asked Questions .....</b>	<b>L-1</b>
<b>Index.....</b>	<b>M</b>



## Description

See alarms as they occur and quickly obtain emergency procedure instructions.

T/MonXM supports many Ethernet applications.

New users should begin with the Quick Start Guides at the front of the manual

T/MonXM is an affordable dual-function network monitoring master that provides network managers with instantaneous and comprehensive network status information while supporting full archiving and control functions. Its windowing features allow operators to see alarms as they occur and quickly obtain emergency procedure instructions.

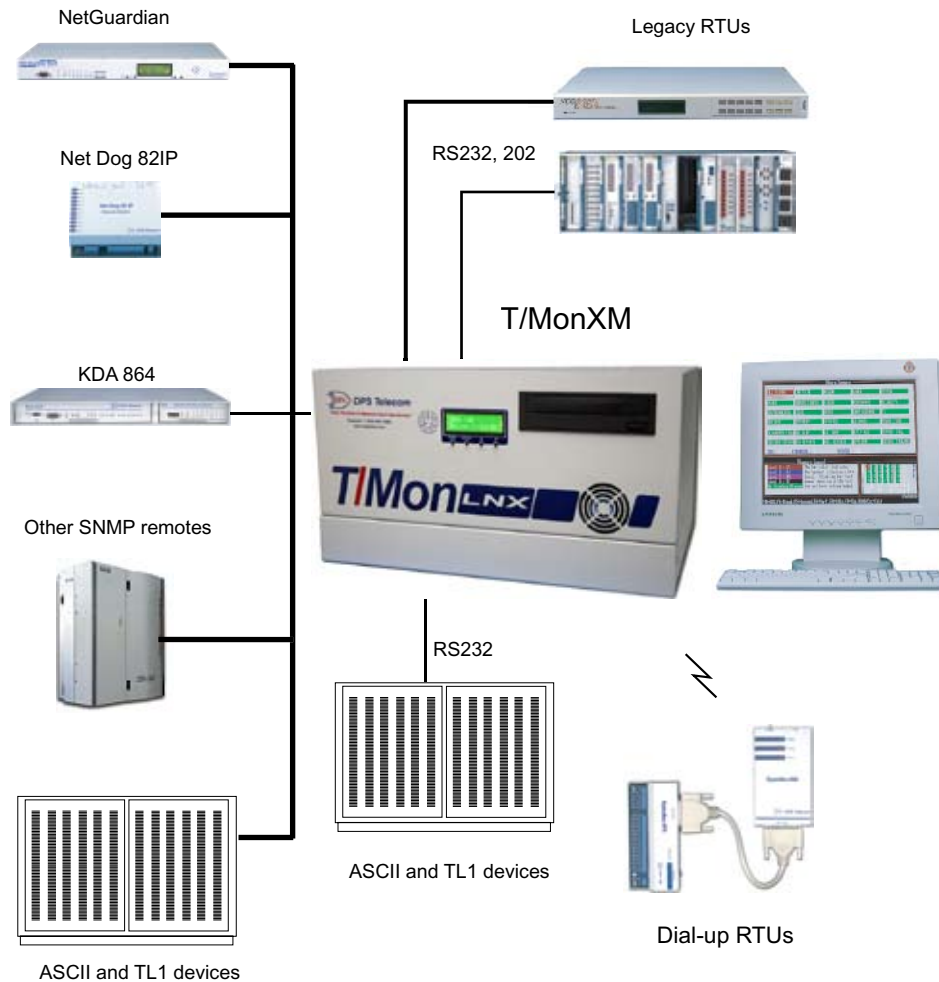
T/MonXM runs on the T/Mon LNX, T/Mon NOC and IAM hardware platforms. This workstation is appropriate for use as the main polling master in a large telecom network management center or as a local monitor in a central office. It is designed to be easily updated and/or enhanced by adding software modules and hardware boards.

This User Manual for T/MonXM Version 6.7 has been updated throughout to reflect the many new features and system enhancements that have been added to T/MonXM. The structure and style of the manual has also been updated to make it a more useful guide to T/MonXM. New task-oriented sections have been written to guide users through system set-up and configuring their system for specific applications.

We especially recommend that new T/MonXM users begin by following the instructions in the T/MonXM New Installations and Software Setup Quick Start Guides at the beginning of the manual.



**T/Mon LNX with T/MonXM**



**Block diagram of network monitoring system with T/Mon master**

T/MonXM is simple and straightforward

### T/MonXM Software

T/MonXM interacts with a large variety of remote devices over many different protocols, synthesizing them into one consistent interface. Because of this, it is not just a matter of starting it up and using it like a word processor or spreadsheet program. Before it can be brought online in user mode, effort must be put into programming and preparing a data base for the devices it will monitor. This effort can be small or great, depending on the number and types of devices involved. Once the programming is complete and a data base is entered, operation of the T/MonXM is simple and straightforward.

T/MonXM software comes in a variety of configurations determined by equipping it with various hardware and software modules. This manual contains information for all standard modules. Some T/MonXM packages may contain new or customized modules. Such modules are documented in the Software Modules section included in the back of the T/MonXM Manual binder.

## What's New in T/MonXM

- **Initial support for Web 3.0 (LNX only) - See version 6.8 Quick Start Guide for more info.**
- Added support for allowing hostnames for DCP interrogator devices.
- Added support for the following devices:
  - NetGuardian LT
  - NetGuardian LT G2
  - NetGuardian 480 G3
  - LAN-based remote device type for BVM
  - TempDefender DCP interrogator device type
  - Polling Interface device RS232 to LAN
  - SMS Interface Box
  - NetGuardian 16 w/ D-Wire sensors
- Added support for forcing users to update their password when they first log in. Accessed by pressing F2 on the System Users window.
- Added support to allow users to update their own password while in monitor mode on the console or T/Windows session. User must have user rights for File Maintenance. Accessed by entering "P" on the logout prompt.
- Added support for assigning an SNMP Trap Feed data connection to an ASCII job and selecting the ASCII job from an SNMP device to forward SNMP traps as ASCII text to the ASCII processor.

### New T/MonXM Enhancements:

- Extended length of user passwords from 8 characters to 16 characters.
- Mail in job now processes commands in the body of an email if it doesn't find a valid command in the subject line for Acking by reply.
- Added ability to ack all SNMP alarms by pressing CTRL+F9 in the standing alarm screen. Requires user rights.
- Added drop down list of pager carriers when editing pager groups. Accessed by pressing TAB on the pager group definition screen.
- Added ability for console users to be able to manually disconnect remote access connections if remote access job has a connection but user hasn't logged in yet. Accessed by pressing Alt+F2 on the alarm summary screen while viewing the performance/stats window for a remote access job.
- Added support for assigning user-defined internal alarms for device offline/failures for T/MonNET Nodes. Accessible by pressing Alt+F3 on the T/MonNET Node screen.
- Added support for user definable TMon hosts for outgoing mail notifications. These are databased on the Remote Parameters screen for the Mail Out job.

### T/MonXM Corrections

- Resolved issue with not being able to view analogs for KDA devices with an 8 analog/4 TBOS expansion.

- Automatically clean up trailing spaces for IP address/hostname field on the data connection screen. Also cleans up the mail in and mail out remote parameter settings. Cleanup is only done after editing each field.
- Resolved issue with pager notifications not sending a notification for clear events if alarm was already standing when entering monitor mode.
- Resolved issue with Pager Carrier override not applying to carriers inside pager groups.
- Resolved issue with AutoSNMP and AutoASCII including non-printable ascii in the point description, aux description, fail status and clear status fields. These normally cause formatting issues when displaying or editing the point information.
- Resolved issue with Import and Exporting of SNMP devices not including the GET/SET Command field for ASCII port. Also resolves issue with the ASCII Action string in the Trap Association not saving to the right ASCII port.
- Resolved issue with pager notifications going out after alarm has been acknowledged. Had previously sent out notifications based on alarm presence in COS and Standing screen regardless of being acknowledged.
- Resolved issue with SNMP Trap Processor not handling SNMPv1 generic trap types other than type 6.
- Resolved issue with T/Windows user not logging out when T/Windows with a dedicated connection is closed without logging out. TCP disconnect will now cause user to log out.
- Resolved issue with SNMP Agent/Responder Authentication failure trap being sent to all databased IP Addresses instead of where the incoming trap came from. Authentication Failure now only sent to the same IP address of the incoming trap.
- Resolved issue with Voice Dialer calls not being logged to the history log.







Alarm monitor screen displays 30 windows at once

## Standard Features

An alarm can appear in more than one window

### Remote Polling

T/MonXM obtains status information (alarms) from remote devices (remotes) by polling them over the telecommunications network via dial-up or dedicated lines or Ethernet. In polling, the T/MonXM issues an address on the network and listens for a response from the remote. The response includes identification of the remote and status of its alarm points. T/MonXM can also issue commands for remotes to operate relay contacts (control points).

### Passive/Active Mode of Operation

In Passive Mode a T/MonXM at a local site can monitor the interrogations from an alarm center and report only those that are of interest to the local site. It may also act as a secondary master, assuming polling if the main alarm center goes down.

### Multiple Alarm Windows

Alarms can be categorized into groups assigned to windows. Windows appear as a rectangular icon on the main viewing screen. Selecting an icon allows opening the windows assigned to the icon, where additional

Access to alarm windows can be controlled by a security code.

details about the alarms are displayed. In making window assignments the alarms can be grouped by geographic area, classification or priority of the alarm, the type of equipment, etc. An alarm can appear in more than one window. The standard T/MonXM software supports 90 alarm windows. It can support up to 720 alarm windows with the Alarm Windows Module option. All alarms are displayed in an All Alarm window, represented by the icon at the top left of the main viewing screen.

### **User Friendly**

T/MonXM is very easy to use. The user interface is consistent in appearance, featuring on-line help and individual field prompts.

### **Text/Messages Window**

Messages that describe actions to be taken in response to an alarm are displayed in a Text/Messages Window on the monitoring screen. Operators can immediately see important information like phone numbers and document references.

### **Historian Function**

Individual alarms may be logged to a history file, along with time stamping information. Reports may be run at any time to retrieve selected information from the history file.

### **System Security**

System security allows security access levels and areas to be defined for each user. System security log-on is accessible from the Master menu and the Monitor Mode screen. Security codes control who is monitoring and working in each area and define the actions a user can perform.

### **Background Polling**

The interrogation/monitoring/responding functions of T/MonXM take place in background. Because of this, the user can interactively perform a large number of tasks without interrupting T/MonXM's operation. For example, polling continues to take place while issuing control commands or while system reports are being generated.

### **Alarm Formatting**

Alarm Formatting allows the user to customize which alarm fields are defined, their position, their width and the colors used when an alarm is reported on the screen. The text displayed for the status field is definable on an alarm-by-alarm basis. Both fail and clear status descriptions can be defined for each alarm. If a status description is not defined for a particular alarm, a global default description is displayed.

Special color options allow the color of a field to be derived from the alarm's state or combination of states (failed, cleared, level A, etc.). The Alarm Format Definition may be up to 2 screens wide (up to 153 characters)

COS ALARMS - ALL MICROWAVE						
!	3/18	15:31:58	NOR	1000, DEDHAM_MSC	DACCS_CRIT	
	3/18	15:33:22	NOR	1123, HOLLISTON	DM-2-12_RX_B_BER	TWD_FRANKLI
!	3/18	15:33:41	ALM	1000, DEDHAM_MSC	DACCS_CRIT	
	3/18	15:35:04	ALM	1123, HOLLISTON	DM-2-12_SITE	TWD_FRANKLI
!	3/18	15:35:23	NOR	1000, DEDHAM_MSC	DACCS_CRIT	
	3/18	15:36:46	ALM	1123, HOLLISTON	DM-2-12_RX_B_FAIL	TWD_FRANKLI
!	3/18	15:37:05	ALM	1000, DEDHAM_MSC	DACCS_CRIT	
!	3/18	15:38:07	NOR	2000, WALTHAM_MSC	DACCS_MAJ	
	3/18	15:38:29	NOR	1123, HOLLISTON	DM-2-12_SITE	TWD_FRANKLI
!	3/18	15:38:47	NOR	1000, DEDHAM_MSC	DACCS_CRIT	
!	3/18	15:38:51	NOR	2000, WALTHAM_MSC	DACCS_MIN	
!	3/18	15:39:56	NOR	3000, BURLINGTON_MSC	DACCS_MIN	
	3/18	15:40:11	NOR	1123, HOLLISTON	DM-2-12_RX_B_FAIL	TWD_FRANKLI
!	3/18	15:40:29	ALM	1000, DEDHAM_MSC	DACCS_CRIT	

Text/Messages		Proactive Monitoring Company																																	
DACCS CRITICAL ALARM!!! MULTIPLE T1'S		<table border="1"> <tr> <td>&gt; A</td><td>E</td><td>I</td><td>M</td><td>Q</td><td>U</td><td>U:</td><td>D</td> </tr> <tr> <td>B</td><td>F</td><td>J</td><td>N</td><td>R</td><td>U</td><td>A:</td><td>P</td> </tr> <tr> <td>C</td><td>G</td><td>K</td><td>O</td><td>S</td><td>W</td><td>S:</td><td>S</td> </tr> <tr> <td>D</td><td>H</td><td>L</td><td>P</td><td>T</td><td>X</td><td>P:X</td><td></td> </tr> </table>		> A	E	I	M	Q	U	U:	D	B	F	J	N	R	U	A:	P	C	G	K	O	S	W	S:	S	D	H	L	P	T	X	P:X	
> A	E	I	M	Q	U	U:	D																												
B	F	J	N	R	U	A:	P																												
C	G	K	O	S	W	S:	S																												
D	H	L	P	T	X	P:X																													
O.O.S-NOTIFY SUPERVISOR!		STAND :30      Silenced:0 COS :44      Off Line:0																																	

26278764

Enter=Ack, F1=Prv, F2=Nxt, F4=Stnd, F5=Txt, F6=Trb, F8=Ctl, F9=Hlp, F10/Esc=Exit

### Alarm display format

#### Event Logging

Event logging is a standard feature of T/MonXM which reports all system events to the History report file. This feature allows retrieval of information on items such as the UPS (optional) going on/off battery power. Other activities reported include printer failures, polling addresses on/off line, LED Displays off-line, and T/MonXM system off-line.

#### Control Point Operation

Control points are described by English text that appears on the screen. Control points may be defined to latch (requiring a release command to unlatch) or operate momentarily. Two methods of operating control points are used in T/MonXM, Labeled Controls and Site Controls.

With the Labeled Controls method, a group of control points can be accessed and operated from any window on the screen. This allows quick operation of controls that have a high level of urgency. Points to be operated via this method are defined during data base preparation.

Points defined as Site Controls can be accessed and operated from only the window for their site. This allows a higher level of security, since access to some windows can be restricted to only certain users. Points to be operated via this method must also be defined in the data base.

#### Derived Alarms/Controls

Matrix formulas can be defined that will evaluate specified alarms and generate a common or higher level alarm from them. The same matrix can be used to automatically operate a control point.

Control Points									
Window Name : MADERA MAIN									
Category : RADSW RADIO SWITCH									
Ent	Description	CMD	Ch	D	Add	Unt	Point(s)		
1	LPA1 SN2 7 HV ON/OFF .....	OPR	RP		14	4	1		
2	LPA1 SN2 7 HV ON/OFF	RLS	RP		14	4	1		
3	LPA2 SN2 7 HV ON/OFF	OPR	RP		14	4	2		
4	LPA2 SN2 7 HV ON/OFF	RLS	RP		14	4	2		
5	BB L/B OFF/ON L 8552	OPR	RP		14	4	3		
6	BB L/B OFF/ON L 8552	RLS	RP		14	4	3		
7	IF L/B OFF/ON L 8552	OPR	RP		14	4	4		
8	IF L/B OFF/ON L 8552	RLS	RP		14	4	4		
9	VIDEO HV ON/OFF	OPR	RP		14	4	6		
10	VIDEO HV ON/OFF	RLS	RP		14	4	6		
Enter description									
F1=GOTO, F3=BLANK, F8=Save, F9=Help, F10/Esc=Exit									

### Control point operation screen

#### Craft Mode Interface

With Craft Mode T/MonXM can access an ASCII port on a remote device for troubleshooting or configuration. In addition, any remote terminal (T/Remote, laptop, etc.) can access the same devices through the T/MonXM. In this mode the T/MonXM or remote terminal operate as a dumb terminal. Example: A DPS DPM reports an alarm on a PABX it is monitoring. A technician requires more detail about the alarm from the PABX. The ASCII port on the PABX can be connected to the technician's laptop computer through T/MonXM's Craft Mode Interface.

#### Pager Support

With Pager Support T/MonXM will call up to 999 pager numbers. Each alarm point can be programmed to call a pager when an alarm occurs or when it clears. Alarm points are assigned to pagers through pager profiles (up to 99 of them), which are groups or categories of 30 operators. Operators use schedules to determine on a 7-day/24 hour basis what pager is called, as well as categorizing who is paged by alarm type, delay, and pager format. Up to 999 paging operator schedules may be entered into the T/MonXM data base. The Pager Support Module includes a schedule exceptions screen that can override the 24 hour schedule to make special changes for holidays, etc. Group mode allows a single event to be issued to multiple pagers.

#### 2-Way Paging

Two-way paging allows the paged technician to immediately acknowledge an alarm from the pager. This halts additional paging activity. A Technician can also acknowledge all alarms at a site, tag alarms for future reference or ignore nuisance alarms.

**DCP/DCP(F) Interrogator**

The DCP(F) Interrogators allows data to be brought into the system from remotes that use DCP, DCP(F), DCP (X), or DCP1 protocol. DCP/(F)/(X) protocols are normally used over dedicated lines via 202 modems or RS 422/485 interfaces. This protocol is used to interrogate all DPS Telecom products as well as other vendors' equipment.

**DCM Interrogator**

The DCM Interrogator allows data to be brought into the system from remotes that use the DCM protocol (MATs and CPMs). The multiple port version of the module is standard.

**TRIP Protocol**

TRIP polls DPS Telecom dial-up remotes via dial-up modem.

**W/Shell Software**

W/Shell is a management software that provides a menu listing for selecting and running all installed DPS programs.

**T/Link Software**

T/Link uses an internal modem to provide access to DPS Telecom Customer Support for system troubleshooting via phone line.

**Unlimited Remote Access Ports**

Remote Access Ports give T/MonXM the ability to have additional users independently access the system via modem or direct connection through Intelligent Controller Card ports (see Hardware Options). Each port may be assigned a different access level for security. Remote access supports the following hardware/software emulations in full T/MonXM color: T/Remote workstation, T/Remote for Windows, and T/Remote for DOS. Remote Access can also emulate VT100s, WYSE50s and ADDSVP. For users of older version of T/Mon, Remote Access ports are limited by the number of Remote Access software modules you have installed. If more ports are required at a future time, additional remote access modules may be purchased. Intelligent Controller Cards or an Ethernet card are required to provide the physical ports for remote access.

In version 3.5 and later, remote access can also be used over Ethernet. Up to 16 remote users can be supported on an Ethernet port.

**T/Windows**

T/Windows software is an advanced version of T/Remote for Windows, except that it provides users with true point-and-click access to all the features of T/Mon — making centralized alarm management easier than ever. T/Windows also provides intensive right-click functionality for quick and easy access to the major functions of T/Mon.

**Web Browser Interface**

This feature, introduced in version 3.5, gives the ability to view and manage alarms via LAN using Internet Explorer™, or Netscape Navigator™. This permits alarm management from non-Windows environments. Features include: Acknowledge individual alarms, view, add and close Trouble Logs, view report files, up 18 simultane-

ous users. See Section 17 (Web Browser Interface) for more information.

### **E-Mail Notification**

Introduced in version 3.5 is alarm notification via E-mail. E-mail notification setup is very similar to pager carrier setup. Each pager carrier can be given an e-mail address as well as a pager number. Response options also allow the e-mail recipient to reply to T/MonXM and acknowledge or Tag alarms via e-mail.

### **Ping Interrogator**

Besides monitoring your Telecom network, T/MonXM can now act as a check on your LAN and network equipment. The Ping Interrogator can be used to ping and IP aware device, i.e. servers, routing equipment, etc. It is a low level device check, simply noting if a device is present or not based on its response or lack of response to a ping.

---

## **Optional Features**

Optional features may be added to T/MonXM by installing software modules. The software modules provide instant access to upgrade features. These modules are briefly described below. See the DPS Catalog for the latest software modules available. Call DPS Telecom at **1-800-693-0351** if you don't see a feature or module that fits your needs. The software modules that are discussed in detail in the Software Modules section at the back of the manual are indicated next to each title by the page number they begin on..

### **Alarm Windows Module**

This installable option allows the basic 90 alarm windows (89 plus an All Alarm window), to be expanded up to 179, 329 or 719 alarm windows plus an All Alarm window. The number of alarm windows available is dependent on whether the 90, 240 or 690 Alarm Windows modules have been installed. Multiple Alarm Windows modules may be installed, up to the 720 alarm windows limit.

Each window can have a verbal description assigned. When a window has an alarm, the window changes color to indicate the level of the alarm and the window name flashes. The operator can place the highlight box around the window and press F3 to move to the COS screen or press F4 to move to the standing alarm screen. The Alarm Windows modules provide flexibility in the assignment of equipment to the alarm system.

### **Alarm Message Forwarding Module**

The Alarm Message Forwarding Module allows the user to assign a alarm window as an ASCII forwarding window. When alarm information is reported to this window, it is redirected out one of the intelligent controller ports in ASCII format. All alarms that are assigned to the forwarding window will be displayed in that window. The alarms will also be sent out the selected port in the same format as they appeared on the screen.

For example, if all of the power related alarms from each central office are assigned to window #8, window #8 can be set to forward

alarms to one of the intelligent controller ports. If this port is tied to a printer in another location, the alarms that appear in window #8 will be printed.

### **Building Access Manager Module**

The Building Access Manager Module software supports security for building access using either DTMF or BAU hardware options.

The DTMF Building Access option allows personnel, without special equipment, to log in using a DTMF telephone. The T/MonXM host computer receives the log in call and (using the DTMF/ASCII converter) logs in personnel at a building site.

The Building Access Unit (BAU) hardware monitors routine door alarms and matches them with log in codes entered into the BAU Keypads at remote sites. Invalid entries and door alarms without keypad entries are sent to T/MonXM. The BAU gives operators a way to identify unsecured illegal entries into equipment sites.

### **ASCII Dial-Up Module**

Available in both multi-port and single port versions, ASCII Dial-Up Modules provide dial-up Support for ASCII Devices. They accept ASCII Messages, create rule tables for parsing ASCII information and support control sequences for interrogating ASCII devices. Requires dial modem.

### **ASCII Interrogator Module**

Available in both multi-port and single port versions, ASCII Interrogator Modules provide support for direct connect ASCII device monitoring. This includes checking all data received from the device for redefined alarm conditions. Once detected, a standard T/MonXM alarm will be generated. Periodic query commands can also be issued and their responses processed.

### **Auto-Databasing ASCII**

The Auto-Databasing ASCII Modules automatically fill in alarm descriptions and assign windows according to user-programmed instructions. Available in direct connect and multi-port versions. Ideal for TL1 and other messages that follow a pre-determined format.

### **TBOS Interrogator and Responder Module**

TBOS Interrogators allow data to be brought into the system from remotes that use TBOS protocol. These modules support up to 8 TBOS displays for a total of 512 alarm points per T/MonXM port. TBOS typically requires an RS 422/485 interface, which can be implemented via an external converter or a docking pad on the 602 card (see Hardware Options).

### **E2A Interrogator and Responder Modules**

E2A Interrogators allow data to be brought into the system from remotes that use E-Telemetry protocol. This protocol supports up to 255 addresses and is primarily used in the Bell System. Requires an E-Telemetry interface (see Hardware Options).



### **FX 8800 Interrogator Module**

The FX 8800 Interrogator software module provides support for the ADC Fibermux MAGNUM 100 fiber optic terminals, supporting point to point as well as ring applications. Once the MAGNUM 100 alarm information is on the T/MonXM platform alarm information can be converted to any of the available protocols supported.

### **TABS Interrogator/Responder S/W (Multi-port)**

Enables the T/MonXM to either interrogate or respond the TABS protocol on multiple T/MonXM ports. The TABS subset implemented is the Alarm Surveillance & Control section (AS&C) of AT&T compatibility bulletin #149.

### **Pulsecom Datalok™ Module**

Allows T/MonXM to support the Pulsecom Datalok 10 Series remote telemetry units. This includes: 10, 10L, 10A, 10A micro, 10D, 10D micro and 10X. The support includes the ability to configure those remote units that are downloadable. Support also includes: Analogs, Controls (Momentaries, latched, SBOs) and point Lockout. DPS Telecom does provide a separate database conversion service to facilitate migration to the T/Mon platform from the aging PDP 11 master.

### **TL1 Combiner Modules**

The TL1 Combiner Modules provide filtering and Flow Control For TL1 Combiner Multiple Incoming TL1 Channels. They support the RS232, RS422/485 communication boards.

### **TL1 Responder Modules**

The TL1 Responder Modules convert T/Mon alarms into TL1. They support autonomous messages as well as various retrieve commands. TL1 controls will be forwarded to the proper device. User may define TL1 attributes on a per alarm basis. (Requires 8 Megabytes of main-board memory on monitoring platform).

### **X.25/ASCII Interrogator Software Module -with X.25 card**

Provides standard ASCII alarm monitoring functions over multiple PVCs on a single X.25 card (included). Each PVC may have its own ASCII rules and is processed independent of other PVCs.

### **ASCII MUX Software Module**

This module enables all direct connect ASCII ports on T/MonXM to have the ability to connect to the DPS 8-Channel MUX. This means that if the T/MonXM workstation already has a single port ASCII interrogator, up to 8 ASCII devices can be connected to that port by using this software module along with the 8-Channel MUX. This is ideal for processing data from a large quantity of ASCII devices without large port allocation requirements. NOTE: Only ONE ASCII MUX software module is required regardless of how many 8 channel MUXs are used.

### **Remote Access Modules**

These modules give T/MonXM the ability to have additional users independently access the system via LAN, modem or direct con-

nection through Intelligent Controller Card ports (see Hardware Options). Each port may be assigned a different access level for security. Remote access supports the following hardware/software emulations: Web Browser Interface, T/Windows, T/Remote workstation, T/Remote for Windows, and T/Remote for DOS. Remote Access can also emulate VT100s, WYSE50s and ADDSVP. Ethernet support is provided for up to 16 users of T/Remote for Windows and color VT100 24 or 25 line drivers. This module is available in 1, 2 or 4 port additive modules. Physical ports for Ethernet or Intelligent controllers require the appropriate hardware modules.

### **ASCII Query Language (AQL) Module**

This module enables T/MonXM to Respond to Commands from a Higher Level Management Computer as well as Reporting Spontaneous Alarm events. Commands Include: Issuing Controls, asking for Standing or Unacknowledged Alarms for a Particular window, Placing devices on/offline. Also supports the reporting of analog data.

### **XMEdit Software**

This software can be used on an off-line computer to prepare and maintain the database for T/MonXM. This allows the system administrator to perform data basing activities without interrupting on-going alarm monitoring at the T/MonXM Workstation.

### **SNMP Agent**

With the SNMP Agent, T/MonXM can forward alarms from multiple sources, using multiple protocols, to an SNMP manager. Alarms can be directed to SNMP as direct displays or as derived alarms, allowing alarms from many different sources to be used. The SNMP Agent transmits an SNMP packet over an Ethernet, SLIP or PPP link. It supports Get, Get Next, Trap and Set Messages. An NE2000 Ethernet card is required - standard in new systems. (Packages are available with or without the Ethernet card.)

### **Network Alarm Controller -NAC**

Allows direct polling through an Ethernet 10BaseT network to KDA remotes that are equipped with an Network Interface Adaptor (NIA). An Ethernet card is required. (Packages are available with or without the Ethernet card.)

### **T/Mon SQL**

The T/Mon SQL job is designed to store history events in a SQL database. Once in the SQL database they can be queried from any number of outside sources. In order to accomplish this the T/Mon must forward it's history events via TCP to the T/Mon SQL Agent which will insert them into the SQL database. The T/Mon SQL Agent is used to manage the SQL database.

### **Cordell Responder Module**

Reports alarms to higher-level Cordell master.

## Hardware Options



**Port Interface Cartridge**

### **Granger Interrogator Module**

Enables T/MonXM to obtain alarms and analog values from Granger 8000 system remotes.

### **Badger Interrogator Module**

Enables T/MonXM to obtain alarms from Badger remotes

### **T/GrafX**

The T/GrafX software module is supplied with the T/GrafX workstation or software. Instructions for using it are included in the T/GrafX Operation Guide or Manual.

You can order additional Port Interface Cartridges (PICs) for different interfaces and terminations.

### **Standard T/Mon NOC Port Interface Cartridges**

**Note:** Refer to the T/Mon NOC hardware user manual for more information.

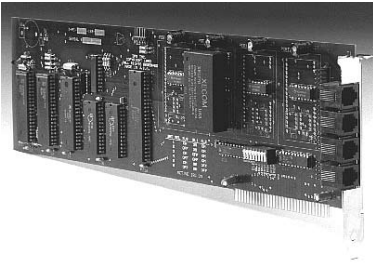
- 202/FSK/PSK Modem Interface Cartridge with Screw Down Termination (D-PK-IC202-12001)
- RS-232 Interface Cartridge with DB9 Termination, RJ11 Termination, or Screw Down Termination (D-PK-IC232-12001)
- Dial (33.6K modem/1200 baud modem) Interface Cartridge with Screw Down Termination (D-PK-IC336-12001)
- RS-422/485 Interface Cartridge with Screw Down Termination (D-PK-IC485-12001)

### **T/MonXM WorkStation Pin-Compatible Port Interface Cartridges**

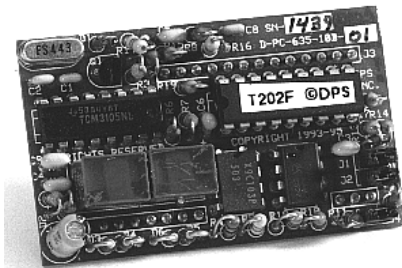
- 202/FSK/PSK Modem Interface Cartridge with RJ11 Termination (D-PK-RC202-12001)
- RS-232 Interface Cartridge with RJ11 Termination (D-PK-RC232-12001)
- Dial (33.6K modem/1200 baud modem) Interface Cartridge with RJ11 Termination (D-PK-RC336-12001)
- RS-422/485 Interface Cartridge with RJ11 Termination (D-PK-RC485-12001)

### **IAM and IAM-5 Pin-Compatible Port Interface Cartridges**

- 202/FSK/PSK Modem Interface Cartridge with DB9 Termination (D-PK-9C202-12001)
- RS-232 Interface Cartridge with DB9 Termination (D-PK-9C232-1001)
- Dial (33.6K modem/1200 baud modem) Interface Cartridge with DB9 Termination (D-PK-9C336-12001)
- RS-422/485 Interface Cartridge with DB9 Termination (D-PK-9C485-12001)



**Fig. 1.7 - Intelligent  
Controller Card**



**Fig. 1.8 - Docking module**

### **IAM-5 and T/MonXM Workstation Port Interface Cartridges Intelligent Controller Card**

The Intelligent Controller Cards are switch addressable for 4 sequential ports at a time. The T/MonXM WorkStation will accept up to 4 cards (limit of 16 ports).

#### **D-PC-600-10A-00 Intelligent Controller Card**

Four (4) Port Intelligent Controller Card for Ports 1-16 with RS232 Interface.

#### **D-PC-602-10A-00 Intelligent Controller Card**

Four (4) Port Intelligent Controller Card for Ports 1-16. Interfaces available with the factory installation of up to four docking modules. Depending on interface requirements, the 602 Card can be equipped with a variety of modules. The 602 Card docking modules are described below.

#### **D-PC-603-10A-00 Intelligent Controller Card for Pentium T/ MONs**

Shorter version of the 602 for use in the short slots of TMON Pentium mother boards. Uses one docking module and three hard-wired RS232 or RS422/485 ports.

### **Docking Modules**

D-PR-140-10A-00 212 Type 1200 Baud Internal Modem

Provides 212 type 1200 baud modem interface for the 602 card.

D-PR-145-10A-00 212 Type 2400 Baud Internal Modem

Provides 212 type 2400 baud modem interface for the 602 card.

D-PC-635-10A-00 202 Type 1200 Baud Internal 4-Wire Modem

Provides 202 Tone Modem interface for the 602 card.

D-PC-645-10A-00 RS232 Docking Module

Provides RS232 interface for the 602 card.

D-PC-655-10A-00 RS422/RS485 Docking Module

Provides RS422/RS485 interface for the 602 card.

In addition to the 602 card described above, versions are available which have the equivalent of the docking modules hard-wired to the card. See the DPS Catalog, or call us at (800) 622-3314 for details.

### **Uninterruptible Power System (UPS)**

The Uninterruptible Power System (UPS) is line-interactive and computer-grade quality. It has outstanding lightning and brownout protection, and RF noise filtering. Because the software is communicating with the UPS, there is no break in power transfer between line power and UPS usage. The UPS has two operational modes: time-out and extended operation. Time-out mode allows a user assignable amount of time, in minutes, after going to battery power before T/MonXM will be shut down. This allows performance of an orderly shutdown without corrupting alarm data files. Extended operation mode allows T/MonXM to continue normal operation until two minutes of battery operation remain before it will be shut down. In the event of an extended overnight power failure this

will permit unmanned operation to continue until shutdown. When power goes back on, T/MonXM will restart the system and go back into Monitor mode or the Master menu Log On screen.

**Special Options**

- D-PC-102-10A-00 Relay Card with Alternate Address
- D-PR-240-10A-00 X.25 Synchronous Channel Card (Channels 1-4)
- D-PR-100-10A-00 Multi-Type Printer - NX1001
- D-PR-130-10A-00 Internal Tape Backup
- D-PR-051-10A-00 Uninterruptible Power System (UPS).

For additional items call us at 1-800-622-3314.

# About This Manual

---

## About this Manual

**This manual is divided into three parts:**

**Part I** contains the T/Mon hardware setup information and procedures for using the core T/MonXM software.

**Part II** represents the Software Modules. This section supports the software modules available in T/MonXM software. Some are standard, others are optional.

**Part III** is the Appendix. Appendixes include tables and other support details that may be referred to in Parts I or II.

**NOTE:** For specifications and basic setup instructions for your T/Mon hardware, please refer to the appropriate Quick Start Guide.



Refer to the  
**T/Mon LNX  
Quick Start  
Guide**



Refer to the  
**T/Mon NOC  
Quick Start  
Guide**

**NOTE:** This manual is continually updated. DPS Telecom will make every effort to provide software owners with the most current manual as it becomes available. To assist us in supporting your manual, please send in the registration card included with your equipment.



# Section 1 - T/Mon NOC/LNX Hardware Installation Guide

## Slide Rack Mounting

The vast majority of T/Mon users order their unit with the accessory Slide Rack. The Slide Rack enables T/Mon to easily slide out of its rack position for installation and service access.

Your T/Mon shipped with the Slide Rack already mounted to the unit and with the specified rack ears in the correct position for installation.

Installing the T/Mon with Slide Rack takes three steps:

1. Removing the Slide Rack from the T/Mon
2. Mounting the Slide Rack on the equipment rack
3. Mounting the T/Mon on the Slide Rack.

**Note:** The T/Mon with Slide Rack occupies 10.5" (6 rack units) of rack space. At least 1 rack unit (1 3/4") should be allowed above the T/Mon for ventilation. The Slide Rack extends nearly 13" — be sure to provide adequate service loop in the connecting cables to allow the T/Mon to extend to this distance. After installation and testing of the T/Mon is completed, the slide lock screws should be installed in the Slide Rack to prevent accidental migration of the unit into the aisle space. The slide lock screws go into the equipment rack when flush mounted.

### Removing the Slide Rack From T/Mon

Removing the Slide Rack makes mounting the T/Mon an easy, one person, job. To remove the Slide Rack, follow these steps:

1. Make sure the T/Mon is off and disconnected from all network interfaces and power supplies.
2. Carefully place the T/Mon upside down on a clean, even surface. (This will not damage the unit.)
3. The T/Mon is secured to the Slide Rack by two screws — see Figure 1.1. Remove these screws and save them for reattaching the unit.
4. Gently lift the Slide Rack to remove it from the T/Mon .



Fig. 1.1 - These screws secure the T/Mon to the Slide Rack

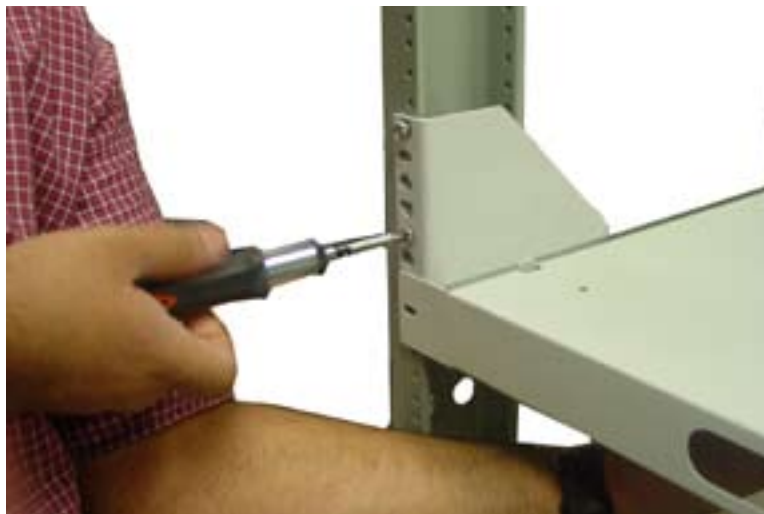


### **Mounting the Slide Rack**

The Slide Rack is light and can easily be mounted to the equipment rack by one person. The rack ears specified with your order (either 19" or 23") are already attached to the Slide Rack. (If the incorrect ears have been attached to the Slide Rack, look for the extra ears included with your shipment.)

To mount the Slide Rack to the equipment rack, follow these steps:

1. Supporting the Slide Rack with one hand, align the mounting holes in the rack ears with the rack rails.
2. Secure both brackets with the rack screws provided in the hardware bag.



**Fig. 1.2 - The Slide Rack can be easily mounted by one person**

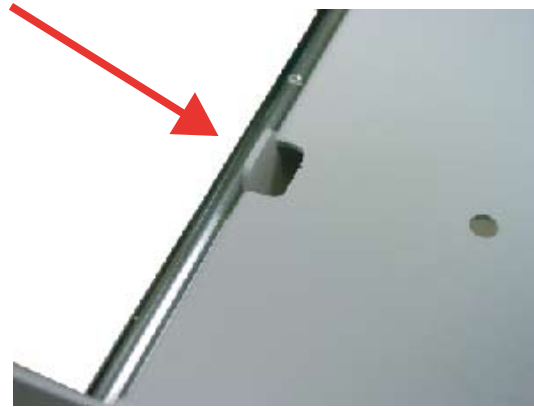
### **Mounting the T/Mon on the Slide Rack**

To mount the T/Mon on the Slide Rack, follow these steps:

1. Extend the Slide Rack.
2. Lift the T/Mon and place it on the Slide Rack.



**Fig. 1.3 - Place the T/Mon on the extended Slide Rack**



**Fig. 1.4 - There is a mounting tab on either side of the Slide Rack approximately 2" from the front of the Slide Rack**

3. Align the notches on the bottom of the T/Mon with the mounting tabs on the Slide Rack — see Figure 1.4. There is a tab on either side of the Slide Rack, approximately 2" from the front of the Rack. Gently place the T/Mon onto the mounting tabs.
4. From below the T/Mon, insert the two screws that secure the T/Mon to the Slide Rack.
5. Slide the Slide Rack back into place.



**Fig. 1.5 - Secure the T/Mon by inserting the two mounting screws from below**

### **Rack Mounting**

If you did not order the Slide Rack, your T/Mon is equipped with rack ears that can be positioned for either 5" projection or flush mounting in either 23" or 19" racks.

To mount the T/Mon directly to the equipment rack, follow these steps:

1. Determine which mounting configuration is required. The T/Mon is supplied with the brackets in the 19"/5" projections position.

2. If a different configuration is required, remove the 8-32 screws, re-orient the brackets and re-install the screws.
3. Place the T/Mon in the rack and align the mounting holes in the brackets with the holes in the rack rails. Secure each bracket with two 12-24 screws (provided in hardware bag).

## Back Panel Connections

Power feeds, serial ports, the LAN port and the internal modem port are located on the back panel of the T/Mon — see Figure 1.6. Here you will also find ports for connecting a VGA monitor and keyboard, and the Cartridge Extractor key used for removing Port Interface Cartridges. Connectors not labeled in Figure 1.6 are reserved for future use.

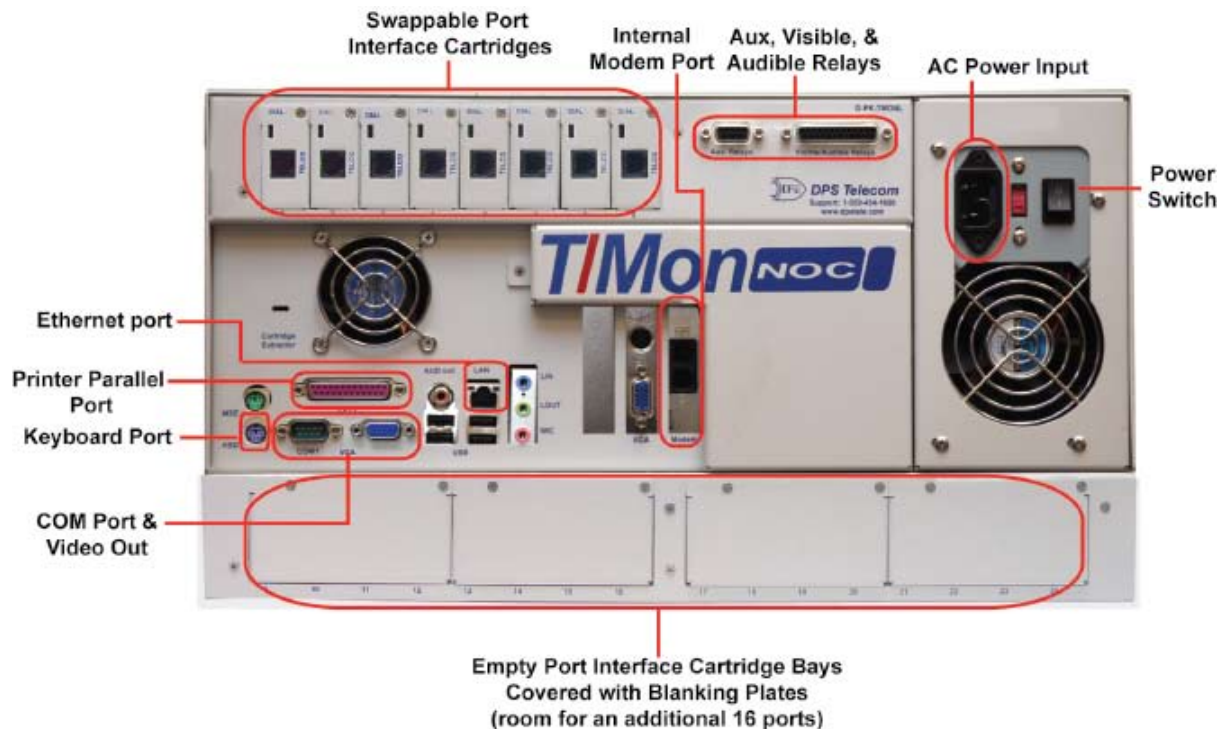


Fig. 1.6 - T/Mon NOC back panel (AC version shown)

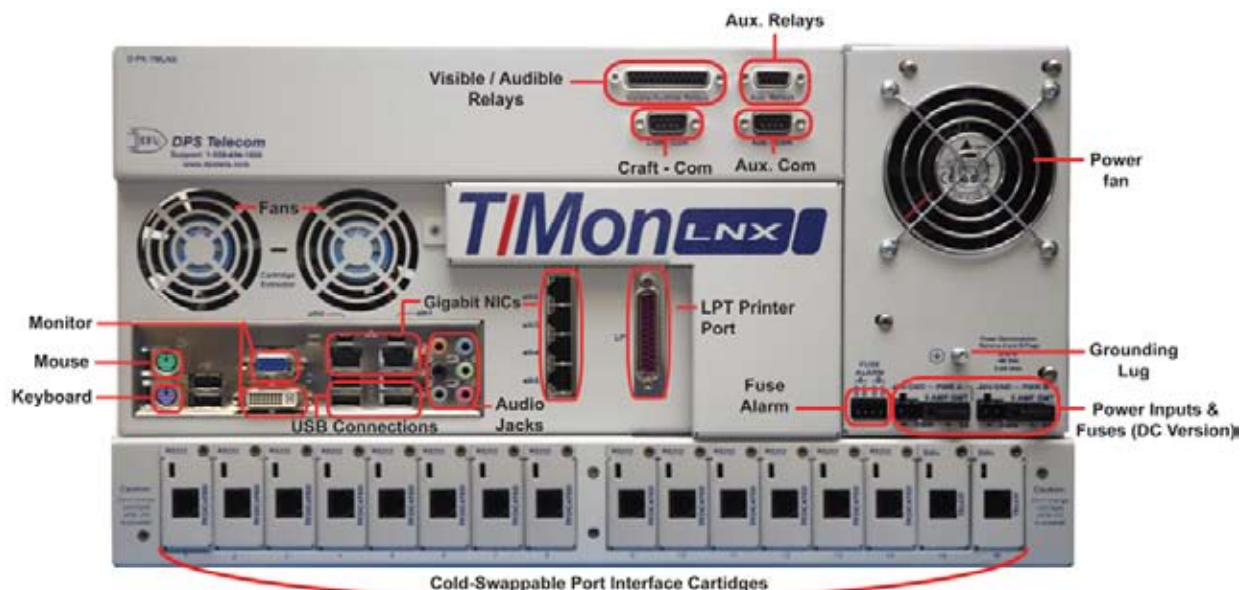


Fig. 1.7 - T/Mon LNX back panel (DC version shown)

## Power Connections

### Dual -48 VDC Models

These instructions apply only to T/Mon models with dual -48 power connections. To connect the T/Mon to a power supply, follow these steps:

1. Remove T/Mon fuses and appropriate fuses from power source.
2. Remove the power connector plugs from T/Mon.
3. Connect a -48 VDC line to the -48 volt terminal and a battery ground to the GND terminal of each power connector plug. Seat the barrier screws firmly, but be careful not to nick the bare wire.
4. Push the power connector plugs firmly into their sockets. Not that the power connector plug is keyed and the plug must be properly aligned within the socket.
5. Reinstall power source fuses.
6. (Optional) Use voltmeter to check polarity. Connect common lead to ground and V lead to -48V power. Meter should read from -48 to -56 volts.
7. Connect fuse alarm relay outputs. The fuse alarm relay provides dry open contact closure, which can hook into a remote or other device to give you visibility of a blown fuse.  
**Note:** T/Mon also has an internal fuse alarm for blown fuses which can be viewed in Monitor Mode.
8. Reinstall T/Mon fuses. The PWR LED for each power connection will light GREEN.



Fig. 1.8 - T/Mon Power Connections

### 110 VAC Models

These instructions apply only to T/Mon models with 110 VAC power connection. To connect the T/Mon to a power supply, follow these steps:

1. Insert the power cord into the power inlet on the back of the T/Mon. Connect the plug end to a 110 VAC outlet.
2. Turn on the power switch on the back panel to start the system.

Previous T/Mon hardware required a security key to be connected to the back panel printer port. This method is no longer used. If the error message below appears on boot up, contact DPS at 559-454-1600.



Fig. 1.9 - Security Key error message - Contact DPS if this message appears.

If you want to connect a printer to your T/Mon to print reports and logs, you can connect any standard parallel printer to the female DB25 connector.

To set up a printer in the T/MonXM software, choose Parameters > Hard Copy from the Master Menu.

## Network Connections

### LAN Connection

Connect the T/Mon to your LAN by inserting a standard Ethernet cable into the 10/100 BaseT port located on the rear of the unit — see Figure 1.10.

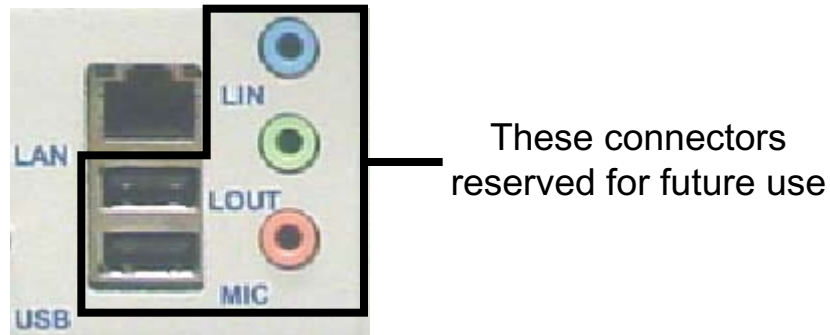


Fig. 1.10 - T/Mon LAN connector

### Internal Modem Connection

To connect to the T/Mon's internal 56K modem (used for dial-up console access), connect a standard phone line to the internal modem port — see Figure 1.11. The modem port is the bottom RJ11 connector, labeled with the icon of an RJ11 plug. If you would like to use a telephone on the same line, plug the phone line into the telephone jack just above the modem port (labeled with a telephone icon).

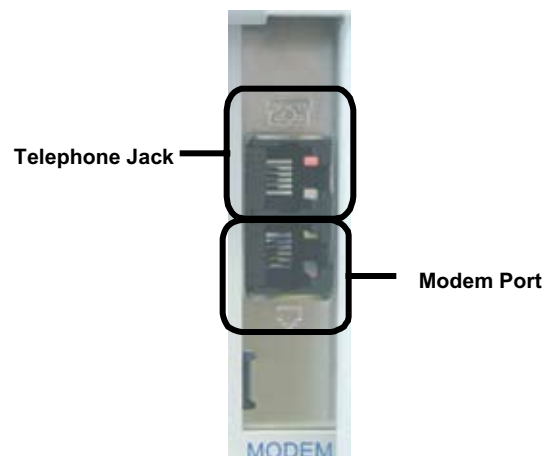


Fig. 1.11 - Internal modem port



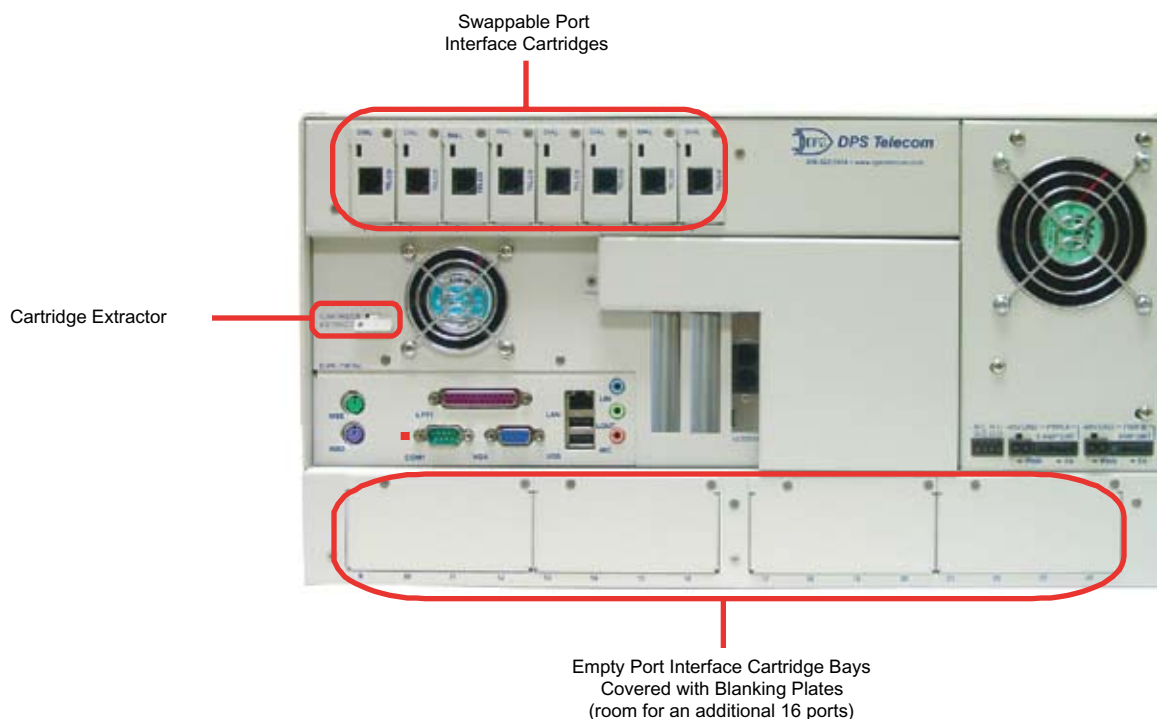
T/Mon 's 24 serial ports can be individually configured for the interface you choose. Each port is housed in a removable Port Interface Cartridge (PIC). If you ever want to change your port configuration, or if a port is damaged, you can replace a single port without opening the case or disconnecting other ports.

If you ordered your T/Mon with less than 24 ports populated, the empty Port Interface Cartridge bays will be covered with a blanking plate. This plate can be removed to add more Port Interface Cartridges later.

Port interface cartridges are available with the following interfaces:

- RS-232
- RS-422/485
- 202 modem
- 33.6K modem
- FSK modem
- PSK modem

T/Mon Port Interface Cartridges are divided into three families, depending on their pinout compatibility: standard; pin compatible with the T/MonXM WorkStation; and pin compatible the IAM and IAM-5.



**Fig. 1.12 - T/Mon serial ports (DC version shown above)**

# Serial Port Pinouts

## IAM-Compatible Port Pinouts

These Port Interface Cartridges are pin compatible with the IAM and IAM-5. Refer to these diagrams when making serial port connections to the T/Mon.

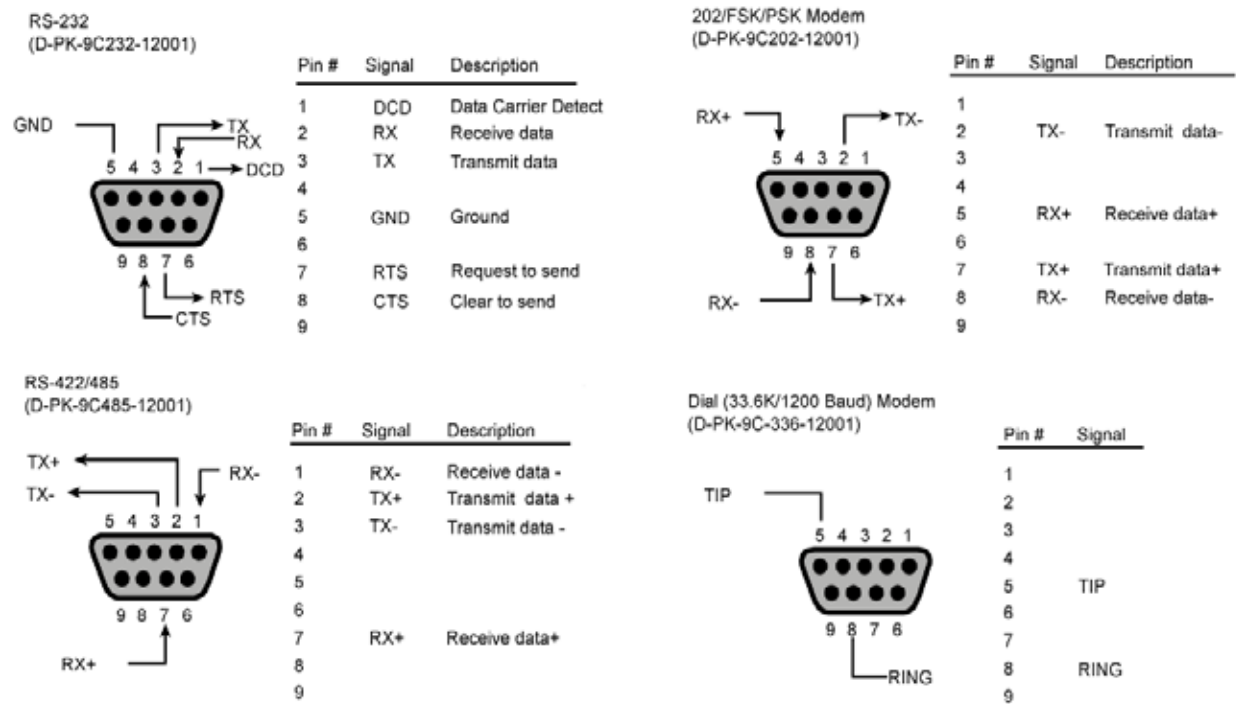


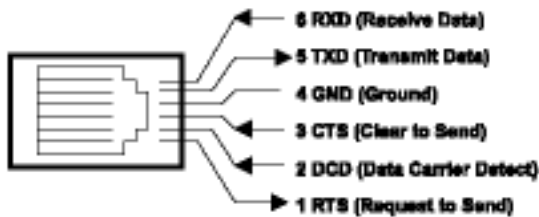
Fig. 1.13 - Pinouts for IAM-compatible Port Interface Cartridges



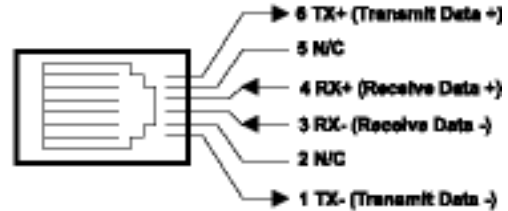
### T/MonXM WorkStation-Compatible Port Pinouts

These Port Interface Cartridges are pin compatible with the IAM and IAM-5. Refer to these diagrams when making serial port connections to the T/Mon.

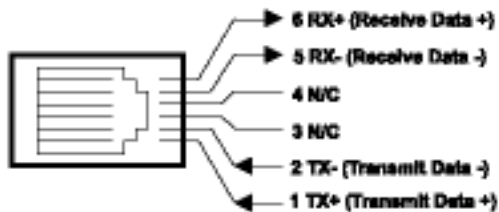
RS-232  
(D-PK-RC232-12001)



202/FSK/PSK Modem  
(D-PK-RC202-12001)



RS-422/485  
(D-PK-RC485-12001)



Dial (33.6K/1200 Baud) Modem  
(D-PK-RC336-12001)

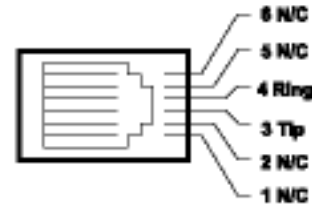


Fig. 1.14 - Pinouts for T/MonXM WorkStation-compatible Port Interface Cartridges

## Changing Port Interface Cartridges



### WARNING!

The Port Interface Cartridges are **NOT** hot-swappable! **DO NOT** remove them while the T/Mon is operational.

Port Interface Cartridges (PICs) can be easily replaced without opening the T/Mon case.

Changing a Port Interface Cartridge takes three steps:

1. Shutting down the T/Mon
2. Changing the Port Interface Cartridge
3. Defining the port parameters in T/MonXM

### Shutting Down T/Mon

1. Exit Monitor Mode by pressing F10 or Esc
2. Exit T/MonXM by pressing F10 or Esc
3. When the W/Shell screen appears, remove the fuses from T/Mon and disconnect the power supply.

1. Remove the screw from the Port Interface Cartridge.
2. Remove the Cartridge Extractor from its slot and insert it into the vertical slot in the Port Interface Cartridge.
3. Turn the Cartridge Extractor and remove the Port Interface Cartridge from the cartridge bay — see Figure 1.15.
4. Insert the new Port Interface Cartridge into the slot. Do not force the PIC into the slot.

**Note:** Make sure the Port Interface Cartridge is compatible with the intended port usage. For example, you wouldn't want a 33.6K dial-up interface on a TBOS port.

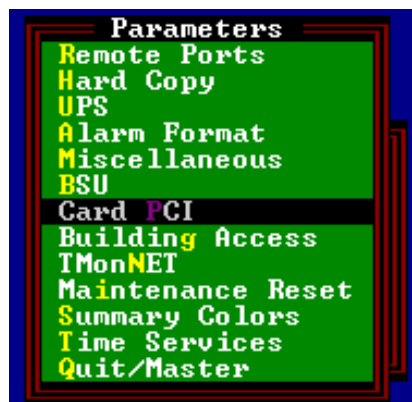
5. Reinsert the screw and tighten to secure the Port Interface Cartridge. Do not overtighten the screw.



**Fig. 1.15 - Use the Cartridge Extractor to remove the old Port Interface Cartridge**

### Configure Port Parameters

1. Reconnect the T/Mon's power supply, and power up the unit.
2. When the W/Shell screen appears, choose Main > T/MonXM > Run T/MonXM to start T/MonXM.



**Fig. 1.16 - Choose Master > Parameters > Card PCI**

- From the T/MonXM Master Menu, choose Parameters > Card PCI — see Figure 1.16.
- In the PCI Card Definition Screen, use the arrow keys to choose the port number you want to change.



Fig. 1.17 - Selecting the Port Interface Cartridge Type in the PCI Card Definition Screen

- Press Tab to select the List Box. Use the arrow keys to choose the correct Port Interface Cartridge type — see Figure 1.17.
- Press F10 or Esc to exit to the Parameters Menu
- Press F10 or Esc to exit to the Master Menu
- From the Master Menu, choose Monitor to enter Monitor Mode

## LCD Display

T/Mon's front panel LCD display provides a convenient listing of system status messages. You can select what information is displayed by using the MODE, SELECT and ▲ and ▼ buttons.

When the T/Mon is in Monitor Mode, the LCD display will show one of six screens.

The first is the Standard Prompt, which is displayed when no other menu item is selected — see Figure 1.18. The standard prompt shows three items:

- T/Mon software version
- Polling status. If the T/Mon is polling alarms, the word “Active” will be displayed in the standard prompt. In redundant dual master configurations, the actively polling T/Mon will display “Active” in the standard prompt, and the back-up T/Mon will display the word “Inactive.”
- Current time

To change the LCD display, press the MODE button.



Fig. 1.18 - The T/Mon LCD display, showing the Standard Prompt

### Standing/COS Alarm Display

This screen lists the current number of standing and change-of-state (COS) alarms.

To see other screens, press the ▼ button to scroll down the list. You can also press the ▲ button to scroll the list backwards.



Fig. 1.19 - Standing/COS Alarm Display

### **Run Time/Mon Time Display**

This screen lists the Run Time (total system uptime since the T/Mon was powered up or rebooted) and the Mon Time (total time in Monitor Mode).



**Fig. 1.20 - Run Time Mon Time Display**

### **System Name and IP Address Display**

This screen lists the system name of the T/Mon and its assigned IP address.



**Fig. 1.21 - Software Version and Serial Number Display**

**Contrast Display**

This screen provides controls for adjusting the contrast of the LCD display. To adjust the contrast, press MODE until this screen is displayed. Use the ▲ and ▼ buttons to adjust the contrast, then press SELECT to set your choice.



**Fig. 1.22 - Contrast Display**

**Other T/Mon Status Messages**

When the T/Mon is not in Monitor Mode, other status messages will appear in the LCD display. These status messages are described in Table 1.A.

**Tbl. 1.A - Additional T/Mon status messages**

Display Message	Description
TCPAgt Outdated	The version of TCP Agent currently loaded is earlier than the earliest recommended version, TCP Agent 1.0D
TCPAgt Not Load	TCP Agent is not loaded
Loading TMon	T/Mon software is loading from disk
Initializing	T/Mon is initializing in preparation for Monitor Mode
Closing Files	T/Mon is closing files during shut down
Offline	T/Mon is currently not monitoring
Halt Monitoring	T/Mon is in the process of leaving Monitor Mode

**W/Shell Status Messages**

Other status messages appear in the LCD display only when the W/Shell program is active. W/Shell status messages are described in Table 1.B.

**Tbl. 1.B - W/Shell status messages**

Display Message	Description
WShell Loading	W/Shell is loading
WShell Active	W/Shell is active.
WShell Format Floppy	W/Shell is formatting a floppy disk
W/Shell Closing Files	W/Shell is closing files and exiting

## Section 2 - Starting T/MonXM Software



Fig. 2.1 - Main W/Shell screen

### W/Shell

**Note:** W/Shell is not available for the T/Mon LNX. The following steps are only for T/Mon NOC, SLIM, and IAM users

W/Shell is the lowest-level user interface for your T/MonXM system. This is the program you see when the system is on and T/MonXM is not running. Normally, you only need to work with W/Shell to start T/MonXM, to update your software, or to setup your network. The following sections explain the options in W/Shell. See the following pages for more information on each selection.

Table 2.A - W/Shell main menu itemized

Selection	Description
NETWORK SETUP	Run the Network Setup Utility for configuring systems IP connection (See Section 3 for details)
TLINK	Run the T/Link Utility for configuring remote connection via COM port or modem
UPDATE SOFTWARE	Upgrade IAM or T/MonXM software from CD
IAM or TMONXM	Run T/MonXM
WORKSTATION INFO	Display your IAM or T/Mon information
Format Floppy Disk	Use system floppy disk drive to initialize a disk
System Time	Manually set system date and time
Update Using T/Install	Upgrade, install, or remove DPS software from floppy disks



## Run T/MonXM from W/Shell

## Upgrading The Software from a CD

**Note:** When a software upgrade is installed, the original on-line/off-line settings and tagged alarms will be lost.

**Note:** The serial numbers of your software upgrade disks and T/Mon or IAM must match. If you have multiple T/Mons, make sure that you use the correct disk set with each machine.

When the T/MonXM system finishes booting, the W/Shell utility will run. Highlight IAM or TMONXM on the menu and press Enter. The program will load and the log on screen will be displayed.

**Note:** The other menu items in W/Shell are used under the direction of DPS Technical Support. The T/Mon comes from the factory with all the software loaded. Software installation is required only to install system upgrades or new software modules, or during system recovery.

The T/MonXM upgrade is installed from within your present T/MonXM installation, using the included T/Install program.

**Note:** This upgrade must be installed directly onto the internal hard disk of the T/Mon or IAM. This software cannot be installed through a remote or LAN connection.

To install the T/MonXM Version 4.6 upgrade, follow these step-by-step instructions.

### Step One: Exit to W/Shell

1. If T/MonXM is running in Monitor Mode, press F10 or Esc to exit Monitor Mode. At the Log Off prompt, press R to return to the Master Menu.
2. From the Master menu, choose Quit to exit T/MonXM.

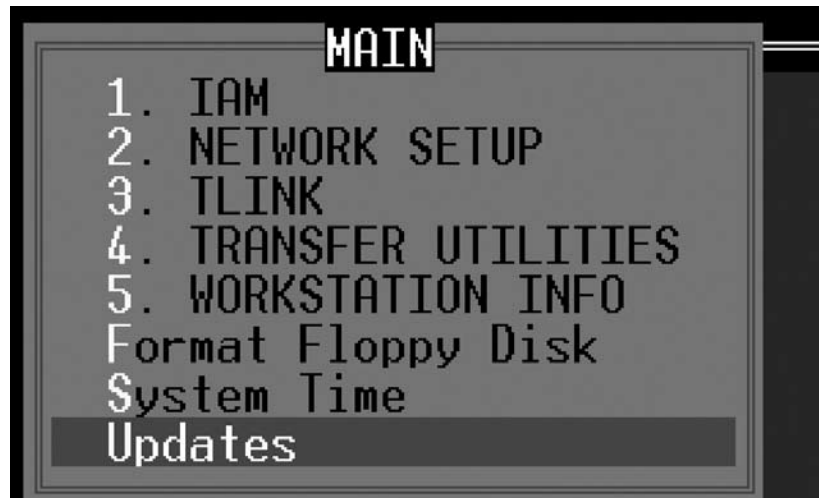


Fig. 2.2. Choose Updates from the W/Shell Main menu.

### Step Two: Install W/Shell CD Support Upgrade

1. Insert the floppy disk labeled “W/Shell CD Upgrade.”
2. After exiting T/MonXM, the W/Shell screen will open to the TMonXM or IAM Menu.
3. Choose Quit to exit to the W/Shell Main menu.
4. Choose “Updates” from the W/Shell Main menu, see Figure 2.2.

5. The Update Menu prompt screen will appear. Press Enter to launch T/Install.

**Note:** You can exit this screen by pressing F10 or Esc.

6. Your T/MonXM system will read the disk and the T/Install program will start.

7. The T/Install screen lists the program to be installed: CDUPG

8. Press Enter to choose the highlighted Install command.

```

      T/Install
    Program Information
Program      : CDUPG                      Version #   : 1.0A
Current disk # : Disk #1 of 1             Serial #    : XXXXX
Type of protection: Hardware              Release Date :
                                           Product Class: PROGRAM

ACTION  MEDIA  BY      DATE      TIME  COMMENT
      (Last 3 Uses)
-----
Installation
Destination drive(A-H): C                Volume Label : MS-DOS_6
Destination path      : \
Name of installer     : MCH
Comment               : 4.5 UPGRADE

Begin installation <Y/N)? N
Type "Y" and press Enter to begin installing the software.
  
```

Fig. 2.3. Installation setup fields

## Step Three

### Setup Installation

The Installation window, similar to that shown in Figure 2.3, will appear. Fill in the fields with appropriate information.

The fields in the Installation window are:

**Destination drive:** The disk on which the upgrade will be installed. On all standard installations you should accept the default destination, C, the internal disk of the T/MonXM system.

**Volume label:** This field will be automatically filled with the label of the destination disk.

**Destination path:** The directory where the upgrade will be installed. On all standard installations you should accept the default path: \ (the root directory).

**Name of installer:** Enter your name or initials here. Installers' names are used by T/Install's history function to track installations.

**Comment:** Enter a comment to identify the installation.

After filling in the installation setup fields, type Y and press Enter to begin installation.

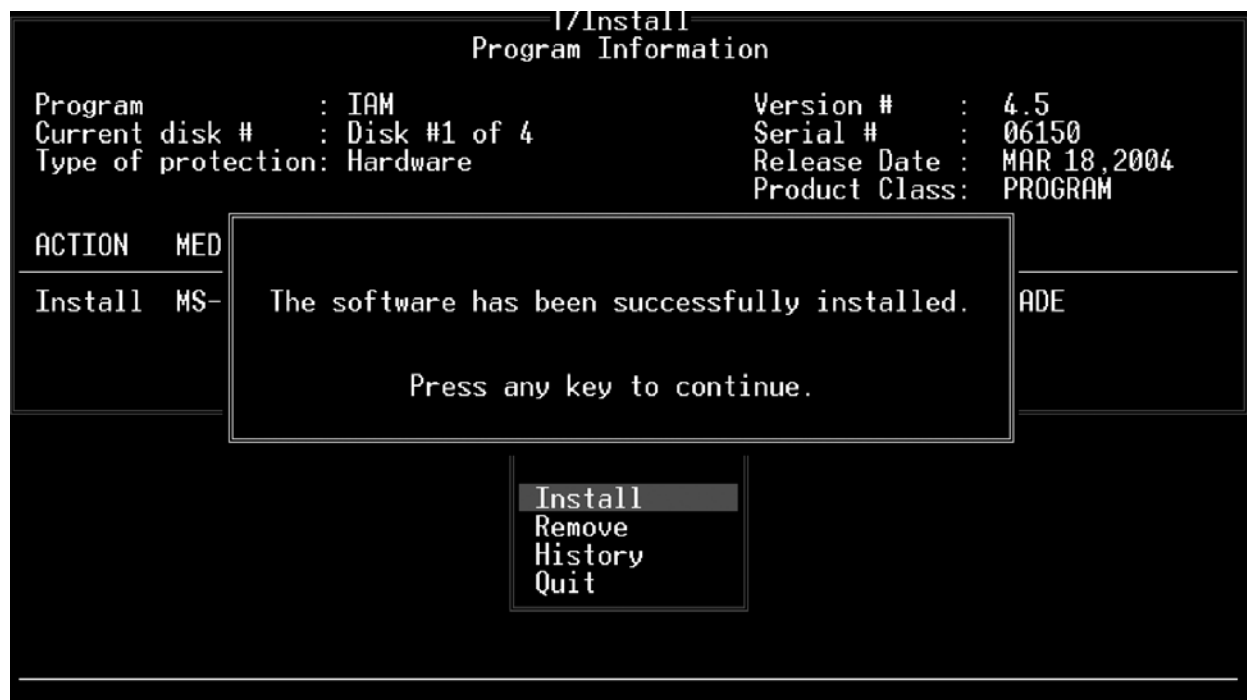


Fig. 2.4. Successful installation message prompt

## Step Four

### Run Installation

The installation process will only take a few minutes. After a successful installation, you will see the screen shown in Figure 2.4. Press any key to exit T/Install and return to the W/Shell Main menu.

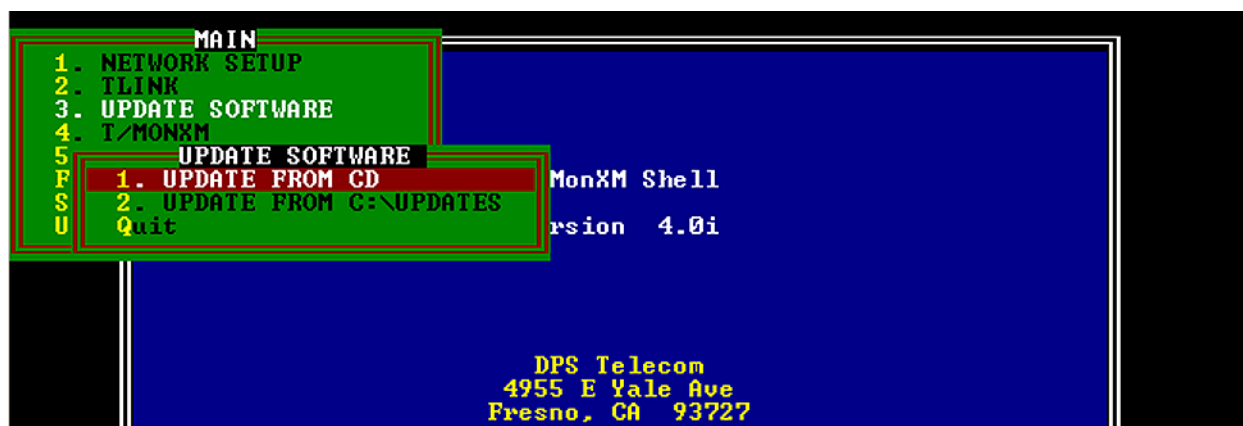


Fig. 2.5. Select Update From CD from the Update Software Menu

## Step Five

### Update W/Shell, T/MonXM, NetSetup and T/Link from the CD

1. Insert the T/Mon or IAM Update CD into the CD-ROM drive of the T/Mon or IAM.
2. Choose "Update Software" from the Main menu. See Figure 2.5.
3. Choose "Update from CD."

```

Reading from CD
Install TLink Upgrade 2.1 to C:\ [Y,N]?Y
Unable to create directory
TLINKUPG\TLINK.EXE
      1 file(s) copied
Install Net Setup Upgrade 2.0E to C:\DPSNET [Y,N]?Y
Directory already exists
NETSUPG\AGENT.EXE
NETSUPG\TCPAGENT.EXE
NETSUPG\INETCFG.EXE
      3 file(s) copied
Install IAM 4.5A04.0630 to C:\TMONXM [Y,N]?_

```

Fig. 2.6. Enter Y to install each software upgrade

4. When prompted, press “Y” to install each software upgrade. See Figure 2.6.

**Note:** “Unable to create directory” or “Directory already exists” messages are a **normal** part of CD installations and do **not** indicate an error.

5. Press any key to return to W/Shell.

6. Restart the computer.

On the **T/MonXM WorkStation**: Press CTRL-ALT-Delete

On the **IAM-5**: In the T/AccessMW menu bar, choose  
Connection > Reboot Remote System.

## Re-installing T/MonXM (complete system recovery)

**Note:** This procedure does not restore your database, but provides a clean copy of the original software.

Under normal circumstances installation will only need to be done for software updates or newly ordered modules. However, the original disks have been supplied with the workstation for archival or emergency recovery procedures.

This procedure should only be done when a complete system recovery is required, as with a hard disk failure. DPS technical support should be notified before undertaking these steps.

To re-install IAM or T/MonXM from a CD follow the instructions from sections 2-2 to 2-5. If you are re-installing IAM or T/MonXM from floppy disks use the instructions on the following sections.

## Upgrading The Software from Floppy Disks

### Step One

**Note:** When a software upgrade is installed, the original on-line/off-line settings and tagged alarms will be lost.

The latest T/MonXM version is installed from within your present T/MonXM installation, using the included T/Install program.

**Note:** This upgrade must be installed directly onto the internal hard disk of the T/Mon or IAM. This software cannot be installed through a remote or LAN connection.

To install the T/MonXM Version 4.6 upgrade, follow these step-by-step instructions.

### Exit to W/Shell

1. If T/MonXM is running in Monitor Mode, press F10 or Esc to exit Monitor Mode. At the Log Off prompt, press R to return to the Master Menu.
2. From the Master menu, choose Quit to exit T/MonXM.
3. Quit again to exit to WShell.

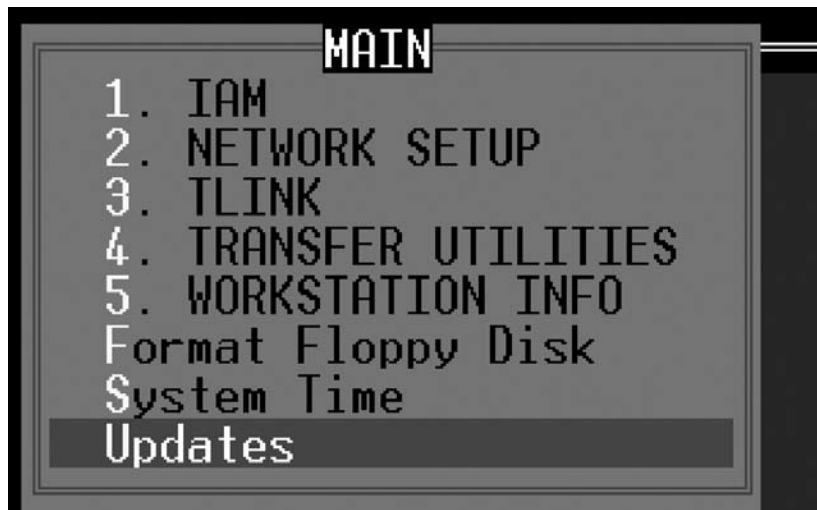


Fig. 2.7. Choose Updates from the W/Shell Main menu.

### Step Two

**Note:** The serial numbers of your software upgrade disks and T/Mon or IAM must match. If you have multiple T/Mons, make sure that you use the correct disk set with each machine.

### Install W/Shell Upgrade

1. Insert the floppy disk labeled “WS XM or IAM UP-.”
- Note:** T/Mon users should use disks labeled “WS XM UP” disk. IAM users will should use disks labeled “WS IAM UP.”
2. After exiting T/MonXM, W/Shell will open to the TMonXM or IAM Menu. Choose Quit to exit to the W/Shell Main menu.
3. Choose “Updates” from the W/Shell Main menu. See Figure 2.7.
4. The Update Menu prompt screen will appear. Press Enter to launch T/Install.
5. Your T/MonXM system will read the disk and the T/Install program will start.
6. The T/Install screen lists the program to be installed: IAM Shell or XM Shell
7. Press Enter to choose the highlighted Install command.

```

T/Install
Program Information
Program      : TMONXM          Version #      : 4.5
Current disk # : Disk #1 of 4   Serial #       : 06150
Type of protection: Hardware    Release Date  : MAR 18,2004
                                   Product Class: PROGRAM

ACTION  MEDIA      BY      DATE      TIME  COMMENT
      (Last 3 Uses)

Installation

Destination drive(A-H): C          Volume Label : MS-DOS_6
Destination path       : \TMONXM
Name of installer      : JRB
Comment               : 4.5 UPGRADE

Begin installation (Y/N)? N

Type "Y" and press Enter to begin installing the software.

```

Fig. 2.8. Installation setup fields

## Step Three

**Note:** Program titles and default destination paths may vary according to your IAM or T/Mon and firmware versions.

## Setup Installation

The Installation window, shown in Figure 2.8, will appear. Fill in the fields with appropriate information.

The fields in the Installation window are:

**Destination drive:** The disk on which the upgrade will be installed. On all standard installations you should accept the default destination, C, the internal disk of the IAM or T/MonXM system.

**Volume label:** This field will be automatically filled with the label of the destination disk.

**Destination path:** The directory where the upgrade will be installed. On all standard installations you should accept the default path: \ (the root directory). **Note:** Accept the default path unless you are instructed to do otherwise by a DPS Technical Support Representative.

**Name of installer:** Enter your name or initials here. Installers' names are used by T/Install's history function to track installations.

**Comment:** Enter a comment to identify the installation.

After filling in the installation setup fields, type Y and press Enter to begin installation.

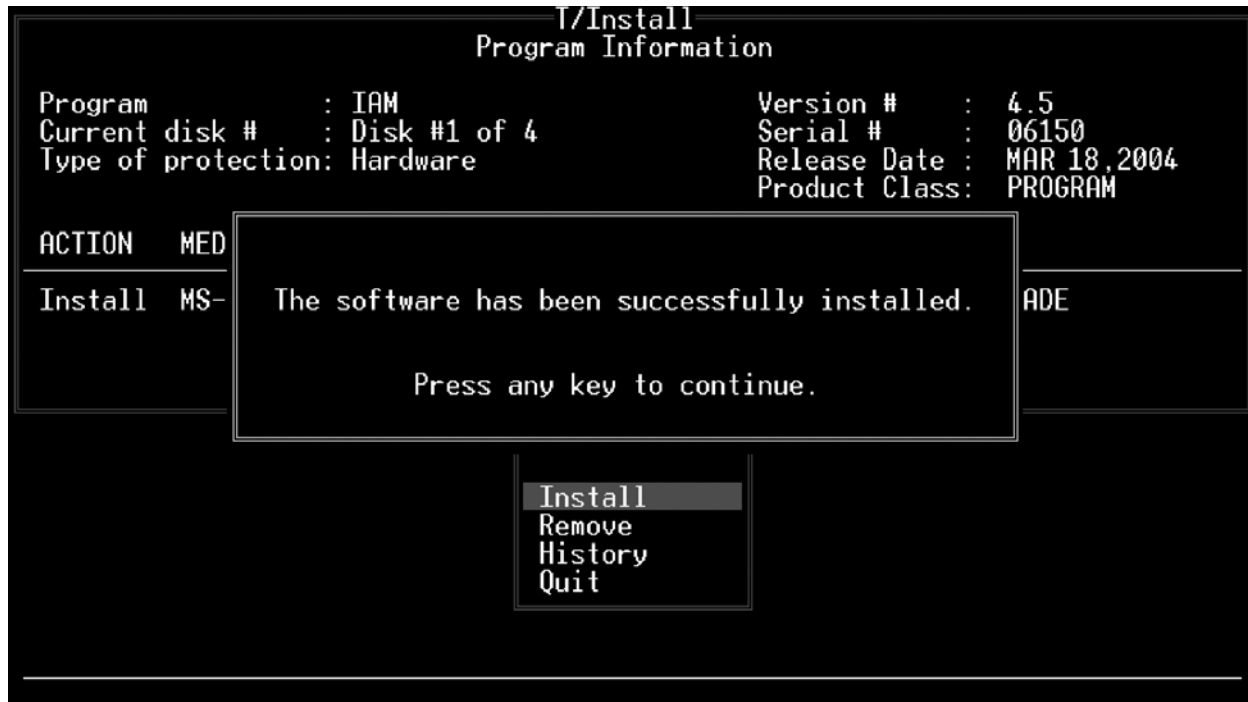


Fig. 2.9. Successful installation message prompt

## Step Four

**Note:** Program titles and default destination paths may vary according to your IAM or T/Mon and firmware versions.

## Run Installation

The installation process will only take a few minutes. The prompt line at the bottom of the screen will list the files being installed and prompt you to swap installation disks when necessary.

After a successful installation, you will see the screen shown in Figure 2.9. Press any key to exit T/Install.

You will return to the W/Shell Main menu. From here you can run your upgraded IAM or T/MonXM software or you can choose Upgrades again to perform more installations.

## Step Five

### Quit T/Install

After the upgrade is finished press Enter to select Quit. Then press “Y” and remove the disk. Now you are ready to install updates, see The following page for more information.

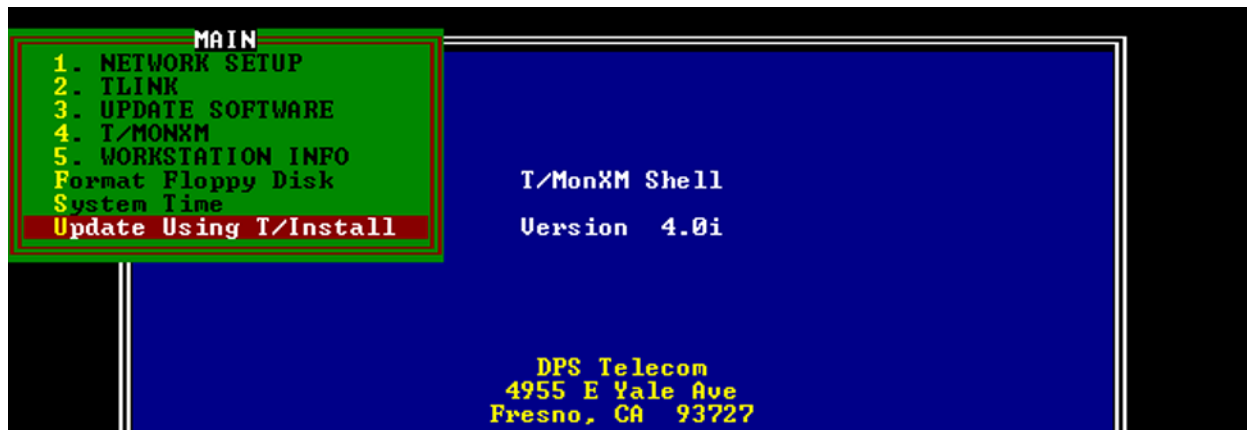


Fig. 2.10 Select Update Using T/Install to install updates from a floppy disk

## Step Six

**Note:** T/Install is not available for the LNX platform. The following instructions apply to T/Mon NOC, SLIM, and IAM models.

## Install Updates Using T/Install

1. Insert Disk 1 of the T/Mon or IAM four-disk set.
2. Choose “Update using T/Install” from the W/Shell Main menu, see Figure 2.10.
3. The Update Menu prompt screen will appear, see Figure 2.11.
4. Repeat Steps 2-4 to install the other T/Mon or IAM floppy disks.

Once you have finished repeat steps 2-4 to install T/Link, NetSetup and any other Utilities using T/Install.

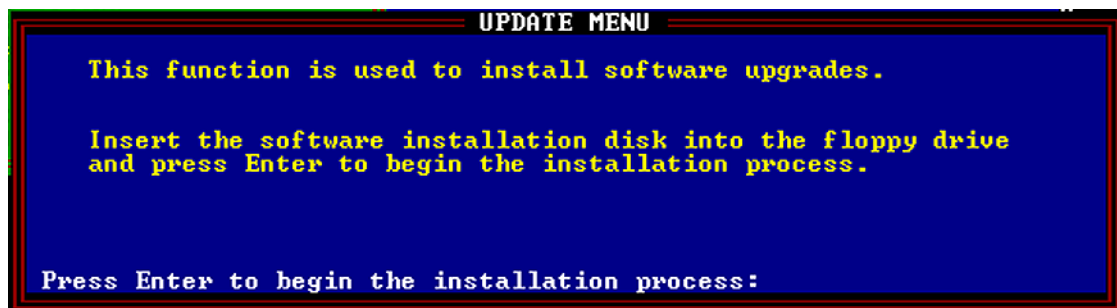


Fig. 2.11 Press Enter to begin installation or F10/Esc to abort



## Remove Software

**Note:** This option is typically not used.

There is no need to remove old versions before installing newer versions.

Start the T/Install utility using the original DPS software disk(s).

**Choose the Remove option.** A removal window will appear at the bottom of the screen. Note that the program will remove program files from the specified drive and path; however, files other than the program files (i.e. data files created by software) will remain. Before a removal starts, the following prompts must be answered.

**Remove software from drive (A-H).** The source drive cannot be the removal drive.

**Drive from which the software will be removed.** Enter the drive letter followed by Enter to select. Valid drives are A - H.

**Path of program files.** Path of installed software to be removed. Drive ID must be omitted since it has been already entered from the previous prompt. If software is in the root directory, type “\” or “ ” (space) followed by Enter.

**Name of Uninstaller.** Enter your name here and press Enter.

**Comment.** Enter an identifying comment in reference to this removal.

**Confirm to remove (Y/N).** Type “Y” and press Enter to start removal or “N” to go back to the beginning of removal procedure.

You have now removed a **working copy** from a disk and restored it back to the original DPS software disk.

```

      T/Install
    Program Information

Program      : IAM                      Version #   : 4.6A05.0406
Current disk # : Disk #1 of 4          Serial #    : 06078
Type of protection: Hardware           Release Date : APR 6.2005
                                           Product Class: PROGRAM

ACTION  MEDIA  BY      DATE      TIME  COMMENT
      (Last 3 Uses)

Removal

Remove programs from drive (A-H) : A      Volume Label :
Path of program files : \
Name of un-installer : DPS
Comment               : .....

Enter comments for tracking purposes (Mandatory field)

ESC/F10/Up-arrow = Edit previous field
  
```

Fig. 2.12 - Removal screen

## Installation History

**Note:** This feature is optional. Information about this feature is included for reference.

A history of installations and removals is kept on file so you may keep track of each transaction. Selecting History from the Main Menu will display the installation/removal history.

**Note:** The last 3 installation/removal histories will be shown at the Main Menu screen at all times, selecting History from the Main Menu will display the last 15 entries.

### History Command Keys

The following keys are applicable when viewing the Installation/Removal History screen:

F1 Toggles the Path column to display the Comment column.

F2 Toggles the Comment column to display the Path where the software was Installed/Removed.

F10/ESC Exits the History screen and returns to the Master Menu.

T/Install Installation/Removal History					
ACTION	MEDIA	BY	DATE	TIME	COMMENT
Remove	A	JOHNNY M.	May 11, 2002	13:08	TAKE TO NEW W/S
Install	A	C. HOWER	May 11, 2002	13:07	INSTALL 1
Install	DISK1_UO.L3	ERB	Jan 27, 2003	16:47	FACTORY TEST

F1=Comment, F2=Path, F10/Esc=Return to Master Menu

Fig. 2.13 - Installation /removal history screen

## Quit

To exit the T/Install utility choose Quit from the Main Menu. You will return to the W/Shell Main Menu depending upon where you started.

The T/Link utility controls remote access of the T/Mon or IAM via T/Access. Normally you do not have to change the default T/Link settings—with one important exception. You should change the default factory password for increased security.

## T/Link

**Note:** T/Link is not available on the LNX platform. The following instructions are for T/Mon NOC, SLIM, and IAM users.

**Note:** Change the factory default password in T/Link for increased security.

### Edit T/Link Configuration Settings

Use the following instructions to edit your T/Link configuration settings:

1. To edit your T/Link configuration settings, use your arrow keys to highlight TLINK and press Enter. The TLINK menu will appear (see Figure 2.14).
2. Highlight and choose “Configure T/Link. The T/Link Configuration screen will appear. See Figure. 2.15.
3. Press E (Edit) to edit your configuration settings.
4. Press F8 to save your changes.



Fig. 2.14 - T/Link Utilities menu

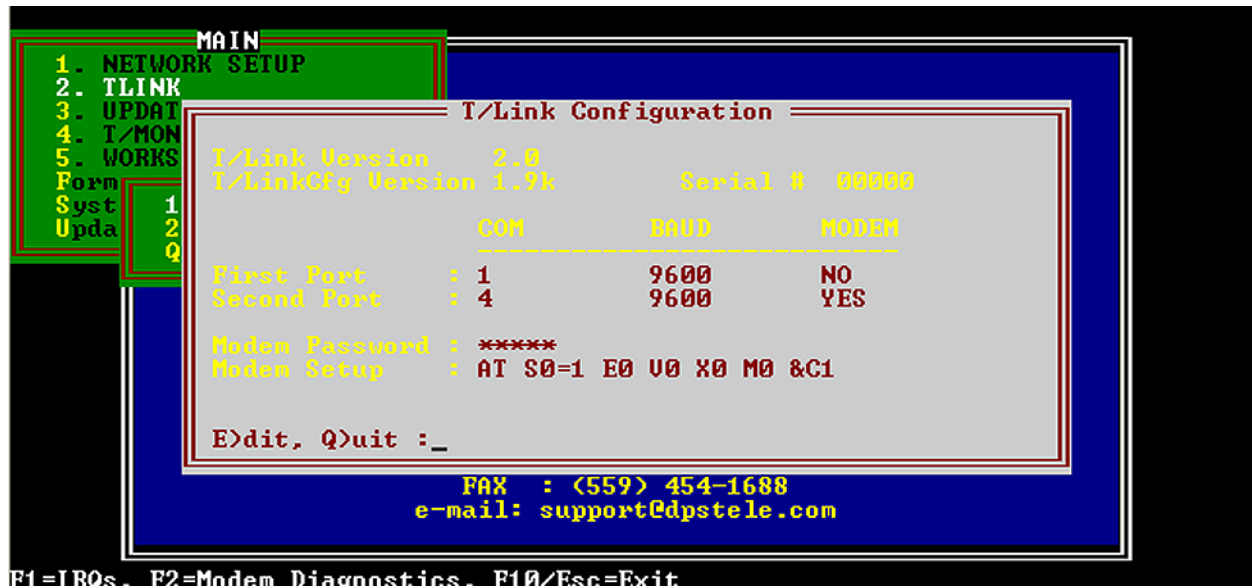


Fig. 2.15 - Press E to edit your T/Link configurations

Table 2.B - Fields in the T/Link Configuration screen

Selection	Description
First Port (Typically T/Access port on computer)	
Com	Enter the T/Access Com port number (1-4, "-" for none)
Baud	Select the baud rate for the T/Access Com port (300, 1200, 2400, 9600). Usually baud rate is 9600. <b>Note:</b> Press the Tab key to select rate from menu. Make sure Caps Lock is off.
Modem	Select N (No) for T/Access port (select No for no modem on this port)
Second Port (Typically Modem port on IAM or T/Mon) *	
Com	Enter the Modem Com port number (1-4, "-" for none)
Baud	Select the baud rate for the T/Access Com port (300, 1200, 2400, 9600). Usually baud rate is 9600. <b>Note:</b> Press the Tab key to select rate from menu. Make sure Caps Lock is off.
Modem	Select Y (Yes) for Modem port
Modem Password	Enter a new password for increased security
Modem Setup	Enter your user defined modem init. string

\* Typically modem for remote access.

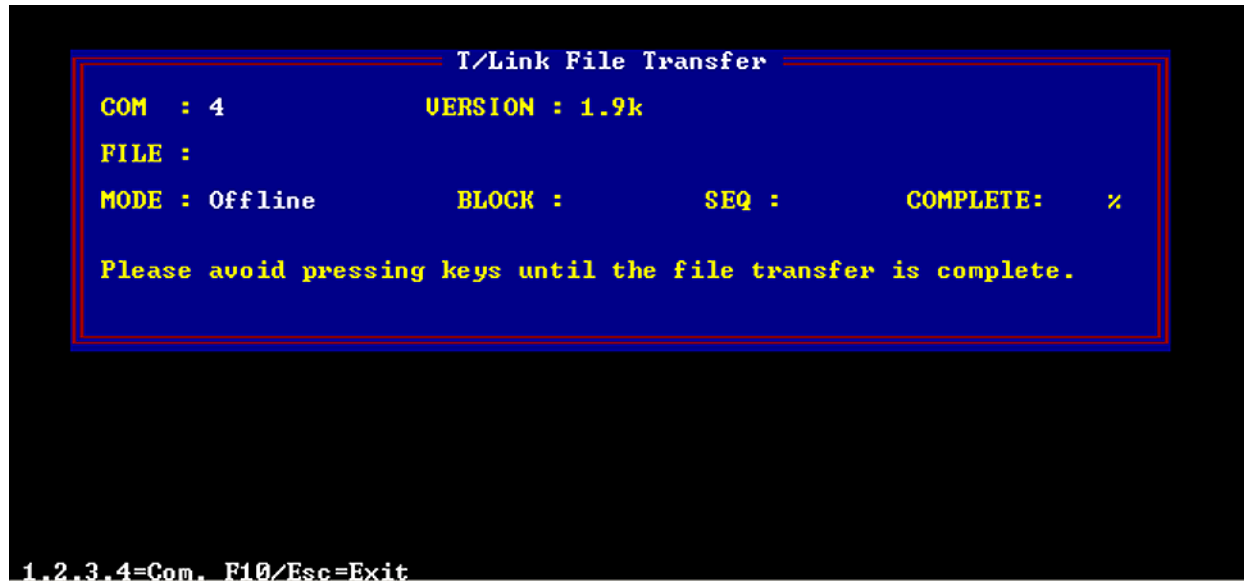


Fig. 2.16 - T/Link File Transfer screen

---

### T/Link File Transfer

Selecting File Transfer from the TLINK menu allows you to transfer files via dial up from DPS Telecom for technical support purposes. Contact DPS Tech Support for more information.

## System Time

Manually set your IAM or T/MonXM workstation system time by selecting System Time from the WShell Main menu. See Figure 2.17.

**Note:** Don't forget to adjust time during day light saving and standard time.

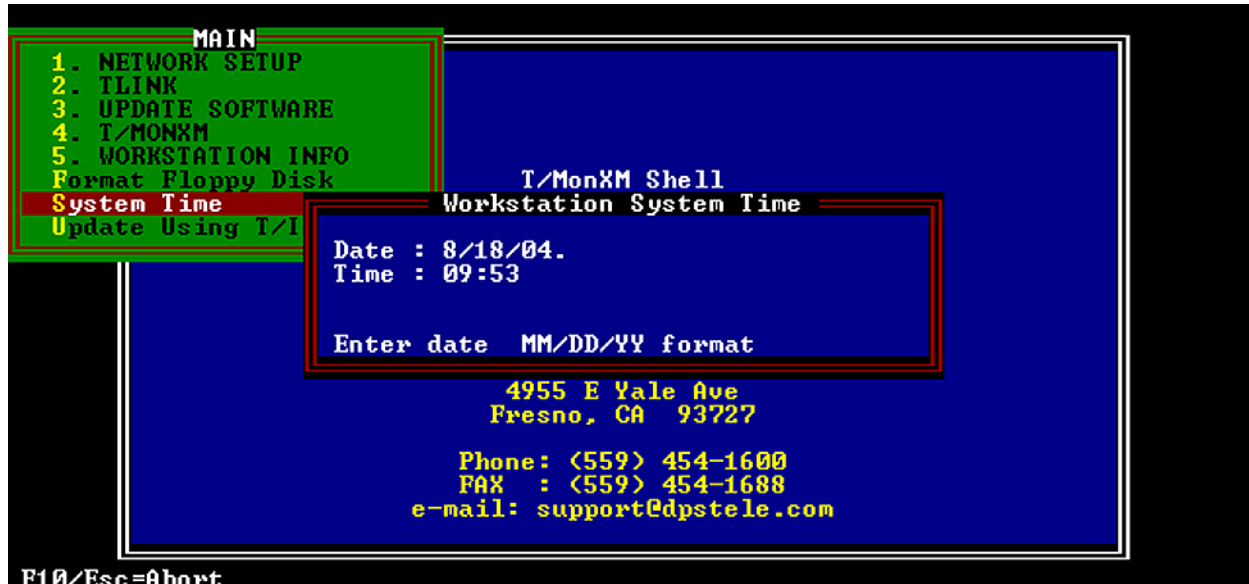


Fig. 2.17 - Manually set your workstation system time

## Format Floppy Disk

You can format floppy disks in your IAM or T/Mon's floppy drive by selecting the Format Floppy Disk option from the WShell Main menu. The Format Floppy Menu will appear — see Figure 2.18.

1. Insert a floppy disk and enter the floppy disk drive letter (normally A).
2. Then select the size of your floppy disk and press Enter to format the floppy disk.

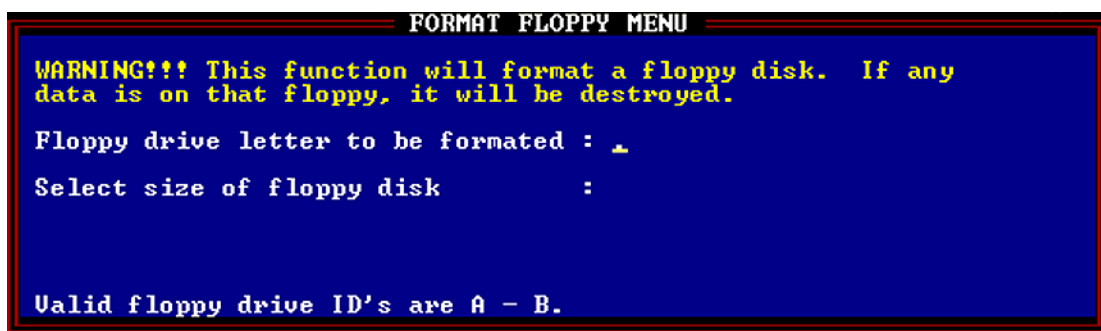


Fig. 2.18 - The Format Floppy Menu screen

## Workstation Info Menu

You can view general information on you IAM or T/Mon by selecting Workstation Info from the WShell Main menu (see Figure 2.18).

**Note:** Menu options will vary according to your IAM or T/Mon unit and firmware versions.

Figure 2.20 shows an example workstation information screen. Information will vary according to your IAM or T/Mon unit.

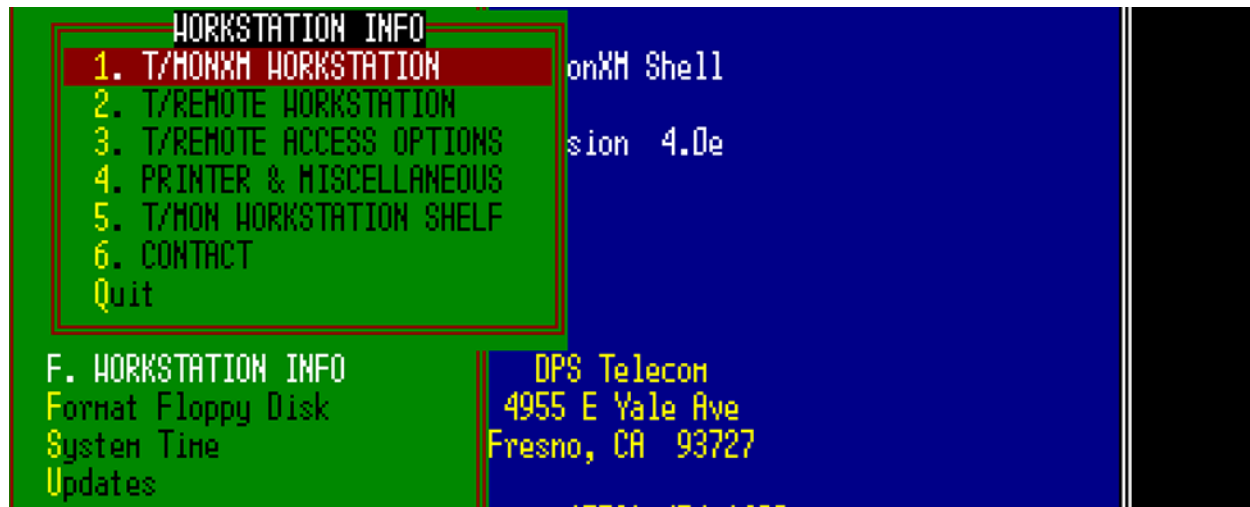


Fig. 2.19 - Example of Workstation Info menu for T/MonXM

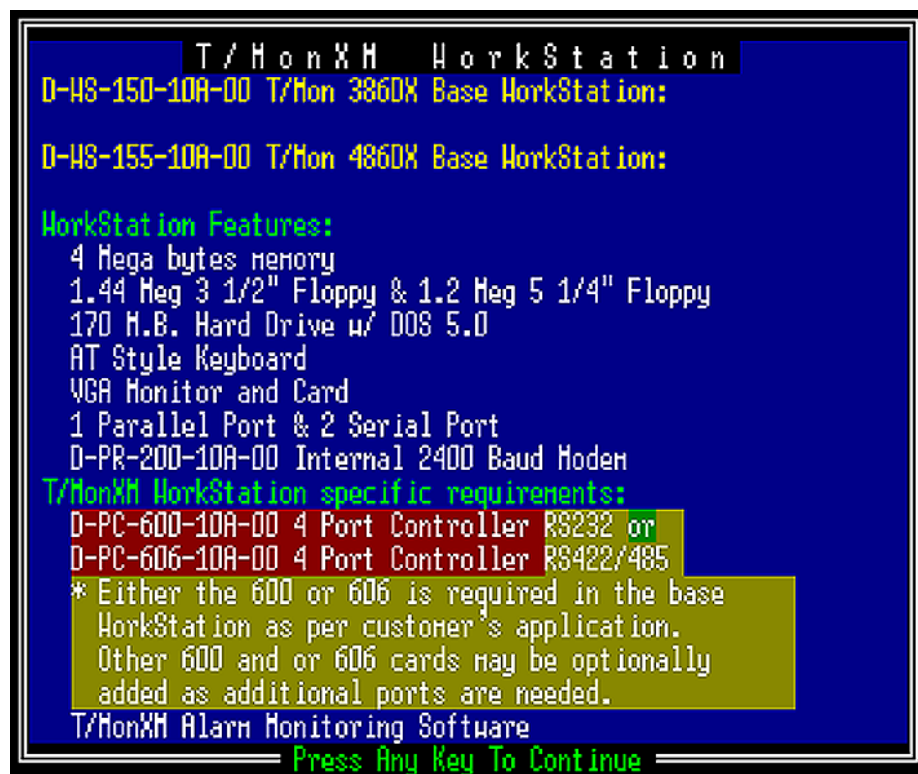


Fig. 2.20 - Example T/MonXM Workstation general information screen

## Automatic Backup

T/Mon has support for automatically backing up its data and application files on the local hard drive at user-definable daily and monthly intervals. This allows for the system to have “go back” functionality, which includes the restoration of data files and the TMon application itself. This is particularly useful for reverting back to a previous version of the database if you find you’ve data-based something incorrectly. This can also be used to revert back to a previous version of the software should you encounter a problem during the upgrade process.

### There are two parts to the Automatic Backup:

The first is to define the Automatic Backup job which is responsible for executing the automatic backups. If you define more backups than you have hard disk space for, only the maximum number of backups that can safely fit on the disk will be stored. The oldest backup will be purged automatically when it is no longer within the user-specified backup windows (“Days Back” or “Months Back”, see Fig. 2.20) or there is not enough disk space to store the newest automatic backup. You do not have to worry about purging old backups or running out of disk space, because the Automatic Backup job will purge old backups for you.

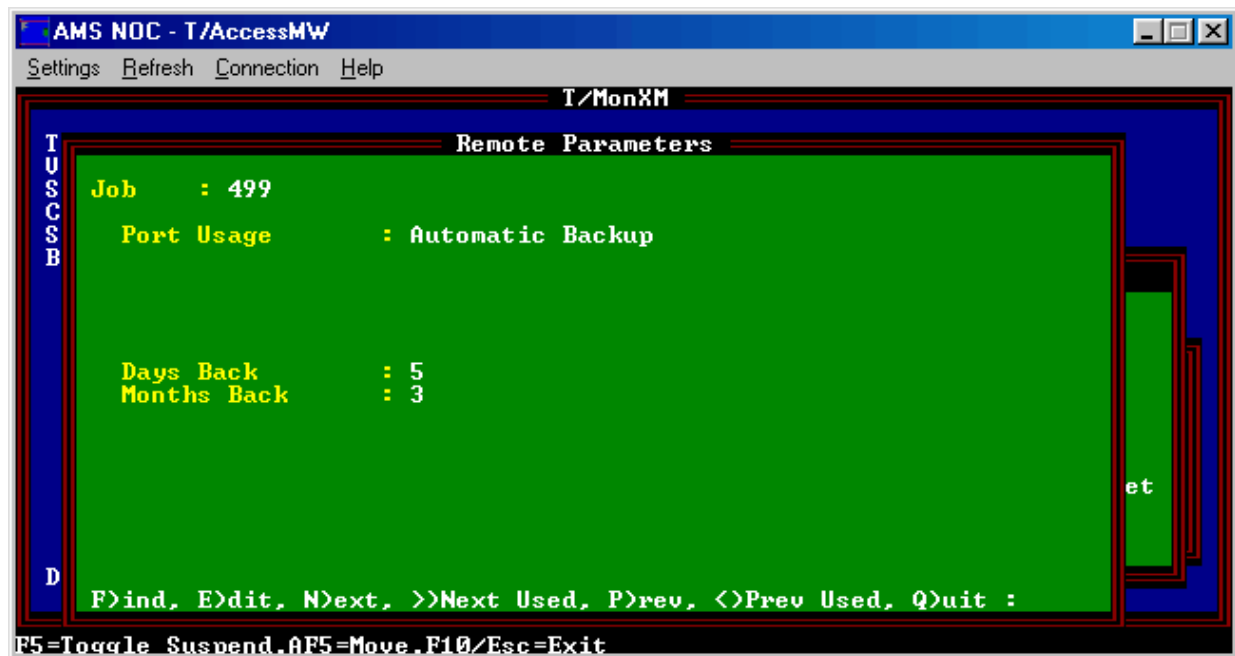


Fig. 2.20 - Remote Parameters screen for Automatic Backup job



The parameters for the Automatic Backup job are as follows:

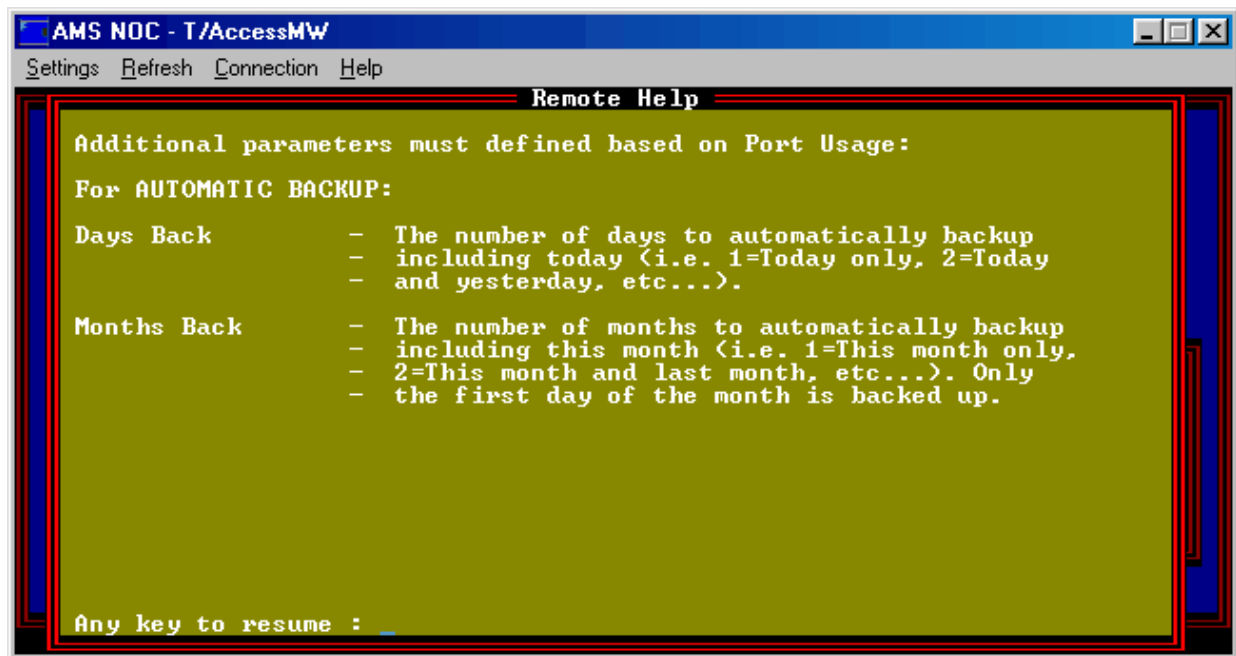


Fig. 2.21 - Remote Help screen for Automatic Backup job

The second part of Automatic Backup is the Backup/Restore Utility, accessible from the "MANAGE DATA FILES" option in WShell. It requires no configuration.

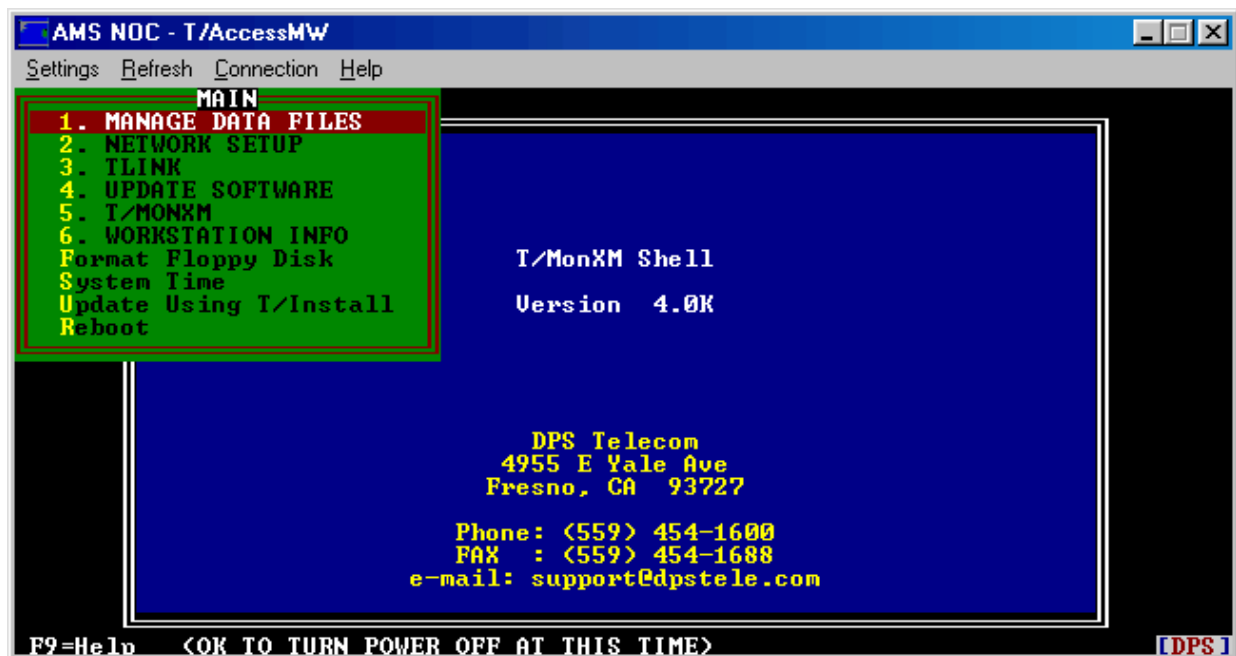


Fig. 2.22 - Select Manage Data Files from the Main Menu

The Master Menu of the Backup/Restore Utility gives the option to backup the data files, restore data files, or quit the program and return to WShell.

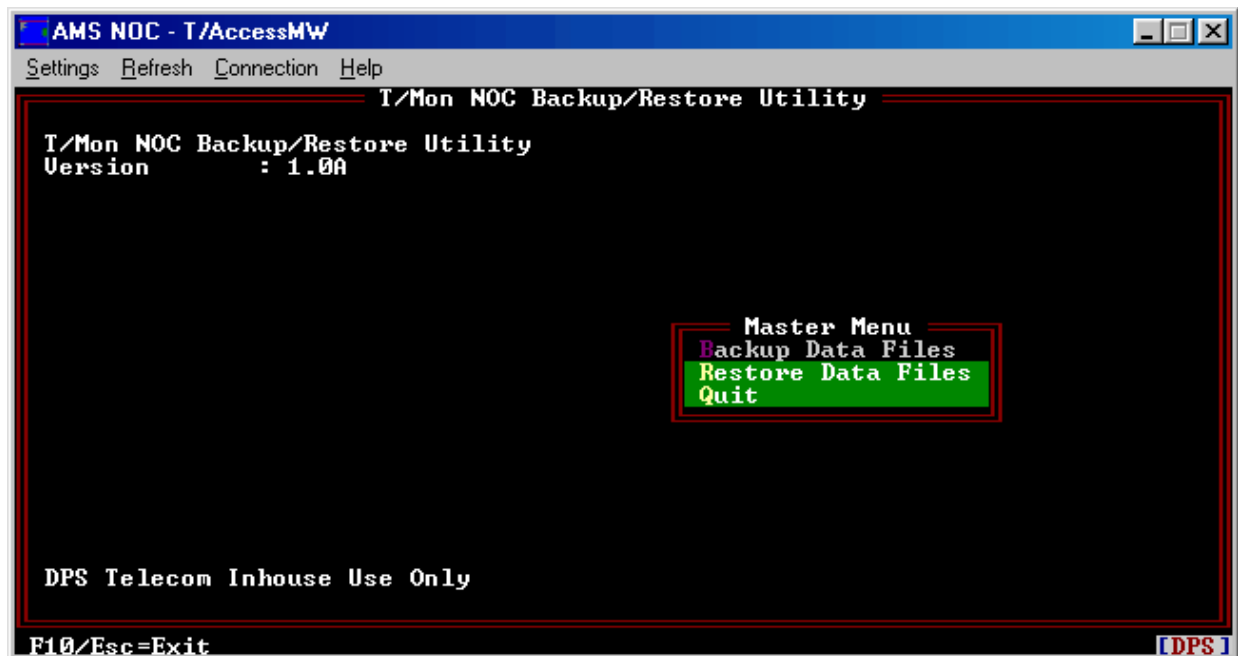


Fig. 2.23 - The T/Mon NOC Backup/Restore Utility

Selecting the “Backup Data Files” option will allow the user to manually backup the data files and T/Mon application files. Only one manual backup can be stored on the local disk at a time. Therefore, **the new manual backup will overwrite the previous manual backup.**

The details of the previous manual backup are displayed upon entering this screen. Using them, you can determine if you want to overwrite your existing manual backup. Remember that this “manual backup” is separate from the “automatic backups” created by the TMon’s Automatic Backup job. Automatic backups will not overwrite the manual backup, even if there is insufficient disk space for the automatic backup. In this case, the oldest automatic backup will be purged.

Remember, there can be only one manual backup, but there can be multiple automatic backups (so long as there is sufficient disk space).

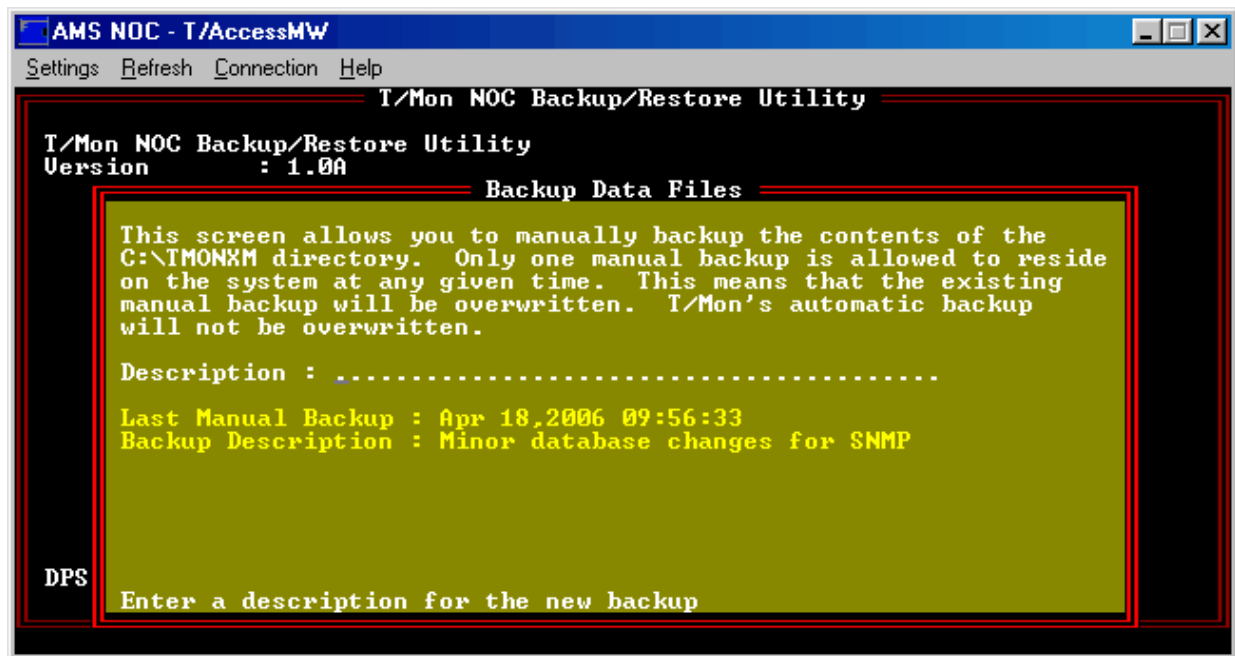


Fig. 2.24 - Backup Overwrite Warning

Selecting the “Restore Data Files” option from the Master Menu will allow the user to manually restore the data files and T/Mon application files from either a manual or automatic backup. The existing TMon data files and application will be overwritten, so use with caution.

If you make database changes, install a new version of the software, then restore an old backup, you will be reverted back to both the old database and software version.

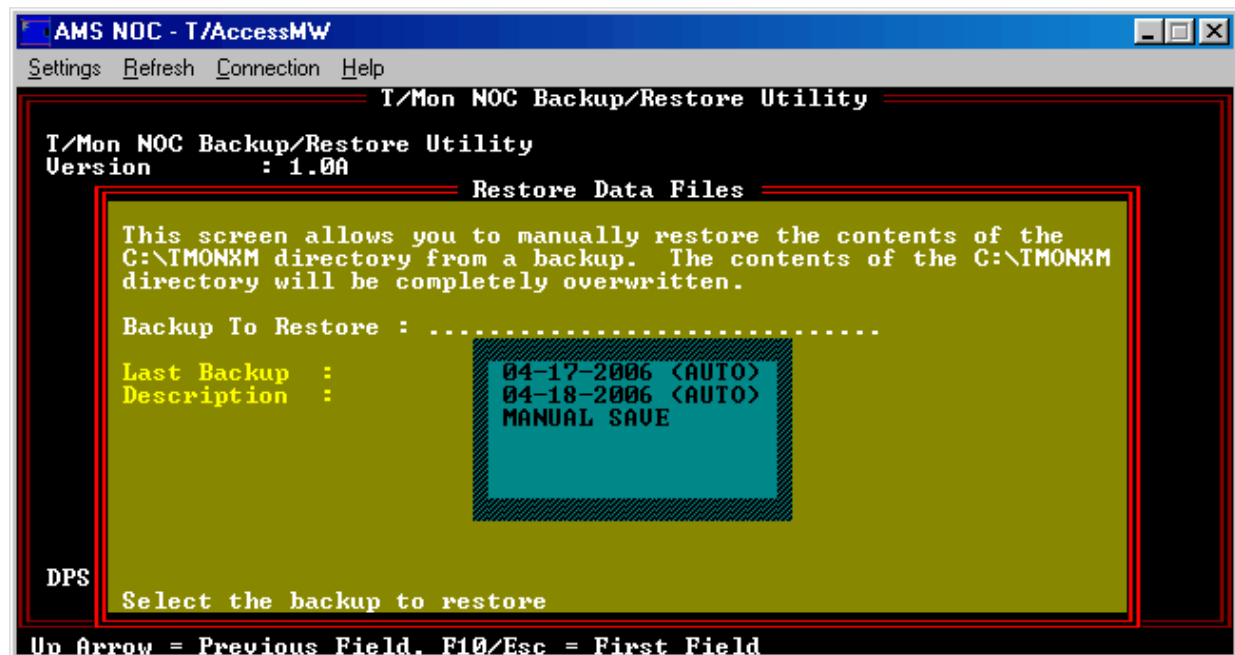


Fig. 2.25 - Selecting a Backup to Restore

Selecting a backup will cause the information about the backup to be displayed and then you will be prompted as to if you want to continue with restoring the backup. **Selecting the backup alone will not restore it.**

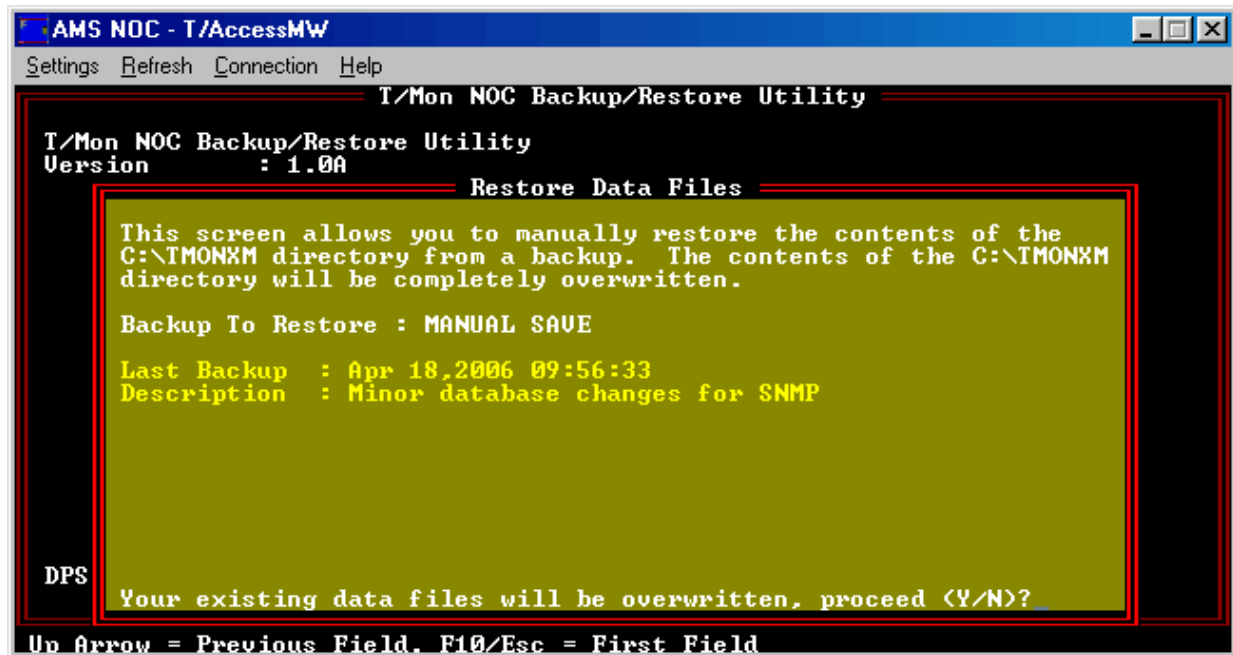


Fig. 2.26 - Overwrite Existing Data Files Warning and Confirmation

**This page intentionally left blank.**

## Section 3 - Network Setup

### Ethernet I/O

All LAN usage is set up on Port 28 within T/MonXM > Parameters > Remote Ports.

**Note:** This step applies only to the T/Mon NOC, SLIM, and IAM platforms. Instructions for changing T/Mon LNX's default IP start on the Following page.

Port 28 is reserved exclusively for configuring Ethernet input and output. This usage can be halted by selecting Halted in the Port Usage field or suspended by pressing F5, but no other usage can be assigned to Port 28.

Port 28 controls the number and type of TCP ports available to T/MonXM. Ethernet I/O must be set up on Port 28 to use LAN jobs on Ports 30-500.

### Step One: T/Mon NOC, SLIM and IAM Network Setup

To configure T/MonXM to use Ethernet I/O, you must first assign your T/MonXM system an IP address. To assign an IP address, follow these steps.

1. Exit T/MonXM to W/Shell.
2. From the W/Shell Main menu, choose Network Setup.



Fig. 3.1 - Choosing Network Setup

**Note:** see Software Module 1 for LAN based remotes — NetGuardian.

3. From the Network Setup menu, choose Run Network Setup. (See Figure 3.1.)
4. From the Network Setup Utility screen, select Edit Settings.
5. The Edit Settings screen will appear. (See Figure 3.2.) Enter IP



Fig. 3.2 - Editing Network Settings

addresses for Network Address, Network Subnet Mask, and Default Gateway. If you don't know the correct addresses, ask your network administrator.

6. In the Edit Settings screen you can also select the number of possible TCP and UDP connections available in T/MonXM. By default, 40 TCP and 5 UDP connections are activated. Up to 49 UDP and TCP connections total can be activated.

**Note:** If you have defined more TCP ports than are activated, T/MonXM will display an error message during initialization indicating that it can't get a network descriptor.

If you want to verify that your T/MonXM system is connected to your LAN, ping the network address assigned to the T/MonXM system from a computer on your network.

7. You must reboot before the changes can take effect.

### T/Mon Data Connection Job Association Feature

When a data connection is assigned to a virtual job the data connection is said to be "associated" with that job. The data connections are edited in the Ethernet TCP Port Definition screen. From this screen you can easily tell if each data connection is associated with a job by checking the "Job" field. If the Job field is 0 then the data connection is not associated with a virtual job. If the Job field is not 0 then the data connection is associated with that job number. The Job field is populated automatically and is non-editable.

Ent	Type	IP/Hostname	TCP Port	Description	Job
1	TCP		2001	t\windows	30
2	TCP		2002	t\windows	47
3	UDP		2030	DCP POLLING PORT <3>	50
4	TELNET-RAW	10.1.4.208	23	windsox	55
5	TCP		2005	I/GrafX	35
6	TCP		80	HTTP Server	80
7	.....				
8					
9	TCP		2008	HTP	0
10	TELNET-RAW	137.118.16.2	25	MAIL.RTCOM.NET	60
11	TELNET-RAW	137.118.129.4	110	POP.RTCOM.NET	61
12	ICMP		3030	ICMP Ping Test	36
13					
14					
15					
16	TCP		21	FTP server	100
17	TELNET-RAW	137.118.214.21	20	FTP Xfer	101

Tab=Defaults. F1=GOTO. F3=BLANK. F8=Save. F10/Esc=Exit

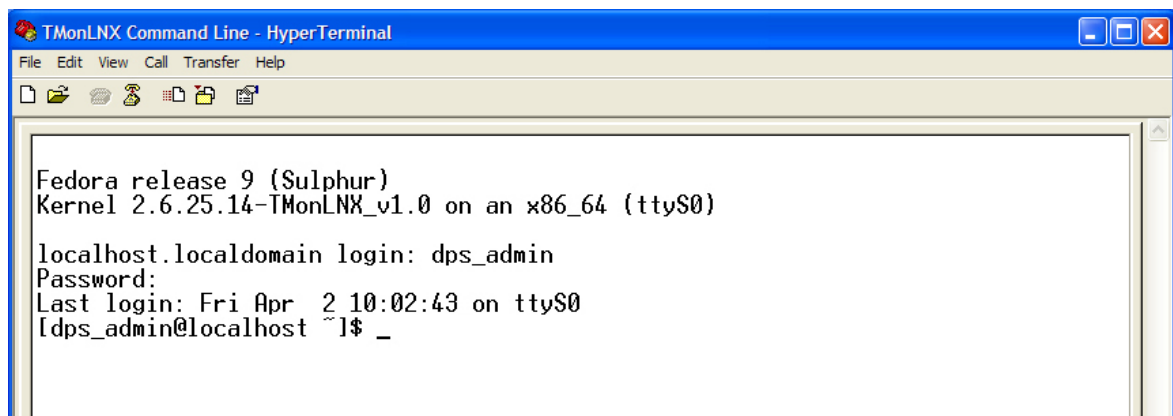
Fig. 3.3 - Ethernet TCP Port Definition Screen

## Step One: Configuring T/Mon LNX's IP address

**Note:** This step explains initial configuration for your main network interface, Eth0. Instructions for configuring Eth1-5 begin at the bottom of this page.

To configure T/MonXM to use Ethernet I/O, you must first assign your T/Mon LNX system an IP address. To assign an IP address:

1. Connect a null terminated serial cable (T/Access cable included with the unit) from a PC's COM port to the T/Mon LNX craft port.
2. Start HyperTerminal on your PC, located in the Start Menu > Programs > Accessories > Communications. Configure a serial port with the following information::
  - a. 38400 bps
  - b. 8 data bits
  - c. No parity
  - d. 1 stop bit
  - e. No flow control
3. Connect HyperTerminal and Press Enter. A login prompt should appear.



**Fig. 3.4 - The Hyperterminal Login Prompt**

4. Enter the default username "dps\_admin" and default password "dpstelecom" (without quotes)
5. Enter "/changeIp" (case-sensitive; type without quotes, leads with a period) and press Enter. Enter in the new IP address, subnet, gateway, and DNS information.
6. Press Y to confirm the new IP address. The script will apply the new IP.

**Note:** This step explains configuration steps for Eth1-5. To configure your primary, Eth0 interface, see the procedure beginning at the top of this page.

## Configuring NIC Interfaces

1. After giving the T/Mon LNX an IP address, open an Internet browser and navigate to the IP at port 10000: <http://xxx.xxx.xxx.xxx:10000> (where x's are T/Mon's IP address)
2. Login with the default username of "dps\_admin" and password "dpstelecom"
3. In the left frame, click on Networking, then click on Network Configuration.
4. In the right frame, click on Network Interfaces. Click on the



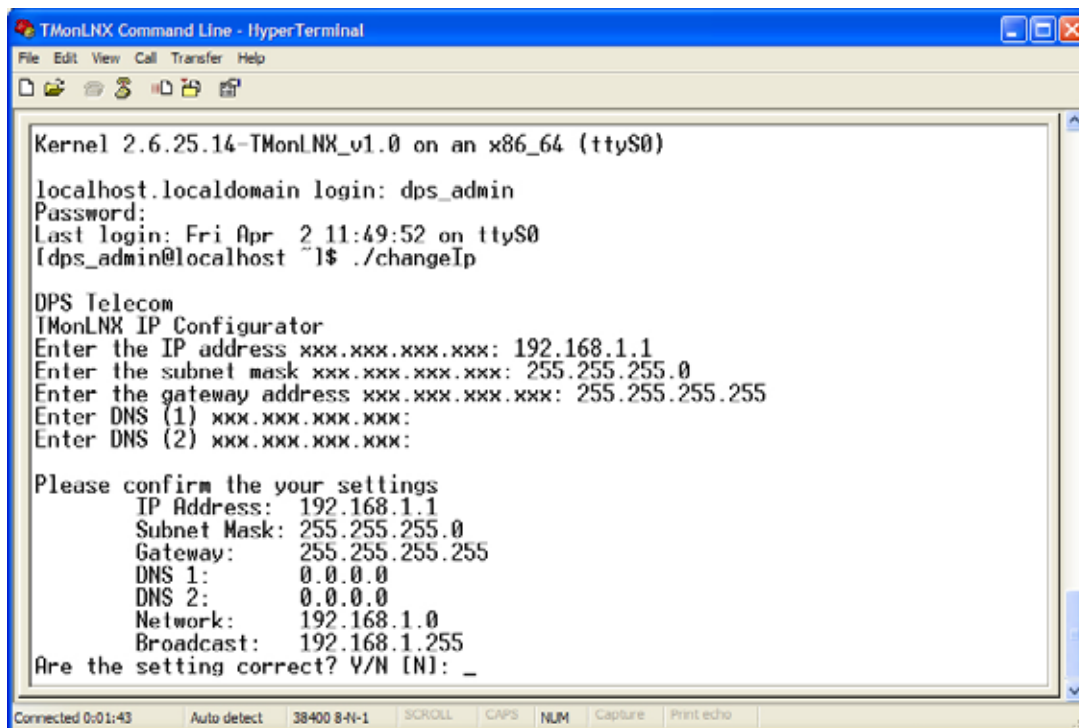


Fig. 3.5 - Hyperterminal IP Configuration Screen

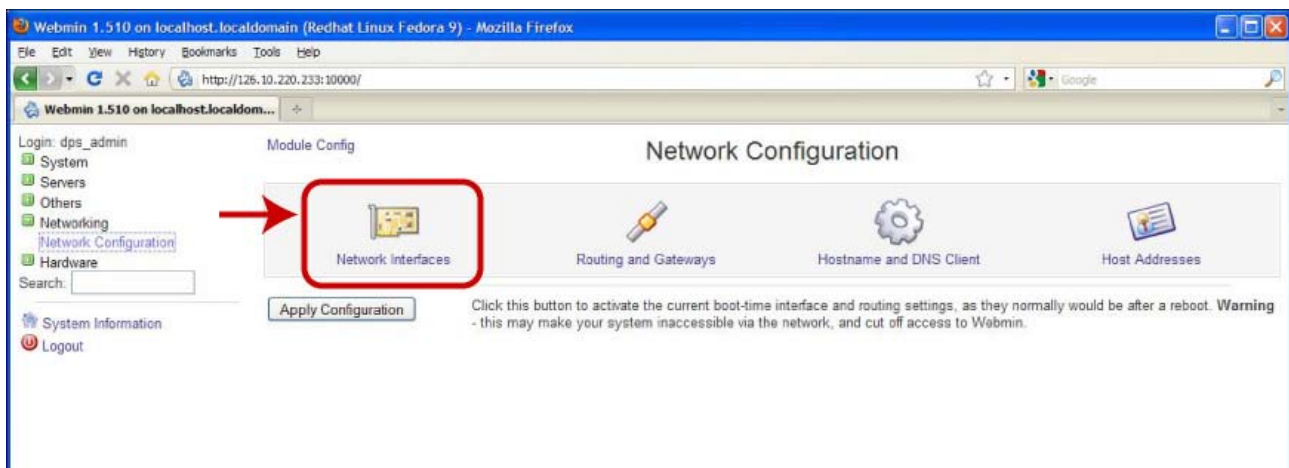


Fig. 3.4 - Network Configuration For the LNX

Activated at Boot tab.

5. Click on Add a New Interface.
6. In the name field, enter the NIC label on the back of the T/Mon LNX unit you want to use: eth1, eth2, eth3, eth4, or eth5. NOTE: If the network is not active, don't define.
7. Click on Create and Apply.
8. The new interface should now appear on the list.
9. Adding gateways to new network interfaces:
  - Return to the Network Configuration page from Step 3 and click on the Routing and Gateways icon.
  - Select the network interface you've just created from the drop-down menu (Eth2 in this example). Enter the gateway information.
  - Select No for Act as router. Click Save to finish.

Fig. 3.4 - Ethernet TCP Port Definition Screen

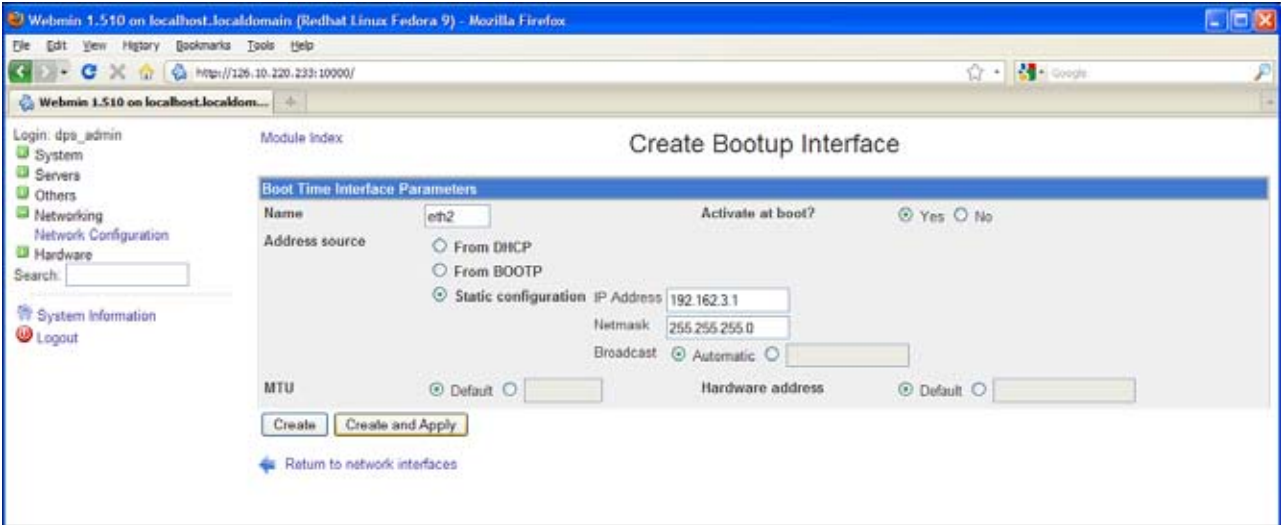


Fig. 3.4 - Define Eth1-Eth5

## Step Two: Port 28

Your next step is to assign Ethernet I/O to Port 28. Follow these steps:

1. Choose Master > Parameters > Remote Ports > F)ind and enter 28 <CR>.
2. Choose E)dit.
3. Press Tab to select the list box. Highlight “Ethernet I/O” and press Enter.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	TELNET-RAW	111.111.111.110	25	SMTP Port
2	TELNET-RAW			
3	UDP			TCP (T/GrafX, T/RemoteW, HTTP, RAS, FTP Server, TMonNet)
4	TCP			TELNET-RAW (ASCII, Craft, E-Mail, FTP Data Transfer)
5	UDP			TELNET (ASCII, CRAFT : if TELNET negotiation required)
6	ICMP			UDP (DPS RTU Polling, SNMP TRAP Processing, SNMP Agent)
7				ICMP (PING)
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

## Step Three: TCP Ports

Finally, TCP ports must be defined to be available for use. Follow these steps:

1. From the Remote Parameters screen for Port 28, press F1. This command opens the Ethernet TCP Port Definition screen — See Figure 3.3.

**Note:** this screen can also be accessed from Ports 30-500 by pressing F6.

2. Press Tab to select the default list for port type. Your choices are TCP, TELNET-Raw, TELNET, UDP, and ICMP. For a description of TCP port types — see Table 3.A.
3. If you selected TELNET or TELNET-Raw, you must enter an IP address. If you selected other port types, the cursor will skip over the IP Address field.
4. You must enter a TCP port number. Certain port numbers are reserved for specific uses. If an application requires a reserved TCP port number, the correct number will be listed in the section of the T/MonXM User Manual that describes the application and on the Remote Parameters screen for the port.
5. If you want, enter a description in the Description field.
6. Press F8 to save your changes.

**Table 3.A - Ethernet TCP Port types and applications**

Field	Description
TCP	Responders, Remote Access, T/GrafX, HTTP Server, RAS, FTP Server, Craft, SNMP Processor Trap
TELNET-RAW	Interrogators, ASCII Input, Craft, E-Mail, FTP Data Transfer
TELNET	Same as Telnet-Raw Note: to be used only when Telnet Negotiation is required.
UDP	Interrogators, Responders, SNMP Trap Processor, SNMP Agent, Network Time
ICMP	Ping

**Table 3.B - Key commands available in the Ethernet TCP Port Definition screen**

Function Key	Description
Tab	Open default list of TCP port types.
F1	Interrogators, ASCII Input, Craft, E-Mail, FTP Data Transfer
F3	BLANK port definition entry.
F8	Save port definition entries.
F10/Esc	Exit Ethernet TCP Port Definition screen without saving changes.

# Assigning a Data Connection

After you have set up the network, you will be able to assign a data connection to your remote ports when defining them to poll your remote devices via LAN.

Assigning a TCP port to a LAN job takes four steps:

- 1. Define the TCP Port in the Ethernet TCP Port Definition screen.
- 2. Define the port usage in the Remote Parameters screen.
- 3. Assign the remote port a TCP port data connection in the Data Connection Assignment screen.
- 4. If necessary, provision the devices that will use the TCP data connection.

For example, let's say you want to configure a data connection for KDAs to report to T/MonXM over LAN. (These instructions apply equally well to the NetGuardian. For instructions on provisioning a NetGuardian, see Section M1-25, LAN-Based Remotes.) You would follow these steps:

## Step One

### Define the TCP port

- 1. Choose Master > Parameters > Remote Ports > F (Find) > 28. Verify that Port 28 is assigned to Ethernet I/O.
- 2. Press F1 to open the Ethernet TCP Port Definition screen.
- 3. Select an unused entry and press Tab to select the default list box for the Type field.
- 4. Highlight UDP and press Enter.
- 5. Type "2001" in the TCP Port field.
- 6. Type a description in the Description field.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	UDP.....		2001	KDA Interface
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Fig. 3.5 - A TCP Port Configuration Suitable for an RTU

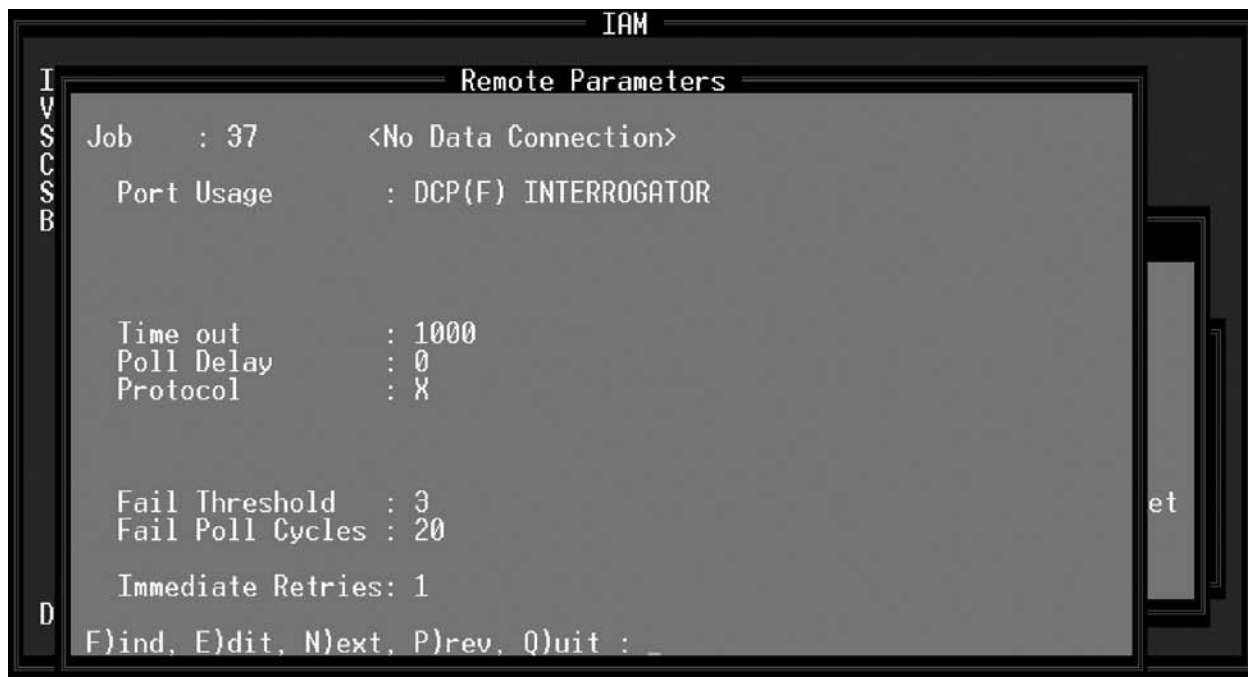


Fig.3.6 - Remote Parameters screen with “No Data Connection” prompt

## Step Two

### Define the port usage

1. Choose Master > Parameters > Remote Ports > F (Find). Select a port numbered 30 or higher. (Ports 30-500 are reserved for LAN jobs.)
2. Press Tab to select the default list box for the Port Usage field.
3. Highlight DCP(F) Interrogator and press Enter. See Fig. 3.5.
4. In the DCP(F) Mode field, select X. Fill in all other fields as you would for any DCP(x) port.

**Note:** If you are setting up a remote port and the selected port usage requires a TCP connection, T/MonXM will inform you by flashing “No Data Connection” at the top of the screen — see Figure 3.6.

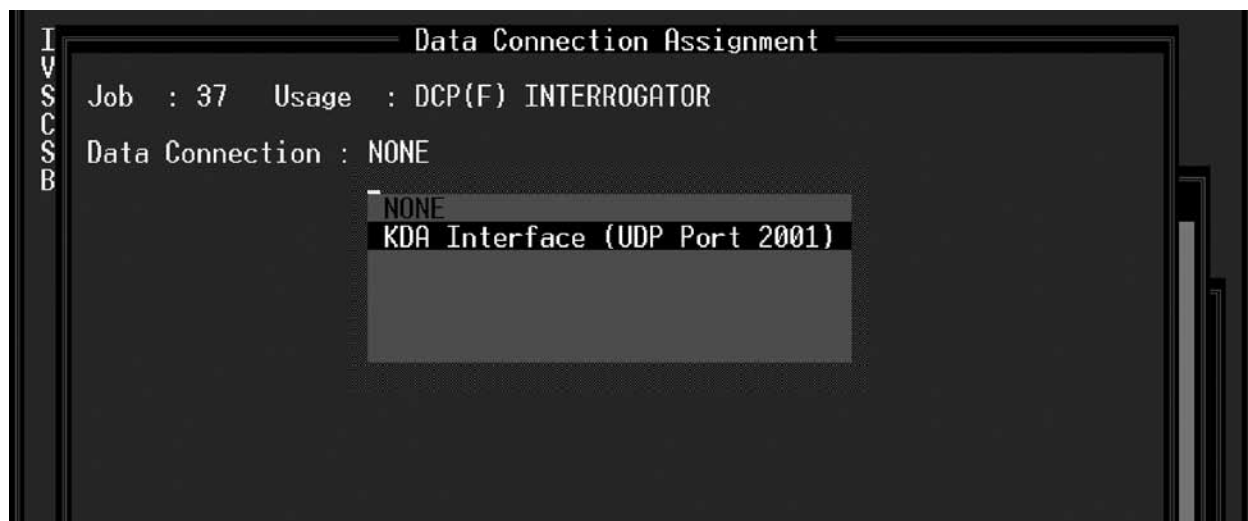


Fig. 3.7 - Assigning a Data Connection to the KDA LAN Job

## Step Three

### Assign the data connection

1. From the Remote Parameters screen, press F6 to open the Data Connection Assignment screen.
2. Press Tab to select the default list box for the Data Connection field.
3. Highlight the data connection created for this port and press Enter.

```

Remote Device Definition
-----
Port / Job      : 37      DCP(F) INTERROGATOR
Device ID      : 5       111.111.111.111 / 2001

Description    : KDA Site 5
Site Name     : FRESNO
Device Type    : Standard
Displays      : 1-99
Poll Type     : U
Refresh Rate  : 175
Firmware Ver  :
Log Undefined: N

----- Address Defaults -----
Polarity      : B       Windows      :
Logging       : L       Message      : 0
History       : H
Level         : A
Status        : A
Reverse       : N
Description   : (Undefined)

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

F1=Pnts, F3=Int Alarms, AF1=Tl1, AF2=Ala, AF3=UDP, AF5=Move, F10/Esc=Exit

```

**Fig. 3.8 - KDA Shelf Remote Device Definition Screen**

For the KDA example, your last step would be to provision the KDA.

1. Provision the KDA according to the instructions in Section M3-7, File Maintenance, KDA Shelves.
2. Repeat for each KDA on the TCP/IP port.
3. Choose Master > Parameters > Remote Ports > F (Find) and select the remote port you assigned for the KDA.
4. Press F1 to open the Remote Device Definition Screen.
5. Choose F)ind and select the ID number for the KDA.
6. Press Alt-F3.
7. Enter the KDA's IP address and UDP port. This information must exactly match the value assigned when the KDA was first configured — see Figure 3.7 above.
8. Repeat steps 5 through 7 for each KDA.

Before uploading the provisioning file to the KDA, you must initialize the system and enter Monitor Mode. Upload the file according to

**This page intentionally left blank.**

## Section 4 - T/MonXM Interface

**The Fast Menu feature allows menu commands to be selected with a single press of the hot key. To turn off Fast Menus, choose the Miscellaneous command on the Parameters menu and set Fast Menus to “N.”**

**Note:** Always exit the program cleanly. This means that you must execute the Quit option from the Master menu. NEVER turn off the computer before exiting the program. Doing so could corrupt the data files!

### T/MonXM Interface Menus

T/MonXM features many pop-up menus, providing quick selection of functions. Menus are displayed in a variety of styles between pages.

When a menu is available, you must select the menu by pressing the Tab key before you can choose commands from the menu.

**Note:** leaving the Caps Lock key on will disable the Tab key selection function. Unlock the Caps Lock key or press Alt-D to select an item from pop-up menus.

Selected menu commands are highlighted by a black bar. Menu commands are chosen by moving the bar to highlight the desired command and pressing the Enter key.

There are two ways to choose commands:

1. Use the Down Arrow or Tab key to move the highlight bar down and the Up Arrow key or Shift Tab to move the highlight bar up. The highlight bar wraps around the menu, so if the highlight bar is at the end of the menu and you continue to press Down Arrow, the highlight bar returns to the top of the menu. Similarly, if the highlight bar is at the top of the menu and you press Up Arrow, the highlight bar moves to the bottom of the menu.

Once you have highlighted the command you want, press the Enter key to execute the command.

2. Use the shortcut key for the command you want. The shortcut key is shown by the highlighted character in the menu command. For example, to choose the command

Monitor

press M. The highlight bar immediately moves to highlight the Monitor command. Shortcut keys are not case sensitive.

If the Fast Menus feature is enabled, menu commands may be chosen by pressing only the shortcut key. If Fast Menus is disabled, press the Enter key to execute the command.



Fig. 4.1 - T/MonXM Master Menu



**Table 4.A - Fast Menu hot key commands**

Keys	Description
1-9	Range of acceptable keys. Examples: 1-9 = range 3- = range to end (all values from 3 to the end of the series) -8 = start to range (all values from the start of the series to 8) 2,4,9 = separate; i.e., 2, 4, 9
A-Z/F1-F10	Press the corresponding letter or function key on the computer keyboard
Alt A-Z/0-9	Press the Alt key at the same time with the corresponding letter key.
Ctrl A-Z/0-9	Press the Control key at the same time with the corresponding letter key.
Enter	Press the Enter key on the computer keyboard.
Space	Press the Space Bar on the computer keyboard.
[ ]	Indicates a default value.

**Function Hot Key Commands**

Some commands in T/MonXM are chosen by pressing function keys. Available key commands are listed in the message line at the bottom of the screen. Certain key commands are always available in T/MonXM:

**F9**

Pressing F9 opens a Help window that explains the currently available commands.

**F10 or Esc**

The F10 and Esc keys are interchangeable. Pressing either F10 or Esc exits the current function.

- If a menu is open, pressing Esc closes the submenu and open the parent menu from which you selected the submenu. Pressing Esc repeatedly moves step by step up the menu hierarchy, eventually returning to the Master menu. If the Master menu is open, pressing Esc quits T/MonXM.
- If you are editing a group of fields, pressing Esc selects the first field. If you are editing the first field in the group, pressing Esc exits the entire group.
- If you are in Monitor Mode, pressing Esc opens the Alarm Summary screen. If the Alarm Summary screen is open, pressing Esc opens the Log Off window.

**Common Key Commands****Down Arrow**

The Down Arrow key selects the next item.

- If you are editing a group of fields, pressing Down Arrow selects the next field.
- If you are monitoring alarms, pressing Down Arrow selects the next item.

Up Arrow

The Up Arrow key selects the previous item.

- In editing modes, pressing Up Arrow selects the previous field.
- In Monitor Mode, pressing Down Arrow selects the previous

Menu List Box

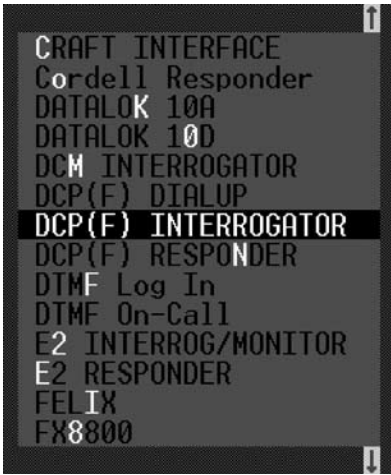


Fig. 4.2 - A typical list box

The Menu List Box is a list of default choices that is available in certain fields. The List Box displays the possible entries for the current field. Figure 4.2 is an example of a list of choices available in the Remote Parameters screen.

To select an entry from the List Box, use the Up Arrow and Down Arrow keys to move the highlight bar to the entry you want. Some entries have highlighted shortcut keys — press the highlighted key to select the entry (refer to Figure 4.2).

**Note:** The highlight bar does not wrap around the menu in the List Box.

Possible entries for fields also appear in the message line at the bottom of the screen — see Figure 4.3. To select an entry from the message line, press its shortcut key or enter the appropriate value.

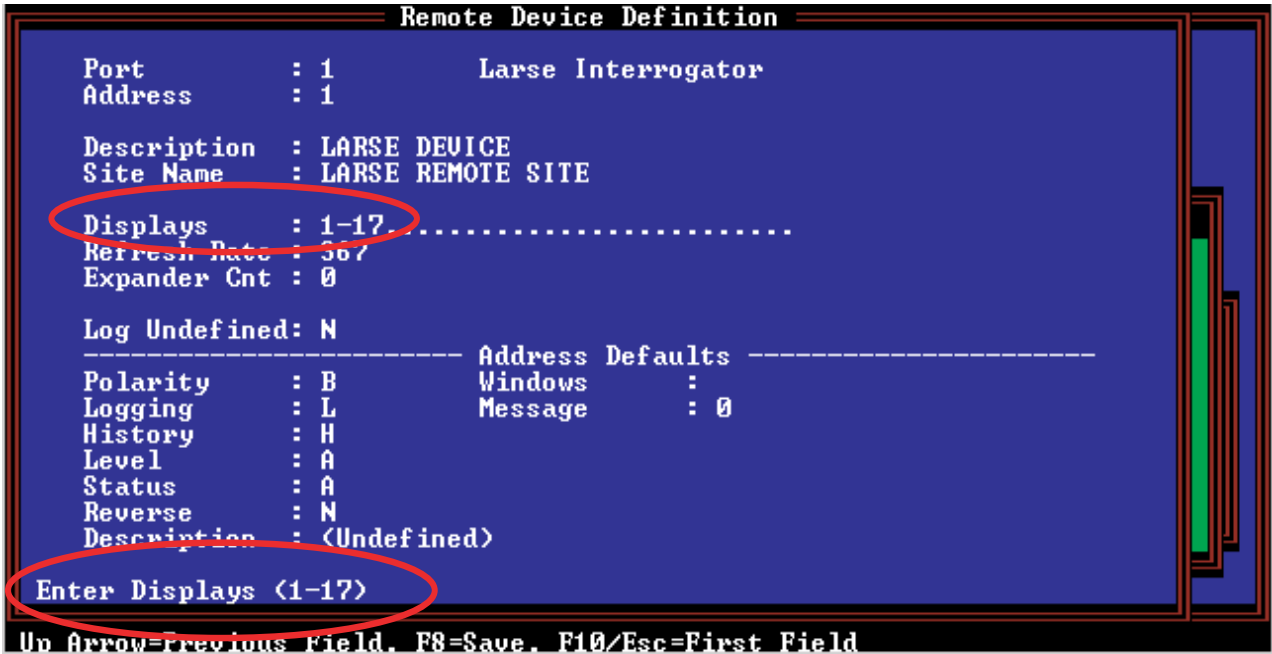


Fig. 4.3 - A typical list box

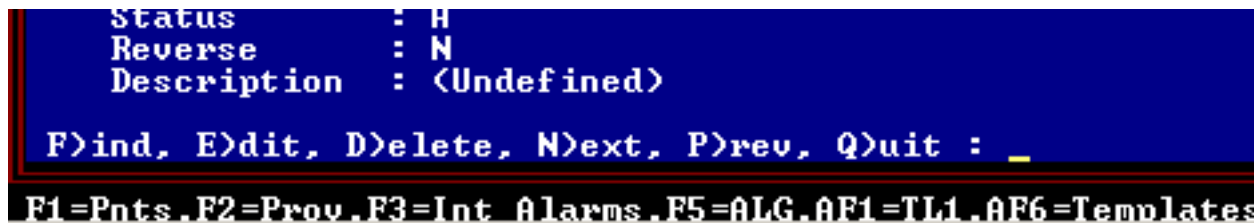


Fig. 4.4 - Hot Key Edit Commands

## Hot Key Edit Commands

In most cases you are first asked to enter an ID field, name, or value. The T/MonXM database management system will then determine whether that ID has been defined previously. If the ID is not found in the database, you will be asked whether you would like to add it. If you don't add it, then the ID and data for the next alphanumeric entry is displayed.

If the ID is found in the database, then the T/MonXM will retrieve the other data associated with the ID and display it on the screen. The following menu of commands will then appear at the bottom of the current window:

**F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit**

These commands are defined as follows:

### Delete

Deletes the current entry. (The current entry is the one that is displayed on the screen).

### Edit

Allows the user to make changes to the current entry.

### Find/(Create)

Searches the database for a specified entry. If the specified entry is in the database, then the other data associated with it is displayed.

The Find command can also be used to create a new entry in the database. To do this, try to Find an entry that is as yet undefined. When it is not found by the database management system, you will be asked if you want to create a new entry. Answer Yes to create the new entry.

### Next

Locates and displays the data associated with the next alphanumeric entry in the database.

### Prev

Locates and displays the data associated with the previous alphanumeric entry in the database.

### Quit

Leaves the current database and returns to the previous command level.

## Standard Database Field Editing

Fields are type checked. For example, if letters are entered in a numeric only field, the user is alerted to the error by a beep.

When editing all fields, the following keys are active:

**Table 4.B - Key commands available in all fields**

Function Key	Description
Backspace	Delete the character to the left of the cursor.
Ctrl-Z	Delete current line.
Ctrl-R	Restore field to its unedited state.
Enter	Enter text and moves cursor to the next field. Only text to the left of the cursor is entered.
Ctrl-H	Open Help screen.

**Table 4.C - Common key commands available in most fields**

Function Key	Description
Left Arrow	Move cursor left one space within field.
Right Arrow	Move cursor right one space within field.
Ctrl-Left Arrow	Move cursor left to the previous word.
Ctrl-Right Arrow	Move cursor right to the next word.
Ctrl-Home	Move cursor to beginning of the current field.
Ctrl-End	Move cursor to end of the current field.
Insert	Toggle insert and overwrite modes.
Del	Delete the character to the right of the cursor.
Ctrl-K or Alt-K	Delete from cursor position to end of line.
Ctrl-D or Tab	Open List Box — see Figure 4.2.

**This page intentionally left blank.**

## Section 5 - Configuring Remote Access

**\* Note:** New T/Mon and IAMs ship with unrestricted Remote Access factory installed. Older versions shipped with a minimum of 2 or no ports of remote access. To determine your capability, select **Diagnostics > Installable Modules > Installation Status**.

The Remote Access software module serves as a terminal server for hosting remote connections to T/MonXM. Remote Access must be set up in order to use the Web Browser Interface, T/RemoteW, T/AccessMW, T/Windows, or any terminal or computer not directly connected to the T/MonXM WorkStation or IAM-5.

The Remote Access software module must be installed before you can use the Remote Access functions of T/MonXM.\* Refer to the Software Module Installation section for installation procedures.

Selecting Remote Ports from the Parameters menu will allow you to select the remote terminals and define the parameters for Remote Access.

See Figure 5.1 for example on following page. The fields on the Remote Parameters screen are as follows:

### Port Usage

Valid port types are Remote Access and Halted. Use Halted (default) if no terminal is connected to the remote port.

### Serial Format (Physical ports only)

Baud rate, word length, parity, and stop bits settings. Default values are 38,400 baud, 8 bits, none, and 1.

### Terminal Type

(Note: XTND VT100 uses graphics characters.)

### Modem Present (Physical ports only)

The Remote Access field Modem Present should be set to “YES” if the remote will be accessed via modem. If no modem is used then set to “NO” (default).

**Table 5.A - T/MonXM or IAM terminal types.**

IAM or T/MonXM Workstation	
Physical	Virtual
T/Windows(ports 1-24)	T/Windows(ports 30-47)
T/Remote	T/RemoteW
T/RemoteW	VT100-24
WYSE	VT100-25
ADDS	HTTP
Xtnd VT100	
VT100-24	
VT100-25	

**Table 5.B - T/Mon NOC terminal types**

T/Mon NOC	
Physical	Virtual
T/Windows(ports 1-24)	Same as IAM-5 or T/MonXM Workstation

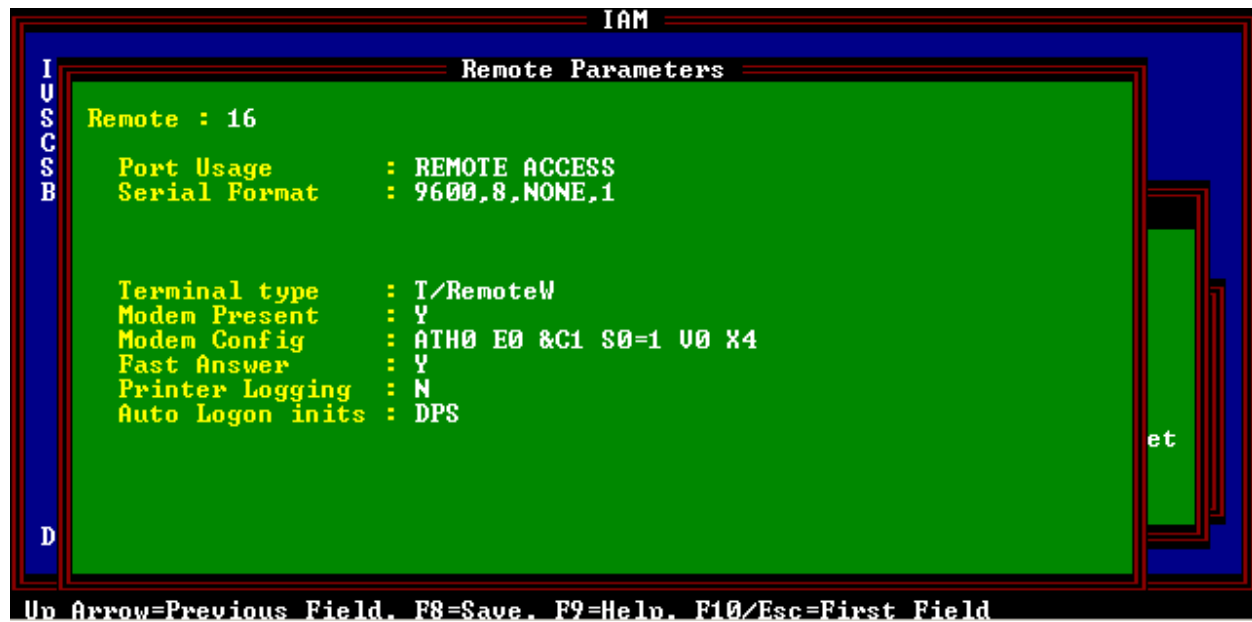


Fig. 5.1 - Remote Parameters screen.

**Modem Config**

T/Windows Internal Modem: ATH E0 IC1 S0=1 V0 X4

T/Windows w/ External Modem: ATH E0 IC1 S0=1 V0 X4  
\$MB9600

**Note:** for all others use default.

**Fast Answer**

If set to Yes (default), T/MonXM will answer dial up connections on the first ring. If set to no, T/MonXM will answer on the third ring.

**Printer Logging**

The Remote Access field Printer Logging allows the operator of a remote to toggle the Printer Logging feature On/Off on the remote printer. The default is "NO"

**Note:** Remote printer logging is only available when the remote is a T/Remote WorkStation.

**Auto Login Inits**

If you would like a user's initials to be automatically entered whenever Remote Access is used, enter the user's initials here. This field

**Table 5.C - Remote Access Parameter defaults**

Parameter	Default Value
Port Usage	Remote Access
Serial Format	3800, 8, None, 1
Terminal Type	T/Windows
Modem Present	No
Fast Answer	Yes
Printer Logging	No
Auto Logon Inits	Blank

is blank by default.

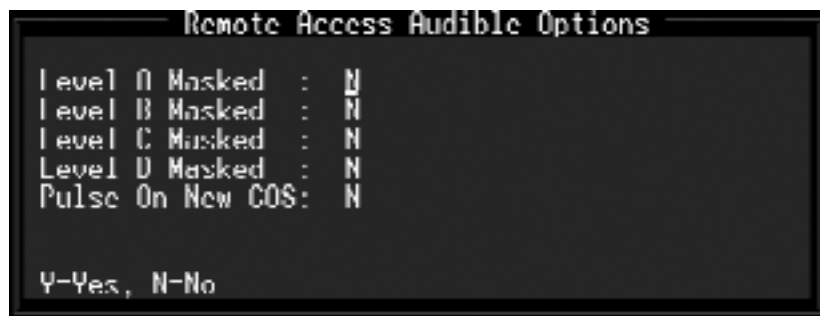
**Note:** Auto Login Inits enters only the initials; the user must still enter his or her password.

Refer to Table 5.D for key commands available in the Remote Parameters screen.

**Table 5.D - Key commands available in Remote Parameters screen**

Function Key	Description
F1	Opens Remote Access Audible Options screen for setting audible alert options.
F5	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
F10/Esc	Leaves the Remote Parameters Screen.

## Remote Access Audible Options



**Fig. 5.2 - Remote Access Audible Options screen**

The Remote Access Audible Options screen is accessed by pressing F1 in the Remote Access Remote Parameters screen.

The audible options provide support for terminals that will make an audible signal when an alarm event occurs. Audible signals can be set for all alarm severity levels and for change-of-state alarms.

The option fields in the Remote Access Audible Options screen are:

**Level A Masked**

No audible alarm will sound for Critical alarms.

**Level B Masked**

No audible alarm will sound for Major alarms.

**Level C Masked**

No audible alarm will sound for Minor alarms.

**Level D Masked**

No audible alarm will sound for Status alarms.

**Pulse on New COS**

An audible alarm will sound whenever a new change-of-state alarm occurs

By default, all fields in the Remote Access Audible Options screen are set to "No."



## Remote Access Server

Remote Access can be configured two ways:

1. Standard Remote Access, through a serial port connection (Ports 1-20) or a virtual LAN connection on ports 30-47.
2. Remote Access Server, through a virtual LAN port (Ports 30 and above).

Standard Remote Access requires a separate remote access port for every simultaneous viewing session. But with Remote Access Server, multiple users can share a pool of available TCP ports. As users log on they are automatically assigned a TCP connection from the pool by T/MonXM.

This section explains how to set up Remote Access Server via LAN, including setting up Remote Access pools.

### Step One

Your first step is to create a Remote Access Server on a LAN port

- a. Choose Master > Parameters > Remote Ports.
- b. Choose F)ind, and enter a port number between 30 and 47.
- c. Select Remote Access Server for the port usage, and enter an optional description in the Description field.
- d. A yellow prompt at the top of the screen will read "<No Data Connection.>."

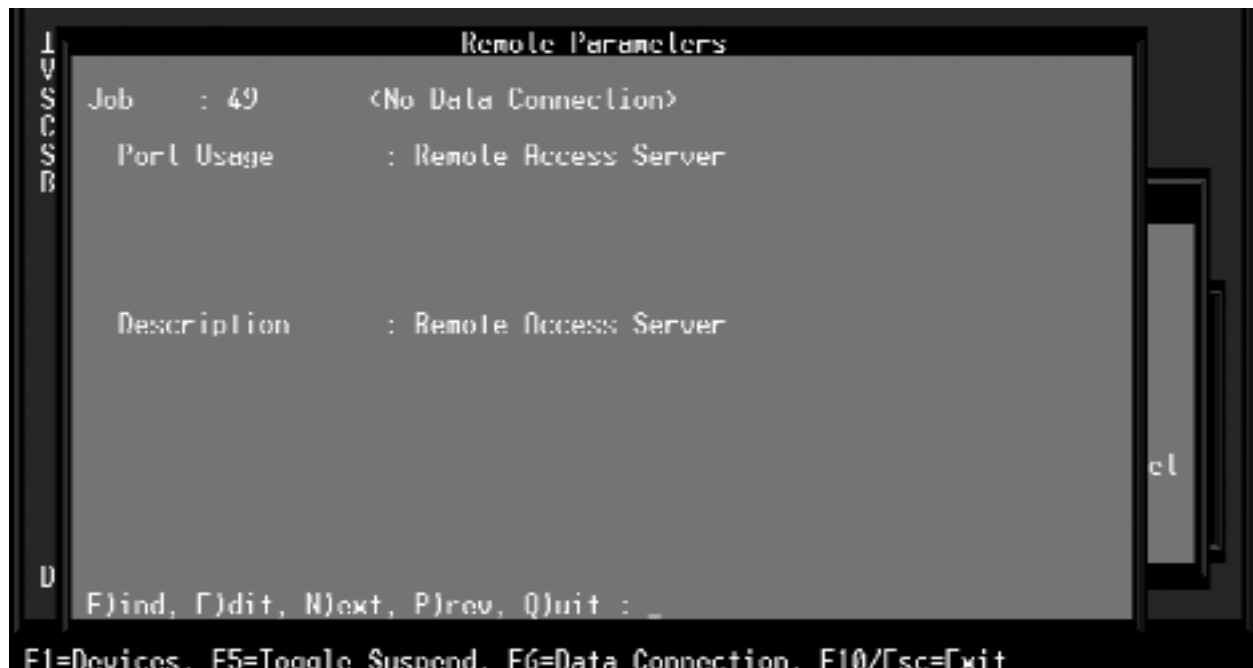


Fig. 5.3 - Remote Access Audible Options screen

## Step Two

**Note:** TCP Port 3000 is the DPS-suggested default.

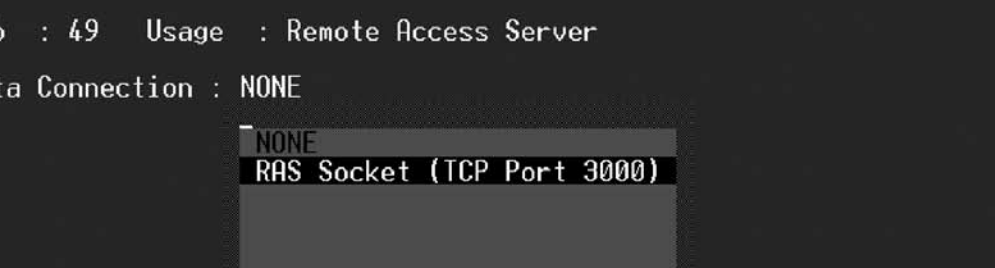
Create a data connection for the Remote Access Server using the following steps:

- Press F6 to open the Data Connection Assignment screen.
- Press F1 to open the Ethernet TCP Port Definition screen.
- Select an used entry and press Tab to open the list box for port type.
- Select TCP from the list box, and enter a port number and description. In the example shown in Figure 5.4, the port number is 3000 and the description is “RAS Socket.”
- Press F8 to save the configuration.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	TCP		3000	RAS Socket
2	.....			
3				

**Fig. 5.4 - TCP Port for Remote Access Server**

- f. At the Data Connection Assignment screen, select the TCP Port you just created. Any user that wants to connect to the T/MonXM system will use this port.



I  
V  
S  
C  
S  
B

Data Connection Assignment

Job : 49 Usage : Remote Access Server

Data Connection : NONE

NONE  
RAS Socket (TCP Port 3000)

D

[LIST BOX] Cursor Keys=Move Highlight Bar, <ENTER>=Select, F10/Esc=Abort

**Fig. 5.5 - Data connection for Remote Access Server**

## Step Three

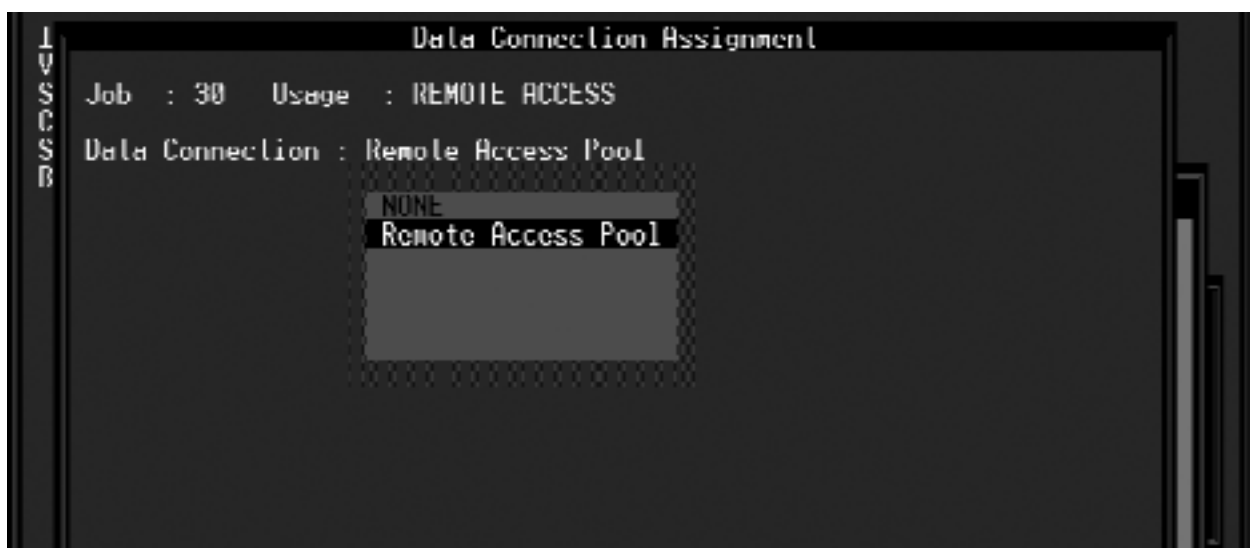
The next step is to set up a Remote Access job that will use Remote Access Server job is pool of data connections.

- Find a halted job number between 30 and 47. These are the only jobs to which you can assign a Remote Access connection.
- Select Remote Access as the port usage and enter all necessary information in the other fields.



**Fig. 5.6 - Select a remote port for the Remote Access Pool**

- Press F6 to open the Data Connection Assignment screen.
- Select Remote Access Pool for the data connection.
- Repeat Step 3a-3d to set up multiple Remote Access jobs.



**Fig. 5.7 - Select Remote Access Pool for the data connection**

## Step Four

Next, initialize the system, and enter Monitor Mode.

- a. Exit to the Master menu.
- b. Choose Initialize.
- c. Choose Monitor

## Step Five

The last step is to configure your T/Windows or T/RemoteW software to use the Remote Access Server.

- a. Run the T/Windows or T/RemoteW software.
- b. From the Settings menu, choose Communications to configure the T/Remote communication settings. To configure T/Windows communication settings choose Settings from the Option menu.
- c. Enter the IP address of the T/MonXM system and the TCP port assigned to the Remote Access Server in T/MonXM. (See Step 2d on page 5-5. Refer to Figure 5.8 for T/Remote and Figure 5.9 for T/Windows.
- d. Click OK to save your settings.

**T/RemoteW Communications Settings**

**Startup Connection Type**  
☐ COM ☐ Modem ☒ Network ☐ None

**COM Port**  
☒ COM 1 ☐ COM 2 ☐ COM 3 ☐ COM 4

**Baud**  
☐ 1200 ☐ 2400 ☐ 4800 ☒ 9600

**Parity**  
☐ Odd ☐ Even ☒ None

**Stop Bits**  
☒ One ☐ Two

**Data Bits**  
☐ Seven ☒ Eight

**Phone Number**

**Primary Network IP Address**

**Primary Network TCP Port**

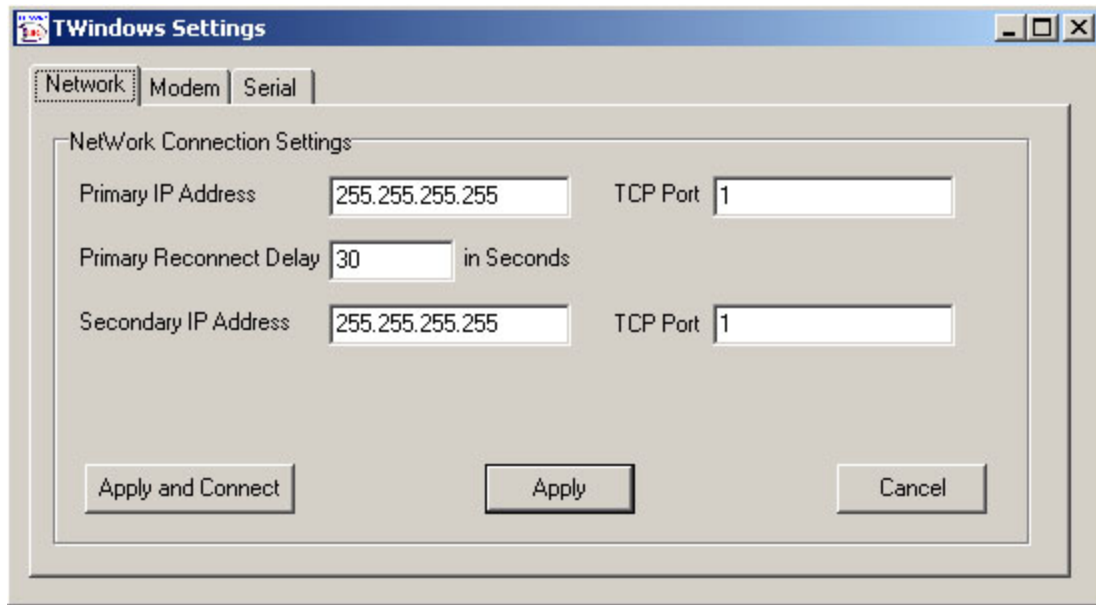
**Retry Interval (sec)**

**Secondary Network IP Address**

**Secondary Network TCP Port**

☒ OK ☐ Cancel

Fig. 5.8 - T/RemoteW communications settings



**Fig. 5.9 - T/Windows communications settings**

## Log On/Off

The procedures for logging on and off T/MonXM while using Remote Access are fundamentally identical to those described in Section 16-61, Exit Monitor Mode. Refer to this section of the manual for more information.

There are only a few differences in log on/log off procedures for Remote Access users:

Users connected to the T/MonXM system by Remote Access Server via LAN need log on and off only when starting the T/MonXM software or after exiting Monitor Mode by logging off.

Users who are connected by standard Remote Access via serial port connection must log on at the following times:

1. Whenever entering Monitor Mode.
2. After using CTRL-T to change terminal drivers — see following page.
3. Remote users who are connected by modem must log on each time a new modem connection is made.

You cannot log on with initials and a password already in use on the host or another remote.

When using a modem to connect to the T/MonXM system, register S7 on the modem must be set to 60 seconds. To set this register use the command "ATS7=60." This step is not required when using T/Windows or T/RemoteW.

When using a modem to connect to T/MonXM, a Disconnect option is available at log off.

## Changing Terminal Drivers

**Note:** Changing terminal drivers is available only when connected by modem using a dumb terminal.

When a remote terminal logs on to the T/MonXM host system by modem, a terminal driver selection menu will appear to allow the remote user to select a terminal driver. The remote terminal user may press CTRL "T" at any time after the log on password is entered to change terminal drivers. The Terminal Driver selection menu is shown below:

### Terminal Driver Query

Currently Affixed Driver == T/Remote Color Driver

1. Accept Current Driver
2. Affix T/Remote Color Driver
3. Affix WYSE 50 Driver
4. Affix ADDSVP (DPS TEST SET) Driver
5. Affix VT-100 Driver
6. Affix ENHANCED VT-100 Driver

To change terminal drivers follow these steps:

- A. Press CTRL T
- B. Enter the number of the terminal driver that you want from the Terminal Driver Selection menu.
- C. Enter "1" for Accept Current Driver
- D. Answer "Y" for the query LOGON WITH DRIVER == (DRIVER NAME) READY (Y/N)

## Remote Terminal Control Keys

Almost all commands that are available on the host T/MonXM system are available on the remote terminals. The procedure for selecting the command key is the only difference. The following key list is only for use with the remote terminals that are connected to the host T/MonXM system.

Once the remote user has chosen the proper terminal driver and has entered the correct security Initials and Password, the following optional features will be available:

### Help Screen

? Help Screen commands. This will bring up a window listing the various commands available at the current screen.

### Refreshing the Terminal Display

**CTRL-Z** Clears and refreshes the remote terminal screen. This should be performed when connecting or turning on a remote terminal after the host system is already operating or if a bad modem connection causes garbage (noise) to be displayed on the screen.

When selecting special keys such as Function, Alternate Function, and Control Function Keys, you must follow the following key-stroke rules shown on the following page.

## Selecting Special Keys on Remotes

**Note:** If you are using a T/Remote or T/Windows, normal function keys may be used as though they were the main T/MonXM system's function keys.

### Selecting Function Keys

Hold down the key and press F then the number of the function key desired. For example: To select Function 4 (F4), Press CTRL, F, and number 4.

### Selecting Alternate Function Keys

Hold down the key and press A then the number of the function key desired. For example: To select Alt Function 6 (Alt-F6), Press CTRL, A, and number 6.

### Selecting Control Function Keys

Hold down the key and press C then the number of the function key desired.

## Selecting Function Keys on Remotes

### Selecting Shift Function Keys

Hold down the key and press S then the number of the function key desired.

Function keys are available as well as the Special Keys operation. For more information refer to Monitor Mode, Section 16, of this manual.

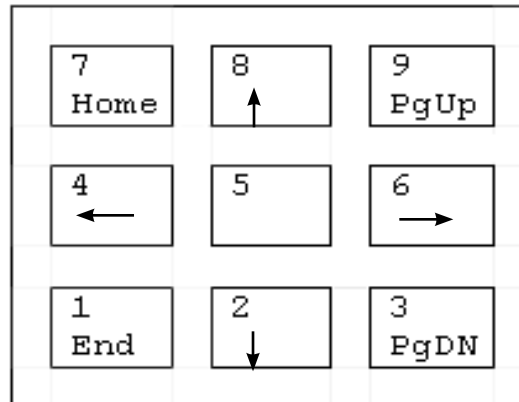
Table 5.E lists operations that do not work on remotes.

**Table 5.E - Functions that will not work on remotes**

Function Key	Description
Alt F8	Protocol Analyzer.
CTRL F4	Toggle relay card Sound Cut Off.

## Cursor Movement Keys

**Note:** If you are using a T/Remote WorkStation, normal function keys may be used as though they were the main T/MonXM system's function keys.



**Fig. 5.10 - Use the keypad to select cursor movement**

When selecting the cursor movement keys on a remote terminal, the following format must be used:

Hold down the key and press P then the corresponding number of cursor action desired (refer to the keypad diagram above).

**Example:**

<CTRL> P 7 Home. Moves to the first screen when viewing in monitor mode.

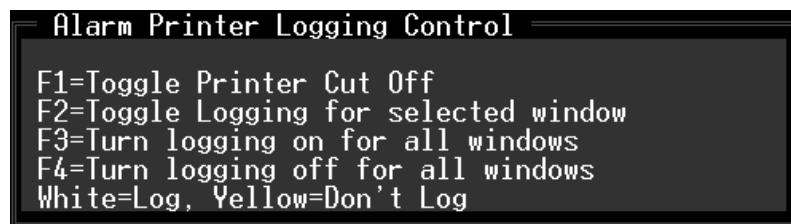
<CTRL> P 3 PgDn. Moves down one screen when viewing in monitor mode.

**Note:** If you are using an IBM-Type keyboard and want to use the numeric keypad, be sure the 570 key is ON.

## Alarm Printer Logging

The Alarm Printer Logging window will allow the remote user to log alarms to the printer. The user can enable Alarm Printer Logging by pressing CTRL F1 from the remote Monitor Mode screen. When the Alarm Printer Logging window appears (in the lower left corner of the screen) the user is requested to respond to printer logging questions.

The Alarm Printer Logging window appears as follows:



**Fig. 5.11 - Alarm Printer Logging window**

The Following operations may be initiated from the Alarm Printer Logging Control window:

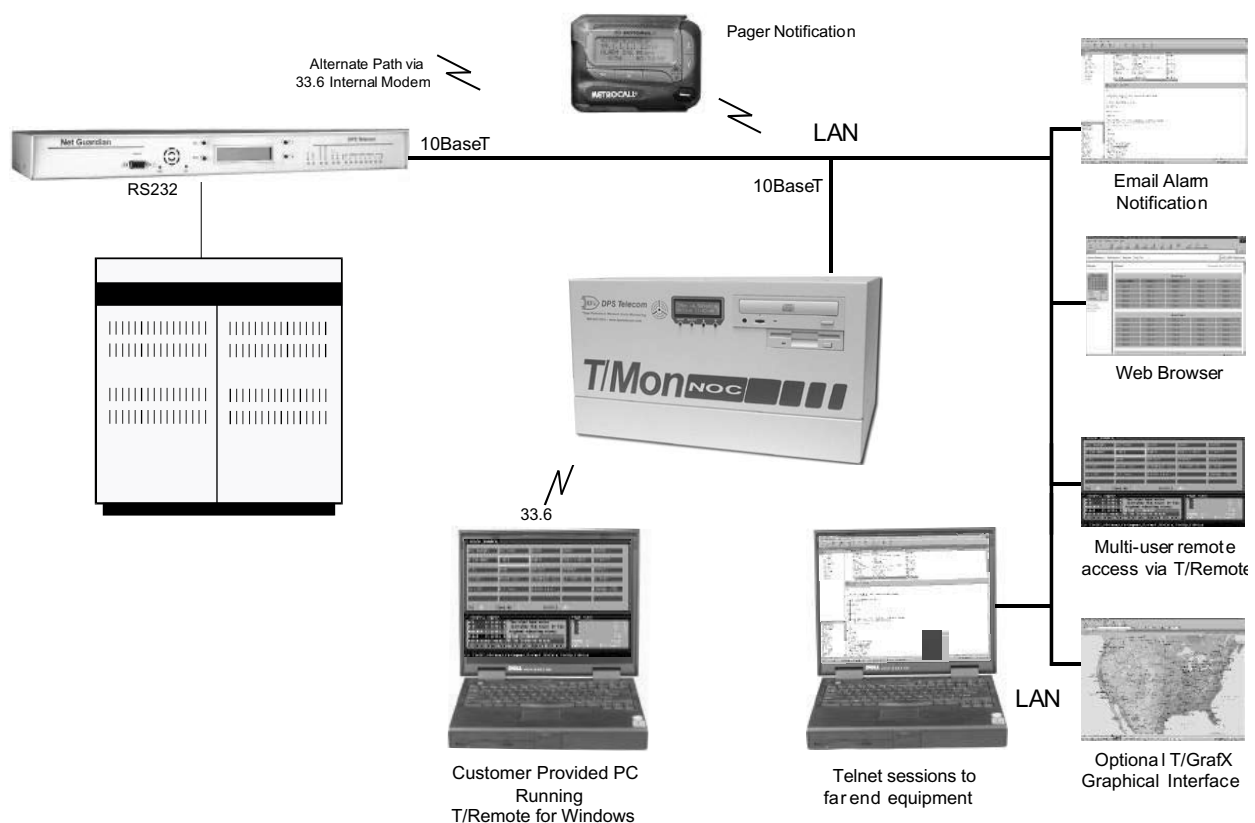
F1 Toggle Printer Cut Off.

When you are in this mode, F1 will toggle printer cut off. This action can be seen by the "P:X" symbols in the Page Index window.



- F2 Toggle Logging for selected window.  
Pressing F2 will toggle selected windows for printing.
- F3 Turn logging on for all windows.  
Pressing F3 turns printer logging On for All Windows.
- F4 Turn logging off for all windows.  
Pressing F4 turns printer logging Off for All Windows.

**Note:** Printer Logging ON is indicated by White Text in the chosen alarm windows. Printer Logging OFF is indicated by Yellow Text in the chosen alarm windows.



**Fig. 5.12 - LAN Network connections example.**

## Remote Users over LAN

The diagram above shows an example of a LAN network with remote users using T/Remote, HTTP, E-mail, T/GrafX, etc. Each of these are described in the following sections of the manual:

LAN-based remotes - Section M1-25.

E-mail notification of alarms - Section 8

Web Browser (HTTP) - Section 17, Web Browser Interface

T/Remote for Windows™ - Section 5, Remote Access (this chapter)

# Section 6 - Define Windows

## Windows Screen

### Define Windows First

- Suggested order of Database Definition:
  - Windows
  - Data Ports\*
  - Addresses\*
  - Alarm Points\*
  - Description\*
  - Control Points
  - Derived Alarms/Controls
  - System Users
- \*Parameters Menu

The Master Menu > Files Maintenance Menu > Windows command organizes alarms into groups called windows. A window is a defined list of alarms that is displayed as a unit. Windows can be defined by geographic area, alarm priority, equipment type, security restrictions, Site 1, or other criteria.

An alarm point can belong to several different windows, defined in different ways, and be displayed in every window to which it belongs. For example, a fire in a generator room in Seattle would be displayed in the All Alarms window, the Critical window, the Fire window, the Power window, and in a Site Alarm window for that location.

Windows should be one of the first database items to be defined. They should be defined before the alarm points. Careful consideration should be given to windows strategy, because a small change to your window definition could entail extensive point modification which may take hours, depending on the complexity of your network.

DPS recommends the following approach to window assignment: Devote the first page of the alarm summary (windows 1 through 30) to severity, type and equipment alarms. Start Site alarms on page 2 (window 31). This will likely leave unused windows on page 1 for future assignment to new equipment types. In addition, all type and equipment alarms will appear on the same page, giving operators an overall picture of system status. This approach is illustrated in the example windows shown in Figure 6.1 and Figure 6.3.

Windows can also be used to conveniently sort alarms for reports.



Fig. 6.1 - Page 1 in Monitor Mode showing Severity and Equipment Alarms

If you regularly need reports on a diverse group of alarms that don't fit into a pre-existing category, they can be assigned to a special reports window and be automatically collected for you.

Severity Windows are usually classified as follows:

- Critical (Highest in severity)
- Major
- Minor
- Status (Lowest in severity)

Type/Equipment Windows Might Include:

- Fire
- Alarm Forwarding
- Site Controls
- Building Status Unit (BSU)
- Security Access to system
- Printer Logging
- History Reports
- Off Line
- Device Fail
- Microwave
- Fiber
- Radio
- Lights
- Door
- Power



Fig. 6.2 - Page 2 in Monitor Mode showing Site Alarms

# Window Definition

90 Alarm Windows is Standard

T/MonXM comes standard with 90 alarm windows. The first window always lists All Alarms. This leaves 89 user-definable windows. Alarm Windows Modules are available from DPS which provide an additional 90, 240 or 690 windows to give a total of 180, 330 and 720 windows, respectively (179, 329 and 719 available)



Fig. 6.3 - The window Definition screen

Window 1 is always the All Alarms window

The All Alarms Window (#1) can be renamed, but it will still show all alarms.

Window 1 is always the All Alarms window. All alarm information will be automatically sent to this window. If an alarm was assigned to another window, then it will be sent to both the All Alarms window and the other windows as well.

To access the Window Definition screen, select Windows from the File Maintenance menu and press Enter. This screen allows you to assign individual names and descriptions to each of the alarm grouping windows. For example, if a group of alarms from fiber optic equipment were assigned to Window 6, you might want to rename Window 6 to "FIBER."

The window data is recorded to disk only when F8 is pressed. After F8 is pressed, the program will go back to the menu.

The Alarm Window Definition screen entries are explained in Table 6.A and Table 6.B.

**Table 6.A - Fields in the Window Definition screen**

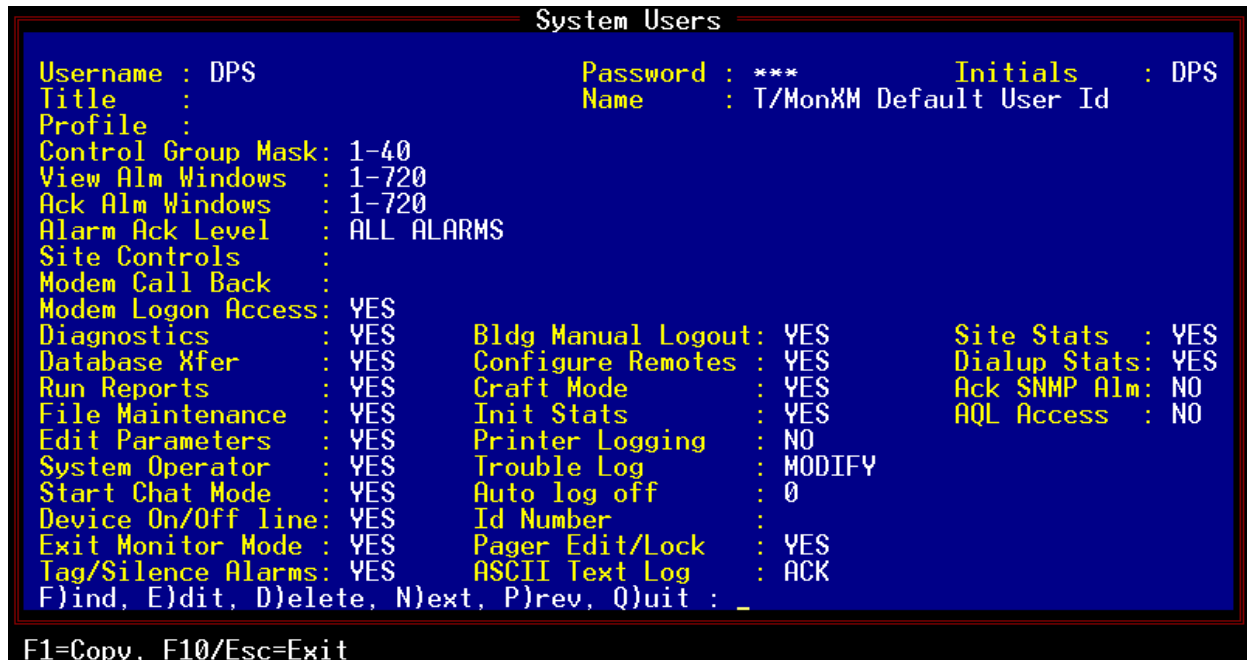
Field	Description
Window	Number of the window being defined. A number from 1 to the total number of windows in your system.
Name	Enter the name (up to 14 alphanumeric characters) for this window. This name will appear in the Alarm Summary Screen and other places in T/MonXM.
Description	When the cursor is moved to the Description field the name will appear in the field. This is the default. Press Enter to accept the default or enter a description up to 30 characters long. This description will appear in the title bar of the COS/LIVE window.

**Table 6.B - Key commands available in the Window Definition screen**

Function Key	Description
F1	Move to a specific window to edit. T/MonXM will prompt for window number.
F2	Activates the BSU Definition Screen to define the relay addresses where T/MonXM will direct alarm status.
F3	Deletes the current window entry. Window 1 can be re-named, but not deleted.
F4	Takes you to the Site Controls Category Definition screen.
F8	Saves the Window Definition database and returns to the File Maintenance menu.
F10/Esc	Returns to the File Maintenance screen without saving any changes.

**Note:** All undefined windows will have their window number displayed in the alarm summary screen to aid with window assignment. Once the window definition is complete, these place holders may be removed by entering a space into the name field.

## Section 7 - Managing System Users



**Fig. 7.1 - Make security restriction assignments at the system users screen**

The System Users screen has been redesigned for better function and clarity.

Users can now log on with usernames instead of initials. New long format users name can be 3–20 characters long. Passwords can now be 3–16 characters long

Please note users can now be forced to update their password upon login. Press F2 from the System Users Window.

**Note:** Some security fields correspond to specific Software Modules and may not appear unless that module is present on your system.

Preventing unauthorized access to your system is very important for maintaining system security. Therefore, system security access controls are included as part of T/MonXM. System security access privileges can be accessed by choosing the System Users option from the File Maintenance menu (see Figure 7.1).

System users are designed to restrict access of the system to authorized users only. The following section explains the databasing of system users. Security rights are defined for each user to set the user's level of authorization. System profiles allow users to be put into groups by assigning multiple users to a single profile. The security rights for each user assigned to a profile are identical between users and to that of the profile itself. This allows the profile to be changed in a single spot and the changes to automatically propagate down to all of the users assigned to it.

Once a user has been assigned to a profile the user's security settings will turn green to indicate that they are locked to that of the profile. The user's security settings cannot be edited while they are green to ensure that all users assigned to a profile have identical settings. If a variation of an existing profile is needed then a new profile should be created to address that need.

It is not necessary for each user to be assigned to a profile. If security rights for a user are unique to that user then there is no reason to create a new profile. In this case the user would just leave

the profile field blank. It is important to note that once a user is assigned to a profile the security settings for that user are permanently overwritten with that of the profile. This means that if a user is assigned and then unassigned from a profile, the original security settings for the user will not be restored after the profile is unassigned. The user would still possess the security settings of the profile, even after it has been unassigned, but would no longer inherit changes to the profile. At this point the user's settings will be white and can be edited.

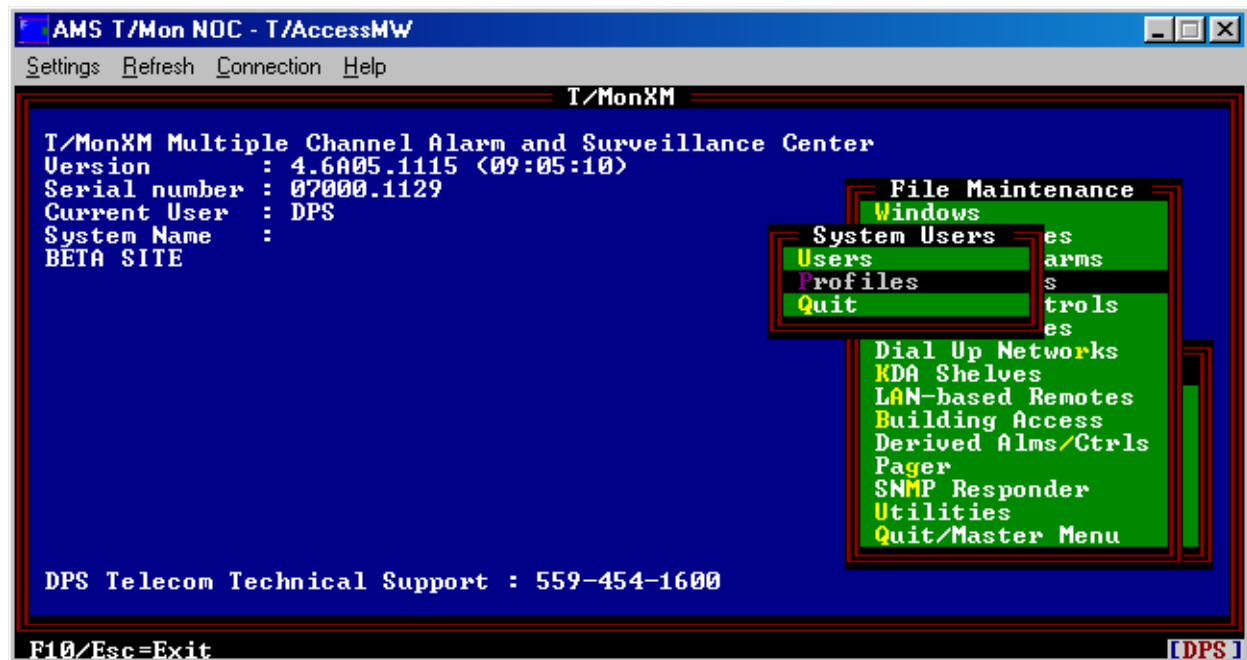


Fig. 7.2 - In the System Users menu you can create Users and Profiles

You can define security access levels for each user and also define the areas that each user is allowed to access. In this way, you are able to control who is monitoring and working in each area and can limit the actions a user can perform.

### System User Access Overview

Many T/MonXM users have found it helpful to establish an access policy much like the following:

1. System Administrator = Full access.
2. Database administrators = Full access to system, except for system administrator features.
3. General Users = Limited to Monitor Mode access to view and acknowledge windows as needed.
4. View-Only Users = Access to view, but not acknowledge, alarms to a specified window.

To define a new user profile, type P from the System Users screen and begin entering new user information. The system will ask for a user name, if the user name is unique, the system requests acknowledgement to add the new user. Once defined, a user profile may be

## Define System Users

Fields will appear on the System Users screen as software modules are installed.

**Note:** For security reasons, after creating your own user database you should delete the DPS default entry from the database.

**Table 7.A - Fields in the System Users screen**

Field	Description
Username	The user's name for T/Mon and Remote Access logons. Must be 3–20 characters long.
Initials	You must enter 3 initials.
Name	The user's name — 3 to 30 characters long.
Password	<p>The user's password. Password must be from 3 to 16 characters long  <b>Suggestion:</b> Avoid initials or names of family members or pets.            Note: If Strict Passwords setting under Miscellaneous Parameters is enabled, the system user password field will enforce a strict password policy.            The following rules will be enforced:</p> <ol style="list-style-type: none"> <li>1. Passwords must be at least 3-16 characters.</li> <li>2. Passwords must not contain the same consecutive character (two of the same characters in a row.)</li> <li>3. Three of the following character classes must be used:               <ul style="list-style-type: none"> <li>• Uppercase alphabetic (A, B, C...)</li> <li>• Lowercase alphabetic (a, b, c...)</li> <li>• Numbers (0-9)</li> <li>• Punctuation (!, @, #...)</li> </ul> </li> <li>4. Password cannot be the same as any of the last four passwords.</li> </ol>
Title	The user's title (e.g., supervisor, engineer). This field is optional. Use up to 20 characters.
Profile	The system profile to reference for security settings. Setting this field to a profile will overwrite the system user with the configuration of the system profile. If the system profile is changed, then the user configuration will be changed automatically. Note: This field is optional, You will be prompted to overwrite the current user rights, Press "Y" to accept.
Control Group Mask	The Labeled Control Categories the user can access. Range is 1-40.*
View Alm Windows	<p>The Alarm Windows the user can view but not necessarily acknowledge. Valid view windows with standard features are 1-90. More view windows are available when additional Alarm Windows software modules are installed. Valid range is 1-720 (or maximum number of installed windows).* System users able to view Window 1 can view all the alarm in T/Mon.</p> <p><b>Note:</b> If additional window software modules are subsequently added, you may need to update your security files.</p>
Ack Alm Windows	<p>The alarm windows in which the user may acknowledge alarms. Valid range is 1-720 (or maximum number of installed windows).*</p> <p><b>Note:</b> Ack Alm windows must be a subset of the View Alm windows.</p>
Alarm Ack Level	<p>The authority level of the user to acknowledge alarms. Valid settings are:</p> <p><b>None:</b> Can't acknowledge alarms.</p> <p><b>Single:</b> Acknowledge only a single alarm at a time.</p> <p><b>All Alarms:</b> Acknowledge alarms one-at-a-time or all at once (Alt F4).</p>

\* These fields are range variables. Numbers entered must be in some valid range. Example 1-3, 7.



**Table 7.A - Fields in the the System Users screen (continued)**

Field	Description
Site Controls	Windows that the user may issue site controls from. Valid range is 1-720 (or maximum number of installed windows).* Note: Must be a subset of view alarm windows.
Modem Call Back	Allows modem access via number listed. User must identify and logon. T/Mon calls back to the specified number. This enables even greater security. Access requires modem and password at pre-designated location. Up to 30 characters.
Modem Logon Access	Allows access to the system using a modem. This permits you to restrict access so a user can only use dedicated terminals. <b>Hint:</b> You can give a user two codes— one is for local use and another for dial-up access with limited capabilities.
Diagnostics	Allows access to the Main Menu and Diagnostics Menu when offline. Y (Yes) or N (No).
Database Xfer	Allows access to Transfer the Database to another T/MonXM when multiple masters are in the system. Y (Yes) or N (No). (Also allows user to read/write via FTP sessions)
Run Reports	Allows access to the Report Generator. Y (Yes) or N (No).
File Maintenance	Allows access to the File Maintenance menu. Y (Yes) or N (No).
Edit Parameters	Allows access to the Parameters menu. Y (Yes) or N (No).
System Operator	Allows access to the System User database. Y (Yes) or N (No).
Start Chat Mode	Allows access to Chat Mode and lets a user chat with others or the host computer. Y (Yes) or N (No).
Device On/Off Line	Allows access to take devices on and off line. Y (Yes) or N (No).
Exit Monitor Mode	Lets the user exit Monitor Mode. Y (Yes) or N (No).
Tag/Silence Alarms	Lets the user tag or silence alarms in Monitor Mode. "Silence" has a time limit that is defined in Monitor mode. Y (Yes) or N (No).
Bldg Manual Logout	Determines whether the operator is allowed to manually log persons out of a Building Access site. Y (Yes) or N (No).
Configure Remotes	Allows downloading configurations to remotes. Y (Yes) or N (No).
Craft Mode	Allows access to Craft Interface Mode which lets you talk to an ASCII device connected to T/MonXM. Y (Yes), N (No) or L (Log - captures all data on the craft port to a file on the hard drive. The files will be named cl-XXX.rep, where XXX=the user initials)
Init Stats	Allows the user to initialize port statistics. Y (Yes) or N (No).
Printer Logging	Allows the user to toggle printer logging. Y (Yes), N (No) Auto On permits the system to automatically begin logging after users log onto the system. Refer to the Printer Logging Section for more information.
Trouble Log	Valid settings are: None: Trouble Logs cannot be viewed or edited. View Only: Trouble Logs may be viewed but not edited. Modify: Trouble logs can be viewed or edited.
Auto log off	The number of minutes of no keyboard activity before the user will be automatically logged off. Valid values are 5-200. Enter 0 to disable. This protects your log-on code.
Id Number	Number used to log in at remote site. Up to 8 digits. Valid settings are: DTMF; 001-899; BAU: 001 - 89999999; Blank: None <b>Note:</b> T/Mon 4.2 and later version users can define Building Access System user profiles in the Main Menu > Files > Building Access > BAS Profiles.
Pager Edit/Lock	Setup pager schedules and set pager locks. Y (Yes) or N (No).

\* These fields are range variables. Numbers entered must be in some valid range. Example 1-3, 7.

## **7-4** Section Seven - Managing System Users

Table 7.A - Fields in the System Users screen (continued)

Field	Description
ASCII Text Log	Allows viewing or acknowledging ASCII text alarms. Valid settings are: <b>None:</b> ASCII text cannot be viewed or acknowledged. <b>View:</b> ASCII text may be viewed but not acknowledged. <b>Ack:</b> ASCII text can be viewed or acknowledged individually. <b>Ack All:</b> All ASCII text messages can be viewed or acknowledged.
Site Stats	Yes or No. Allows or prevents access to Site Statistics screens.
Dialup Stats	Yes or No. Allows or prevents access to Dial Up Site Monitor Screens.
Ack SNMP Alm	Yes or No. Allows manual acknowledging of an SNMP alarm in Monitor Mode while viewing the Standing List.
AQL Access	Yes or No. Allows access to view alarm windows through the AQL job.

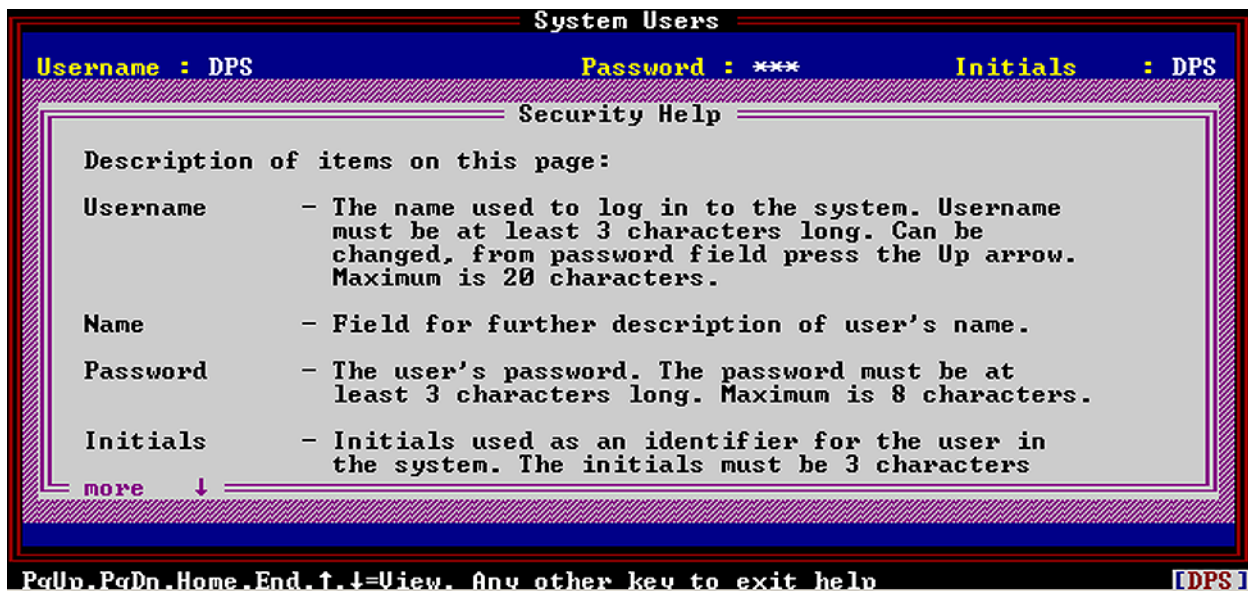


Fig. 7.3 - Detailed definitions for each field can be found in the Security Help screen

## Security Help Screen

You can always find detailed definitions for each field in Security Help. To go to Security Help, press F9 in the File Maintenance > System Users > press E (Edit screen).

If you already have a Systems Users database and wish to keep it, your current database will transfer when you load the newer version of T/MonXM software.

You can edit user names and passwords from old databases by choosing Edit in the new version software. If you wish to edit your current username, you will have to create a new one and log on again.

If a user loses his password, you will not be able to retrieve it, but a user with System Operator privileges can access the Systems Users screen and change the password to a new password.



Fig. 7.4 - Copy attributes from existing users to a new user

## Copy System User Attributes

The Copy User command copies user permissions and attributes from an existing user to a new user. This makes it easier to access. To copy the current System User's attributes, press F1 from the System Users screen and enter the new user name and initials.

All other settings, including password will be copied to the new user.

The copy functionality (F1) is supported by both the user and profile editor. It is important to note that users can only copy users and profiles can only copy profiles.

# Section 8 - Configure Pager and Email Alarm Notification

---

## Introduction

**Note:** Text/Messages can still be used to define paging in version 3.5 and later — see Appendix K.

View the Pager Status in Monitor Mode — see Section 16 (Monitor Mode) for more information.

With T/Mon's pager support you can define pager carriers (technicians to be paged when reportable alarms occur), pager phone numbers, pager carrier initials, and much more.

Weekly Schedules can be created to dial pagers when an alarm is received. Special changes for holidays, and other exceptions can be made at the Schedule Exceptions screen — a 24-hour schedule that overrides the Weekly Schedule. An additional schedule override can be performed by using the Lock function while in the Monitor mode. A page can also be initiated manually while in the Monitor Mode — see section 16-60 (Pager Status in Monitor Mode).

T/Mon can also be set up to send an email notification of alarm events. Email notification is integrated with the paging system. An email address can be defined for each pager carrier. When the system needs to send a notification to a pager carrier, it will send an email if an email address is defined for that carrier.

In order to use email notification, the system will need to be able to connect to a mail server via LAN. It cannot connect via dial-up, though it can co-exist with paging via dial-up. The system uses SMTP to send messages and POP3 to retrieve them. An email account for the system will need to be setup on your mail server to receive email from T/Mon. The configuration procedure described in this section only sets up the email resource.

T/Mon can be setup to send SNPP (Simple Network Pager Protocol) pages for alarm events. SNPP paging is integrated with the paging system. An SNPP pager carrier must be defined for each pager. In order to send SNPP pages the system's SNPP Client job will need to be able to connect to an SNPP Server via the LAN. The SNPP Server must be a service provider for the pager used. Typically services providers support only their own pagers. The system cannot connect via dial-up, though it can co-exist with paging via dialup and email.

### **Pager and Email Alarm Notification Setup Overview**

The following is an overview of setup procedures. For more detailed instructions on defining each section, see the corresponding sections on the following pages.

1. Setup a pager remote port job in the Main menu > Files Maintenance > Remote Ports option.
2. If you are using email notification, as well, then setup a virtual port job for email notification in the Main menu > Files Maintenance > Remote Ports option.
3. Return to the Files Maintenance menu and select the Pagers option.
4. Select each option and fill in the fields with the appropriate information. Pager Carriers should be defined first.
5. You may also select which system users have system security access to set up pager schedules and pager locks in the Main menu > Files Maintenance > System Users option. See Section 7 (System Users) for more information on defining system users options.

A drop down list of pager carriers has been added. Access this drop down list by pressing TAB on the pager group definition screen.

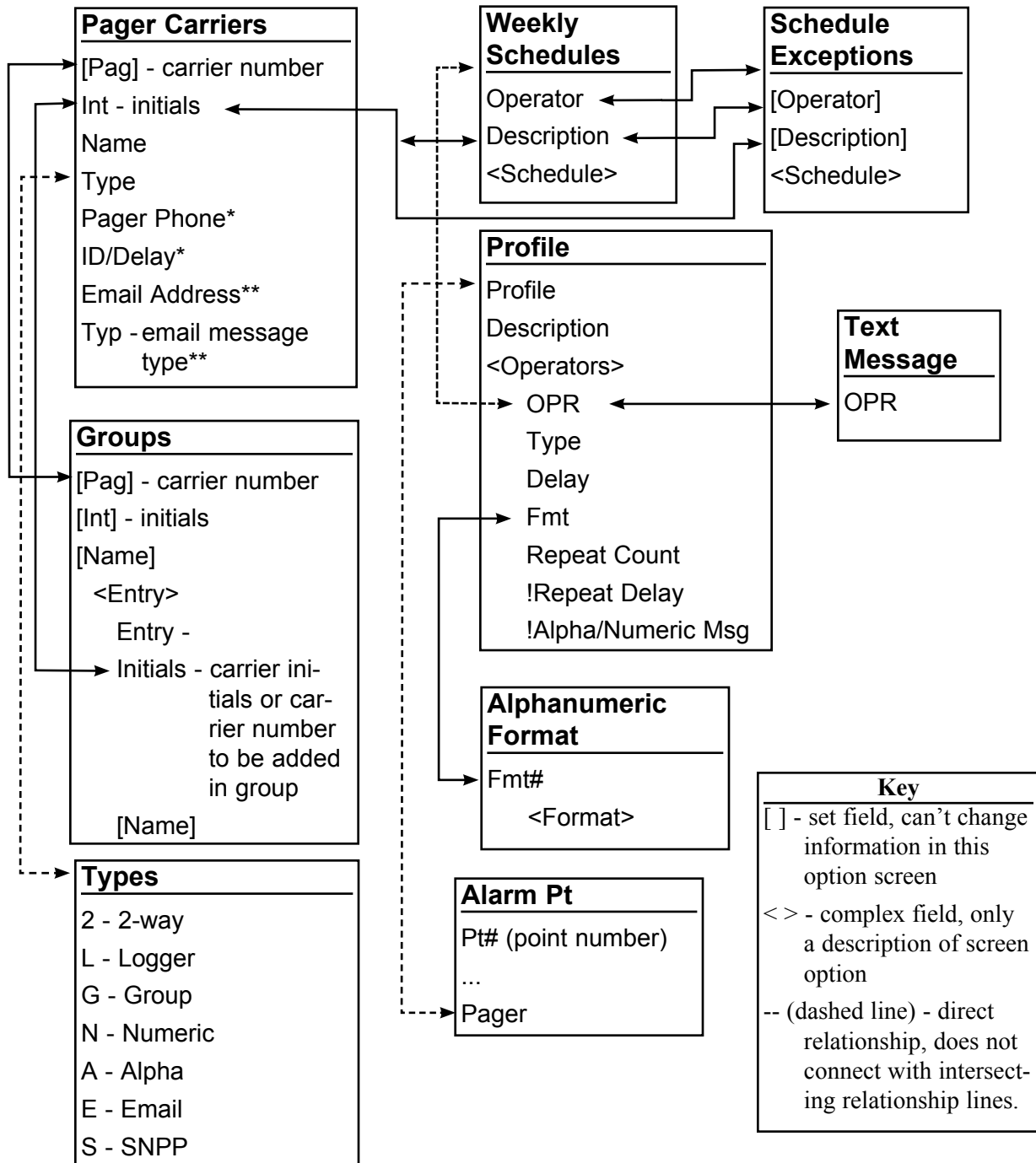


Fig. 8.1 Pager and email database relations

\* Field appears if either Numeric or Alpha is selected.

\*\* Field appears only if Email is selected.

**Note:** Pager Phone and ID/Delay fields will not appear if Email is selected.

### Pager and Email Field Options Relationships

Figure 8.1 illustrates the relationships between some of the fields in the Files Maintenance > Pager submenu options. Some of these fields are dependent upon one another. For example, the Pager Phone, ID/Delay, Email Addresses, and Typ fields appear according to the selection you make in the Type field — see side note. The initials you define in the Pager Carriers screen also carries over to the Schedule and Exemptions screens, and can only be altered in the Pager Carriers screen. Other relationships are shown in the illustration above.



Fig. 8.2 - Main menu > Files Maintenance menu > Pager submenu

In T/MonXM 3.0 and later, you may assign up to 999 operators.

Access to pager scheduling and the lock function are under system security protection.

**Pager Remote Port**  
Parameters are defined in the Parameters > Remote Ports menu.

The following section is an overview of the options available in the Parameters > Pager submenu and their functions. For detailed information and instructions on defining a Pager submenu option, see the appropriate sections that follow.

#### System Security

Selecting the System Users option from the File Maintenance menu allows you to define which system users have system security access to set up pager schedules and pager locks. This is accomplished by the setting of the Pager Edit/Lock field for each user who is to have access.

#### Parameters

Define the Pager Queue Max and enable Smart Paging in this screen option. Smart paging will only page on Un-ack COS and when current alarm status matches pager Alarm status.

#### Pager Profiles

Pager profiles can be configured to indicate a page notification and to which operator (schedule) it is to be directed. This method allows many profiles to be defined. The pager profiles are later assigned to each alarm point in the Point Definition screens.

#### Pager Scheduling

Pager scheduling (including weekly schedules and schedule exceptions) is done under the Pager selection in the files menu, which is described in this section. Alphanumeric formats are also defined under this menu.

An Operator is a schedule of pager carriers who are to be called during a particular hour.

Pager Carriers on call can be changed from hour-to-hour, per the operators schedule.

## Operators

Pager scheduling uses a function referred to as operators to aid in defining the pagers to be called at a particular time. The term “operator” is not to be confused with the term “pager carrier.” The operator is a schedule in T/MonXM’s database that performs the same duty as a human operator issuing pages according to a schedule. Up to 999 Operators may be defined, so that as many as 999 different pagers will be on call at a time. Each one may be called for a different type of alarm.

## Pager Carrier

The Pager Carrier is the person who has a certain pager that is accessed by dialing a defined phone number. The Pager Carrier is defined in the Pager Carrier screen and is thereafter identified by initials or number. Up to 999 Pager Carriers can be defined. Email address information for email notification is also entered in the Pager Carrier screen.

## Pager Scheduling

Selecting Pager from the File Maintenance menu will allow you to access the Pager menu. The pager menu items are: Pager Carriers, Weekly Schedules, Schedule Exceptions, Alphanumeric, Group and Quit. Each of these menu items will be used in turn during the following procedure.

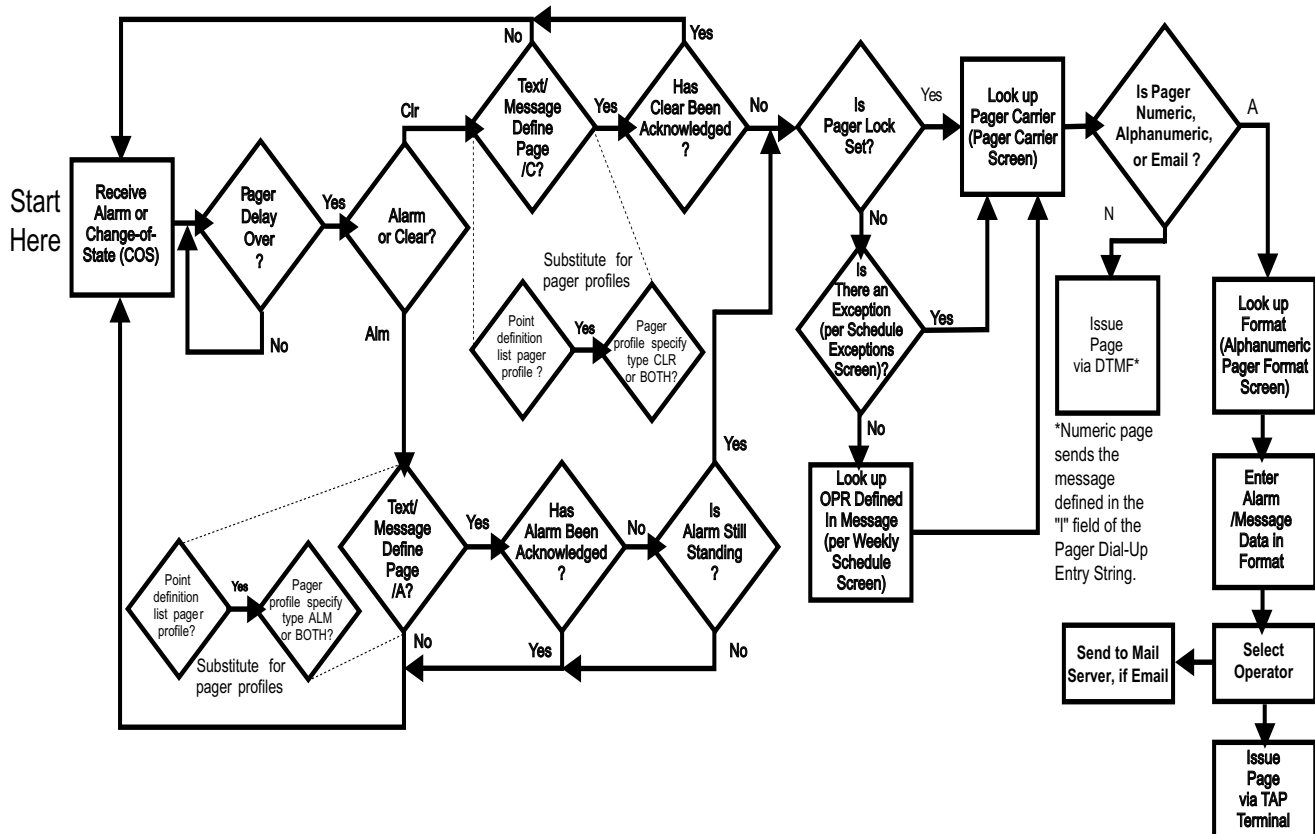


Fig. 8.3 - Pager and email function flow diagram



## Pager Alarm Notification Port Setup

**Note:** go to section 8.4 if you only need to setup an email notification port job.

With a pager port, T/Mon can send a message to a pager when there is a reportable alarm event. Use the following steps to setup your port parameters:

1. Go to Main menu > Parameters > Remote Ports.
2. Press F (Find) or N(Next) to find the next available port.
3. Press the Tab and select Pager from the port usage sub-menu, then press Enter.
4. Fill in the rest of the fields — see Table 8.A for field descriptions.



**Fig. 8.4 - Pager remote parameters settings**

**Table 8.A - Fields in the Pager remote parameters screen**

Field	Description
Port Usage	The Port Usage field shows the selected port usage option. Press the Tab key to open the submenu, and select Pager.
Serial Format	Baud rate, parity, word length, and stop bits settings that T/MonXM will use to communicate with the equipment.
Pager Speaker	Allows you to set the computer's speaker so you can hear the dialing tones. "Y" to turn on, "N" to turn off. [N]
Modem Config	30 character configuration string. (Normally blank) T/MonXM uses the following modem initialization string: AT M0 Q0 X4 if the Pager Speaker is off AT M2 Q0 X4 if the Pager Speaker is on It is not necessary to make an entry in this field unless you need additional characters to implement some feature or to use an external modem. See Appendix J or consult your pager manufacturer's instructions for details.

**Note:** Table 8.A continues on following page.

**Table 8.A - Fields in the Pager remote parameters screen continued**

Field	Description
Multi Alpha Pages	Send multiple Alpha pages per call. If your paging service allows you to issue multiple messages with a single call, enabling this feature will dramatically improve paging through-put. The actual pages will be issued separately by the pager service. When this feature is used be sure that phone numbers on the Pager Carrier screen for carriers using the same terminal are typed in IDENTICALLY as this is how the software determines whether a given message is for the same terminal. Y = Multiple messages per call N = One message per call.
Check Back Delay	Time to wait before checking for a response from a 2-Way pager (2 to 60 min.) [5]
Check Back Times	Maximum number of times to check for a response from a 2-Way pager (1 to 20 times). [2]
Direct connection	Use to set port for either direct or modem connection to the paging terminal. Y=Direct connection. N = Modem connection.

**\*Note:** For a 2-way pager, Parity = None, Word Length = 8 and Stop Bits = 1.

**Table 8.B - Key commands available in the Remote Parameters screen, pager usage**

Function Key	Description
F5	Toggle suspension. Allows temporary suspension of defined port. Available only when cursor is on prompt line at bottom of window.
Up Arrow	Move to the previous field.
F8	Save
F9	Help online
F10/Esc	Exit Ethernet TCP Port Definition screen without saving changes.
Tab	List port usages (while cursor is in the Port Usage field).

**Note:** The Pager remote port usage only assigns the pager port. Refer to Files Maintenance > Pager Profiles (section 8-24), for full details on how to implement a successful paging strategy.

Now you can set up your pager carriers by going to the Main Menu > File Maintenance > Pager >Pager Carriers submenu to enter your pager information — see section 8.12.

For email notification, you must first set up email port jobs for incoming and outgoing mail — see following pages.

## SNPP Alarm Notification Port Setup

Setup a job for sending SNPP pages (SNPP Client)

Define SNPP pager carriers with Pager IDs.

Setup a pager schedule (if necessary).

### Setup Procedure Detail

**Note:** This procedure assumes that you already have a network card installed your system.

1. Contact your network administrator to determine the SNPP service provider for the pagers you use. You will need the IP address and listening port of the SNPP Server in order to send pages. The default listening port for SNPP Servers is 444.
2. Navigate to job 28. This job should already have it's port usage set to "Ethernet I/O".
3. Define a TELNET-RAW data connection with the IP address of the SNPP Server and port 444.
4. Navigate to a halted LAN job.
5. Define the job's port usage as "SNPP Client".
6. Enter a description of the SNPP Server in the Description field (optional).

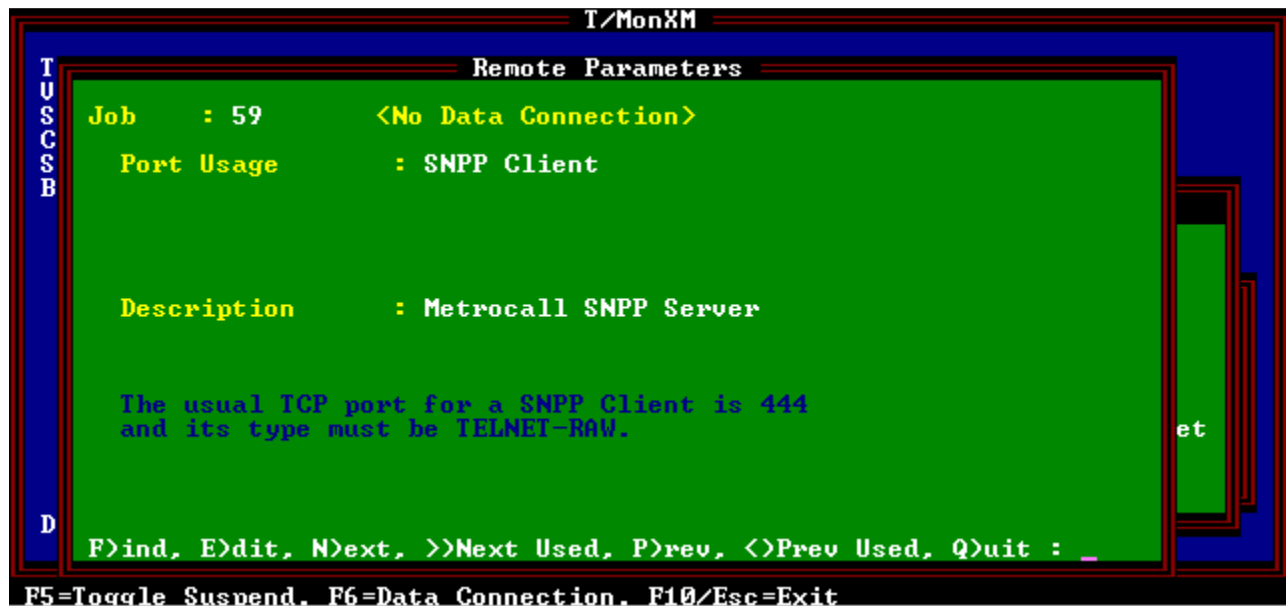


Fig. 8.5- Remote Parameters window

7. Press F6 to assign a data connection.

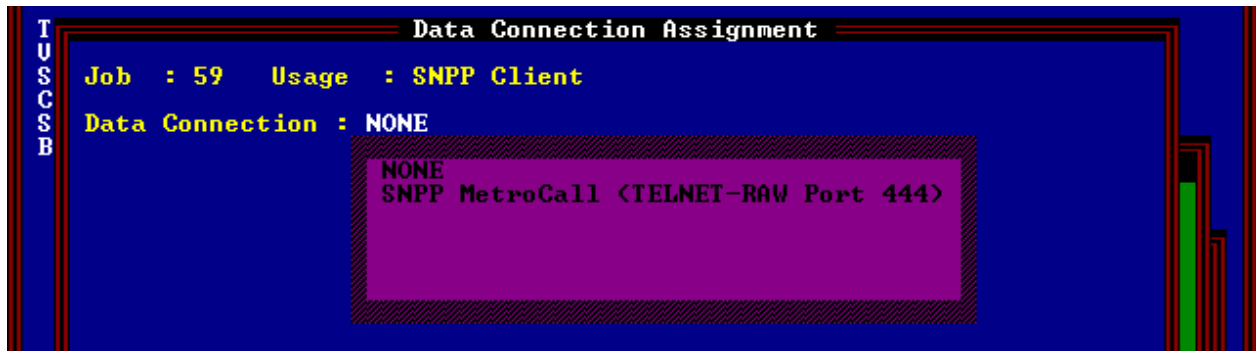


Fig. 8.6 - Data Connection Assignment window

8. Select the data connection you just created.

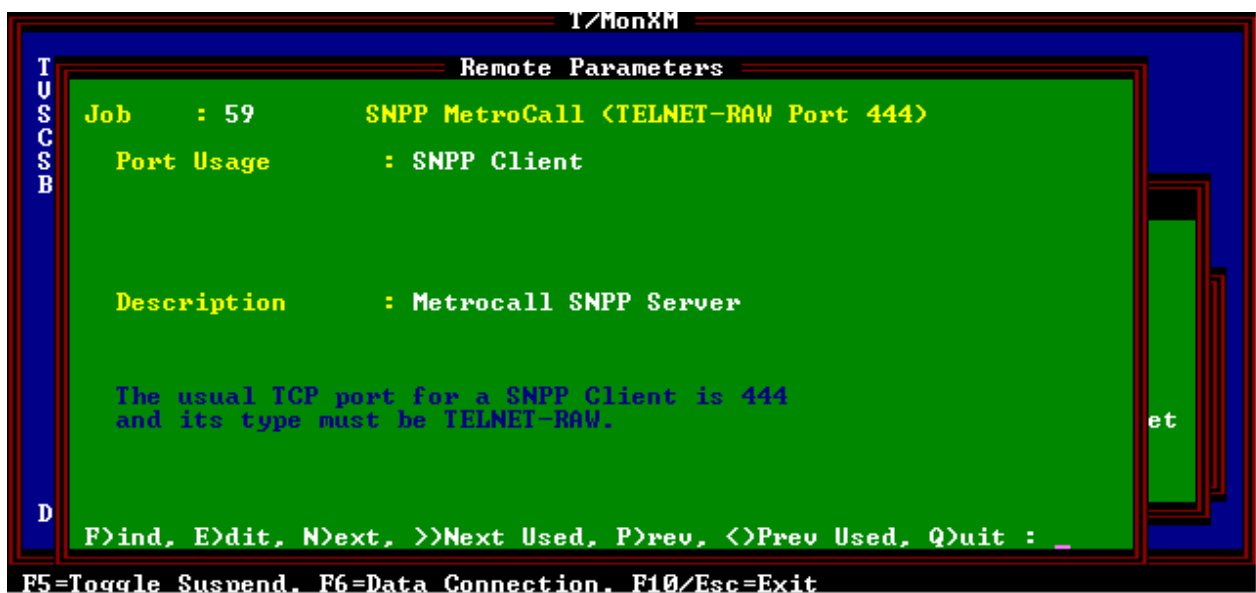


Fig. 8.7 - Remote Parameters window

## Email Alarm Notification Port Setup

Email notification requires T/MonXM version 3.5 or later.

**Note:** the configuration procedure described in this section only sets up the email resource.

### Setup Procedure Overview

Set up a Job for sending outgoing mail (SMTP).

Set up a Job for the system to receive mail (POP3).

Assign email addresses to pager carriers and enable response options.

Set up pager scheduling (if necessary).

### Setup Procedure Detail

**Note:** This procedure assumes that you already have a network card installed and working in your T/Mon or IAM.

1. Contact your network administrator to discuss having an email account setup for your T/Mon or IAM. Note that SMTP is used to send mail and POP3 is used to retrieve it. You will need an account name and password, and the email server IP address.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	TELNET-RAW	111.111.111.111	25	SMTP Port
2	TELNET-RAW	111.111.111.112	110	POP3 Port
3				
4				TCP (T/GrafX, T/RemoteW, HTTP, RAS, FTP Server, TMonNet)
5				TELNET-RAW (ASCII, Craft, E-Mail, FTP Data Transfer)
6				TELNET (ASCII, CRAFT : if TELNET negotiation required)
7				UDP (DPS RTU Polling, SNMP TRAP Processing, SNMP Agent)
8				ICMP (PING)
9				
10				
11				
12				

Fig. 8.8 - Creating TCP ports for email protocols

2. Go to Parameters/remote Ports. Navigate to job 28. This job should already have its port usage set to "Ethernet I/O."
  - a. Press F1 to bring up the Ethernet TCP Port Definition screen.
  - c.. Add an entry of type TELNET-RAW.
  - d. Set the entry's IP address to the IP address of your mail server.
  - e. Set the TCP port to 25 (this is the standard SMTP port).
  - f. Set the description to "Outgoing-SMTP."
  - g. Add another entry of the type TELNET-RAW and set its IP address to the IP address of your mail server.
  - h. Set the TCP port to 110 (this is the standard POP3 port).
  - i. Set the description to "Incoming-POP3."
  - j. Press F8 to save the changes.
3. Navigate to an open LAN job — press F for find, then type "50" and press Enter. Press N until you find a halted job.



Fig. 8.9 - Mail Outgoing SMTP screen.

**Note:** this only sets the domain in the “from” email address field.

4. Press E for Edit and set up the job’s port usage as “Mail (Outgoing-SMTP).”
  - a. Set Domain Name to your company’s email domain name (for example: dpstele.com).
  - b. For Account Name enter the account name that you received from your network administrator.

**Note:** the account name field is the portion of the email address before the “@” symbol. The Domain Name field is the portion of the email address after the “@” symbol. The T/Mon will use these two fields to create the from address when sending email notifications.

5. Press F6 to assign the data connection of this job to the SMTP port defined on the previous page in step 2. Press Tab, select SMTP PORT (TELNET RAW Port 25) and press Enter.
6. In the Remote Parameters screen, press N (Next) until you find another halted job.

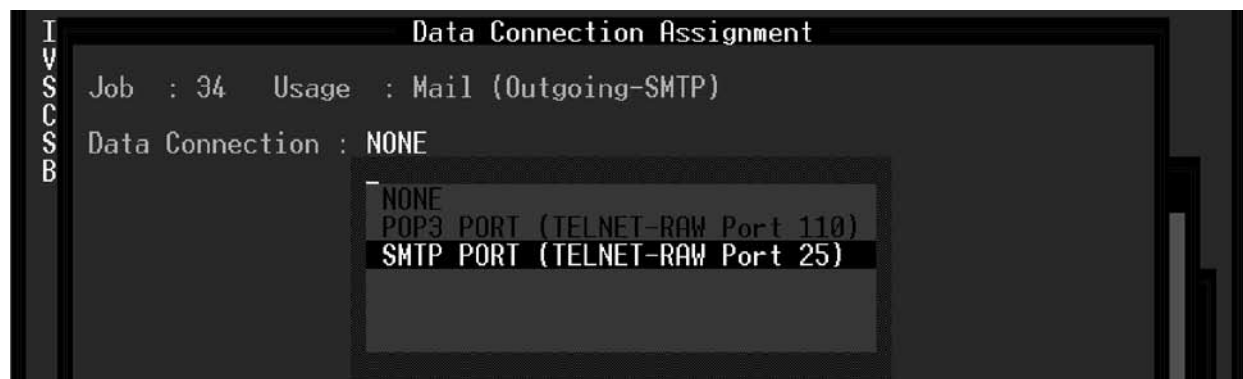


Fig. 8.10 - SMTP Data Connection

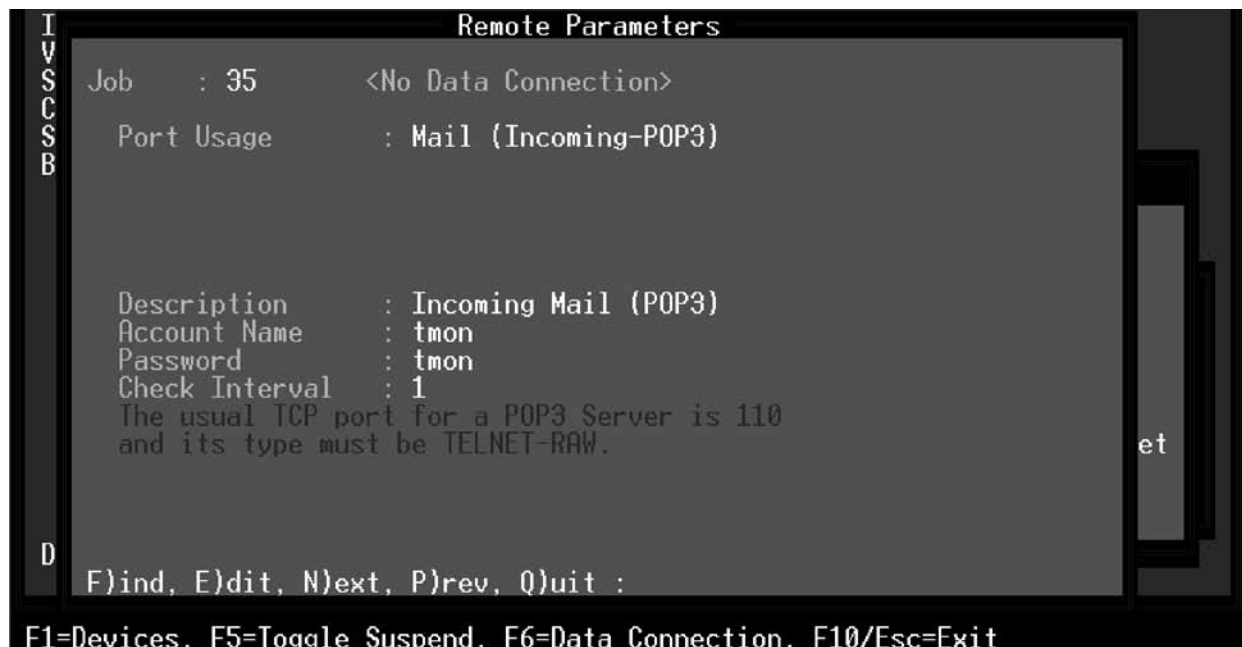


Fig. 8.11 - Mail Incoming POP3 screen.

7. Press E for Edit and set up the job's port usage as "Mail (Incoming-POP3)." Enter the account name and password that you received from your network administrator. In the Check Interval field, enter the frequency (in minutes) that the system should check for new mail.
8. Press F6 to assign the data connection of this job to the POP3 port defined in step 2.
9. Remote port job is now complete. Enter email addresses in the Pager Carriers screen — see following section for details.

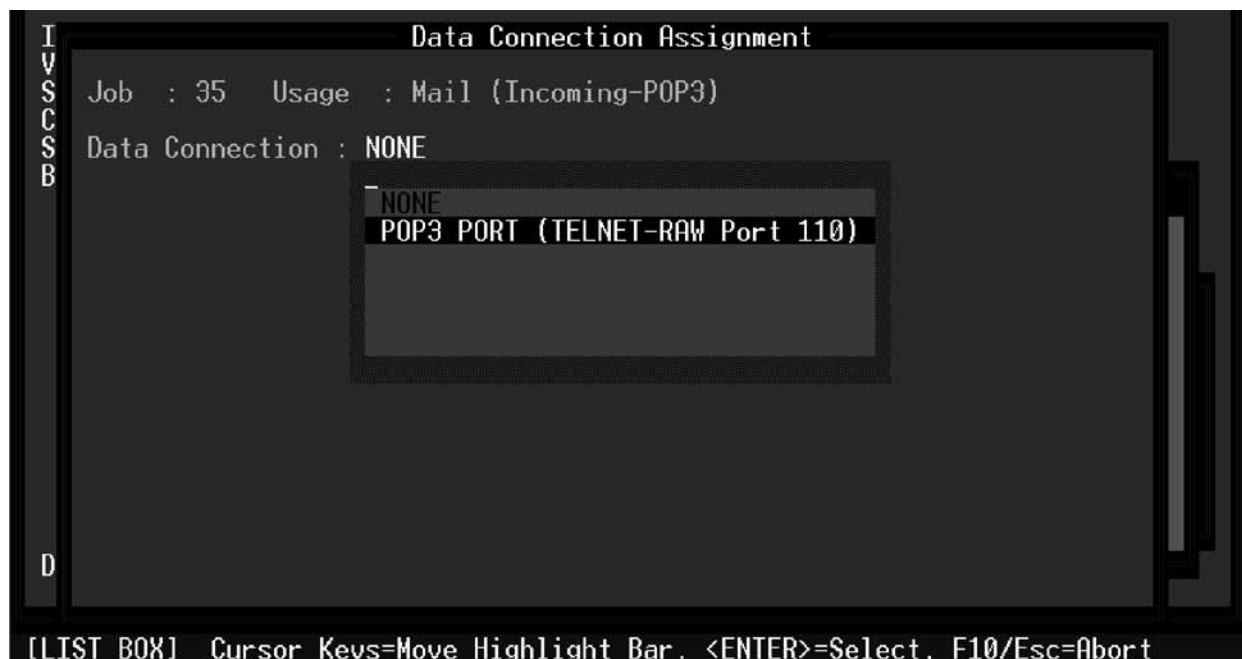


Fig. 8.12 - POP3 Data Connection

## Pager Carriers

At the Pager Carriers screen you can define up to 999 pager carriers.

To access the Pager Carriers screen select Pager Carriers from the Pager menu and press Enter.

Once defined, Pager Carrier initials can be assigned to an operator in the Weekly Schedules screen. (Initials can also be assigned in the Alarm Summary Screen.) Fill in each field per Table 8.C. After completing a Pager Carrier field set, press F8 to save and return to the Pager menu.

Email address information for email notification is entered in a sub-screen in the Pager Carriers screen — see section 8-13.

Pager Carriers					
Pag	Int	Name	Type	Pager Phone	ID/Delay
1	AGP	ALPHA GROUP	G		
2	TWR	TOWER PRINTER	L	352-2251	0
3	BGP	BETA GROUP	G		
4	CRS	CLIFF SAMPSON	2	477-2152	4002990
5	TMC	TOM COLEMAN	A	577-2943	4002991
6	KJ	KIM JENSEN	N	599-0203	10
7	AJK	AL KAUFMAN	A	688-2209	4002562
8	TRD	TERRY DOWLE	2	448-1255	3223322
9	MRD	MACK DONALD	N	352-1664	10
10	DGP	DELTA GROUP	G		
11	JPG	JARED GEESEY	A	251-5454	1689433
12	RIS	RAY SORENSON	A	251-5389	1857412
13	AJM	A.J. MACINTYRE	2	448-4562	6572348
14	FRG	FRANK GUILDER	N	448-9632	10
15	PEM	PHIL MONTGOMERY	N	448-3872	10
Enter initials					
F3=BLANK, F6=E-Mail, F8=Save, F9=Help, F10/Esc=Exit					

Fig. 8.13 - Pager carriers screen

Table 8.C - Fields in the Pager Carriers screen

Field	Description
Page	Pager number. This field cannot be edited. Move cursor to the desired number.
Int	The cursor will be on this field when the screen is opened. Enter pager carrier's initials. Initials must be unique for each carrier. Must be at least 2 characters. Use alpha or numeric characters.
Name	Enter name of the pager carrier. Up to 30 alpha or numeric characters.



**Table 8.C - Fields for the Pager Carriers screen (continued)**

Field	Description
Pager Phone	Enter phone number of pager. For alpha pagers use the number of the Tap terminal, not your PIN. (If unknown, this number can be obtained from the pager company.) Neither parentheses nor hyphens are needed in the phone number listed here, but can be entered for clarity. This field can have a dial code before the actual number for routing pager calls out of buildings that have their own local phone network.
Type	Enter the pager type. Valid entries are:
	E Email notification. Press F6 to enter an email address and select "N" for a normal email message notification, or "S" for a short email notification type.
	S SNPP pager
	N Numeric pager
	A Alphanumeric pager
	2 2-Way pager - Two-way paging allows acknowledgment to occur immediately, from the carrier's pager, halting additional paging activity. Two-way paging can ack an individual alarm or it can be used to tag an alarm, preventing additional COS alarms if the alarm is repeatedly occurring. An ignore response prevents further pages to the same carrier. Follows format for alphanumeric pagers.
	G Group - Pages a group of pager carriers. Pager Phone and ID/Delay fields are skipped when type "G" is entered. See further details on p. 8-28.
ID/Delay	L Logger - Sends Alphanumeric pager message string (as defined on p. 8-10) to a printer or ASCII terminal. Logger stays on line for time specified in the ID/Delay field.
	Enter 1 to 10 digits for the pager ID (pin) when "A" (Alphanumeric) or "S" (SNPP) is entered in the Type field. Enter the Delay when "N" (Numeric) is entered. Delay is the amount of time, after dialing, before pager information is sent. This varies with the paging company. Numeric users may manually dial the number to determine the correct time before the tone. (0-99 sec) Enter the Hang up Delay when "L" (Logger) is entered in the Type field. Hang up Delay is the amount of time the logger is to remain on line to print out additional alarms. Set for 0 to 99 minutes.

**Table 8.D - Key commands Available in the Pager Carriers Screen**

Function Key	Description
F3	BLANK. Deletes the current pager entry.
F8	Save. Saves the Pager Carrier database.
F9	Help. On line Pager Carrier help.
F10/Esc	Exit. Leaves the Pager Carrier screen without saving changes.

Pager Carriers				
Pag	Int	Name	E-Mail Address	Typ
1	AGP	ALPHA GROUP		N
2	TWR	TOWER PRINTER		N
3	BGP	BETA GROUP		N
4	CRS	CLIFF SAMPSON	cliff@proactive.com	N
5	IMC	TOM COLEMAN	tom@proactive.com	S
6	KJ	KIM JENSEN	kim@proactive.com	N
7	AJK	AL KAUFMAN	al@proactive.com	N
8	TRD	TERRY DOWLE	terry@proactive.com	N
9	MRD	MACK DONALD	mackd@proactive.com	N
10	GGP	GAMMA GROUP		N
11	WDT	WILL TOTTON	will@proactive.com	N
12	RIS	RAY SOPRENSEN	rays@proactive.com	N
13	AJM	A.J. MACINTYRE	ajm@proactive.com	N
14	FRG	FRANK GUILDER	frank@proactive.com	N
15	PEM	PHIL MONTGOMERY	phil@proactive.com	N

Enter initials

F1=Response Options, F3=BLANK, F6=Pager, F8=Save, F9=Help, F10/Esc=Exit

Fig. 8.14 - Pager Carriers email screen.

**Note:** in order for T/Mon to send email notification of reportable alarms, you must first create a remote port job in the Parameters > Remote Ports screen option — see section “Pager Alarm Notification Port Setup”.

#### Entering Email Addresses

Use the following steps to enter email address for pager carriers to receive email notification from T/Mon:

1. Enter your initials and your name. Leave the Type field blank and press Enter.
2. Press F6 to toggle from pager information to email addresses. Enter email addresses as appropriate. Here is a sample demonstration of the format that is expected: support@dpstele.com
3. The Typ field allows the option for short email messages. Select “S” for short format, and “N” for normal format.

**Note:** Short contains just the alarm notification information, while Normal format contains a header and footer containing general T/Mon alarm notification information.

Pager Carriers				
Pag	Int	Na	Response Options	Typ
1	AGP	ALP	Name :WILL TOTTON	N
2	TWR	TOW	Initials :WDT	N
3	BGP	BET		N
4	CRS	CLI	Ack Single Alarm : Y	N
5	TMC	TOM	by Reply : Y	S
6	KJ	KIM	Ack Site : Y	N
7	AJK	AL	Tag Single Alarm : Y	N
8	TRD	TER		N
9	MRD	MAC		N
10	GGP	GAM		N
11	WDT	WIL	Include AckAlarm link (Y/N)	N
12	RIS	RAY		N
13	AJM	A.J.MACINTYRE	ajm@proactive.com	N
14	FRG	FRANK GUILDER	frank@proactive.com	N
15	PEM	PHIL MONTGOMERY	phil@proactive.com	N

F8=Save, F10/Esc=Exit

Fig. 8.15 - Pager Carrier Response Options.

- Pager carriers who have their email address listed in the pager profile will be emailed of a reportable alarm event. You can also setup the pager carrier to receive a pager notification, but you will need to enter the pager carrier as a new entry.
- Place the cursor at the initials for an entry and press F1 to edit response options for the selected carrier. All response options are disabled by default. (Note that the response options settings apply to 2-way paging, DTMF Acknowledgement and email).

## Weekly Operator Schedules

Up to 999 Operator Schedules can be Specified

**Note:** If you have complex or rotational schedules it is best to use Schedule Exception exclusively — see section 8-19.

In the Weekly Schedule screen assign pager carriers to a 24 hour weekly paging schedule. Pager carriers whose Initials are entered at the day and time indicated in the weekly schedule will be paged.

The Weekly Schedule screen is divided into 999 operator groups. When alarms come in that have a pager response assigned, T/MonXM references the operator. The operator determines who will be paged by its Weekly Operator Schedule. Special changes for holidays etc. can be made at the Schedule Exceptions screen.

Use the following steps to schedule weekly operators:

1. To access the Weekly Schedules screen select Weekly Schedules from the Pager menu and press Enter.
2. When the screen comes up it will display the entries for the last operator viewed.
3. To select another operator number (1-999) type F, the number and Enter, or type N for next or P for previous. To add a schedule type F (Find), then the new number, press Enter, and type Y (Yes) when prompted to add. To edit the screen type E, to quit type Q, and to delete type D.

Weekly Operator Schedule							
Operator : 1		Description : On-Call Technicians					
Hour	SUN	MON	TUE	WED	THU	FRI	SAT
0:00	TMC	WDT	WDT	WDT	WDT	WDT	TMC
1:00	TMC	WDT	WDT	WDT	WDT	WDT	TMC
2:00	TMC	WDT	WDT	WDT	WDT	WDT	TMC
3:00	TMC	WDT	WDT	WDT	WDT	WDT	TMC
4:00	TMC	WDT	WDT	WDT	WDT	WDT	TMC
5:00	TMC	WDT	WDT	WDT	WDT	WDT	TMC
6:00	KJ	AJK	TRD	MRD	RIS	FRG	KJ
7:00	KJ	AJK	TRD	MRD	RIS	FRG	KJ
8:00	KJ	AJK	TRD	MRD	RIS	FRG	KJ
9:00	KJ	AJK	TRD	MRD	RIS	FRG	KJ
10:00	KJ	AJK	TRD	MRD	RIS	FRG	KJ
11:00	KJ	AJK	TRD	MRD	RIS	FRG	KJ
F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :							
F1=Edit Description, F10/Esc=Exit							

Fig. 8.16 - Weekly operator schedule screen

Operators will be paged on a cleared alarm only if they are paged on the occurrence of the alarm.

6. The Weekly Schedules screen shows hours 0:00 to 23:00 in the left column and days across the top.
7. When Edit is selected the cursor will appear at the SUN, 0:00 field.
8. Enter the initials or pager number (1-999) of the person to be paged between midnight and 1:00 AM on Sundays.  
**Note:** If no one is to be paged during that hour on Sunday, pressing Enter will move the cursor to Monday.
9. To skip hour 0:00 for the entire week use the down arrow key.
10. To see a listing of the assigned pager carriers press F1. The F2, F3 and F5 keys can be used to speed entries by copying or entering several fields at once. F4 translates initials from one carrier to another — see Table 8.E.

**Table 8.E - Key commands Available in the Weekly Schedules screen  
(when Edit command is selected)**

Function Key	Description
Down Arrow	Moves the cursor down the screen.
Up Arrow	Moves the cursor up the screen.
PgDn/End	Moves the cursor to the second half of the screen (12:00 to 23:00)
F10/Esc	Exit. Leaves the Pager Carrier screen without saving changes.
F1	List. Displays a list of pager numbers and the Initials and Names eligible to be listed on this screen. Enter the initials or pager number.
F2	Copy. A small window will appear for specifying an hour entry to be copied to another hour or hours. The “copy to” entry may be a range (as 8-17) or separate hours (as 8, 10, 13). This action copies the entire week’s line for the hour(s).
F3	Fill. A small window will appear for specifying initials (or pager number) to be entered in several hours on a specific day. The hours entry may be a range (as 8-17) or separate hours (as 8, 10, 13).
F4	Translate. Changes all entries for one pager carrier’s initials to another. Affects only selected operator schedule.
F5	Repeat. The repeat option allows you to repeat the last entered initials for one line.
F10/Esc	Exit. Exits from the Weekly Operator Schedules screen.

## Schedule Exceptions

The Schedule Exceptions schedule overrides the Weekly Schedule.

Users with complex rotational schedules may use schedule exceptions exclusively.

Remember to press Enter at the end of your additions and then press F8 to save your selections.

“/” indicates the schedule will take no action.

The Schedule Exceptions screen allows special schedule changes for holidays, etc.

Pager carriers whose initials are entered at the time indicated in the Schedule Exceptions screen will be paged at that date and time. Schedule Exceptions can be prepared weeks or months into the future.

There is special color coding on the Schedule Exceptions screen. Entries from the Weekly Schedule are displayed in Green. Schedule Exceptions entries are displayed in Red.

To access the Schedule Exceptions screen select Schedule Exceptions from the Pager menu and press Enter.

To enter a new date and operator select Find. Enter a date in the future (use the MM/DD/YY format) and press Enter. Type in the operator number and press Enter. Answer “Yes” when the prompt asks if you wish to add. The Selected Operator Schedule will then appear on the screen.

To copy another exception schedule, press F1 (Read). The existing exception schedule dates will appear in a default box. Press Tab, highlight a date from the list and press Enter to select. The copied exception schedule may then be further edited.

Schedule Exceptions														
Week Of : 9/13/98														
OPR : 1														
Hour	AM							PM						
	SUN	MON	TUE	WED	THR	FRI	SAT	SUN	MON	TUE	WED	THR	FRI	SAT
	13	14	15	16	17	18	19	13	14	15	16	17	18	19
12:00	RAB	CRS	CRS	CRS	CRS	CRS	RAB	---	---	---	---	---	---	---
1:00	RAB	CRS	CRS	CRS	CRS	CRS	RAB	---	---	---	---	---	---	---
2:00	RAB	CRS	CRS	CRS	CRS	CRS	RAB	---	---	---	---	---	---	---
3:00	RAB	CRS	CRS	CRS	CRS	CRS	RAB	---	---	---	---	---	---	---
4:00	RAB	CRS	CRS	CRS	CRS	CRS	RAB	---	---	---	---	---	---	---
5:00	RAB	CRS	CRS	CRS	CRS	CRS	RAB	---	---	---	---	---	---	---
6:00	MRD	AJK	KJ	TRD	PLM	CRS	MRD	---	---	---	---	---	---	---
7:00	MRD	AJK	KJ	TRD	PLM	CRS	MRD	---	---	---	---	---	---	---
8:00	MRD	AJK	KJ	TRD	PLM	CRS	MRD	---	---	---	---	---	---	---
9:00	MRD	AJK	KJ	TRD	PLM	CRS	MRD	---	---	---	---	---	---	---
10:00	MRD	AJK	KJ	TRD	PLM	CRS	MRD	---	---	---	---	---	---	---
11:00	MRD	AJK	KJ	TRD	PLM	CRS	MRD	---	---	---	---	---	---	---
F)ind, E)dit, N)ext OPR, P)rev OPR, Q)uit :														
F1=Prev Week, F2=Next Week, F3=Copy Week, F4=Copy Day, F9=Help, F10/Esc=Exit														

Fig. 8.17 - Schedule exceptions screen

## Alphanumeric Pager Formats

Configure and access up to four preset formats with Alphanumeric Formats menu.

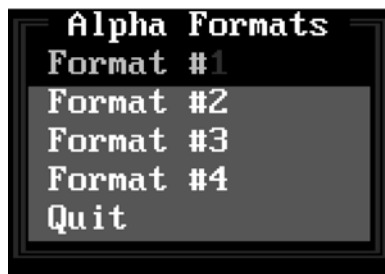


Fig. 8.18 - Select from four alpha pager formats

**Note:** By default, the first field starts at character 6.

The Alphanumeric Formats menu allows you to configure and access up to four preset formats for the alarm descriptions and other information that will be sent to the pager. This allows formatting the pager message to suit the level of detail required by the person being paged and to address restrictions of your pager provider. The Alphanumeric Formats screens are similar in operation to the Edit Alarm Format screen in the Parameters menu.

To access the Alphanumeric Formats screen select Alphanumeric Formats from the Pager menu and press Enter. A small menu with four different format choices will appear. Highlight one of these and press Enter. (All four of these are the same until configured.)

The screen presents status information at the top and a format bar immediately below. The status information includes the format number (1-4), page, status, level and total width. This information tells you what the format bar is showing. The format bar illustrates the message that would be sent to the pager. The table that follows explains how the format bar and associated function keys can be used to quickly pre-view a message.

For further information refer to Table 8.F and Table 8.G.

When the Alpha Pager Format screen first appears, the cursor is placed in the Name field. Up to 14 fields can be defined with a total of 153 characters.

FLD	START	NAME	WIDTH	SPACE
1	6	ASC Extract...	40	YES
2	47	Alarm Id	13	YES
3	61	Alarm Status	1	YES
4	63	Level	1	YES
5	65	Description	40	YES
6	106	Site Name	15	YES
7	122	Device Type	4	YES
8				
9				
10				

Enter Field Name

Tab=List, F1=Ins, F2=Del, F4=Lu&St, F6=Sim, F7=Pan, F8=Save, F9=Help, F10=Exit

Fig. 8.19 - The alphanumeric pager format screen

**Table 8.F - Status information fields in the Edit Alpha Pager Format screen**

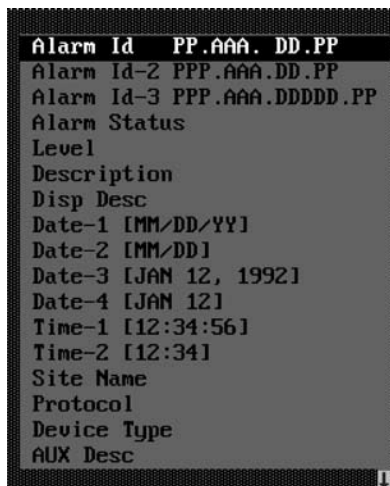
Field	Description
Page	Portion of format bar shown. Page 1 shows columns 2 - 77. Page 2 shows columns 77 - 153. Press F7 to toggle between pages.
Status	Alarm status (F = Failed, C = Clear). Use F6 to step through the status characters to see how the message changes with status. Use F4 to change the words used to describe the status.
Level	The alarm level (A, B, C, D). Use F6 to step through the levels to see how the message changes with alarm levels. Use F4 to change the words used to describe the level. (See Table 8.G.)
Total Width	Number of characters the message occupies at its present state of configuration. This number will increase as further fields are defined.

For each field enter a name, width and whether a space is to separate it from the following field. Press TAB while the cursor is in the name column to view the list of field names. Each name has a default value for the field width, which can be edited while the cursor is in the width column. See Table 8.G for details.

**Table 8.G - Fields in the Edit Alpha Pager Format screen**

Field	Description
FLD	Field position.
START	Starting column of the field. Note: This item cannot be edited.
NAME	Field name. Press Tab to view name list. Use Tab to move the highlight bar and press <ENTER> to select the item. See Table 8.H. for descriptions of selections and descriptions.
WIDTH	Width of the field. If the width is set to be less than the amount of data in the field then the right-hand part of the field will be truncated.
SPACE	Puts trailing space after field. Select Yes or No with Tab.

**Note:** When alpha pages are transmitted, all extra spaces will be removed to produce more readable messages.

**Fig. 8.20 - Selections appear in a menu window**



**Table 8.H - Menu selection available in the Alpha Pager Format screen**

Field	Description
Alarm ID1 [PP.AAA.DD.PP]	Port. Alarm. Display. Point
Alarm ID2 [PPP.AAA.DD.PP]	Port. Alarm. Display. Point
Alarm ID3 [PPP.AAA.DDDDD.PP]	Port. Alarm. Display. Point
Alarm Status	Fail and clear description
Level	Severity (CR, MJ, MN, ST)
Description	Alarm description
Disp Desc	Display description
Date-1 [MM/DD/YY]	Month/Day/Year
Date-2 [MM/DD]	Month/Day
Date-3 [JAN 12 1992]	Date (text description)
Date-4 [JAN 12]	Date (text description, year omitted)
Time-1 [12:34:56]	Time (hour:minute:second)
Time-2 [12:34]	Time (hour:minute)
Site Name	Site name as defined in Parameters > Remote Ports > Device Definition screen.
Protocol	Port type description
Device Type	Device type description
Aux Desc	Auxiliary description <b>Note:</b> you must enable this feature in the Parameters > Miscellaneous screen option.
System Name	System name as defined in Parameters > Miscellaneous screen option.
Message Text	Following /T in a pager dial-up entry string
ASC Extract	ASCII text that was parsed to create alarm condition — see “Extracting Text for Alpha Pagers.” <b>Note:</b> available only if ASCII Processor module installed.
Text Message	Text/Message defined for the point.
Numeric Data	Information that normally goes to a numeric pager
Item Number	Used to identify pager carrier and alarm to T/Mon for DTMF On-Call — see Software Module 18 “DTMF On-Call” <b>Note:</b> must be included if acknowledging alarm by replying to email.

**Table 8.1 - Key commands available in the Edit Alpha Pager Format screen**

Function Key	Description
Tab	List. This key displays optional entries in the field.
F1	Ins. Inserts a blank field entry at the current cursor position.
F2	Del. Deletes the field entry that the cursor is under.
F4	Level and Status. Allows editing of the text in the level and status fields. F4 brings up an editing window. Up to 8 characters can be used for each level and status. Field sizes must be adjusted in the format to see all the text. See Figure 8.14.
F6	Sim. Cycles through all combinations of level and status to allow pre-viewing the message in the format bar.
F7	Pan. Toggles the page # and format bar to show the portion not currently on the screen.
F8	Save. Saves the Pager Alarm Format definition.
F9	Help. Online Help.
F10/Esc	Exit. Exits without saving any changes that may have been made.

**Edit Alpha Pager Format #1**

PAGE : 1    STATUS : F    LEVEL : A    TOTAL WIDTH : 133

FLD	ST	TEXT
1	6	LEVEL A    CRIT....
2	47	LEVEL B    MAJ
3	61	LEVEL C    MIN
4	63	LEVEL D    STAT
5	72	CLEAR    C
6	11	FAIL    F
7	12	TAGGED    TAG
8		
9		
10		

Enter Text

F8=Save, F10/Esc=Exit

**Fig. 8.21 - Level and status text can be edited in this window**

To define level and status attributes, press F4 in the Edit Alpha Pager Format screen. Then fill in the fields with the appropriate information. Defaults are shown above.

## Pager Profiles

To use Pager Profiles, Select Pager Profiles from the Pager sub-menu.

The Pager Profiles screen will appear. Enter a description for each desired profile, up to 99. A pager profile description can use any type of category, such as alarm type, equipment type, location, region, etc. Up to 30 operators may be defined for each profile, meaning that any alarm that uses that profile will cause a page to go to each of the defined operators. Each operator's definition can be customized for the type of alarm that causes the page (alarm, clear or both), a delay, which pager format to use (alpha pagers only), the number of times to repeat, the delay time between repeats, a message to go to alpha pagers and a message to go to numeric pagers.

Once the pager descriptions are entered, move the cursor to the first profile and press F2. The Pager Profile Entries screen for Alpha Pager Settings will appear (Figure 8.23). Make entries per Table 8.J.

Press F5 to toggle to the Numeric Pager Entries screen — see Figure 8.24. Make entries per Table 8.J.

Pager Profiles	
Profile	Description
1	Power Plant
2	Transmission
3	Security.....
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	

Enter Profile Description

F1=GOTO, F2=Pager Entries, F3=Delete, F8=Save, F9=Help, F10/Esc=Exit

Fig. 8.22 - Up to 99 pager profiles can be assigned to any type of category

Key commands are defined in Table 8.K.

The profile number will later be entered in the alarm point definition screen for each point that is to produce a page.

Pager Profile Entries							
Profile 1: Power Plant				Editing : Alpha Pager Settings			
OPR	Type	Delay	Fmt	Repeat Count	Repeat Delay	Alpha Pager Message	
1	001	ALM	0	1	3	5	REPORT TO SITE
2	5	ALM	0	1	3	5	CONTACT SITE SUPER
3	1	CLR	0	1	3	3	CANCEL EMERGENCY
4	12	BOTH	1	2	1	1	POWER ALARM
5	...						
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							

Enter Operator Number (1-999)

F1=GOTO, F3=Blank, F5=Toggle Alpha/Numeric, F8=Save, F9=Help, F10/Esc=Exit

Fig. 8.23 - Alpha pager settings for profile 1 are entered in this screen

Pager Profile Entries						
Profile 1: Power Plant				Editing : Numeric Pager Settings		
OPR	Type	Delay		Repeat Delay	Numeric Pager Message	
1	1	ALM	0	0	145	
2	5	ALM	0	0		
3	1	CLR	0	0		
4	12	BOTH	1	0		
5	25	ALM	0	1	020	
6	...					
7						
8						
9						
10						
11						
12						
13						
14						
15						

Enter Operator Number (1-999)

F1=GOTO, F3=Blank, F5=Toggle Alpha/Numeric, F8=Save, F9=Help, F10/Esc=Exit

Fig. 8.24 - Numeric pager settings for profile 1 are entered in this screen

Use both types of profile settings if both kinds of pagers are defined in the operator. Numeric pagers carriers will get the numeric message and alpha pager carriers will get the alpha message.

**Note:** X=Enabled. Table 8.J continues on following page.

**Table 8.J - Fields in the Pager Profile Entries Screen > Numeric Pager Settings**

Field	Numeric	Alpha	Description
OPR	X	X	The operator associated with the page (assigned through the pager weekly schedules screen). Entry common to alpha and numeric pagers.
Type	X	X	Alarm events that are to be paged — either alarm (ALM), clear (CLR) or both (BOTH). Entry is common to alpha and numeric pagers. <b>Note:</b> This also allows for escalation by paging the appropriate parties, based on alarm clearing or acknowledgement. Stage 2 paging could be notified if the alarm has not cleared or been acknowledged within a certain time period.
Delay	X	X	Time in minutes to wait before dialing pager. Keeps transitory “nuisance” alarms from being paged, also prevents paging if alarm is acknowledged by a T/MonXM attendant within the delay time. Entry is common to alpha and numeric.
Fmt		X	The format number to use, as defined under Pager Alphanumeric Formats (applies to alpha pagers only).
Repeat Count		X	The number of times an alpha page will be repeated, as long as the page is not acknowledged and the condition being paged persists (applied to alpha pagers only).
Repeat Delay	X	X	Interval in minutes between repeat pages. Alpha and Numeric pagers have separate repeat delays. <b>Note:</b> Numeric pages continue to be repeated until the alarm is acknowledged or corrected
Alpha Pager Message		X	The message that will appear in the Message Text field for the format selected by the Fmt entry above (applies to alpha pagers only).
Numeric Pager Message	X		The message that will appear in a numeric pager view window (applies to numeric pagers only).

**Table 8.K - Key commands available in the Page Profile Entries screen**

Function Key	Description
F1	GOTO - Moves the cursor to a selected pager entry.
F3	Blank - Deletes the current pager entry
F5	Toggle Alpha/Numeric - Switches from alpha to numeric pager entry fields, and vice versa
F8	Save - Saves the pager entries and returns to the Pager Profile screen
F9	Help - opens the help screen
F10/Esc	Exit - Returns to Pager Profiles screen without saving any changes

## Entering Pager Profiles

In the Alarm Point Definition screen.

Once pager profiles have been defined, any profile can be assigned to any alarm point in the Point Definition screen. Alarm point definition is fully explained in Section 10. Figure 8.25 is provided here for reference only.

To assign a pager profile to an alarm point, use the following steps:

1. Go to the Main menu > Parameters > Remote Ports submenu option.
2. Press F (Find), enter the port number of the appropriate device.
3. Press E (Edit).
4. Press F1. The Remote Device Definition screen will appear.
5. Press F1. The Point Definition screen will appear.
6. Press Enter to move to the Pager field. Assign the appropriate pager profile number and press Enter.
7. Press F8 to save your changes.

Point Definition											
Port	:	K1	Addr:	1	Disp:	1	Display Desc :				
P	L	H	L	S	R						
o	o	s	e	t	v						
Pt	l	g	t	v	s	s	Windows	Msg	Qual	Counter	Pager
1	B	L	H	A	A	N	3,6,9,22.....	1	0	0	1
2	B	L	H	A	A	N	2,5,67	4	0	0	9
3	B	L	H	A	A	N	33,35	1	10M	0	0
4	B	L	H	A	A	N	2,5	0	0	30M/10	0
5	B	L	H	A	A	N	44,70	2	10M	10M/5	8
6	B	L	H	A	A	N	22,23	3	0	0	0
7	B	L	H	A	A	N	2,5,7-9	1	1H	1H/7	4
8	B	L	H	A	A	N	2,4-6,10	3	0	0	0

Enter windows. (2-720; 8 max) %,%,%,%

Message

File Critical Action Report

Notify duty engineer at ext. 2152

Up Arrow=Previous Field, F10/Esc=First Field

Fig. 8.25 - Enter profile number in the Point Definition screen pager column

## Groups

Page up to 30 people on an alarm.

Groups are treated by the rest of the scheduling system as a pager carrier.

Easily add or remove group members without affecting other aspects of the alarm or scheduling database.

To access the Groups screen, highlight Groups on the Pager sub-menu and press Enter. The group must first be databased in the Pager Carriers section.

T/MonXM can be programmed to page a group of pager carriers rather than a single carrier. The group is given an initial (e.g.: AGP) and name (e.g.: Alpha Group). The group is further defined in the group screen (Figure 8.26)

A group can consist of carriers with different types of pagers, including numerical, alphanumeric, 2-way and loggers.

**Note:** In order to be entered in a group, an individual carrier must first be defined in the Pager Carriers screen. Individual carriers may still be assigned to operator schedules as individuals after they have been placed in a group.

Individual carriers in groups will be called in the order listed. Once an acknowledgement is received from any carrier, the rest of the group will not be called.

**Note:** If a logger is included in the group list it should be placed first on the list to be sure all alarms are logged before they are acknowledged.

**Pager Groups**

Pag	Int	Name
1	AGP	ALPHA GROUP
3	BGP	BETA GROUP
10	DGP	DELTA GROUP

**Pager Group Definition**

Entry : 1    Initials: AGP    Name: ALPHA GROUP

Entry	Initials	Name
1	MRB	MARK DONALD
2	ALB	AL BARTMAN
3	TDB	TERRY DONLE
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

Enter the initials of the carrier or the entry number

F1=Back, F8=Save, F10=Esc=Exit

Press Enter to edit entries for the highlighted group

F10/Esc=Exit

Fig. 8.26 - Highlight a group and press Enter to edit group entries

# Section 9 - Define Remote Ports and Virtual / LAN Jobs

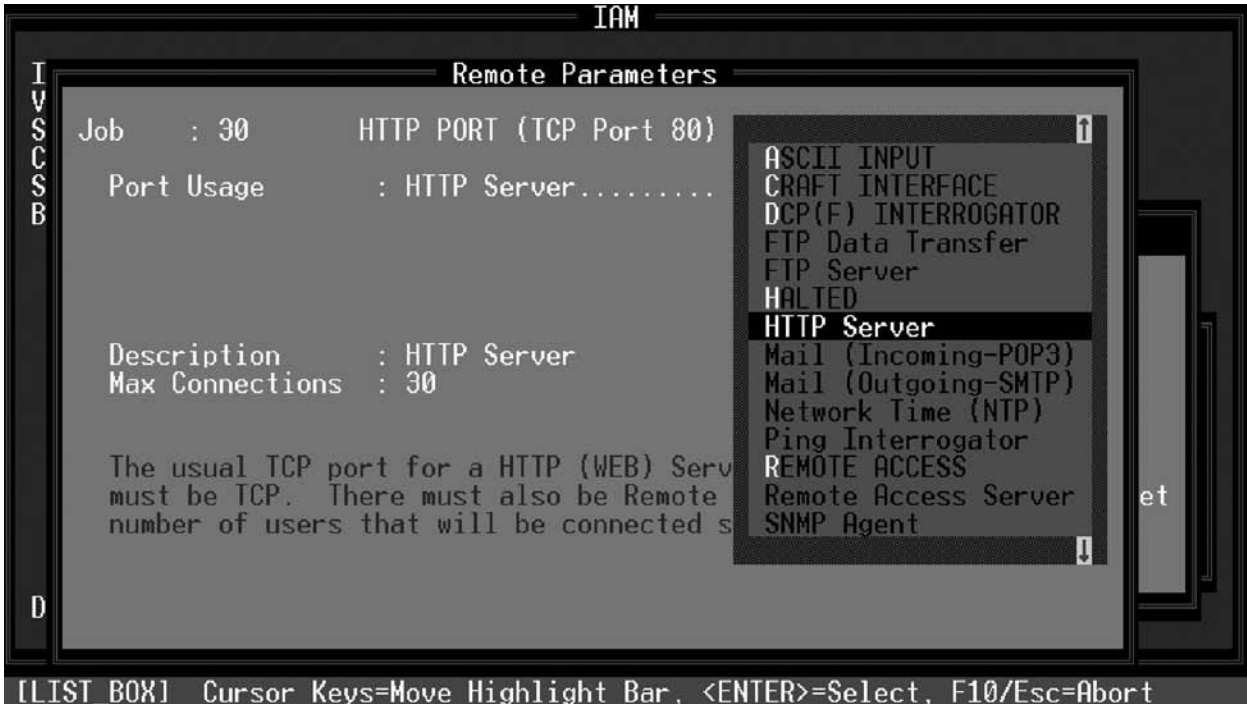


Fig. 9.1 - Remote ports screen with port usage window

The Remote Ports command on the Parameters menu (see Figure 9.1, above) opens the Remote Ports screen, which is used to assign input and output functions to your T/MonXM system.

There are two kinds of Remote Ports in T/MonXM: “real” ports, which correspond to the physical serial ports of your T/Mon NOC, IAM or T/MonXM WorkStation; and “virtual ports” or “LAN jobs.” Virtual ports are a convenient way of configuring LAN-based network services on your T/MonXM system, such as polling LAN-based remotes, e-mail alarm notifications, and Internet-based system clock synchronization.

Port numbers are reserved for specific uses. Table 9.A illustrates remote port functions in the IAM. See Table 9.B for port functions in T/Mon NOC.



**Table 9.A - Available port numbers and their functions in IAM-5**

Field	Description
1-4	Intelligent Controller Card #1
5-8	Intelligent Controller Card #2
9-12	Intelligent Controller Card #3
13-16	Intelligent Controller Card #4
17-20	Intelligent Controller Card #5 (IAM-5 only)
21-24	Not used
25-27	X.25 (see Appendix C)
28	Ethernet I/O (see Section 3)
29	IAM 5 Front Panel
30-500	Virtual Ports/LAN Jobs

**Table 9.B - Available port numbers and their functions in T/Mon NOC**

Field	Description
1-24	External Serial Ports (Port Interface Cartridge) - "real ports"
25-27	X.25
28	Ethernet I/O (see Section 3 for more information)
29	Blank
30-500	Virtual Ports/LAN Jobs

**Note:** Only virtual ports 30-47 can be used for Remote Access. For more information, see Section 5, Remote Access.

Port functions must match the physical configuration of the port interface. For example, a pager or dial-up application must use a port that is equipped with a dial-up modem. Incorrect port assignments will cause system initialization to fail.

The remote ports you are able to define are dependent on the software modules you have installed.

**Table 9.C - Typical T/Mon NOC Job and IP Port Associations**

Job	IP Port	Application	Connection Type
1-24	-	Physical NOC ports	-
28	-	Ethernet	-
30-46	User-definable	Remote Access Jobs Remote Access Pool HTTP Pool	TCP
47	User-definable	Remote Access Server Job	TCP
80	80	HTTP Server	TCP
110	110	Incoming POP3	Telnet Raw
161	161	SNMP Agent (Responder)	UDP
162	162	Trap Processor	UDP (typical) TCP (rare)
420	20	FTP Transfer	Telnet Raw
421	21	FTP Server	TCP
425	25	Mail-Out SMTP	Telnet Raw
443	443	HTTPS (SSL)	TCP
444	444	SNPP (Paging)	Telnet Raw
500	-	Hard Drive Mirroring	-

**NOTE:** Jobs 48 and above are open for any LAN-based application. The jobs listed above are, however, generally associated with the listed functions/IP.

## Remote Port Definition

To begin remote port definition you must first select a port to be defined. While in the Remote Parameters screen press F and enter the port number. You can also use the P (previous) and N (next) keys to move up and down the full list of available ports

Once a port number is selected press E and the cursor will be placed at the Port Usage field and you will see a window displaying all port usages. Use the Tab key or down arrow to move down the list and shift tab or up arrow to move up the list. When the desired usage is highlighted, press Enter to select it. The rest of the fields on the screen will be specific for that port usage. Refer to the corresponding Software Module sections for specific information and instructions. Table 9.C lists the port usages available in T/MonXM, see following page.

Table 9.D - Port usages available in T/MonXM

USAGE	STD	OPT	USAGE	STD	OPT
ABC Pattern Input		X	Hard Drive Mirroring		X
Direct Route		X	HTTP Server	X	
21SV Interrogator		X	LED Bar		X
ABC Pattern Output		X	Larse Interrogator		X
Alarm Forward		X	Mail (Incoming-POP3)	X	
ASCII Dial Up		X	Mail (Outgoing-SMTP)	X	
ASCII Input		X	Modbus Interrogator	X	
ASCII Query Language		X	Network Time (NTP)	X	
ASCII Responder		X	Pager	X	
Auto Databased TL1		X	Ping Interrogator	X	
Badger Interrogator		X	RAC Port		X
Craft Interface	X	X	Remote Access	X	
CSM Interrogator		X	Remote Access Server	X	
Cordell Responder		X	SNMP Agent		X
Datalok 10A		X	SNMP Trap Processor		X
Datalok 10D		X	T/Grafx Responder		X
DCM Interrogator		X	T/MonNET Responder		X
DCP (f/x) Dial-Up	X		TABS Interrogator		X
DCP (f/x) Interrogator	X		TABS Responder		X
DCP (f/x) Responder	X		TBOS Interrogator		X
DTMF Log In		X	TBOS Responder		X
DTMF On-call		X	Teltrac Interrogator		X
E2 Interrog/Monitor		X	TL1 Monitor		X
E2 Responder		X	TL1 Multiplexed Out		X
Environmental Interrogator	X		TL1 Responder Out		x
Ethernet I/O	X		TL1 Source In		X
Felix		X	TMonNET Interrogator		X
FTP Data Transfer		X	TMonNET Responder		X
FTP server		X	TMon SQL		X
FX8800		X	Trip Dial-Up	X	
Granger Interrogator		X	X 25 Audit		X
Halted	X				

## Remote Port Parameter Defaults

Parameter	Default Value
Port usage	: HALTED
Baud	: “Blank” (Unassigned)
Parity	: “Blank” (Unassigned)
Word Length	: “Blank” (Unassigned)
Stop Bits	: “Blank” (Unassigned)

## Ping Interrogator

The Ping Interrogator monitors basic IP connectivity. The Ping Interrogator can be used to ping any IP aware device, such as servers, routing equipment, etc.

You can only have one remote port configured for ping interrogation.

To prepare a T/Mon to utilize the Ping Interrogator, perform the following steps.

1. Go to Parameters/Remote ports. Navigate to Job (Remote) 28. This job should already have its port usage set to "Ethernet I/O." Press F1 to open the Ethernet TCP Port Definition screen. Add an entry of type ICMP. Set the entry's TCP Port to an ID number 1-65535 (this can be any arbitrary value, usually a number such as 9000, and simply identifies the process that is ping-ing).

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	ICMP.....		9000	Ping Interrogator
2				
3				
4				TCP (T/GrafX, T/RemoteW, HTTP, RAS, FTP Server, TMonNet)
5				TELNET-RAW (ASCII, Craft, E-Mail, FTP Data Transfer)
6				TELNET (ASCII, CRAFT : if TELNET negotiation required)
7				UDP (DPS RTU Polling, SNMP TRAP Processing, SNMP Agent)
8				ICMP (PING)
9				
10				
11				
12				
13				
14				
15				
16				
17				

Fig. 9.2 - Ping Interrogator TCP Port Definition screen

2. Navigate to any unused job (Remote) 30 or higher.
3. Press "E" to choose the Edit command and set the job's port usage as "Ping Interrogator." Set Timeout to a value between 200 and 9999 milliseconds - an alarm will be declared if a PING response is not received in this time. A suggested initial value is 1000 (1 second), but this may need to be adjusted for optimum performance on your network. If you are failing to receive a ping response, try increasing this value. Also verify that you can ping the device from another PC.

The Ping Interrogator can access 15 displays of 64 points each, for a total capacity of 960 devices that can be pinged.

4. Press F6 to assign the TCP port entry that was defined under Step 1.
5. Press F1 to assign the devices to be pinged. Address will usually be 1. You will need 1 display for every 64 IP addresses that you will be pinged, which can be entered as one or more numbers 1-15 separated by commas or hyphens. You can usually accept defaults for other entries on this screen.



Fig. 9.3 - Ping Interrogator port usage screen

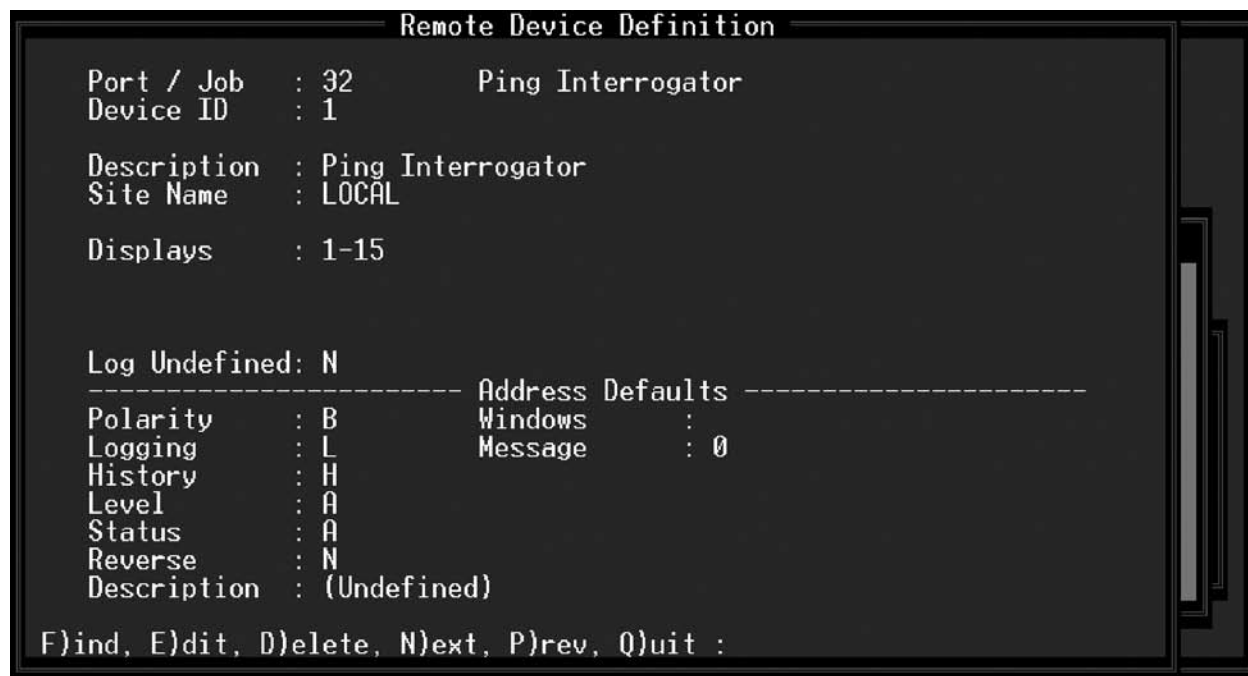


Fig. 9.4 - Ping Interrogator Device Definition screen

Remote Device Definition				
Port / Job	: 32	Ping Interrogator		
Device ID	: 1			
Ping Definitions				
Descr Site	Display : 1			
Displ	Point	IP Address	Description	Interval
	1	126.10.220.1	Gateway	60
Log U	2	.....		
-----	3			
Polar	4			
Loggi	5			
Histo	6			
Level	7			
Statu	8			
Rever	9			
Descr	10			
Enter the IP address to ping (XXX.XXX.XXX.XXX)				
F3=Blank, F8=Save, F10/Esc=Exit				

Fig. 9.5 - Ping Interrogator Definitions screen

An alarm is generated if a device fails to respond to a single ping. If this creates nuisance alarms for you, set the alarm qualification time to 2.5 to 3.5 times the frequency. This is done in the Point definition screen, F1=Pnts.

- Press F2 to assign IP addresses. On the PING definition screen enter each address to be pinged, a brief description, and an interval in seconds (15-900) between pings.
- Press F1 to assign corresponding alarms. Use the same display and point number for each IP address that you assigned in Step 6.
- Initialize the system and go to Monitor mode. PING alarms should now be active, and can be tested by disconnecting or disabling the various devices on your network.

Table 9.E - Fields in the Ping Definitions screen

Field	Description
IP Address	Enter the IP address of each device to be pinged. Range is 000.000.000.000 to 255.255.255.255.
Description	Enter a description of the device being pinged. (A similar description should be entered in the point description as well.)
Interval	Interval in seconds (15-900) that the device is pinged. <b>Recommended:</b> 60 = 1 min or 300 = 5 min.

**Caution:** Do not set the ping frequency too low, especially with a large number of devices, or the network may become severely bogged down.

## Craft Interface

**Note:** Refer to the Craft Mode sub-section in Section 16 (Monitor Mode) for more information on accessing Craft Mode from T/MonXM Monitor Mode.

Using the Craft Mode the T/MonXM can access an ASCII port, or any other port, on a remote device for troubleshooting and configuration. In addition, any remote terminal (T/Remote, T/Windows, laptop, etc.) can access the same devices through the T/MonXM. In this mode the T/MonXM or remote terminal operate as a dumb terminal. Example: A DPS DPM reports an alarm on a PABX it is monitoring. A technician is paged and requires more detail about the alarm from the PABX. The ASCII port on the PABX can be connected to the technician's laptop computer through T/MonXM's Craft Mode Interface.

Pressing Ctrl-F7 from the Alarm Summary Monitor mode screen will allow you go into Craft Mode from either the Main terminal or a Remote terminal — see Craft Mode sub-section in Section 16 (Monitor Mode) for more information. From the Craft Interface Mode window you will be able to select from a list of Craft terminals or ASCII ports. The Main terminal or T/Remote will be connected to the terminal of the port that you pick. You can at that time, send and receive from the Craft Mode Dialog window.

Selecting the Craft Interface port usage displays the associated fields which are explained in the table below. A prompt line at the bottom of the window list the choices for each field.



Fig. 9.6 - Define a remote port job for Craft Interface

**Table 9.F - Fields in the remote parameters screen, craft interface usage**

Field	Description
Port Usage	The Port Usage shows the selected port usage option. Refer to Table 9.B for a complete list of all standard and optional usages.
Serial Format	Baud rate, parity, word length, and stop bits settings that T/MonXM will use to communicate with the equipment.
Handshaking	The Handshaking field allows the user to select the type of communicate handshaking that the equipment is using to communicate. Valid entries are N (None), X (Xon/Xoff) and R (Rts/Cts). [N]
Craft Description	This field is optional and allows you to simply enter a 30 character description for the port and the device that it is communicating with.
Full Duplex	Determines whether the terminal operates in Full Duplex mode. When Full Duplex mode is active, characters typed on the keyboard are assumed to be echoed back to the screen by the terminal device. Valid entries are Y (full duplex) or N (half duplex). [Y]

**Table 9.G - Key commands available in the Remote Parameters Screen, craft interface usage**

Field	Description
F5	Allows you to suspend use of this port without loss of configuration data. Toggles the suspension state. Available only when cursor is on the prompt line at the bottom of the window.
F6	Data Connection
Up Arrow	Move to the previous field.
F8	Save.
F9	Help.
F10/Esc	Move to the first field or exit without saving (depending on which field the cursor is in).
Tab	List port usage (while cursor is in the Port Usage field.)



## Network Time (NTP)

Network Time Protocol is available as a virtual job on Remote Ports numbered 48 or higher. An NTP job requires a UDP data connection. Typically, you should do Port | Job 23 as that is the port to be used

Now you can update the T/MonXM system clock using Internet Network Time Protocol servers at regular definable intervals.

The United States Naval Observatory provides a list of public Internet Network Time Protocol (NTP) servers at <http://tycho.usno.navy.mil/ntp.html>. Consult your network administrator for information about using an NTP server with your network.

**Note:** AZ is in the Mountain Time Zone and does not observe DST.



**Fig. 9.7 - Network time port usage**

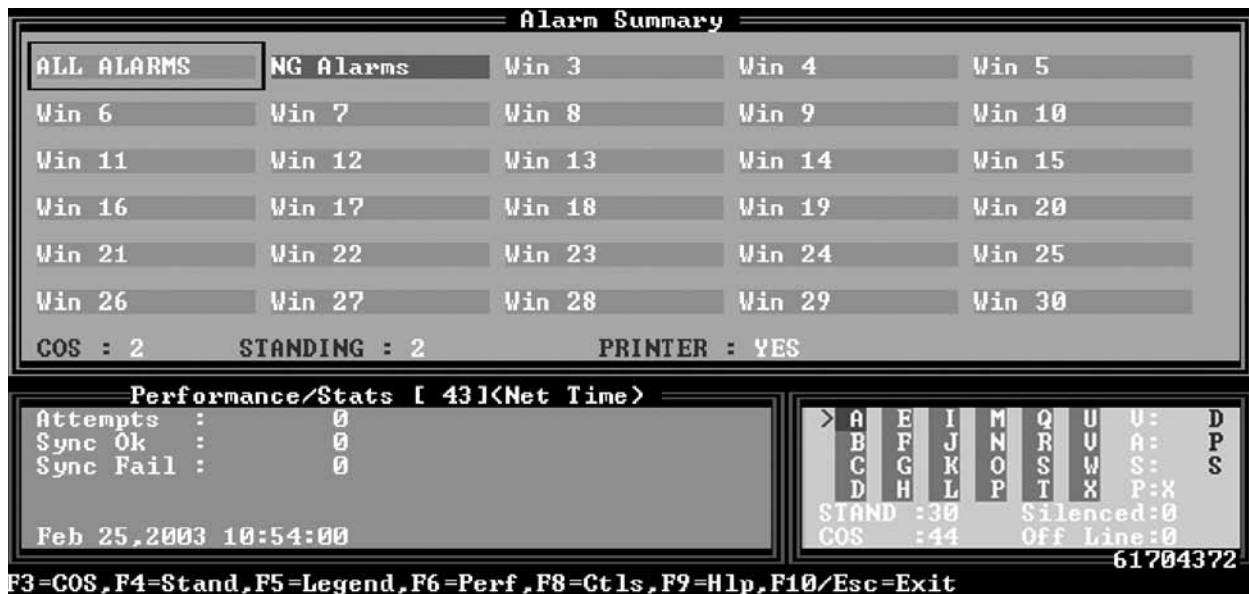
**Table 9.H - Fields in the Remote Parameters Screen, Network Time usage**

Field	Description
Server IP Address	IP Address of your network time server.
Day to Check	Select everyday or a day of the week to check the network time server. Use the Tab key to display the choices. Highlight a choice and press Enter.
Time to Check	This field selects the time of day to check the network time server. Type in time (0:00 to 23:59) and press Enter.
Zone Offset	Select your time zone as an offset of UST. Use the Tab key to display pre-calculated values for U.S. time zones. For time zones not listed type in the factor (-11 to 12) and press Enter.
Observe DST	Daylight Savings Time. If Daylight Savings Time is observed, selecting Y will cause T/MonXM to automatically adjust the internal clock at the appropriate time. Select N for no DST adjustment.  <b>Note:</b> If set to 'Yes', a local RTC process will adjust the local time every 2 hours if needed up to 10 days after the DST dates. This will make sure that the local time will be adjusted even if NTP hasn't synced yet.

**Table 9.1 - Key commands available in the Remote Parameters Screen, Network Time usage**

Field	Description
F5	Allows you to suspend use of this port without loss of configuration data. Toggles the suspension state. Available only when cursor is on the prompt line at the bottom of the window.
F6	Data Connection
Up Arrow	Move to the previous field.
F8	Save.
F9	Help.
F10/Esc	Move to the first field or exit without saving (depending on which field the cursor is in).

In Monitor Mode the Performance/Stats for the NTP job can be viewed along with the local time and date.

**Fig. 9.8 - Network time performance statistics**

Performance/Stats Description:

Attempts: Number of attempts made at synchronizing time with NTP Server.

Sync Ok: Number of successful attempts at synchronizing time with NTP Server.

Sync Fail: Number of failed attempts at synchronizing time with NTP Server.

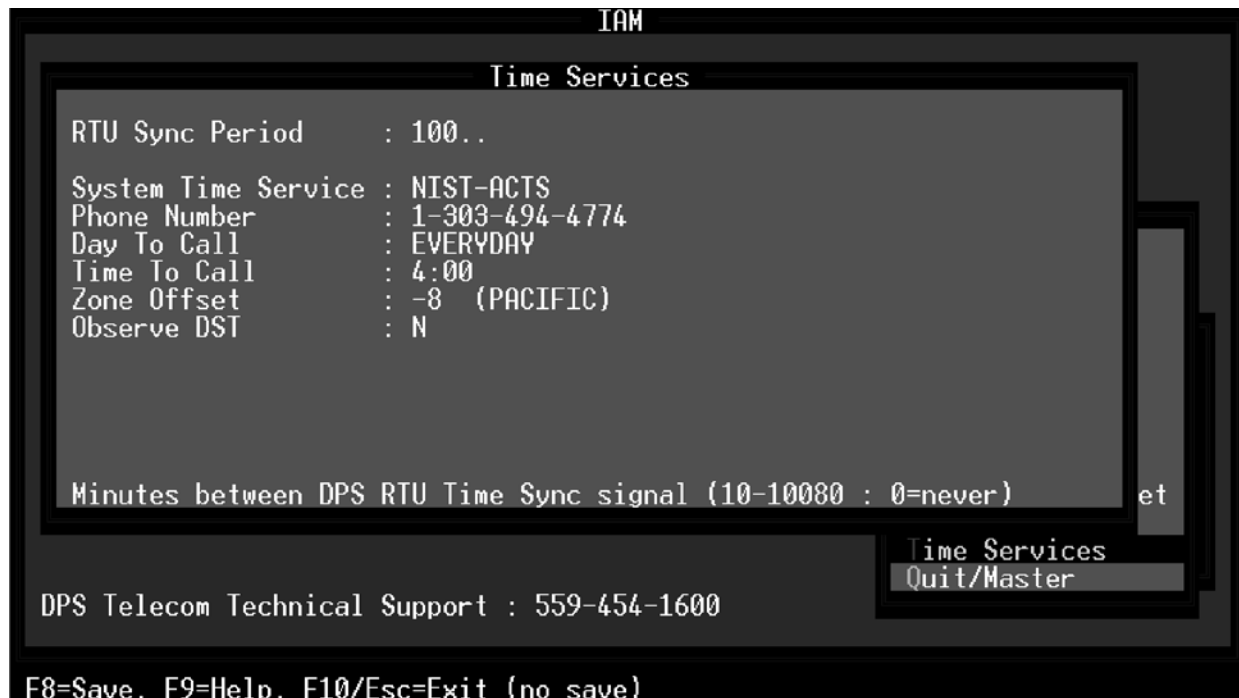
## Time Service

**Note:** Dial-up Time Service cannot be used in conjunction with Network Time Protocol.

The Time Service function causes T/MonXM to periodically dial the National Institute of Standards and Technology's (NIST) Automated Computer Telephone Service in Denver, Colorado, to update the system clock. This feature uses the pager port. Be sure pager parameters have been set in Remote Ports and in the Pager sub-section of the File Maintenance section.

Table 9.I lists the screen options for the Time Service screen.

**Note:** Table 9.I continues on following page.



**Fig. 9.9 - The Time Service window**

**Table 9.J - Fields in the Time Service screen**

Field	Description
RTU Sync Period	The number of minutes between automated synchronization of certain clock-enabled DPS Remote Telemetry Units. (10-10080, 0 = never) <b>Note:</b> RTU Sync period will synchronize RTU times with or without the System Time Service enabled.
Service	This field selects whether to use time service. Use the Tab key to display the choices. Highlight a choice and press Enter. NONE returns you to the Parameters menu. NIST-ACTS turns the feature on and move the cursor to the next field. [NONE]
Day to Call	Select daily or a day of the week to call time service. Use the Tab key to display the choices. Highlight a choice and press Enter.
Time to Call	This field selects the time of day to call time service. Type in time (0:00 to 23:59) and press Enter.
Zone Offset	This field is for the correction to apply to the UTC-based time transmitted by NIST. Use the Tab key to display pre-calculated values for U.S. time zones. Highlight a choice and press enter. For time zones not listed type in the factor (-11 to 12) and press Enter.

**Table 9.K - Fields in the Time Service screen (continued)**

Field	Description
Observe DST	Daylight Saving Time. If Daylight Savings Time is observed, selecting Y will cause T/MonXM to automatically adjust the internal clock at the appropriate time. Select N for no DST adjustment. Note: This field is editable even when System Time service is set to NONE. When it is, this option will be used by a local RTC process that will adjust the local date and time for Daylight Savings Time. If NTP-job defined, the RTC process will use the setting from the NTP job instead.
Phone Number	This field defaults to 1 (303) 494-4774, which is the phone number for NIST-ACTS. A different number may be manually entered. If a different time service is selected be sure to correct the Zone Offset value as appropriate.]

**Table 9.L - Key commands available in the Time Service screen**

Function Key	Description
F8	Save
F9	On-line help.
F10/Esc	Return to first field, or exit without saving when cursor is in the last field.

# Section 10 - Point Definition Tutorial

---

## Introduction

This Section provides you with many helpful tips and shortcuts for preparing the alarm point definitions in your T/MonXM database. Suggested Routines in sub-section 1.0 outlines a quick method of database preparation based on the experience of many T/MonXM users. Editing Shortcuts in sub-section 2.0 lists all the editing functions and their associated “hot keys.” Special Operations in sub-sections 4.0 through 10.0 describe some editing procedures that use more complex series of steps. These features are only available by selecting the Range function (press F5) from the Point Definition screen — see sub-section 4.0.

---

## 1.0 Suggested Routines

### 1.1. Develop a Generic display

Evaluate your network for similarities in equipment and alarming characteristics (i.e.: number of doors, environmental sensors, power source and backup, security devices) at each site. Try to develop a generic alarm display for each major piece of equipment (up to 64 alarms) and for a typical site. List those alarm points that are used at every location at the front of the display, those that are less common next and leave the last part of the display open for later addition of unique alarms. Leave a few blank points within the display for insertion of additional alarms (example: skip 2 lines between door alarms and fire alarms for insertion of additional door alarms.) A generic display should be designed for the location that has the most alarms, then they can be eliminated for the locations that have fewer alarms.

**Note:** When developing displays for equipment with embedded protocol, such as TBOS, alarms may be preassigned in the equipment. Check equipment manuals for alarm assignments before proceeding.

### 1.2. Create the Generic display

- 1.1. 2. Develop a generic point (line), such as that illustrated in Figure 10.2.
- 1.2.2. Enter the line as point 1.
- 1.2.3. Copy the line to the total range of points\* to be used. Use the procedure in sub-section 6.0. (See Figure 10.3.)
- 1.2.4. Change any column entries for individual points or ranges of points using the procedure in sub-section 4.0. (See Figure 10.4.)
- 1.2.5. Modify descriptions using the procedure in sub-section 5.0. (See Figure 10.5, 10.6, Figure 10.7 and Figure 10.8.)
- 1.3. Clone the display using the procedure in sub-section 8.0.
- 1.4. Modify each clone as required using the procedures outlined in sub-sections 4.0 through 8.0.

## 2.0 Point Editing

1.5. Repeat process for other generic displays.

\*Ranges can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.

**2.1** The following are descriptions of the fields in the point editing area:

### **Pt**

The individual Alarm Point number. Note that there are 64 alarm points in one DCP(F) display.

### **Pol**

Polarity attribute. This specifies if the alarm point will show alarm on Change of State (COS screen). "B" - Alarm point is to be Bipolar (show both alarm and clear). "U" - Alarm point is Unipolar (show only on alarm failure).

### **Log**

Screen Logging attribute. "L" - Log alarms on the screen as well as to the printer (if Printer Logging is enabled, see Miscellaneous Parameters). "N" - Do not log alarms on the screen.

### **Hst**

History Logging attribute. "H" - Log alarms to the History file on the disk. "N" - Do not log alarms to the History file.

### **Lev**

Point Alarm Level. This specifies the priority of the alarm. Level "A" being the highest or "critical" priority. Valid values are A, B, C and D.

A = Critical

B = Major

C = Minor

D = Status

The default value for this parameter can be set by using the Parameters menu option (under the Misc. category).

### **Sts**

Status Point. Specifies if the alarm point is to be indicated as an [A]larm point or a [S]tatus point. When this point is masked off the action of the point coming and going will not affect the DPS relay card.

### **Rvs**

Reverse Attribute. Determines whether the point will be processed as "Not Reversed" or "Reversed" (for points that are reversed, a "0-state" is considered as failed and a "1-state" is considered clear). Not reversed is the default value.

### **Description**

An English description of the alarm point that will appear when the alarm fails or changes state. The width of the description field is 40 characters.

### **Fail**

This is the Fail Status Description. This will appear along with the alarm description when the alarm is in a failed state.

#### **Clear**

This is the Clear Status Description. This will appear along with the alarm description when the alarm is in a normal or cleared state.

#### **Windows**

Alarm Windows. Enter a value here if you desire the alarm point to appear in one of the Alarm Windows. Notice that alarms will always appear in the “All Alarms” window. Valid Values are 2-90 (expandable up to 720) alarm windows with the basic setup. Installation of Alarm Windows software modules will allow you to choose from more windows.

**Note:** You can assign a maximum of 8 separate alarm windows, with 3 digit window numbers, to a point. You can use the full 31 characters in the windows field to define a range of windows.

#### **Msg**

Text Message Number. Enter a value here if you desire to assign a Text Message/Pager Number to the alarm point. If no message is desired enter “0”. Pressing “N” will allow you to create a new text message. This message will be numbered as the next available text/message.

**Note:** Many different alarms can use the same standard Text/Message.

#### **Qual**

Enter the duration qualification for the alarm. The alarm will qualify only if it remains set for a period of time specified in the field. Set a value between 0 and 99 and a letter indicating the unit of time used. For more information, press F9 with the cursor is in the Qual field.

#### **Counter**

The Counter field qualifies an alarm when it occurs a specified number of times. Enter a qualification time as in the qual field followed by a slash and the number of occurrences necessary to qualify the alarm. (The maximum number of occurrences is 250.)

#### **Pager**

Enter the paging profile, 0-99.

#### **RootGroupID**

You may assign the alarm to a root group by inputting the ID of the root group in this field. Root Groups can be up to 12 characters long. There is no limit to the number of alarms that may be assigned to a root group.

#### **RGType**

An alarm belonging to a root group can be either a root alarm or a member alarm. If any root alarm in a group is set, it will silence any members.

## Point Definition Commands

While editing the Point Definitions Screen, you can access the “Line Edit Help Screen” for assistance on available editing keys by pressing “Ctrl-.H. The editing keys available are shown in Table 10.D.

The commands described in Table 10.A are for defining and editing point definitions. These commands are only available when your cursor is on the first field (Polarity field) in the entry.

**Table 10.A - Point Definition Commands for defining and editing**

Function Key	Command
F1	Goto Point
F3	Blank
F5	Range Functions
F6	Read
F8	Save
F9	Help
Alt-F3	Delete Point
Alt-F4	Insert Point
Alt-F5	Block Move
Alt-F6	Block Copy
F10/Esc	Exit

Each of these commands is described in the following text:

### **(F1) Goto Point**

This function allows the user to go directly to any point in the display currently being defined.

### **(F2) Desc**

This function allows the user enter the display description.

Note: Accepts current value and F10/Esc=Exit returns you to point editing.

### **(F3) Blank Point**

Deletes the attributes and english description for the current point.

### **(F5) Range Functions**

Allows the user to use several field editing features that greatly enhance point editing. Refer to sub-section 4.0-9.0 for more information.

Once the Range function is invoked, the following commands are available:

**DES** Description. Selects special description functions that work with the specified range. The following commands are available:

Set	Will prompt for a descriptive string and place that string in the specified range.
Prefix	Will ask for a descriptive and prefix it to the fields.



Insert	This will ask for a position value to indent into the description fields and then also a descriptive string. This string will then be inserted in the fields.
Append	This will ask for a descriptive string and append it to the fields.
Translate	This option will change target strings into desired replacement strings for the range specified.
<b>POL</b>	Polarity. Use to set the Polarity attributes for the range specified.
<b>LOG</b>	Logging. Use to set the Logging attribute for the range specified.
<b>HST</b>	History. Use to set the History attribute for the range specified.
<b>LEV</b>	Alarm Level. Use to set the alarm priority level attribute for the range specified.
<b>STS</b>	Status Point. Specifies if the alarm point is to be indicated as an “A”larm point or a “S”tatus point.
<b>RVS</b>	Reverse. Used to set the Reverse attribute for the range specified.
<b>WIN</b>	Window. Use to set which alarm windows the alarms will be logged to for the range specified.
<b>MSG</b>	Message. Use to assign the text message number for the range specified.  fai (fail column) clr (clear) qua (qualification) aux (auxiliary) pag (pager) cou (counter)
<b>RANGE</b>	Will prompt the user to specify the range parameters to be involved in the editing process. The following range parameters are acceptable:
<b>COPY</b>	Copy Point. This will ask for the point to be copied and then the range of points to copy it to. The range will default to previously set range parameters.

Table 10.B - Acceptable Range Parameters

Range Field Entry	Points Specified
30	30
5-10	5, 6, 7, 8, 9, 10
20-30,35,37	20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 35, 37

**(F6) Read**

The Read function is very powerful because it allows “reading in” the point definitions from an existing display (Source) into another display (Target). This powerful function will save you time because it will eliminate the necessity of re-entering already defined data.

You are able to access data created from any device that the point definition data never changes. For example, to get data from a source display to a target display you must do the following:

- 1) First, choose “Point” from the Remote Device Definition screen. From the Point Definition screen, enter the “Target” display you wish to create or update (such as Address 1, Display 5) and press <Enter>. Your “Target” display is the display in which you want to use the data.

**Note:** Make sure your addresses are defined on the DCP Address Definition screen.

- 2) Press “Edit” and then press the F6 key and you will be prompted for the following information:

**Address** The Address from which the point definitions are to be read.

**Display** The Display of the address from which the point definitions are to be read.

Enter the display data (such as Address 0, Display 4) from your “Source” display.

- 3) Finally, press <Enter> and your “Target” display will have the identical data you “Read In” from the “Source” display.

**(F8) Save**

Saves any and all changes to the point definitions.

**(F9) Help**

Brings up the Help screen that explains these commands.

**(Alt-F3) Delete Point**

This command will delete the point definition that the cursor is currently on and cause all points below it to move up one position.

**(Alt-F4) Insert Point**

This command causes points under the current cursor position to move down one position so that a new point definition can be added. The last point will roll off the end of the definition list.

**(Alt- F5) Block Move**

The Block Move command will ask for a Start point, End point, and a Destination point with which it will move (Cut) this block of point definitions and place it (Paste) in another location within the point definitions list. This then sets the default range to the destination area.

For example, a Start point of 7 and a End point of 10 with a Destination point of 17 will change the default range to points 17 - 20. After selecting the block move function (press “Alt-F5”) the

following screen will appear.

**Note:** The selected destination block must be large enough to receive the entire source block. (For example, the block starting at point 1 and ending at point 10 could not be moved to a block starting at point 60 since there are only 5 positions available beginning at point 60.) This rule also applies to Block Copy.

The parameters for the Block Move screen are defined below:

```

      BLOCK MOVE

START POINT      :  ..
END POINT       :
DESTINATION POINT :

Enter starting point (1-64)
  
```

Fig. 10.1 - Block Move screen

Table 10.C - Parameters for the Block Move screen

Prompt	Meaning
Start Point	The first point of the block to be moved.
End Point	The last point of the block to be moved.
Destination Point	The start of the new location for the block.

#### (Alt-F6) Block Copy

The Block Copy command will ask for a Start point, End point, and a Destination point with which it will copy this block of point definitions and place it in another location within the point definitions list. This then sets the default range to the destination area just as Block Move does.

**Note:** Block Copy is just like Block Move except that points in the source block are only changed if they're overwritten by the action of the copy itself. (Whereas with Block Move, all of the points in the source block will be either blanked or overwritten).

## Address Defaults

The fields shown below are “Address Defaults” at the bottom of the Remote Device Definition screen. These are “values” that will be used as the defaults for undefined points that come into the alarm.

### **Polarity**

Enter B=Bipolar, or U=Unipolar.

### **Logging**

Enter L=Log, or N=No log.

### **History**

Enter H=History, or N=No history.

### **Level**

Enter default alarm level A, B, C, D.

### **Status**

Enter A=Alarm, or S=Status.

### **Reverse**

Enter R=Reverse, or N=No Reverse.

### **Description**

Enter default point description.

### **Windows**

Enter default windows with the basic setup. Installation of Alarm Windows software modules will allow you to choose from more windows. 8 windows maximum can be assigned here.

### **Message**

Enter the message number. Enter “0” for no message. The maximum messages available are limited by the number of messages in the message file.

## 3.0. Editing Shortcuts

The procedures and tips outlined here apply to point definition for all protocols.

3.1. Key commands used to edit the current field are listed in Table 10.A

3.2. Keys used to move between fields are listed in Table 10.E.

**Table 10.D - Field Editing Key Commands**

Key	Function
BackSpace Arrow	Backspace and delete
Ctrl-R	Restore Default
Ctrl-Z	Zap - Clear field (Does not work on T/Access)
Ctrl-E	Erase - Clear field
Left Arrow	Move left
Right Arrow	Move right
Ctrl-Home	Start of field
Ctrl-End	End of field
Ctrl-K	Kill to end of line
Del	Delete character
Ins	Toggle insert mode (cursor expands vertically)
Ctrl-Left Arrow	Move to previous word
Ctrl-Right Arrow	Move to next word

**Table 10.E - Vertical Editing Key Commands**

Key	Function
Ctrl PgUp	Move to previous defined entry, but the current field.
Ctrl PgDn	Move to next defined entry, but in the current field.
PgUp, PgDn	Up/Down to the next page with a defined entry
Home, End	Move to first or last page with a defined entry
Ctrl Enter	Save field and record
Ctrl F	Move to first field (no save)
Ctrl L	Move to last field (no save)
Ctrl Q	Save cursor position and insert mode (no save). (See sub-section 3.4.3.)

3.3. Additional key combinations that perform useful editing functions are listed in Table 10.F.

**Table 10.F - Point Editing Key Commands**

Function	Key	Description
<b>NOTE:</b> The following keys are available only when the cursor is on the first column field, "POL."		
Toggle	F4	Moves between the two halves* of the point definition screen
Blank	F3	Deletes the contents of a line, leaving the line blank. (Figure 1)
Range	F5	To activate the line and column editing functions — see sub-section 4.0.
Read	F6	Copy an entire display to some other port, address and display location in the database. The display can then be further edited in the new location. (Original display is left intact.) (sub-section 8.0)
Delete	Alt-F3	Deletes the contents of a line and moves all lines below it up one position. (Figure 1)
Insert	Alt-F4	Moves all lines under the cursor and below, down one position, leaving an open line. (Figure 1) <b>Note:</b> The 64th point configuration will be deleted and replaced with the 63rd point configuration.
Block Move**	Alt-F5	Move a block of point lines. A box will appear for specifying the start and end lines of the block and the destination line for the new start position. The start and end lines will be left blank after the move.
Block Copy**	Alt-F6	Copy a block of point lines. A box will appear for specifying the start and end lines of the block and the destination line for the new start position. The start and end lines will be left intact after the move.
Extended Read*	Ctrl-F6	Copy selected portions of a display to some other port, address and display location in the database. The display can then be further edited in the new location. (Original display is left intact.) (sub-section 8.0)

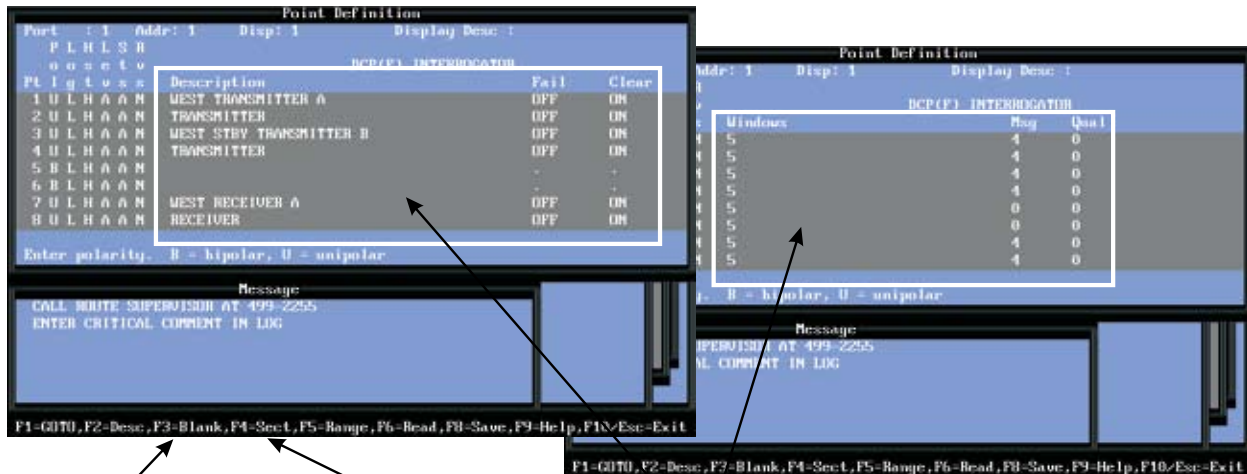
\*If the Auxiliary Description is turned on, (in the Miscellaneous Parameters screen) there will be three parts to the screen. Press F4 to move through the three parts.

\*\*These two functions automatically set the range for the "SET ATTR" functions (sub-sections 4.0 through 8.0).

### 3.4. Vertical Editing

- 3.4.1. Vertical editing is available in the point editing mode via the Ctrl-PgUp and Ctrl-PgDn keys.
- 3.4.2. The Ctrl-PgUp and Ctrl-PgDn key combinations move the cursor up and down the point list, within the same field. No matter where in the field the cursor is located, it will move to the start of the same field in the adjacent line when Ctrl-PgUp or Ctrl-PgDn is used.
- 3.4.3. If Ctrl-Q is pressed first, the cursor will remain on the same character position in the field when Ctrl-PgUp or Ctrl-PgDn is used. Once Ctrl-Q is invoked, the cur-

sor will return to the specified character position when Ctrl-PgUp or Ctrl-PgDn is used. The position can be changed by moving the cursor with the left and right arrow keys and pressing Ctrl-Q. The cursor will then use the new position until again changed, the field is exited or the editing function is exited



F3 Blanks a line

Alt-F3 Deletes a line

Alt-F4 Inserts an open line

F4 moves between the two or three sections of the Point Definition Screen

**Fig. 10.2 - F3 blanks a line, F4 toggles the screen view**

## 4.0. Point (Line) Editing

4.1 Pressing F5 (Range) opens a sub-menu for point (line) editing functions. These functions allow a full display of point attributes and descriptions to be quickly defined by copying common elements from one point to another. Before the editing functions can be used at least one full point (line) must be defined. Editing functions are started by entering them in a SET ATTR field at the bottom of the window. The editing functions are listed on the prompt line.

## 5.0. Point (Line) Copying

5.1. The copy function copies all attributes from one specified point to other specified points (lines) within the same display.

5.1.1. Press F5 to activate the line and column editing functions.

5.1.2. To copy a full point (line) definition from one point to one or more others type RAN (or R) in the SET ATTR field <ENTER>. (See Figure 10.2)

5.1.4. Type in the numbers\* of the points (lines) to be copied to (destination or target) <ENTER>.

5.1.4. Type COP (or C) for copy <ENTER>.

5.1.5. Type in the number of the point (line) to be copied <ENTER>. The point to be copied will appear on the

lines (range) specified.

\*Ranges can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.

1. Press F5 to activate the Line and Column Editing functions.

2. Type "R" in the SET ATTR field <ENTER>.

3. Type in destination/target points (lines) <ENTER>.

4. Type "C" to specify the Copy function <ENTER>.

5. Type "1" to copy point (line) 1 <ENTER>

The active Range is displayed in the "Range" field

The entries for point 1 have been copied to points 2, 3, 4, 7, 8, 9, 10, 24, 25, 26 and 27.

Port	Addr	Disp	Display Desc	Fail	Clear
1	B L H A A N	TRANSMITTER	OFF	ON	
2	B L H A A N	TRANSMITTER	OFF	ON	
3	B L H A A N	TRANSMITTER	OFF	ON	
4	B L H A A N	TRANSMITTER	OFF	ON	
5	B L H A A N	TRANSMITTER	OFF	ON	
6	B L H A A N	TRANSMITTER	OFF	ON	
7	B L H A A N	TRANSMITTER	OFF	ON	
8	B L H A A N	TRANSMITTER	OFF	ON	
9	B L H A A N	TRANSMITTER	OFF	ON	
10	B L H A A N	TRANSMITTER	OFF	ON	
24	B L H A A N	TRANSMITTER	OFF	ON	
25	B L H A A N	TRANSMITTER	OFF	ON	
26	B L H A A N	TRANSMITTER	OFF	ON	
27	B L H A A N	TRANSMITTER	OFF	ON	


Fig. 10.3 - The Line Copy function copies a selected source line to multiple target lines



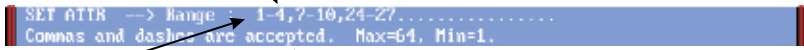
## 6.0. Column (Attribute) Entry

- 6.1. Press F5 (Range).
- 6.2 To enter any attribute (column entry) into several points (lines) at once type RAN (or R) in the SET ATTR field <ENTER>. (See Figure 10.4)
- 6.5. Type in the numbers of the points (lines) to be entered into (destination or target) <ENTER>. These can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.
- 6.4. Type in the abbreviation for the desired attribute (column). (pol, log, hst, lev, sts, rvs, msg, fail, clear or qual.) <ENTER>
- 6.5. Type in the characters to be entered in that attribute (column) <ENTER>. The characters will appear in the column designated.


1. Press F5 to activate the Line and Column Editing functions.




2. Type "R" in the SET ATTR field <ENTER>.



3. Type in destination/target points (lines) <ENTER>.



4. Type "P" to copy the "pol" column (or substitute appropriate character) <ENTER>.



5. Type "U" for character to be entered in column (or substitute appropriate character) <ENTER>.

The active Range is displayed in the "Range" field

The value "U" has been entered in the "pol" column for points 1, 2, 3, 4, 7, 8, 9, 10, 24, 25, 26 and 27.




Fig. 10.4 - The Column Entry Function enters a value in a range of target columns

## 7.0

# Description Modification

Be sure to use a unique pattern to prevent unwanted results.

- 7.1. Press F5 (Range). Description modification: You can add to, delete from or change the Description over a range of points. To modify the description type RAN (or R) in the SET ATTR field <ENTER>. (See Figure 10.4)
  - 7.1.1. Type in the numbers\* of the points (lines) to be modified <ENTER>.
  - 7.1.2. Type in DES (or D) <ENTER>.
  - 7.1.3. Type in the 3 letter abbreviation for the desired option (options are listed at the bottom of the window) <ENTER>.
    - 7.1.3.1. Type SET (or S) <ENTER> to change the entire description. Type in description (1 to 40 characters) <ENTER>.
    - 7.1.3.2. Type PRE (or P) <ENTER> to add something in front of the description. Type in the prefix (1 to 40 characters) <ENTER>. (See Figure 10.5)
    - 7.1.3.3. Type APP (or A) <ENTER> to add something at the end of the description. Type in the suffix (1 to 40 characters) <ENTER>. (See Figure 10.8)
    - 7.1.3.4. Type TRA (or T) <ENTER> to change a pattern of characters. Type in the characters to be changed (target) <ENTER>. Type in the characters to be inserted (replacement) <ENTER>. (See Figure 10.7)
    - 7.1.3.5. Type INS (or I) <ENTER> to add something within the description. Type in the position number (1-40) <ENTER>. This is the character position where the insert will begin. All text past this point will be moved to the right of the inserted text. Type in the string to be inserted (1 to 40 characters) <ENTER>. (See Figure 10.8)

\*Ranges can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.

**Note:** Modifications can be done only to lines that are already defined.

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

## PREFIX

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

1. Press F5 to activate the Line and Column Editing functions.

2. Type "R" in the SET ATTR field <ENTER>.

3. Type in destination/target points (lines) <ENTER>.

NOTE: If you have just completed a description modification function without exiting, you will be starting here.

4. Type "D" to specify the Description Modification function <ENTER>.

5. Type "P" to add a prefix <ENTER>.

6. Type character to be prefixed (include space at end, if appropriate) <ENTER>.

The active Range is displayed in the "Range" field

The prefix "WEST" has been added to the descriptions for points 1, 3, 7, 9, 10, 24, and 26.

**Point Definition**

Port	Addr	Disp	Display Desc	Fail	Clear
1	B L H A A N		TRANSMITTER	OFF	ON
2	B L H A A N				
3	B L H A A N				
4	B L H A A N				
5	B L H A A N				
6	B L H A A N				
7	B L H A A N				
8	B L H A A N				

SET ATTR --> Enter Attribute or Special Option Abbreviation : R..  
des,pol,log,hst,lev,sts,rvs,win,msg,fai,clr,qua,aux,Range,Cong

SET ATTR --> Range : 1,3,7,9,24,26.....  
Commas and dashes are accepted. Max=64, Min=1.

SET ATTR --> Enter Attribute or Special Option Abbreviation : D..  
des,pol,log,hst,lev,sts,rvs,win,msg,fai,clr,qua,aux,Range,Copu

Description --> Enter Option : P..  
Set,Prefix,Insert,Append,Translate,Range

Description --> Prefix : WEST .....  
Enter Prefix

**Point Definition**

Port	Addr	Disp	Display Desc	Fail	Clear
1	B L H A A N		WEST TRANSMITTER	OFF	ON
2	U L H A A N		TRANSMITTER	OFF	ON
3	U L H A A N		WEST TRANSMITTER	OFF	ON
4	U L H A A N		TRANSMITTER	OFF	ON
5	B L H A A N				
6	B L H A A N				
7	U L H A A N		WEST TRANSMITTER	OFF	ON
8	U L H A A N		TRANSMITTER	OFF	ON

Description --> Enter Option : P..  
Set,Prefix,Insert,Append,Translate,Range

**Fig. 10.5 - Add a PREFIX to selected point descriptions with the Description Modification Function**

## APPEND

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

## WHILE STILL IN THE EDITING FUNCTION

1. Change Range for points (lines) to be appended <ENTER>.

NOTE: If you have just completed a description modification function without exiting, you will be starting here.

```
SET ATTR --> Range : 1,7,24.....
Commas and dashes are accepted. Max=64, Min=1.
```

```
SET ATTR --> Enter Attribute or Special Option Abbreviation : D..
des,pol,log,hst,lev,sts,rvs,win,msg,fai,clr,qua,aux,Range,Comp
```

2. Type "D" to specify the Description Modification function <ENTER>.

```
Description --> Enter Option : A..
Set,Prefix,Insert,Append,Translate,Range
```

3. Type "A" to add (append) a suffix <ENTER>.

```
Description --> Append : A.....
Enter characters to append
```

4. Type character to be appended (include space before, if appropriate) <ENTER>.

The active Range is displayed in the "Range" field

The suffix "A" has been appended to the descriptions for points 1, 7, and 24.

Point Definition									
Port	: 1	Addr	: 1	Disp	: 1	Display Desc :			
P L H L S R						Range : 1,7,24			
U S E T V						DCP(F) INTERROGATOR			
Pt	l	g	t	u	s	Description		Fail	Clear
1	B	L	H	A	A	N	WEST TRANSMITTER	OFF	ON
2	U	L	H	A	A	N	TRANSMITTER	OFF	ON
3	U	L	H	A	A	N	WEST TRANSMITTER	OFF	ON
4	U	L	H	A	A	N	TRANSMITTER	OFF	ON
5	B	L	H	A	A	N	.	.	.
6	B	L	H	A	A	N	.	.	.
7	U	L	H	A	A	N	WEST TRANSMITTER	OFF	ON
8	U	L	H	A	A	N	TRANSMITTER	OFF	ON
Description --> Enter Option : A..									
Set,Prefix,Insert,Append,Translate,Range									

Fig. 10.6 - Append a SUFFIX to selected point descriptions with the Append Function

TRANSLATION

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

**Hint:** This function is a very powerful and frequently used tool.

WHILE STILL IN THE EDITING FUNCTION

Description --> Range : 7-10.....  
Commas and dashes are accepted. Max=64, Min=1.

1. Change Range for points (lines) to be translated <ENTER>.

SET ATTR --> Enter Attribute or Special Option Abbreviation : D..  
des,pol,log,hst,lev,sts,rvs,uin,msg,fai,clr,qua,aux,Range,Copy

NOTE: If you have just completed a description modification function without exiting, you will be starting here.

2. Type "D" to specify the Description Modification function <ENTER>.

Description --> Enter Option : T..  
Set,Prefix,Insert,Append,Translate,Range

3. Type "T" to specify the Translate function <ENTER>.

Description --> Enter Option : T  
TRANSLATE Target : TRANSMITTER.....

4. Type in the Target character string "TRANSMITTER" <ENTER>.

Description --> Enter Option : T  
TRANSLATE Replacement : RECEIVER.....

5. Type in the Replacement character string "RECEIVER" <ENTER>.

The active Range is displayed in the "Range" field

The character string "RECEIVER" has replaced "TRANSMITTER" in the descriptions for points 7, 8, 9 and 10.

Point Definition

Port	: 1	Addr: 1	Disp: 1	Display Desc :
P L H L S R				Range : 7-10
o o s e t v				DCP(F) INTERROGATOR
Pt l g t v s s		Description	Fail	Clear
3 U L H A A N		WEST TRANSMITTER B	OFF	ON
4 U L H A A N		TRANSMITTER	OFF	ON
5 U L H A A N			.	.
6 B L H A A N			.	.
7 U L H A A N		WEST RECEIVER	OFF	ON
8 U L H A A N		RECEIVER	OFF	ON
9 U L H A A N		WEST RECEIVER	OFF	ON
10 U L H A A N		RECEIVER	OFF	ON
SET ATTR	-->	Enter Attribute or Special Option Abbreviation : ...		
des,pol,log,hst,lev,sts,rvs,uin,msg,fai,clr,qua,aux,Range,Copy				

Fig. 10.7 - TRANSLATE a character string in a range of to point descriptions with the Translate Function

**INSERT**

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

**WHILE STILL IN THE EDITING FUNCTION**

```
SET ATTR --> Range : 3,9,26.....
Commas and dashes are accepted. Max=64, Min=1.
```

1. Change Range for points (lines) to be inserted <ENTER>.

```
SET ATTR --> Enter Attribute or Special Option Abbreviation : D..
des,pol,log,hst,lev,sts,rvs,win,msg,fai,clr,qua,aux,Range,Comp
```

NOTE: If you have just completed a description modification function without exiting, you will be starting here.

2. Type "D" to specify the Description Modification function <ENTER>.

```
Description --> Enter Option : I..
Set,Prefix,Insert,Append,Translate,Range
```

3. Type "I" to specify the Insert function <ENTER>.
4. Type in the character position for the start of the string <ENTER>.

```
Description --> Pos : 6 String : STBY .....
Enter string to be inserted
```

5. Type in the character string to be inserted "STBY" <ENTER> (Include appropriate spaces).

The active Range is displayed in the "Range" field

The character string "STBY" has been inserted at character position 6 in the descriptions for points 3, 9 and 26.

Point Definition						
Port	: 1	Addr	: 1	Disp	: 1	Display Desc :
P L H L S R						Range : 3,9,26
o o s e t v						DCP(F) INTERROGATOR
Pt l g t v s s		Description		Fail	Clear	
3 U L H A A N	WEST	STBY TRANSMITTER B	OFF	ON		
4 U L H A A N		TRANSMITTER	OFF	ON		
5 B L H A A N			.	.		
6 B L H A A N			.	.		
7 U L H A A N	WEST	RECEIVER A	OFF	ON		
8 U L H A A N		RECEIVER	OFF	ON		
9 U L H A A N	WEST	STBY RECEIVER B	OFF	ON		
10 U L H A A N		RECEIVER	OFF	ON		
Description --> Enter Option : I..						
Set,Prefix,Insert,Append,Translate,Range						

**Fig. 10.8 - Insert a Character String in a Range of Point Description with the Insert Function**

## 8.0. Windows Modification

This function is typically used after cloning a site to change the site window designation. Using the DEL and ADD options allows the window designation to be quickly changed without disturbing the “severity,” “type” or other window designations.

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

**Note:** Modifications can be done only to lines that are already defined.

8.1. Windows modification: You can add to, delete from or change the Windows field over a range of points. Press F4 to see the “Windows” portion of the screen. Press F5 (Range). To modify the windows field type RAN (or R) in the SET ATTR field <ENTER>.

8.1.1. Type in the numbers\* of the points (lines) to be modified <ENTER>.

8.1.2. Type in WIN (or W) <ENTER>.

8.1.3. Type in the 3 letter abbreviation for the desired option (options are listed at the bottom of the window) <ENTER>.

8.1.3.1. Type SET (or S) <ENTER> to change the windows field over the range.

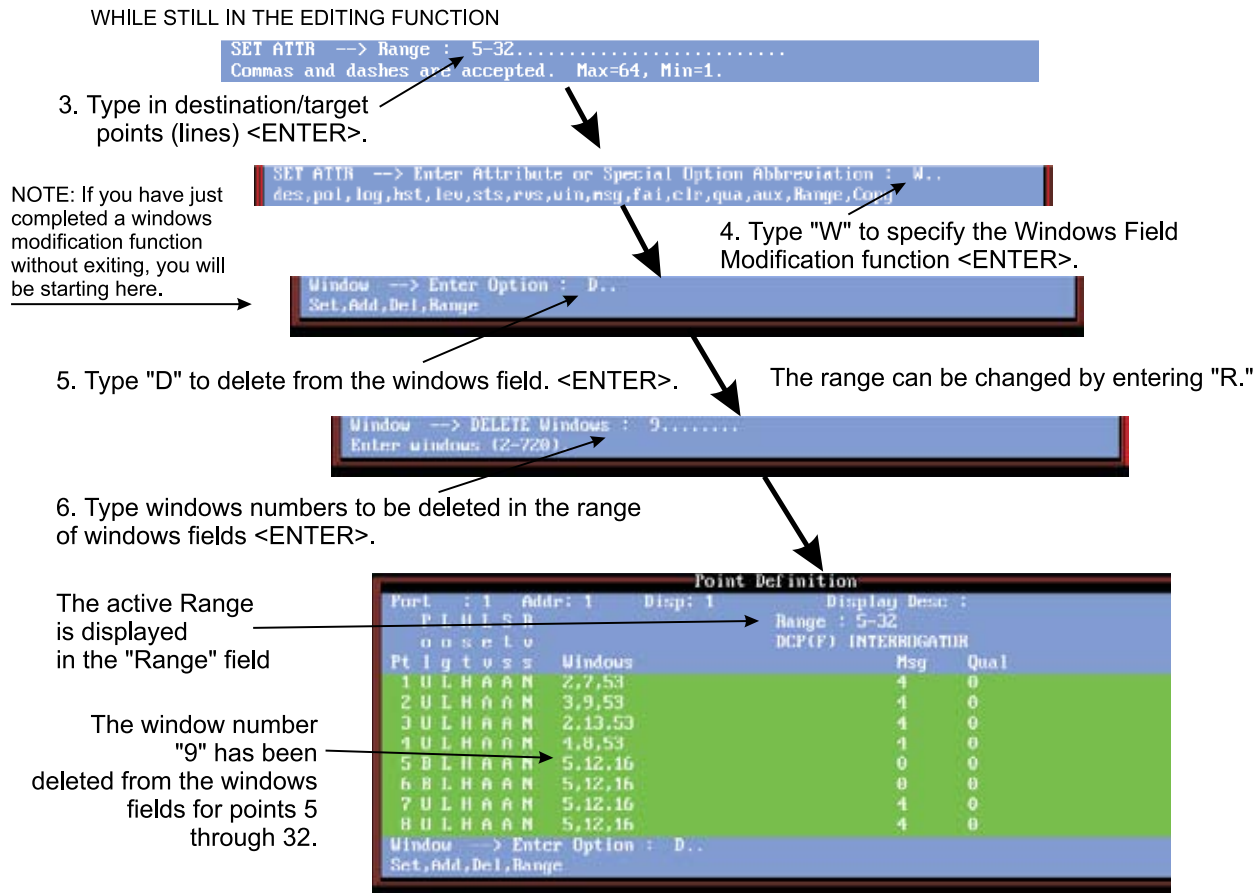
**Note:** this will replace everything that’s in the corresponding window with your new value. Set the corresponding window to your new value.

Type in window numbers <ENTER>. (2-90 or greater, depending on equipped options. There is a maximum of 8 windows per point.)

8.1.3.2. Type ADD (or A) <ENTER> to add something in the windows field over the range. Type in window numbers <ENTER>. (2-90 or greater, depending on equipped options. There is a maximum of 8 windows per point.)

8.1.3.3. Type DEL (or D) <ENTER> to delete something from the windows field over the range. Type in window numbers <ENTER>. (2-90 or greater, depending on equipped options. There is a maximum of 8 windows per point.) (See Figure 10.10)

\*Ranges can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.



**Fig. 10.9 - Add a window number(s) in a range of points with the Windows Modification Function**

## 9.0. Message Translation

This function is typically used after cloning a site to change the message field. Using the SET and TRANSLATE options allows the message number to be quickly changed.

Once a range is specified, all subsequent actions will apply to that range until the range is changed.

9.1. Message Translation: You can enter the same message number or translate a given message number (target) to another (replacement) in the Message field over a range of points. Press F4 to see the "Message" portion of the screen. Press F5 (Range). To modify the windows field type "R" in the SET ATTR field <ENTER>.

9.1.1. Type in the numbers\* of the points (lines) to be modified <ENTER>.

9.1.2. Type "M" <ENTER>.

9.1.3. Type in the first letter for the desired option (options are listed at the bottom of the window) <ENTER>.

9.1.3.1. SET: Type "S" <ENTER> to change the message field over the range. Type in message number <ENTER>. (from 0 to the maximum number of messages that have been defined.) The chosen message will be displayed in the message window. The prompt line will ask if you wish to continue. Type "Y" to accept or <ENTER> to reject.



\*Ranges can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.

9.1.3.2. TRANSLATE: Type “T” <ENTER> to change all target message numbers over the range to a replacement message number. Type in target and replacement numbers. NOTE: This function will affect only the lines within the range that contain the target message number.

9.1.3.3. RANGE: Type “R” <ENTER> to set a new range of points without leaving the message function.

\*Ranges can be individual points (1,3,5,10), continuous points (8-20) or a combination of individual and continuous points (1,5,8-12). Do not use spaces.

---

## 10.0. Cloning Entire Displays or Sites

- 10.1. An entire display can be copied from one display to another within the same address and port or to another address and/or port.
  - 10.1.1. The display to be copied (source) must be defined.
  - 10.1.2. Enter the destination (target) port, address and display:
    - 10.1.2.1. From the Main Menu select Parameters.
    - 10.1.2.2. Select Remote Ports.
    - 10.1.2.3. Select the destination port by using the P)revious, N)ext, or F)ind keys.
    - 10.1.2.4. Press F1 (Devices).
    - 10.1.2.5. Select the destination address by using the P)revious, N)ext, or F)ind keys.
 

**Note:** To create a new display, press F)ind and enter the appropriate display. T/Mon will prompt you to add the new display to the database. Press Y (yes) to save or Esc to cancel without saving.
    - 10.1.2.5. Press F1 (Points).
    - 10.1.2.6. Press E (Edit).
  - 10.1.3. Press F6 (Read).
  - 10.1.4. Enter the source port number (1-n or “RP, KI, and NG” for dial-up port), device number, address number and display number. (The cursor will skip fields that are not applicable to the type of port.)
  - 10.1.5. The specified source display will be copied to the screen. It may now be modified as needed, using the procedures outlined in sub-sections 4.0-8.0.

## 11.0. Cloning Part of a Display

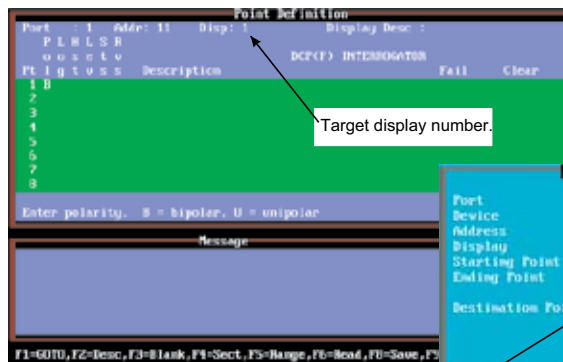
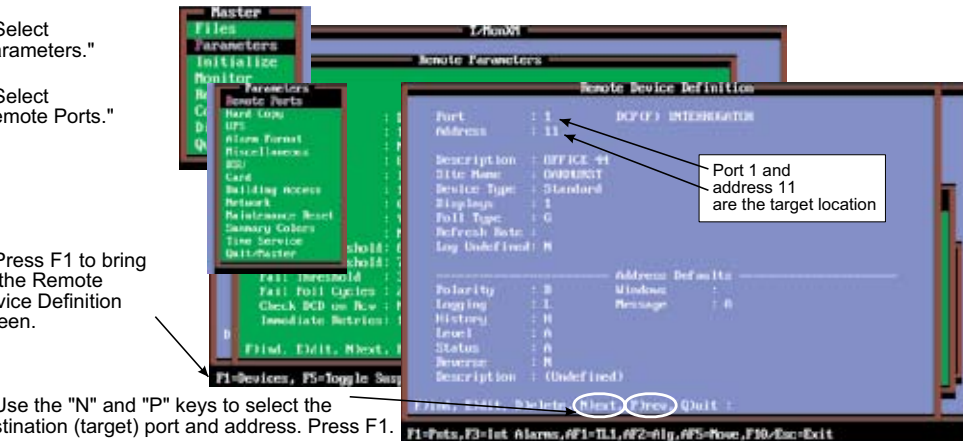
- 11.1. A portion of a display can be copied from one display to another within the same address and port or to another address and/or port. (See Figure 10.9) The advantage of this is that multiple parts of different displays can be quickly copied into a common display.
  - 11.1.1. The display to be copied (source) must be defined.
  - 11.1.2. Enter the destination (target) port, address and display:
    - 11.1.2.1. From the Main Menu select Parameters.
    - 11.1.2.2. Select Remote Ports.
    - 11.1.2.3. Select the destination port by using the P)revious, N)ext, or F)ind keys.
    - 11.1.2.4. Press F1 (Devices).
    - 11.1.2.5. Select the destination address by using the P)revious, N)ext, or F)ind keys.  
**Note:** To create a new display, press F)ind and enter the appropriate display. T/Mon will prompt you to add the new display to the database. Press Y (yes) to save or Esc to cancel without saving.
    - 11.1.2.6. Press F1 (Points).
    - 11.1.2.7. Press E (Edit).
  - 11.1.3. Press Ctrl-F6 (Extended Read).
  - 11.1.4. Enter the source Port number (1-n or “RP, KI, and NG” for dial-up port), Device number, Address number, Display number, Starting Point and Ending Point. (The cursor will skip fields that are not applicable to the type of port.)
  - 11.1.5. Enter the Destination Point number. (Point to place the source “Starting Point” in the target.)
  - 11.1.6. The specified source display will be copied to the screen. It may now be modified as needed, using the procedures outlined in sub-sections 4.0 through 9.0.

1. Select  
"Parameters."

2. Select  
"Remote Ports."

3. Press F1 to bring  
up the Remote  
Device Definition  
screen.

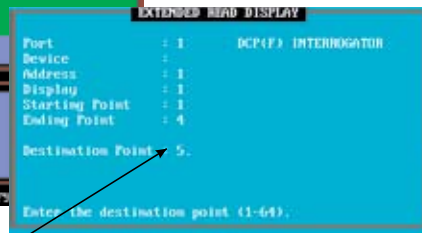
4. Use the "N" and "P" keys to select the  
destination (target) port and address. Press F1.



5. Press "E" to edit. Add target display  
number, if not already there. Press Ctrl-F6.

6. Enter the source port no. (1), address (1)  
display (1), Starting Point and Ending Point  
in the Read function fields. Enter the  
Destination Point (where to place the  
source "starting point.")  
Press <ENTER> after each entry.  
NOTE: The "Device" field is used only for ports  
defined for "DCM" protocol.

7. Point 1-4 definitions from the source  
display are entered in the target display,  
starting at point 5.

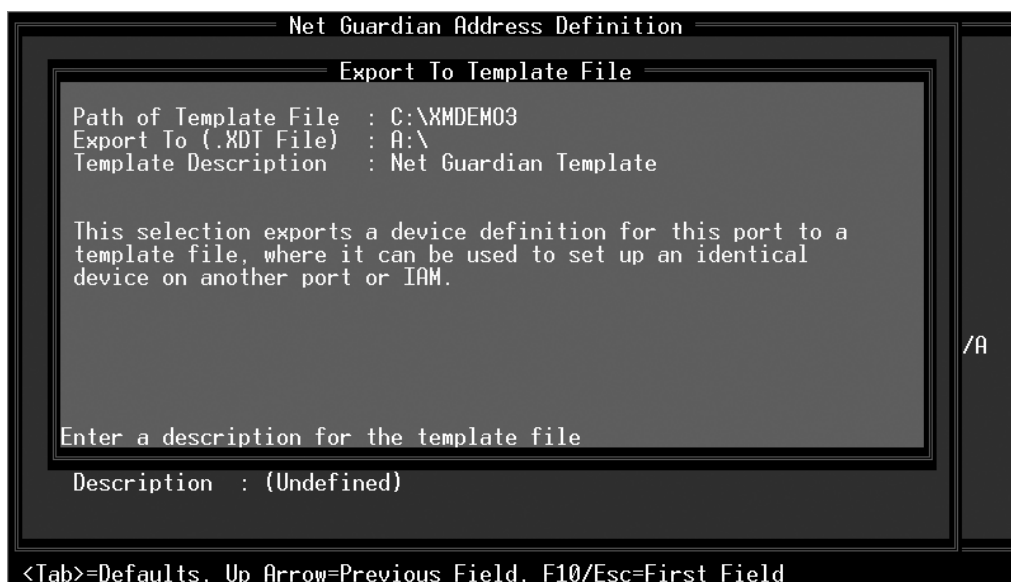


**Fig. 10.10 - A portion of a display can be copied to another port, address and display**

## 12.0 Device Templates

T/MonXM is the capability to create **device templates**, which can greatly speed the provisioning of KDAs, NetGuardians, and other devices.

Templates provide the ability to save device configurations and import that information into similar device profiles (available for dial-up and LAN devices). Once in the device configuration screen, hit Alt-F6 to bring up the Template Import/Export Menu. To export the devices' configuration into a template, select "Export to Template" and press Enter. Enter the path of the template file and the drive to export to. To import an existing template into a device, select "Import from Template" from the Template Menu and press Enter. Then enter the path of the template file and the drive where the file exists.



**Fig. 10-11 - Example of device templates use**

# Section 11 - DPS Display Mapping Guide

## Introduction

This section will assist you in determining the locations of alarms from remotes within the addressing and display scheme used by T/MonXM. Mapping varies with the device being used, so the section is organized with a different section for each device.

## NetGuardian 832A/ NetMediator

Tables 11.A and 11.B refer to display mapping for NetGuardian 832A and NetMediator remotes.

**Note:** NetMediator display mapping may differ, see your NetMediator user manual for more details.

**Table 11.A - Display mapping for the NetGuardian 832A/NetMediator**

Display	Points	Description
1	1-32	Discrete Alarms
2	1-32	Ping Alarms
3	1-4	Analog Channel 1
4	1-4	Analog Channel 2
5	1-4	Analog Channel 3
6	1-4	Analog Channel 4
7	1-4	Analog Channel 5
8	1-4	Analog Channel 6
9	1-4	Analog Channel 7
10	1-4	Analog Channel 8
11	Relays/Housekeeping (See detail in Table 11.B below)	
Displays 12-17 refer to the NetGuardian Expansion (NetGuardian DX)		
12	NetGuardian Expansion 1 Alarms 1-48	
13	Expansion 1 Relays 1-8	
14	NetGuardian Expansion 2 Alarms 1-48	
15	Expansion 2 Relays 1-8	
16	NetGuardian Expansion 3 Alarms 1-48	
17	Expansion 3 Relays 1-8	

**Table 11.B - Display Relays/Housekeeping Alarms for the NetGuardian 832A/NetMediator**

Points	Description	Points	Description
1	Relays	47	Modem RcvQ Full
2	Relays	48	Serial 1 RcvQ Full
3	Relays	49	Serial 2 RcvQ Full
4	Relays	50	Serial 3 RcvQ Full
5	Relays	51	Serial 4 RcvQ Full
6	Relays	52	Serial 5 RcvQ Full
7	Relays	53	Serial 6 RcvQ Full
8	Relays	54	Serial 7 RcvQ Full
17	Timed Tick	55	Serial 8 RcvQ Full
33	Power Up	56	NetGuardian DX 1 Fail
36	Lost Provisioning	57	NetGuardian DX 2 Fail
37	DCP Poller Inactive	58	NetGuardian DX 3 Fail
38	LAN Not Active	59	GLD 1 Fail
41	Modem Not Responding	60	GLD 2 Fail
42	No Dial Tone	61	GLD 3+ Fail
44	Pager Queue Overflow	62	Channel Port Timeout
45	Notification Failed	63	Craft Timeout
46	Craft RcvQ Full	64	Event Queue Full

## NetGuardian 216

Tables 10.C refer to display mapping for NetGuardian-216 SNMP remotes.

**Table 11.C - Mapping in NetGuardian 216**

Display	Description	Display	Points
Disp 1	Discrete Alarms and Controls	1	1-16
	Relays	1	17-18
	Undefined**	1	19-24
	Default Configurations	1	25
	Undefined**	1	26
	MAC Address Not Set	1	27
	IP Address Not Set	1	28
	LAN Hardware Not Found	1	29
	SNMP Processing Error	1	30
	SNMP Community Error	1	31
	LAN Tx Packet Drop	1	32

**Note:** Table 11.C continues on the following page.

\*\* “Undefined” indicates that the alarm point is not used.

**Table 11.C - Mapping in NetGuardian 216**

Display	Description	Display	Points
Disp 2	Analog 1 MjO	2	1
	Analog 1 MnO	2	2
	Analog 1 MnU	2	3
	Analog 1 MjU	2	4
	Undefined**	2	5
	Undefined**	2	6
	Undefined**	2	7
	Undefined**	2	8
Disp 3	Analog 1 MjO	3	1
	Analog 1 MnO	3	2
	Analog 1 MnU	3	3
	Analog 1 MjU	3	4
	Undefined**	3	5
	Undefined**	3	6
	Undefined**	3	7
	Undefined**	3	8

\*\* “Undefined” indicates that the alarm point is not used.

## NetGuardian- Q8

Tables 11.D and 11.E refer to display mapping for NetGuardian-Q8 remotes.

**Table 11.D - Display descriptions and SNMP Trap numbers for the NetGuardian-Q8**

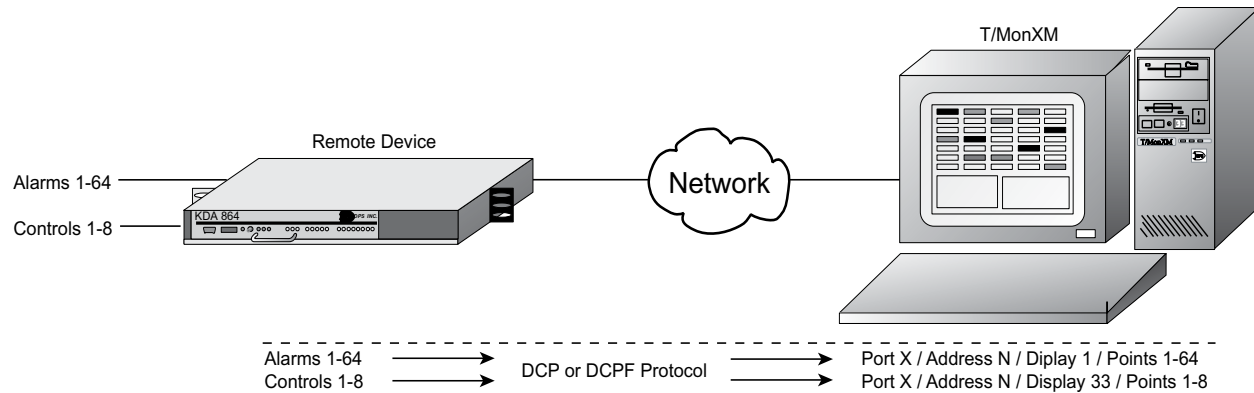
Display	Description	Set	Clear
1	Discrete Alarms 1-10	8001-8010	9001-9010
2	Ping Table	8065-8096	9065-9096
11	System Alarms	8641-8674	9641-9674

**Table 11.E - Display 11 System Alarms point descriptions for NetGuardian-Q8**

Points	Description	SNMP Trap #s	
		Set	Clear
17	Timed Tick	8657	9657
33	Unit Reset	8673	9673
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	LAN not active	8678	9678
46	Craft RcvQ full	8686	9686
47	Modem RcvQ full	8687	9687

## KDA Remotes

Use Table 11.F, 10.G, and 10.H for KDA Remotes. Control points are mapped as alarms to reflect point status. Define control points like alarms to get meaningful status reports.



**Fig. 10.1 - Mapping alarms places them in the correct location in the data base**

**Table 11.F - Mapping in KDA Remotes**

Remote			T/MonXM		
Device	Product	Points	Address	Display	Point
Standard	Base KDA 864	Alarms 1-64	N	1	1-64
		Controls 1-8	N	33	1-8
	LR-24 Relay Expansion in Base	Control 1-24	M*	1	1-24
	4-Port TBOS Expansion in Base	Port 1, Displays 1-3	M*	1-8	1-64 in each display
		Port 2, Displays 1-8	M*	9-16	
		Port 3, Displays 1-8	M*	17-24	
		Port 4, Displays 1-8	M*	25-32	
		TBOS Device Failure	M*	65	See Table 11.H
	8-Port TBOS Expansion in Base	Port 1, Displays 1-3	M*	1-8	1-64 in each display
		Port 2, Displays 1-3	M*	9-16	
		Port 3, Displays 1-8	M*	17-24	
		Port 4, Displays 1-3	M*	25-32	

\* When using KDA versions earlier than 2.1, M = N+2 and L = N-2. In versions 2.1 and later, M and L can be any address not already assigned to another device.

**Note:** Table 11.F continues on the following page.



Table 11.F - Mapping in KDA Remotes (continued)

Remote			T/MonXM		
Device	Product	Points	Address	Display	Point
Standard	8-Port TBOS Expansion in Base	TBOS Device Failure	M*	65	See Table 11.H
		Port 5, Displays 1-3	L*	1-8	1-64 in each display
		Port 6, Displays 1-8	L*	9-16	
		Port 7, Displays 1-8	L*	17-24	
		Port 8, Displays 1-8	L*	25-32	
		TBOS Device Failure	L*	65	See Table 11.H
	EXP 832 Expansion in Base	Alarms 1-32	M*	1	1-32
		Controls 1-8	M*	33	1-8
	KDA 864 Satellite 1	Alarms 1-64	N	2	1-64
		Controls 1-8	N	35	1-8
	LR-25 in Satellite 2	Controls 1-24	N	5	1-24
	KDA 864 Satellite 3	Alarms 1-64	N	4	1-64
		Controls 1-8	N	36	1-8
	DPM 216	Alarms 1-16	N	1	1-16
		Controls 1-2	N	33	1-2
	DCM 216	Alarms 1-2	N	1	1-2
		Controls 1-16	N	33	1-16
8 Channel Analog Expansion Card in KDA 864 Base	Version A or B	Channel 1	M*	1	1 = Min Udr 2 = Min Ovr 3 = Maj Udr 4 = Maj Ovr 5-33 = Absolute value bits (no alarms to map)
		Channel 2	M*	2	
		Channel 3	M*	3	
		Channel 4	M*	4	
		Channel 5	M*	5	
		Channel 6	M*	6	
		Channel 7	M*	7	
		Channel 8	M*	8	
16 Channel Analog Expansion Card in KDA 864 Base and KDA 864 Time-Stamp Base		Channel 1	M*	1	1 = Min Udr 2 = Min Ovr 3 = Maj Udr 4 = Maj Ovr 5-33 = Absolute value bits (no alarms to map)
		Channel 2	M*	2	
		Channel 3	M*	3	

\*When using KDA versions earlier than 2.1, M = N+2 and L = N=2. In versions 2.1 and later,, M and L can be any address not already assigned to another device.

Table 11.F - Mapping in KDA Remotes (continued)

Remote			T/MonXM		
Device	Product	Points	Address	Display	Point
16 Channel Analog Expansion Card in KDA 864 Base and KDA 864 Time-Stamp Base		Channel 4	M*	4	1 = Min Udr 2 = Min Ovr 3 = Maj Udr 4 = Maj Ovr 5-33 = Absolute value bits (no alarms to map)
		Channel 5	M*	5	
		Channel 6	M*	6	
		Channel 7	M*	7	
		Channel 8	M*	8	
		Channel 9	M*	9	
		Channel 10	M*	10	
		Channel 11	M*	11	
		Channel 12	M*	12	
		Channel 13	M*	13	
		Channel 14	M*	14	
		Channel 15	M*	15	
		Channel 16	M*	16	
TBOS / ASCII (7 Port Serial) Expansion Card in KDA 864 Base		ASCII Ports 1,2, 3	M*		
		TBOS Port 4	L*	1-8	1-64 in each display
		TBOS Port 5	L*	9-16	
		TBOS Port 6	L*	17-24	
		TBOS Port 7	L*	25-32	
		TBOS Device Failure	L*	65	See Table 11.H
KDA 864 Time-Stamp	Base	Alarms 1-64	N	1	1-64
		Controls 1-64	N	33	1-8
		Housekeeping	N		See Table 11.G
	16 Channel Analog Expansion Card in Base Unit	See above mapping information for Analog Card in KDA 864 Base			
	LR-24 Relay Expansion in Base	Controls 1-24	M*	1	1-24
	Satellite 1	Alarms 1-64	N	2	1-64
		Controls 1-3	N	34	1-8
		Satellite 1 Failure	N	33	25
	LR-24 in Satellite 1	Controls 1-24	N	5	1-24
	Satellite 2	Alarms 1-64	N	3	1-64
		Controls 1-8	N	35	1-8
		Satellite 2 Failure	N	33	26
	LR-24 in Satellite 2	Controls 1-24	N	6	1-24

\* When using KDA versions earlier than 2.1, M = N+2 and L = N=2. In versions 2.1 and later,, M and L can be any address not already assigned to another device.

**Table 11.F - Mapping in KDA Remotes (continued)**

Remote			T/MonXM		
Device	Product	Points	Address	Display	Point
KDA 864 Time-Stamp	Satellite 3	Alarms 1-64	N	4	1-64
		Controls 1-8	N	36	1-8
		Satellite 3 Failure	N	33	27
	LR-24 in Satellite 3	Controls 1-24	N	7	1-24
KDA 832-T8	Base TBOS	Port 1, Displays 1-8	N	1-8	1-64 in each display
		Port 2, Displays 1-8	N	9-16	
		Port 3, Displays 1-8	N	17-24	
		Port 4 Displays 1-8	N	25-32	
		TBOS Device Failure	N	65	See Table 11.H
		Port 5, Displays 1-8	N	33-40	1-64 in each display
		Port 6, Displays 1-8	N	41-48	
		Port 7, Displays 1-8	N	49-56	
		Port 8, Displays 1-8	N	57-64	
		TBOS Device Failure	N	66	See Table 11.H
	Base	Alarms 1-64	N	69	1-64
		Controls 1-8	N	73	1-8
		Housekeeping	N	81	See Table 11.G
	Satellite 1	Alarms 1-64	N	70	1-64
		Controls 1-8	N	74	1-8
		Housekeeping	N	82	See Table 11.G
	Satellite 2	Alarms 1-64	N	71	1-64
		Controls 1-8	N	75	1-8
		Housekeeping	N	83	See Table 11.G
	Satellite 3	Alarms 1-64	N	72	1-64
		Controls 1-8	N	76	1-9
		Housekeeping	N	84	See Table 11.G
	LR-24 Relay Card in Base	Controls 1-24	N	77	1-24
	LR-24 Relay Card in Satellite 1	Controls 1-24	N	78	1-24
	LR-24 Relay Card in Satellite 2	Controls 1-24	N	79	1-24
	LR-24 Relay Card in Satellite 3	Controls 1-24	N	80	1-24

**Table 11.G - Housekeeping Alarms (applies to all KDA Remotes with housekeeping alarms)**

Point	Alarm Description
33	Power up
34	Watchdog reset
35	Points are locked
36	Lost provisioning
37	Memory diagnostic failed
38	CPU diagnostic failed
39	Expansion card error
40	Reserved
41	Modem not responding
42	No dial tone
43	Time stamp queue overflow

**Table 11.H - TBOS Device Failures**

TBOS Display at Remote			T/MonXM Alarm Point		
Device	TBOS Port	Displays	Address	Display	Point**
4-Port Expansion in KDA 864 Base or KDA 832-T8 Base	1	1-8	M*	65	1-8
	2	1-8			9-16
	3	1-8			17-24
	4	1-8			25-32
8-Port Expansion in KDA 864 Base or KDA 832-T8 Base	1	1-8	M*	65	1-8
	2	1-8			9-16
	3	1-8			17-24
	4	1-8			25-32
	5	1-8	L*	65	1-8
	6	1-8			9-16
	7	1-8			17-24
	8	1-8			25-32
TBOS/ASCII Expansion	4	1-8	L*	65	1-8
	5	1-8			9-16
	6	1-8			17-24
	7	1-8			25-32

**Note:** Table 11.H continues on the following page.

\* When using KDA versions earlier than 2.1, M = N+1 and L = N+2. In version 2.1 and later, M and L can be any address not already assigned to another device.

\*\* Failure of TBOS Port 2, Display 1 is reported at Point 1; port 1, Display 2 at Point 2;....;Port 2 Display 1 at Point 9; Port 2, Display 2 at Point 10, etc.

**Table 11.H - TBOS Device Failures (continued)**

TBOS Display at Remote			T/MonXM Alarm Point		
Device	TBOS Port	Displays	Address	Display	Point**
KDA 832-T8	1	1-8	N	65	1-8
	2	1-8			9-16
	3	1-8			17-24
	4	1-8			25-32
	5	1-8		66	1-8
	6	1-8			9-16
	7	1-8			17-24
	8	1-8			25-32

\* When using KDA versions earlier than 2.1, M = N+1 and L = N+2. In version 2.1 and later, M and L can be any address not already assigned to another device.

\*\* Failure of TBOS Port 2, Display 1 is reported at Point 1; port 1, Display 2 at Point 2;....;Port 2 Display 1 at Point 9; Port 2, Display 2 at Point 10, etc.

## TBOS Protocol

Alarms received on ports that are set for TBOS are reported directly as received, display-for-display and point-for-point. A port defined as TBOS accepts a maximum of 8 displays (512 points).

**Table 11.I - Base KDA 864 Device Failure Alarms**

Display	Point	Meaning
33	25	Failure in Satellite 1
	26	Failure in Satellite 2
	27	Failure in Satellite 3
	31	Failure in Expansion Card
	32	Failure in Expansion Card, Address #2 (8-port TBOS card only)

# Modular Alarm System

Table 11.J refers to display mapping in Modular Alarm System devices.

**Table 11.I - Mapping in Modular Alarm System**

Remote			T/MonXM		
Device	Product	Points	Address	Display	Point
MAS 46009 MAT	Modular Alarm Transmitter (400Type)	Alarms 1-32	N	1	1-32
		Controls 1-4	N	33	1-4
		Acknowledge	N	33	31
		Reset	N	33	32
MAS 46028 CPM	Control Processing Module (400 Type)	Alarms 1-8	N	1	1-8
		Controls 1-4	N	33	1-16
		Acknowledge	N	33	31
		Reset	N	33	32
MAS 46030 ADC	16 Channel Analog Card (400 Type)	Channels 1-16	N	1-16	1 = Min Udr 2 = Min Ovr 3 = Maj Udr 4 = Maj Ovr 5-33 = Absolute value bits (no alarms to map)
MAS 46040	TBOS Collector (400 Type)	Port 1, Displays 1-8	N	1-8	1-64**
		Port 2, Displays 1-8	N	9-16	1-64**
		Port 3, Displays 1-8	N	17-24	1-64**
		Port 4, Displays 1-8	N	25-32	1-64**
		Port 5, Displays 1-8	N	33-40	1-64**
		Port 6, Displays 1-8	N	41-48	1-64**
		Port 7, Displays 1-8	N	49-56	1-64**
		Port 8, Displays 1-8	N	57-64	1-64**

\*\* Bit 64 indicates a TBOS communications failure.

## Protection Switch

Tables 10.K refers to display mapping in Protection Switch units.

**Table 11.K - Mapping in Protection Switch**

Remote			T/MonXM		
Device	Product	Points	Address	Display	Point
Protection Switch		Primary System Online	241-246	1	1
		Secondary System Online	241-246	1	2

## NetMediator T2S

Tables 10.L-10.Q refer to NetMediator T2S remotes.

**Table 11.L - Display mapping in NetMediator T2S**

DISPLAY	DESCRIPTION	SNMP TRAP #	
		SET	CLEAR
1	BASE ALARMS	8001–8064	9001–9064
2	PING TARGET ALARMS	8065–8128	9065–9128
3–10	ANALOG CHANNEL 1..8	8129–8640	9129–9640
11	RELAY/HOUSEKEEPING	8641–8704	9641–9704
12	EXPANSION 1 ALARMS	6001–6064	7001–7064
13	EXPANSION 1 RELAY/HOUSEKEEPING	6065–6128	7065–7128
14	EXPANSION 2 ALARMS	6129–6192	7129–7192
15	EXPANSION 2 RELAY/HOUSEKEEPING	6129–6192	7129-7162
16	EXPANSION 3 ALARMS	6256–6320	7256–7320
17	EXPANSION 3 RELAY/HOUSEKEEPING	6321–6384	7321–7384
18–25	TBOS PORT 1 DISPLAYS 1–8	10001–10512	11001–11512
26–33	TBOS PORT 2 DISPLAYS 1–8	12001–12512	13001–13512
34–41	TBOS PORT 3 DISPLAYS 1–8	14001–14512	15001–15512
42–49	TBOS PORT 4 DISPLAYS 1–8	16001–16512	17001–17512
50–57	TBOS PORT 5 DISPLAYS 1–8	18001–18512	19001–19512
58–65	TBOS PORT 6 DISPLAYS 1–8	20001–20512	21001–21512
66–73	TBOS PORT 7 DISPLAYS 1–8	22001–22512	23001–23512
74–81	TBOS PORT 8 DISPLAYS 1–8	24001–24512	25001–25512

**Table 11.M - Relay/Housekeeping Alarm Mapping in NetMediator T2S**

POINTS	DESCRIPTION	SNMP TRAP #S	
		SET	CLEAR
1	RELAYS	8641	9641
2	RELAYS	8642	9642
3	RELAYS	8643	9643
4	RELAYS	8644	9644
5	RELAYS	8645	9645
6	RELAYS	8646	9646
7	RELAYS	8647	9647
8	RELAYS	8648	9648
17	TIMED TICK	8657	9657
18	EXP. MODULE CALLOUT	8658	9658
19	NETWORK TIME SERVER	8659	9659
33	UNIT RESET	8673	9673
36	LOST PROVISIONING	8676	9676
37	DCP POLLER INACTIVE	8677	9677
38	LAN NOT ACTIVE	8678	9678
41	MODEM NOT RESPONDING	8681	9681
42	NO DIAL TONE	8682	9682
43	SNMP TRAP NOT SENT	8683	9683
44	PAGER QUE OVERFLOW	8684	9684
45	NOTIFICATION FAILED	8685	9685
46	CRAFT RCVQ FULL	8686	9686
47	MODEM RCVQ FULL	8687	9687
48	DATA 1 RCVQ FULL	8688	9688
49	DATA 2 RCVQ FULL	8689	9689
50	DATA 3 RCVQ FULL	8690	9690
51	DATA 4 RCVQ FULL	8691	9691
52	DATA 5 RCVQ FULL	8692	9692
53	DATA 6 RCVQ FULL	8693	9693
54	DATA 7 RCVQ FULL	8694	9694
55	DATA 8 RCVQ FULL	8695	9695
56	NETGUARDIAN DX 1 FAIL	8696	9696
57	NETGUARDIAN DX 2 FAIL	8697	9697
58	NETGUARDIAN DX 3 FAIL	8698	9698
59	GLD 1 FAIL	8699	9699
60	GLD 2 FAIL	8700	9700
61	GLD 3+ FAIL	8701	9701
62	CHAN. PORT TIMEOUT	8702	9702
63	CRAFT TIMEOUT	8703	9703
64	EVENT QUE FULL	8704	9704



**Table 11.N - MDR-4000E DS-3 point descriptions in NetMediator T2S**

<b>PT #</b>	<b>MDR-4000E DS-3</b>	<b>PT #</b>	<b>MDR-4000E DS-3</b>
1	A COMMON LOSS ALARM	33	A COMBINER ALARM
2	A COMMON POWER SUPPLY	34	A CHANNEL FAIL
3	A RF TRANSMIT POWER ALARM	35	A RADIO FRAME LOSS
4	A PA POWER SUPPLY	36	A EYE CLOSURE
5	A TRANSMIT LO LOCK	37	A RECEIVER DS3 FAIL
6	A ATPC HIGH POWER	38	A WS DS1 RECEIVER ALARM
7	A TRANSMIT DS3 FAIL	39	NOT USED
8	A DS1 INPUT ALARM	40	A SYNC LOSS
9	B COMMON LOSS ALARM	41	B COMBINER ALARM
10	B COMMON POWER SUPPLY	42	B CHANNEL FAIL
11	B RF TRANSMIT POWER ALARM	43	B RADIO FRAME LOSS
12	B PA POWER SUPPLY	44	B EYE CLOSURE
13	B TRANSMIT LO LOCK	45	B RECEIVER DS3 FAIL
14	B ATPC HIGH POWER	46	B DS1 RECEIVER ALARM
15	B TRANSMIT DS3 FAIL	47	NOT USED
16	B DS1 INPUT ALARM	48	B SYNC LOSS
17	A TRANSMIT ON LINE	49	RECEIVER ON LINE
18	A TRANSMIT SERVICE CHANNEL	50	A RECEIVER SERVICE CHANNEL
19	ONLINE	51	ONLINE
20	A ATPC ACTIVE	52	A WS DS1 ON LINE
21	A AIS DETECT	53	A AIS DETECT
22	TRANSMIT OVERRIDE	54	PCA LOCKOUT
23	SWITCH OFF NORMAL	55	A ATPC DOWN COMMAND
24	COMMAND PATH FAIL	56	A ATPC UP COMMAND
25	CONTROLLER ALARM	57	RECEIVER OVERRIDE
26	B TRANSMIT ON LINE	58	B RECEIVER ON LINE
27	B TRANSMIT SERVICE CHANNEL ON	59	B RECEIVER SERVICE CHANNEL
28	LINE	60	ONLINE
29	B ATPC ACTIVE	61	B WS DS1 ON LINE
30	B AIS DETECT	62	B AIS DETECT
31	WS DS1 LOOPBACK LINE 1	63	PCA LOCKIN
32	WS DS1 LOOPBACK LINE 2	64	B ATPC DOWN COMMAND

**Table 11.O - MDR-6000 alarm point descriptions in NetMediator T2S**

PT #	MDR-6000	RELAY	PT #	MDR-6000	RELAY
1	A-SIDE COMMON LOSS ALARM	NO/NC	34	A-SIDE CHANNEL FAIL	NO/NC
2	A-SIDE POWER SUPPLY	NO/NC	35	A-SIDE RADIO FRAME LOSS	NO/NC
3	A-SIDE RF TRANSMIT POWER	NO/NC	36	A-SIDE EYE CLOSURE	NO/NC
6	A-SIDE ATPC HIGH POWER	NO/NC	37	A-SIDE RADIO DADE	
7	A-SIDE DS1/E1 MUX ALARM	NO/NC	38	A-SIDE DS1/E1 DEMUX ALARM	NO/NC
8	A-SIDE DS1/E1 INPUT ALARM		39	A-SIDE AGC STATUS	NO/NC
9	B-SIDE COMMON LOSS ALARM	NO/NC	40	A-SIDE SYNC ALARM	NO/NC
10	B-SIDE POWER SUPPLY	NO/NC	41	B-SIDE PATH DISTORTION	
11	B-SIDE RF TRANSMIT POWER	NO/NC	42	B-SIDE CHANNEL FAIL	NO/NC
14	B-SIDE ATPC HIGH POWER	NO/NC	43	B-SIDE RADIO FRAME LOSS	NO/NC
15	B-SIDE DS1/E1 MUX ALARM	NO/NC	44	B-SIDE EYE CLOSURE	NO/NC
16	B-SIDE DS1/E1 INPUT ALARM		45	B-SIDE RADIO DADE	
17	A-SIDE TRANSMIT ON LINE	NO/NC	46	B-SIDE DS1/E1 DEMUX ALARM	NO/NC
19	TRANSMIT OVERRIDE		47	B-SIDE AGC STATUS	NO/NC
20	A-SIDE ATPC ACTIVE		48	B-SIDE SYNC LOSS	NO/NC
21	PREVIOUS SECTION		49	A-SIDE RECEIVE ON LINE	NO/NC
22	SWITCH OFF-NORMAL	NO/NC	50	A-SIDE I/O ON LINE	NO/NC
23	COMMAND PATH FAIL		51	RECEIVE OVERRIDE	
24	CONTROLLER ALARM	NO/NC	52	A-SIDE ATPC DOWN COMMAND	
25	B-SIDE TRANSMIT ON LINE	NO/NC	55	A-SIDE ATPC UP COMMAND	
27	B-SIDE ATPC ACTIVE		56	B-SIDE RECEIVE ON LINE	NO/NC
29	DS1/E1 LOOPBACK LINES 1-4		57	B-SIDE I/O ON LINE	NO/NC
30	DS1/E1 LOOPBACK LINES 5-8		59	I/O OVERRIDE	
31	DS1/E1 LOOPBACK LINES 9-12		62	B-SIDE ATPC DOWN COMMAND	
32	DS1/E1 LOOPBACK LINES 13-16		63	B-SIDE ATPC UP COMMAND	
33	A-SIDE PATH DISTORTION		64	COMM FAILURE	

**Table 11.P - MDR-7000 descriptions in NetMediator T2S**

<b>PT #</b>	<b>MDR-7000</b>	<b>PT #</b>	<b>MDR-7000</b>
1	A-SIDE COMMON LOSS ALARM	32*	DS1/E1 LOOPBACK LINES 13-16
2	A-SIDE IDU POWER SUPPLY	33	A-SIDE BER ALARM
3	A-SIDE RF TRANSMIT POWER	34	A-SIDE CARRIER UNLOCK
4	A-SIDE ODU POWER SUPPLY	35	A-SIDE RX RADIO FRAME LOSS
5	A-SIDE TRANSMIT BLOCK SYNC	36	A-SIDE TX RADIO FRAME LOSS
6	A-SIDE PROVISIONING ERROR	37	A-SIDE RADIO DADE
7	A-SIDE DS1/E1 MUX ALARM	38	A-SIDE DS1/E1 DEMUX ALARM
8	A-SIDE DS1/E1 INPUT ALARM	39	A-SIDE RECEIVE RSL ALARM
9	B-SIDE COMMON LOSS ALARM	40	A-SIDE SYNC LOSS
10	B-SIDE IDU POWER SUPPLY	41	B-SIDE BER ALARM
11	B-SIDE RF TRANSMIT POWER	42	B-SIDE CARRIER UNLOCK
12	B-SIDE ODU POWER SUPPLY	43	B-SIDE RX RADIO FRAME LOSS
13	B-SIDE TRANSMIT BLOCK SYNC	44	B-SIDE TX RADIO FRAME LOSS
14	B-SIDE PROVISIONING ERROR	45	B-SIDE RADIO DADE
15	B-SIDE DS1/E1 MUX ALARM	46	B-SIDE DS1/E1 DEMUX ALARM
16	B-SIDE DS1/E1 INPUT ALARM	47	B-SIDE RECEIVE RSL ALARM
17*	A-SIDE TRANSMIT ONLINE	48	B-SIDE SYNC LOSS
18	A-SIDE IF SYNTHESIZER	49*	A-SIDE RECEIVE ONLINE
19	TRANSMIT OVERRIDE	50	A-SIDE SUPERVISORY ALARM
20	A-SIDE ODU RF SYNTHESIZER	51	A-SIDE I/O ONLINE
21	PREVIOUS SECTION	52	RECEIVE OVERRIDE
22	SWITCH OFF-NORMAL	53	TEMPERATURE ALARM
23	COMMAND PATH FAIL	54	OPTION KEY ABSENT
24	CONTROLLER ALARM	55	DS3 ID MISMATCH
25*	B-SIDE TRANSMIT ONLINE	57*	B-SIDE RECEIVE ONLINE
26	B-SIDE IF SYNTHESIZER	58	B-SIDE SUPERVISORY ALARM
28	B-SIDE ODU RF SYNTHESIZER	59	B-SIDE I/O ONLINE
29*	DS1/E1 LOOPBACK LINES 1-4	60	I/O OVERRIDE
30*	DS1/E1 LOOPBACK LINES 5-8	61-63	NOT USED
31*	DS1/E1 LOOPBACK LINES 9-12	64	COMM FAILURE

**Table 11.Q - MDR-8000 DS-3 point descriptions in NetMediator T2S**

<b>PT #</b>	<b>MDR-8000 DS-3</b>	<b>PT #</b>	<b>MDR-8000 DS-3</b>
1	A COMMON LOSS ALARM	33	A COMBINER ALARM
2	A POWER SUPPLY ALARM	34	A CHANNEL FAIL
3	A PA POWER ALARM	35	A RADIO FRAME LOSS
4	A TRANSMIT POWER ALARM	36	A EYE CLOSURE
5	A PA POWER SUPPLY	37	A RECEIVER DS3 FAIL
6	A ATPC HIGH POWER	38	A WS DS1 RECEIVER ALARM
7	A WS DS1 TRANSMIT ALARM	39	A RECEIVE SIGNAL LEVEL ALARM
8	A WS DS1 TRANSMIT LOSS OF INPUT	40	A REPEATER SYNC ALARM
9	ALARM	41	B COMBINER ALARM
10	B COMMON LOSS ALARM	42	B CHANNEL FAIL
11	B POWER SUPPLY ALARM	43	B RADIO FRAME LOSS
12	B PA POWER ALARM	44	B EYE CLOSURE
13	B TRANSMIT POWER ALARM	45	B RECEIVER DS3 FAIL
14	B PA POWER SUPPLY	46	B WS DS1 RECEIVER
15	B ATPC HIGH POWER	47	B RECEIVE SIGNAL LEVEL ALARM
16	B WS DS1 TRANSMIT ALARM	48	B REPEATER SYNC ALARM
17	B WS DS1 TRANSMIT LOSS OF INPUT	49	A RECEIVER ON LINE
18	ALARM	50	A RECEIVER SERVICE CHANNEL
19	A TRANSMIT ON LINE	51	ON LINE
20	A PA TEMPERATURE ALARM	52	A I/O ON LINE
21	TRANSMIT OVERRIDE	53	RECEIVER OVERRIDE
22	A ATPC OFF NORMAL	54	A RECEIVER AIS DETECT
23	A TRANSMIT AIS DETECT	55	FAN ALARM
24	OFF NORMAL	56	A ATPC LOCKED LOW
25	RF COMMAND PATH ALARM	57	A ATPC LOCKED HIGH
26	CONTROLLER POWER ON RESET	58	B RECEIVER ONLINE
27	B TRANSMIT ON LINE	59	B RECEIVER SERVICE CHANNEL
28	B PA TEMPERATURE ALARM	60	ON LINE
29	A ATPC OFF NORMAL	61	B I/O ON LINE
30	B TRANSMIT AIS DETECT	62	I/O OVERRIDE
31	WS DS1 LOOPBACK LINE 1	63	B RECEIVER AIS DETECT
32	WS DS1 LOOPBACK LINE 2	64	B ATPC LOCKED LOW

**Table 11.R - MDR-8000 DS-1 point descriptions in NetMediator T2S**

<b>PT #</b>	<b>MDR-8000 DS-1</b>	<b>PT #</b>	<b>MDR-8000 DS-1</b>
1	A COMMON LOSS ALARM	33	A PATH DISTORTION
2	A POWER SUPPLY ALARM	34	A CHANNEL FAIL
3	A PA POWER ALARM	35	A RADIO FRAME LOSS
4	A TRANSMIT POWER ALARM	36	A EYE CLOSURE
5	A PA POWER SUPPLY	37	A TERMINAL SYNC ALARM
6	A ATPC HIGH POWER	38	A DS1 RECEIVER ALARM
7	A WS DS1 TRANSMIT ALARM	39	A RECEIVE SIGNAL LEVEL ALARM
8	A WS DS1 TRANSMIT LOSS OF INPUT	40	A REPEATER SYNC ALARM
9	ALARM	41	B PATH DISTORTION
10	B COMMON LOSS ALARM	42	B CHANNEL FAIL
11	B POWER SUPPLY ALARM	43	B RADIO FRAME LOSS
12	B PA POWER ALARM	44	B EYE CLOSURE
13	B TRANSMIT POWER ALARM	45	B TERMINAL SYNC ALARM
14	B PA POWER SUPPLY	46	B DS1 RECEIVER ALARM
15	B ATPC HIGH POWER	47	B RECEIVE SIGNAL LEVEL ALARM
16	B WS DS1 TRANSMIT ALARM	48	B REPEATER SYNC ALARM
17	B WS DS1 TRANSMIT LOSS OF INPUT	49	A RECEIVER ON LINE
18	ALARM	50	NOT USED
19	A TRANSMIT ON LINE	51	A I/O ON LINE
20	A PA TEMPERATURE ALARM	52	RECEIVER OVERRIDE
21	TRANSMIT OVERRIDE	53	NOT USED
22	A ATPC OFF NORMAL	54	FAN ALARM
23	PREVIOUS SECTION ALARM	55	A ATPC LOCKED LOW
24	OFF NORMAL	56	A ATPC LOCKED HIGH
25	RF COMMAND PATH ALARM	57	B RECEIVER ONLINE
26	CONTROLLER POWER ON RESET	58	NOT USED
27	B TRANSMIT ON LINE	59	B I/O ON LINE
28	B PA TEMPERATURE ALARM	60	I/O OVERRIDE
29	A ATPC OFF NORMAL	61	NOT USED
30	DAD E ALARM	62	B ATPC LOCKED LOW
31	DS1 LOOPBACK LINE 1 - 4	63	B ATPC LOCKED HIGH
32	DS1 LOOPBACK LINE 5 - 8	64	COMM FAILURE

**Table 11.S - JungleMux point descriptions in NetMediator T2S**

<b>PT #</b>	<b>JungleMux</b>	<b>PT #</b>	<b>JungleMux</b>
1	NODE A MINOR	33	NODE B MINOR
2	NODE A SYNC/L	34	NODE B SYNC/L
3	NODE A MAJOR	35	NODE B MAJOR
4	NODE A POWER	36	NODE B POWER
5	NODE A CHAN/L	37	NODE B CHAN/L
6	NODE A JMUX/L	38	NODE B JMUX/L
7	NODE A SPE/L	39	NODE B SPE/L
8	NODE A AIS/L	40	NODE B AIS/L
10	NODE A SYNC/R	42	NODE B SYNC/R
13	NODE A CHAN/R	45	NODE B CHAN/R
14	NODE A JMUX/R	46	NODE B JMUX/R
15	NODE A SPE/R	47	NODE B SPE/R
16	NODE A AIS/R	48	NODE B AIS/R
32	NOT USED	64	COMM FAILURE

**Table 11.T - Multiplex Lynx SC point descriptions in NetMediator T2S**

PT #	Multiplex Lynx SC	PT #	Description
1	MODEL ID MSB	33	LINE CODE CH1
2	MODEL ID LSB+2	34	LINE CODE CH2
3	MODEL ID LSB+1	35	LINE CODE CH3
4	MODEL ID LSB	36	LINE CODE CH4
5	NOT USED	37	FAR-END ADDRESS INVALID
6	CHANNEL ID MSB	38	FAR-END ADDRESS MSB
7	CHANNEL ID LSB	39	FAR-END ADDRESS LSB+1
8	CHANNEL ID TX (HIGH/LOW)	40	FAR-END ADDRESS LSB
9	RADIO FAIL	41	NEAR-END RSL MSB
10	AIS OUT	42	NEAR-END RSL MSB-1
11	FAN	43	NEAR-END RSL MSB-2
12	RX SYNC	44	NEAR-END RSL MSB-3
13	LOOPBACK ERROR	45	NEAR-END RSL MSB-4
14	BER	46	NEAR-END RSL MSB-5
15	FAR END	47	NEAR-END RSL MSB-6
16	TELEMETRY DOWN	48	NEAR-END RSL MSB-7
17	DATA LOSS CH 1	49	NEAR-END TX MSB
18	DATA LOSS CH 2	50	NEAR-END TX MSB-1
19	DATA LOSS CH 3	51	NEAR-END TX MSB-2
20	DATA LOSS CH 4	52	NEAR-END TX MSB-3
21	DATA LOSS DISABLE CH 1	53	NEAR-END TX MSB-4
22	DATA LOSS DISABLE CH 2	54	NEAR-END TX MSB-5
23	DATA LOSS DISABLE CH 3	55	NEAR-END TX MSB-6
24	DATA LOSS DISABLE CH 4	56	NEAR-END TX MSB-7
25	LOOPBACK SOURCE	57	DUAL FAN FAIL
26	LOOPBACK ERROR MODE	58	TX SYNC UNLOCK
27	LOOPBACK CH1 ENABLE	59	RX SYNC UNLOCK
28	LOOPBACK CH2 ENABLE	60	INPUT LINEAR DRIVER
29	LOOPBACK CH3 ENABLE	61	DIGITAL HARDWARE
30	LOOPBACK CH4 ENABLE	62	NOT USED
31	AIS DISABLED	63	NOT USED
32	BRIDGE DISABLED	64	COMM FAILURE

## NetGuardian 480

**Table 11.U - Display Descriptions and SNMP Trap Numbers for the NetGuardian 480**

Address	Display	Points	Description	Set	Clear
1	1	1-64	Discrete Alarms 1-64	8001-8064	9001-9064
1	2	1-16	Discrete Alarms 65-80	8065-8080	9065-9080
1	2	17-20	Relays 1-4	8081-8085	9081-9085
1	2	57-64	Housekeeping	8121-8128	9121-9128

**Table A.1** Display descriptions and SNMP Trap numbers for the NetGuardian 480

The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap “Set” number for alarm 1 (in Display 1) is 8000, “Set” for alarm 2 is 8001, “Set” for alarm 3 is 8002, etc.

**Table 11.V - Housekeeping Alarm Point Descriptions**

			SNMP TRAP #s	
Disp	Alarm Point	Description	Set	Clear
2	17	Relays	8081	9081
2	18	Relays	8082	9082
2	19	Relays	8083	9083
2	20	Relays	8084	9084
2	21-56	Undefined*	8085-8120	9085-9120
2	57	Default Configuration	8121	9121
2	58	DIP Switch Config	8122	9122
2	59	MAC Address Not Set	8123	9123
2	60	IP Address Not Set	8124	9124
2	61	Net Hardware Error	8125	9125
2	62	SNMP Processing Error	8126	9126
2	63	SNMP Community Error	8127	9127
2	64	LAN Tx Packet Drop	8128	9128

**Table A.2** Housekeeping alarm point descriptions

\* “Undefined” indicates that the alarm point is not used.



# NetGuardian 216T

**Table 11.W - Display descriptions and SNMP Trap numbers for the NetGuardian 216T**

Display	Description	Set	Clear
1	Discrete Alarms 1-16	8001-8032	9001-9032
2	Ping Table	8065-8096	9065-9096
3	Analog Channel 1**	8129-8132	9129-9132
4	Analog Channel 2**	8193-8196	9193-9196
5	Analog Channel 3**	8257-8260	9257-9260
6	Analog Channel 4**	8321-8324	9321-9324
7	Analog Channel 5— <b>Power Feed A</b> **	8385-8388	9385-9388
8	Analog Channel 6— <b>Power Feed B</b> **	8449-8452	9449-9452
9	Analog Channel 7— <b>Internal Temp Sensor</b> **	8513-8516	9513-9516
10	Analog Channel 8— <b>External Temp Sensor</b> **	8577-8580	9577-9580
11	Relays/System Alarms (See table below)	8641-8674	9641-9674
12	NetGuardian Expansion 1 Alarms 1-48	6001-6064	7001-7064
13	NetGuardian Expansion 1 Relays 1-8	6065-6072	7065-7072
14	NetGuardian Expansion 2 Alarms 1-48	6129-6177	7129-7177
15	NetGuardian Expansion 2 Relays 1-8	6193-6200	7193-7200
16	NetGuardian Expansion 3 Alarms 1-48	6257-6305	7257-7305
17	NetGuardian Expansion 3 Relays 1-8	6321-6328	7321-7328

\* The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap “Set” number for alarm 1 (in Display 1) is 8001, “Set” for alarm 2 is 8002, “Set” for alarm 3 is 8003, etc.

\*\* The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor over, major under, and major over. For example, for Analog channel 1, the “Set” number for minor under is 8129, minor over is 8130, major under is 8131, and major over is 8132.

**Table 11.W - Display 11 System Alarms point descriptions**

Points	Description	SNMP Trap #s	
		Set	Clear
1	Relays	8641	9641
2	Relays	8642	9642
17	Timed Tick	8657	9657
19	Network Time Server	8659	9659
21	Duplicate IP Address	8661	9661
22	External Sensor Down	8662	9662
33	Unit Reset	8673	9673
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	T1 WAN Inactive	8678	9678
39	LAN Inactive	8679	9679
43	SNMP Trap not Sent	8683	9683
44	Pager Que Overflow	8684	9684
45	Notification failed	8685	9685
46	Craft RcvQ full	8686	9686
48	Data 1 RcvQ full	8688	9688
56	NetGuardian DX 1 fail	8696	9696
57	NetGuardian DX 2 fail	8697	9697
58	NetGuardian DX 3 fail	8698	9698
63	Craft Timeout	8703	9703
64	Event Que Full	8704	9704

**Table 11.X - System Alarms Descriptions**

Display	Points	Alarm Point	Description	Solution
11	17	Timed Tick	Toggles state at constant rate as configured by the Timed Tick timer variable. Useful in testing integrity of SNMP trap alarm reporting.	To turn the feature off, set the Timed Tick timer to 0.
	19	Network Time Server	Communication with Network Time Server has failed.	Try pinging the Network Time Server's IP address as it is configured. If the ping test is successful, then check the port setting and verify the port is not being blocked on your network.
	20	Accumulation Event	An alarm has been standing for the time configured under Accum. Timer. The Accumulation timer enables you to monitor how long an alarm has been standing despite system reboots. Only the user may reset the accumulated time; a reboot will not.	To turn off the feature, under Accum. Timer, set the display and point reference to 0.
	21	Duplicate IP Address	The unit has detected another node with the same IP Address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP address, reboot the unit to clear the System alarm.
	22	External Sensor Down	External Sensor is not active	Check to see if External Sensor cable is properly connected.
	33	Unit Reset	The unit has just come online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web or Edit216T to configure the unit. Power the cycle to see if the alarm goes away. May require RMA.

**Note:** Table 11.X continues on next page

Display	Points	Alarm Point	Description	Solution
11	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP Timer setting.	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under Timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	T1 WAN not active	T1 WAN port is down.	Check LAN/WAN cable. Ping to and from the unit.
	39	Ethernet not active	Ethernet LAN ports are down.	
	40	LNK Alarm	Hardware failure between integrated Ethernet Hub and the unit.	
	43	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP trap event occurred.	Define the IP address where you would like to send SNMP trap events, or configure the event not to trap.
	44	Pager Que Overflow	Over 250 events are currently queued in the pager que and are still trying to report.	Check for failed notification events that may be filling up the pager queue. There may be a configuration or communication problem with the notification events.
	45	Notification failed	A notification event, like a page or email, was unsuccessful.	Use RPT filter debug to help diagnose notification problems.
	46	Craft RcvQ full	The Craft port received more data than it was able to process.	Disconnect whatever device is connected to the craft serial port. This alarm should not occur.
	48	Data 1 RcvQ full	Data port 1 receiver filled with 8 K of data.	Check proxy connection. The serial port data may not be getting collected as expected.
	56	NetGuardian DX 1 fail	NGDdx 1 Fail (Expansion shelf 1 communication link failure)	Under Ports>Options, verify the number of configured NGDdx units. Use EXP filter debug and port LEDs to help diagnose the problem. Use of DB9M to DB9M will null crossover for cabling. Verify the DIP addressing on the back of the NGDdx unit
	57	NetGuardian DX 2 fail	NGDdx 2 Fail (Expansion shelf 2 communication link failure)	
	58	NetGuardian DX 3 fail	NGDdx 3 Fail (Expansion shelf 3 communication link failure)	
	63	Craft Timeout	The Craft Timeout Timer has not been reset to the specified time. This feature is designed so other machines may keep the TTY link active. If the TTY interface becomes unavailable to the machine, then the Craft Timeout alarm is set.	Change the Craft Timeout Timer to 0 to disable the feature.
	64	Event Que Full	The Event Que is filled with more than 500 uncollected events.	Enable DCP timestamp polling on the master so events are collected, or reboot the system to clear the alarm.

# NetGuardian 16S

**Table 11.Y - NetGuardian 16S Alarm Map**

			SNMP Trap #s	
Description	Display	Points	Set	Clear
<b>NetGuardian-16S Base Unit</b>				
Discrete Alarms	1	1-32	8001–8032	9001–9032
Ping Alarms	2	1-32	8065–8096	9065–9096
Control Relays	11	1-8	8641–8648	9641–9648
System Alarms 9–15	11	9-15	8649–8655	9649–9655
System Alarms 33–50	11	33-50	8673–8690	9673–9690
<b>NetGuardian Expansion #1</b>				
Discrete Alarms	12	1-48	6001–6064	7001–7064
Control Relays	13	1-8	6065–6072	7065–7072
<b>NetGuardian Expansion #2</b>				
Discrete Alarms	14	1-48	6129–6177	7129–7177
Control Relays	15	1-8	6193–6200	7193–7200
<b>NetGuardian Expansion #3</b>				
Discrete Alarms	16	1-48	6257–6305	7257–7305
Control Relays	17	1-8	6321–6328	7321–7328

**Note:** Table 11.Z - System alarm descriptions on next page

Point	System Alarm	Description
9	Modem not Responding	Modem not responding to initialization string
10	No Dialtone	Dial tone not detected during dial-out attempt
11	Pager Que Overflow	Over 250 unsent events in pager queue
12	Pager Notify Failed	Attempted pager notification unsuccessful
13	Callout Que Overflow	Over 8 unsent calls in Voice Call Out queue
14	Callout Notify Failed	Attempted Voice Call Out unsuccessful
15	Exp. Module Callout	Alarm collected from Entry Control Unit (ECU)
33	Unit Reset	Toggles whenever unit reboots
34	Lost Provisioning	Unit using default configuration settings. NVRAM may be damaged
35	Intra-communication Fail	Communications failure between the NetGuardian-16S's two circuit boards
36	Private LAN not Active	Ethernet link not detected on Private port
37	Public LAN not Active	Ethernet link not detected on Public port
38	Duplicate Private IPA	Unit detects another node with same IP address as the Private port
39	Duplicate Public IPA	Unit detects another node with same IP address as the Public port
40	DCP Poller Inactive	Unit has not received poll from T/Mon for longer than DCP Timer period set by system administrator
41	DCP Event Que Full	More than 500 uncollected events in DCP event queue
42	SNMP Trap not Sent	SNMP trap address is not defined and an SNMP Trap event occurred
43	Network Time Server	Communication to network time server failure
44	BSU Standalone Mode	Communication with CopperControler failure and BSU enters Standalone Mode.
45	Serial Rcv Overflow	UART hardware overflowed during receive
46	Serial Rcv Que Full	Alarm set when any data port is filled with more than 16K of information
47	Timed Tick	Toggles state at constant rate set by Timed Tick period configured by system administrator
48	Channel Port Timeout	Channel port has not forwarded any traffic for longer than Channel Port Timeout period set by system administrator
49	Craft Port Timeout	Craft Timeout Timer has not been reset in the period set by system administrator
50	NGDdx Expansion Fail	Communication to NetGuardian Expansion unit(s) failure

## BAS for NetGuardian

Table 12.A - N2 Mapping (BAS Device)

Note: See next table for specific ECU mapping

Display	Mapping	Display	Mapping	Display	Mapping
1	Internal	7	ECU 5	13	ECU 11
2	Internal	8	ECU 6	14	ECU 12
3	ECU1	9	ECU 7	15	ECU 13
4	ECU 2	10	ECU 8	16	ECU 14
5	ECU 3	11	ECU 9	17	ECU 15
6	ECU 4	12	ECU 10	18	ECU 16

Table 12.B - ECU Mapping

Point	Description	Mode
1-8	Unused	N/A
9	Door Sensor (Opto 1)	Status**
10	Motion Sensor (Opto 2)	Status**
11	Opto 3 sensor	Status**
12	Door violation alarm	Status
13-16	Unused	N/A
17	Door strike active (relay #1)	Status/Control * **
18	Relay #2 active	Status/Control * **
19	Hack lockout	Status
20	Exit password OK	Status**
21	Propped-Door Mode active	Status/Control*
22	Stay-Open Door or Extended Propped-Door Mode active	N/A
23	Unused	N/A
24	Speaker active	Status**
25-61	Unused	N/A
62	ECU is using defaults	Status
63	ECU enabled	Status**
64	ECU polling error (device failure)	Status

\* When using controls from alarm masters, only issue the momentary (MOM) commands

\*\* DPS recommends these alarms be set to "No Log" and "No History" in T/Mon point setup

## RAB 176N

**Table 12.C - Display Descriptions and SNMP Trap Numbers for the RAB 176N**

Display	Description	Set	Clear
1	Discrete Alarms 1-64	8001-8064	9001-0964
2	Discrete Alarms 65-128	8065-8128	9065-9128
3	Discrete Alarms 129-175	8129-8175	9129-9175
3	Relays/System Alarms (See Table Below)	8176-8191	9176-9191

The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap “Set” number for alarm 1 (in Display 1) is 8000, “Set” for alarm 2 is 8001, “Set” for alarm 3 is 8002, etc.

**Table 12.D- Housekeeping Alarm Point Descriptions**

Points	Description	Set	Clear
49	Relays	8176	9176
50	Relays	8177	9177
51	Relays	8178	9178
52	Relays	8179	9179
53	Relays	8180	9180
54	Relays	8181	9181
55	Relays	8182	9182
56	Relays	8183	9183
57	Default Configuration	8184	9184
58	DIP Switch Config	8185	9185
59	MAC Address Not Set	8186	9186
60	IP Address Not Set	8187	9187
61	Net Hardware Error	8188	9188
62	SNMP Processing Error	8189	9189
63	SNMP Community Error	8190	9190
64	LAN Tx Packet Drop	8191	9191



## NetDog-82IP G2

**Table 12.E- Display Descriptions and SNMP Trap Numbers for the NetDog G2**

Display	Description	Set	Clear
1	Discrete Alarms 1-8	8001-8008	9001-9008
2	Ping Table	8065-8096	9065-9096
3	Analog Channel 1**	8129-8132	9129-9132
4	Analog Channel 2**	8193-8196	9193-9196
5	Internal Temp. Sensor*	8257-8260	9257-9260
6	External Temp. Sensor*	8321-8324	9321-9324
7	Reserved	8385-8388	9385-9388
8	Reserved	8449-8452	9449-9452
9	Reserved	8513-8516	9513-9516
10	Reserved	8577-8580	9577-9580
11	Relays/System Alarms (See Table Below)	8641-8704	9641-9704

\* The TRAP number ranges shown correspond to the point range of each display. For example, the SNMP Trap “Set” number for alarm 1 (in Display 1) is 8001, “Set” for alarm 2 is 8002, “Set” for alarm 3 is 8003, etc.

\*\* The TRAP number descriptions for the Analog channels (1-8) are in the following order: minor under, minor over, major under, major over. For example, for Analog channel 1, the “Set” number for minor under is 8129, minor over is 8130, major under is 8131, and major over is 8132.

**Table 12.F- Display 11 System Alarms Point Descriptions**

		SNMP Trap #s	
Points	Description	Set	Clear
1	Relays	8641	9641
2	Relays	8642	9642
17	Timed Tick	8657	9657
19	Network Time Server	8659	9659
21	Duplicate IP Address	8661	9661
33	Power Up	8673	9673
36	Lost Provisioning	8676	9676
37	DCP Poller Inactive	8677	9677
38	LAN not active	8678	9678
41	Modem not responding	8681	9681
42	No Dial Tone	8682	9682
43	SNMP Trap not Sent	8683	9683
44	Pager Que Overflow	8684	9684
45	Notification failed	8685	9685
46	Craft RcvQ full	8686	9686
47	Modem RcvQ full	8687	9687
63	Craft Timeout	8703	9703
64	Event Que Full	8704	9704

See Table 12.G “System Alarms Display Map” for detailed descriptions of the NetDog’s system alarms.

**Table 12.G- System Alarms Display Map and Descriptions**

Display	Points	Alarm Point	Description	Solution
11	17	Timed Tick	Toggles state at constant rate as configured by the Timed Tick timer variable. useful in testing integrity of SNMP trap alarm reporting.	To turn feature off, set the Timed Tick timer to 0.
	19	Network Time Server	Communication with Network Time Server has failed.	Try pinging the Network Time Server's IP address as it is configured. If the Ping test is successful, then check the port setting and verify the port is not being blocked on your network.
	20	Accumulation Event	An alarm has been standing for the time configured under Accu. Timer. The Accumulation timer enables you to monitor how long an alarm has been standing despite system reboots. Only the user may rest the accumulated time, a reboot will not.	To turn off the feature, under the Accum. Timer, set the display and point reference to 0.
	21	Duplicate IP Address	The unit has detected another node with the same IP address.	Unplug the LAN cable and contact your network administrator. Your network and the unit will most likely behave incorrectly. After assigning a correct IP Address, reboot the unit to clear the System alarm.
	33	Power Up	The unit has just come online. The set alarm condition is followed immediately by a clear alarm condition.	Seeing this alarm is normal if the unit is powering up.
	36	Lost Provisioning	The internal NVRAM may be damaged. The unit is using default configuration settings.	Use Web or latest version of NG Edit4 to configure unit. Power cycle to see if alarm goes away. May require RMA.

**Table 12.G** continues on the following page

**Table 12.G (continued)- System Alarms Display Map and Descriptions**

Display	Points	Alarm Point	Description	Solution
11	37	DCP Poller Inactive	The unit has not seen a poll from the Master for the time specified by the DCP timer setting	If DCP responder is not being used, then set the DCP Unit ID to 0. Otherwise, try increasing the DCP timer setting under timers, or check how long it takes to cycle through the current polling chain on the Master system.
	38	NET1 not active	The Net1 LAN port is down	Check LAN cable. Ping to and from the unit.
	39	NET2 not active	The Net2 LAN port is down	
	40	LNK Alarm	No network connection detected	
	41	Modem not responding	An error has been detected during modem initialization. The modem did not respond to the initialization string.	Remove configured modem initialization string, then power cycle the unit. If alarm persists, try resetting the Modem port from the TTY interface, or contact DPS for possible RMA.
	42	No Dial Tone	During dial-out attempt, the unit did not detect a dial tone.	Check the integrity of the phone line and cable.
	43	SNMP Trap not sent	SNMP trap address is not defined and an SNMP trap event occurred.	Define the IP Address where you would like to send SNMP trap events, or configure the event not to trap.
	44	Pager Queue Overflow	Over 250 events are currently queued in the pager queued and are still trying to report	Check for failed notification events that may be filling up the pager queue. There may be a configuration or communication problem with the notification events.
	45	Notification failed	A notification event, like a page or email, was unsuccessful.	Use RPT filter debug to help diagnose notification problems
	46	Craft RcvQ full	The Craft port received more data than it was able to process.	Disconnect whatever device is connected to the craft serial port. This alarm should not occur.
	47	Modem RcvQ full	The modem port received more data than it was able to process.	Check what is connecting to the NetDog. This alarm should not occur.
	63	Craft Timeout		
	64	Event Queue full	The Event Queue is filled with more than 500 uncollected events	Enable DCP timestamp polling on the master so events are collected, or reboot the system to clear the alarm.

## Larse 1200/Badger RTU

**Table 12.G- Display Map and Descriptions**

Display	Point	Description
1	1-32	Discrete Alarms
2	1	Analog- Channel 1 Minor Over
2	2	Analog- Channel 1 Minor Under
2	3	Analog- Channel 1 Major Under
2	4	Analog- Channel 1 Major Over
2	5-64	Analog Data- Channel 1
3	1	Analog- Channel 2 Minor Over
3	2	Analog- Channel 2 Minor Under
3	3	Analog- Channel 2 Major Under
3	4	Analog- Channel 2 Major Over
3	5-64	Analog Data- Channel 2
4	1	Analog- Channel 3 Minor Over
4	2	Analog- Channel 3 Minor Under
4	3	Analog- Channel 3 Major Under
4	4	Analog- Channel 3 Major Over
4	5-64	Analog Data- Channel 3
17	1	Analog- Channel 16 Minor Over
17	2	Analog- Channel 16 Minor Under
17	3	Analog- Channel 16 Major Under
17	4	Analog Channel 16 Major Over
17	5-64	Analog Data- Channel 16
18	1-32	Relay Status (Base 1-16, Expansion 17-32)

**Note:** Badger is the same except without Display 18-34

**Table 12.G (cont.) - Display Map and Descriptions**

Display	Point	Description
19	1	Analog - Channel 17 Minor Over
19	2	Analog - Channel 17 Minor Under
19	3	Analog - Channel 17 Major Under
19	4	Analog - Channel 17 Major Over
19	5-64	Analog Data - Channel 17
20	1	Analog - Channel 18 Minor Over
20	2	Analog - Channel 18 Minor Under
20	3	Analog - Channel 18 Major Under
20	4	Analog - Channel 18 Major Over
20	5-64	Analog Data - Channel 18
34	1	Analog - Channel 32 Minor Over
34	2	Analog - Channel 32 Minor Under
34	3	Analog - Channel 32 Major Under
34	4	Analog - Channel 32 Major Over
34	5-64	Analog Data - Channel 32

## DPM/DCM

**Table 12.H- DPM Display Map**

Display*	Points	Description
1	1	Discrete Point
	2	Discrete Point
	3	Discrete Point
	4	Discrete Point
	5	Discrete Point
	6	Discrete Point
	7	Discrete Point
	8	Discrete Point
	9	Discrete Point
	10	Discrete Point
	11	Discrete Point
	12	Discrete Point
	13	Discrete Point
	14	Discrete Point
	15	Discrete Point
	16	Discrete Point
33	17	Control/Relay
	18	Control/Relay

Note: The DPM and DCM 216 use the DCP protocol and require display information shown.

**Table 12.I- DCM Display Map**

Display	Points	Description
1	1	Control/Relay
	2	Control/Relay
	3	Control/Relay
	4	Control/Relay
	5	Control/Relay
	6	Control/Relay
	7	Control/Relay
	8	Control/Relay
	9	Control/Relay
	10	Control/Relay
	11	Control/Relay
	12	Control/Relay
	13	Control/Relay
	14	Control/Relay
	15	Control/Relay
	16	Control/Relay
33	17	Discrete Point
	18	Discrete Point





## Section 12 - Configure Controls

**Site Controls Category Definition**

Window Name : MADERA MAIN

Group	Category	Description
1	RADSW	RADIO SWITCH
2	DRLCK	DOOR LOCK
3	TOWER	TOWER LIGHTS
4	.....	
5		
6		
7		
8		
9		
10		

Enter category id

\_\_\_\_\_

F2=Points, F3=BLANK, AF3=DELETE, AF4=Ins, F8=Save, F9=Help, F10/Esc=Exit

Fig. 12.1 - The site controls category definition screen.

### Site Controls

Site controls are operated from the Monitor Mode, see Section 16 for more information.

The Site Controls Definition function is accessed while in the Window Definition screen by pressing F4. They allow you to define English look-up tables that can be accessed from Monitor Mode for operating control equipment within the alarm network. Site controls are normally assigned to each equipment site window that has control points. This makes it easy to quickly select the right control since you are only selecting from one site as opposed to the whole network. The fact that these controls can be initiated by referring to an English table instead of cryptically (DCPF Address, Display, etc.), makes it easier for the end user to work with the system and less likely to cause inadvertent error.

T/MonXM provides three methods of operating control points at RTU's: Site Controls, Labeled Controls and Derived Controls. Site Controls, described here, are operated through windows, by site or other window category. Labeled Controls, are very similar to site controls, but are operated from a type of control grouping rather than from a site window. Derived controls are automatically operated by T/MonXM from user-defined formulas that evaluate certain alarm points to determine if an automatic control point operation is appropriate. See description of derived controls in this section.

Refer to Figure 12.2 for an illustrated explanation of the differences between Site Controls and Labeled Controls.

Site Controls are issued in the Monitor Mode by selecting a site window and pressing F8. The Site controls Category table for the site appears. Highlight the desired category and press Enter. The Control Point table for that category at that site then appears. To operate the point, highlight the point and press Enter. Follow instructions in the Controls window at the lower left corner. Press F10/Esc when done.

Site Controls are a privileged area and users must be granted access in order to issue controls. This is done in the System Users window.

The Site Controls Definition section consists of two input screens, the Site Controls Category Definition screen (Figure 12.1) and the Control Point Definition screen (Figure 12.3).

You can define up to 40 categories of control points. Each category can consist of up to 200 control point entries. Before you can define a control point entry you must define a category. Enter a category name and description, then go on to Control Point Definition.

**Note:** System Security provides security lockouts on Site Controls by Windows, not by category group or control point entries. Keep this in mind when setting up your control categories and the control point entries under them. See Table 12.A.

**Table 12.A - Fields in the Site Controls Category Definition screen**

Field	Description
Category	A six-character title for the category.
Description	The description for the category.

**Table 12.B - Key commands available in the Site Controls Category Definition screen**

Function Key	Description
F2	Move to the Control Point Definition screen.
F3	Blank - Deletes current category entry and control point definitions for the category. Leaves an open line. Control Point Definitions deleted in this way cannot be recovered by using F10 or Esc.
Alt-F3	Delete - Deletes entry N and its points. Moves all other lines up.
Alt-F4	Inserts an undefined point above cursor.
F8	Save point definitions and return to polling list.
F9	Save the category database.
F10/Esc	Exit.

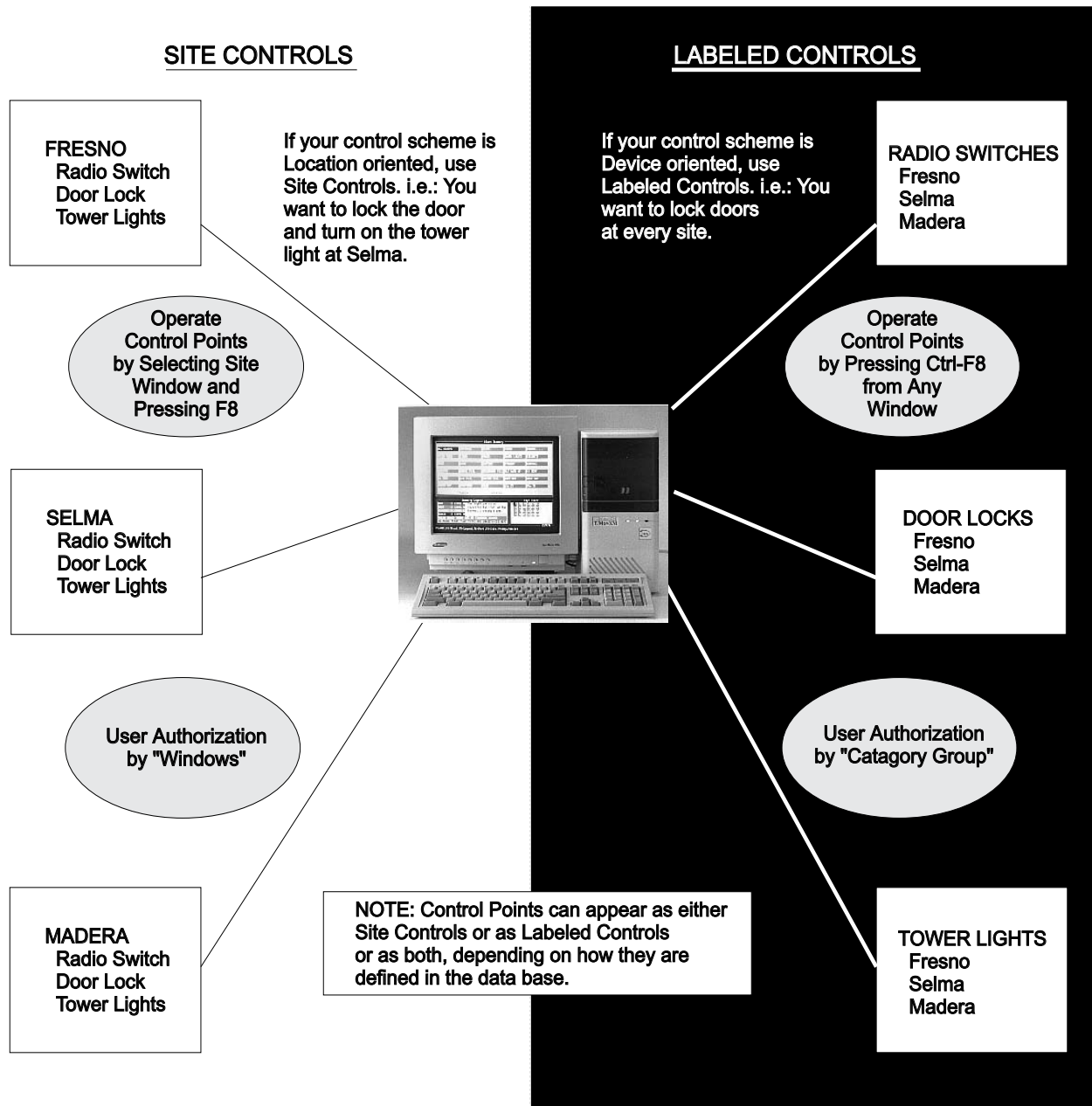


Fig. 12.2 - The differences between site controls and labeled controls

**Note:** Site controls are the most commonly used method among T/Mon users.

Site Control Points						
Window Name : FRESNO						
Category : CTRLS NET GUARDIAN SITE CONTROLS						
Ent	Description	CMD	Ch	T	ID	Point(s)
1	ENABLE TX A.....	MON	NG		5	11 1
2	ENABLE TX B	MON	NG		5	11 2
3	OPEN MAIN GATE	MON	NG		5	11 3
4	TURN ON FLOOD LIGHTS	OPR	NG		5	11 4
5	TURN OFF FLOOD LIGHTS	RLS	NG		5	11 4
6						
7						
8						
9						
10						

Enter description

DPS Telecom Technical Support : 559-454-1600

F1=GOTO F3=BLANK AF3=DEL AF4=INS F5=Range F6=Read F8=Save F9=Help F10/Esc=Exit

Fig. 12.3 - Point definition screen

## Control Point Definition

The Control Points Definition screen is used to define the control points for Site Controls.

Table 12.C - Fields in the Control Point Definition screen

Field	Description
Ent	The entry number within the group selected (200 entries per group).
Description	The description of the control points. Up to 40 characters
CMD	<p>The command to be sent to the control point.</p> <p>OPR = OPERATE RELAY</p> <p>RLS = RELEASE RELAY</p> <p>MON = MOMENTARY ON</p> <p>MOF = MOMENTARY OFF</p> <p>SOP = SBO Operate*</p> <p>SRL = SBO Release*</p> <p>SMO = SBO Momentary On*</p> <p>EXE = SBO Execute*</p> <p>CLR = SCO Clear All*</p>

\*SBO = Select before operate. This method of control point operation offers extra security by requiring two operator steps before the point actually operates. The desired operation (SOP, SRL, SMO or CLR) is specified and a response from the remote is displayed, indicating that the point is "selected." Then the EXE command is sent to perform the specified operation. Another use of SBO is to operate several control points simultaneously. The desired control points are "selected" at the remote and one execute command operates all at the same time. This is useful in controlling functions that must occur together, such as channel switching.

**Table 12.C - Fields in the Control Point Definition screen (continued)**

Field	Description
Ch	Channel Number. NG = NetGuardians N2 = Building Access System K1 = VIRTUAL PORT (base and satellite KDAs with relay exp. card) K2 = VIRTUAL PORT (relay and other expansion cards in base KDAs) RP = REMOTE PORT (Modem port) RC = RELAY CARD (102 card - local controls only) AV = AUDIO/VISUAL CARD (108 Card -Only relays 9-12 can be used.) 1-29 = Port Number. IAM Users - Relays 9-12 are not available on IAM.
D	Device Type. This field is selected only when the selected port is defined for DCM protocol. Selections are: C = CPM S = SBP (Smart Bypass Card -Used only with the Building Access Unit. Three controls may be user-defined for a BAU. See the BAU Operation Guide for details.)
Add	The device address. Valid range is 1-999. This field is skipped when the selected port has been defined for TBOS protocol.
Unt	Unit. The Display (1-64) in which the control points reside. This field is skipped when the selected port has been defined for DCM protocol.
Points	A control point or range of control points that you wish to operate. Ranges may be entered using dashes and/or commas (no spaces). Valid control point ranges may be from 1-64.

**Table 12.D - Key commands available in the (Site) Control Point Definition screen**

Function Key	Description
F1	Moves the cursor to a selected entry point.
F3	Blank - Deletes current point entry. Leaves an open line. Control Points deleted in this way cannot be recovered by using F10 or Esc.
Alt-F3	Delete - Deletes entry and moves all other lines up.
Alt-F4	Insert - Moves current line down one group and inserts a blank line.
F6	Read - Read points from window____, Group____. Enter window number to read from (1-720, or 0 for labeled controls)
F8	Saves the control point entries and returns to the Site Controls Category Definition screen.
F9	Displays help for this screen.
F10/Esc	Exit or return to start of line.

Labeled Controls Category Definition		
Group	Category	Description
1	GEN 01	EAST WING GENERATOR
2	GEN 02	WEST WING GENERATOR
3	GEN 03	NORTH WING GENERATOR
4	GEN 04	SOUTH EING GENERATOR
5	BAU 01	WEST DOOR
6	.....	
7		
8		
9		
10		

Enter category id

F2=Points, F3=BLANK, AF3=DELETE, AF4=Ins, F8=Save, F9=Help, F10/Esc=Exit

Fig. 12.4 - The labeled controls category definition screen

## Labeled Controls Definition

The Labeled Controls Definition function is accessed by selecting Labeled Controls from the File Maintenance Menu. Labeled Controls allow you to define English look-up tables that can be accessed from Monitor Mode for operating control equipment within the alarm network.\* The fact that these controls can be initiated by referring to an English table instead of cryptically (DCPF Address, Display, etc.), makes it easier for the end user to work with the system and less likely to cause inadvertent error.

T/MonXM provides three methods of operating control points at RTUs: Site Controls, Labeled Controls and Derived Controls. Site Controls are operated through windows, by site or other window category. Labeled Controls, described here, are very similar to site controls, but are operated from a type of control grouping rather than from a site window. Derived controls are automatically operated by T/MonXM from user-defined formulas that evaluate certain alarm points to determine if an automatic control point operation is appropriate.

\* Labeled controls are assigned to equipment types (radio switches, door locks, tower lights) rather than site windows. This makes it easy to control similar devices across the network without having to move between site windows.

Refer to Section 16 - Monitor Mode for details on operating labeled controls.

Before operating Labeled Controls authorize the System User to operate controls. This is done in the System Users definition.

A higher level of system security can be assigned to the use of Labeled Controls because of the grouping structure with which they are built. Control groups can be setup with system security arrangements so that accessibility is on a user-by-user basis.

Labeled Controls are easily operated in the Monitor Mode by pressing Ctrl F8 regardless of which site window is highlighted. The Labeled Controls Category table for the entire system appears. Highlight the desired group/category and press Enter. The control point table for that group/category over the entire system then appears (see Figure 12.4). The point is operated by highlighting the desired point and pressing Enter. Follow instructions in the controls window at the lower left corner of the screen. Press Esc/F10 when done.

The Labeled Controls Definition section consists of two input screens. The first screen (see Figure 12.4) is the Labeled Controls Category Definition screen and control points are defined on the second screen, the Control Point Definition screen (see Figure 12.5).

You can define up to 40 categories of control groups. Each group can consist of up to 200 control point entries. In order to define a control point entry you must first define a category. Defining a category requires that you Enter a category name and description. After you've done this you can go on to Control Point Definition.

**Note:** System Security provides security lockouts on Labeled Controls by Category not by control point entries. Keep this in mind when setting up your control categories and the control point entries under them. (See Table 12.A.)

Refer to Figure 12.2 for an illustrated explanation of the differences between Labeled Controls and Site Controls.

**Table 12.E - Key commands available in the Labeled Controls Category Definition screen**

Function Key	Description
F2	Go to the Control Point Definition screen (see Figure 12.5) for the category that the cursor is on.
F3	Blank - Deletes the current category entry. Also deletes any control point definitions for the category. <b>Note:</b> Control Point Definitions deleted in this way cannot be recovered by exiting the screen using F10 or Esc.
Alt-F3	Delete - Deletes entry and moves all other lines up.
Alt-F4	Insert - Moves current line down one group and inserts a blank line.
F8	Save the category database.
F9	Displays help for this screen.
F10/Esc	Exit.



Control Points				
Category : GEN 01 EAST WING GENERATOR				
Ent	Description	CMD	Ch D	Add Unt Point(s)
1	GENERATOR ON.....	MON	RC	1
2	GENERATOR OFF	RLS	RC	1
3	GENERATOR ALARM OFF	RLS	RC	2
4				
5				
6				
7				
8				
9				
10				
Enter description				
<div style="border: 1px solid black; height: 20px; width: 100%;"></div>				

F1=GOTO F3=BLANK AF3=DEL AF4=INS F5=Range F6=Read F8=Save F9=Help F10/Esc=Exit

Fig. 12.5 - The control point definition screen

## Control Point Definition Screen

The Control Points Definition screen is used to define the control points for Labeled Controls. See Figure 12.5, Table 12.F, and Table 12.G.

Table 12.F - Fields in the (Labeled) Control Points Definition screen

Field	Description
Ent	The entry number within the group selected (200 entries per group).
Description	The description of the control points. Up to 40 characters
CMD	<p>The command to be sent to the control point.</p> <p>OPR = OPERATE RELAY            RLS = RELEASE RELAY            MON = MOMENTARY ON            MOF = MOMENTARY OFF            SOP = SBO Operate*            SRL = SBO Release*            SMO = SBO Momentary On*            EXE = SBO Execute*            CLR = SCO Clear All*</p> <p>*See Table 12.C for an explanation of the SBO Commands.</p>

**Table 12.F - Fields in the (Labeled) Control Points Definition screen (continued)**

Field	Description
Ch	Channel Number. NG = NetGuardians N2 = Building Access System K1 = VIRTUAL PORT (base and satellite KDAs with relay exp. card) K2 = VIRTUAL PORT (relay and other expansion cards in base KDA's) RP = REMOTE PORT (Modem port) RC = RELAY CARD (102 card - local controls only) AV = AUDIO/VISUAL CARD (108 Card -Only relays 9-12 can be used.) 1-29 = Port Number. IAM Users - Relays 9-12 are not available on AV Card.
D	Device Type. This field is selected only when the selected port is defined for DCM protocol. Selections are: C = CPM S = SBP (Smart Bypass Card - Used only with the Building Access Unit. Three controls may be user-defined for a BAU. See the BAU Operation Guide for details.)
Add	The device address. Valid range is 1-999. This field is skipped when the selected port has been defined for TBOS protocol.
Unt	Unit. The Display (1-64) in which the control points reside. This field is skipped when the selected port has been defined for DCM protocol.
Points	A control point or range of control points that you wish to operate. Ranges may be entered using dashes and/or commas. Valid control point ranges may be from 1-64.

**Table 12.G - Key commands Available in the (Labeled) Control Point Definition screen**

Function Key	Description
F1	Moves the cursor to a selected entry point.
F3	Blank - Deletes current point entry. Leaves an open line. Control Points deleted in this way cannot be recovered by using F10 or Esc.
Alt-F3	Delete - Deletes entry and moves all other lines up.
Alt-F4	Insert - Moves current line down one group and inserts a blank line.
F8	Saves the control point entries and returns to the Site Controls Category Definition screen.
F9	Displays help for this screen.
F10/Esc	Exit or return to start of line.

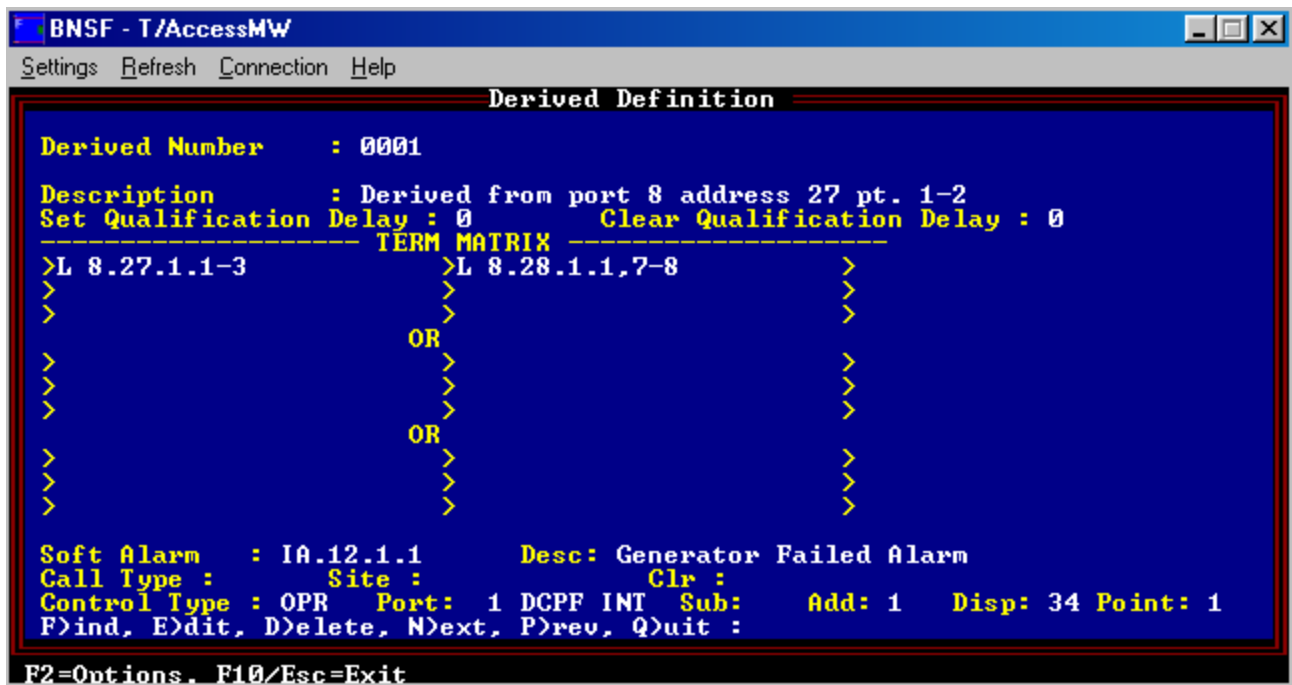


Fig. 12.6 - The derived alarm definition screen

## Derived Alarms/ Controls

Devices must be defined before entering them in an equation.

A derived equation can trigger an alarm, control or both.

Soft alarms are User Defined Internal alarms at address 11 thru 13.

Derived Alarms allow you to take the alarm status of various other alarm points and feed them into an equation to develop a virtual alarm. Based on that, you can declare an alarm or issue a control or do both. Derived Alarms process alarms by using three sections of OR statements. If either of the three sections of OR statements are true then the alarm is considered true. Within each of the OR statements there are up to nine fields. Every field listed in that section is put together using the AND statement. For example, on the Derived Definition screen shown in Figure 12.6 you will note the following equation in the Term Matrix:

>L 8.27.1.1-3	>L 8.28.1.7,8
---------------	---------------

The alarms to be evaluated are live (standing) alarms at port 8, address 27, display 1, points 1 or 2 or 3 and at port 8, address 28, display 1, points 1, 7 or 8. The condition is considered true (alarm state) if both sides of the statement are true (alarm state). You can use up to 9 statements but only two are shown here. Any set of OR statements can have elements from both Live or COS alarms. Live must be currently in the standing alarms list. COS must be currently in the unacknowledged alarms list.

The example screen also defines the Soft alarm that is to occur:

Soft Alarm : IA.12.1.1...
---------------------------

When a derived alarm is determined from this equation, the soft alarm will produce a User Defined Internal Alarm at Port IA address 12, display 1, point 1.

The bottom of the Derived Definition screen (see Figure 12.6), defines the control to be issued. Shown are the following settings:  
Control Type:OPR Port: 2 DCPF INT Add: 1 Disp: 34 Point: 1

When this equation evaluates true, T/MonXM will issue that control. When the condition is no longer true, then T/MonXM will issue the inversion of that control. In this situation, a release (RLS) control would be issued instead of an operate (OPR) control. If it originally issued a momentary (Mon) control it would issue another momentary control.

Equations can also be cascaded. The Soft Alarm that you set can in turn be used as an input into another equation.

Example application of derived alarms:

For example, a power failure alarm might not be a critical alarm, nor a low backup battery. But it is a critical situation if the power fails when the backup battery is low, and you can create a derived alarm, with a severity level of critical, that will occur in that situation. You can also create derived alarms that take time into account. For example, a exterior light failure alarm can be a minor alarm between 6 A.M. and 7 P.M., and a major alarm between 6 P.M. and 7 A.M.

**Table 12.H- Fields in the Derived Definition screen**

Field	Description
Description	Enter the description of the derived definition.
Set Qualification Delay	Time in minutes that is waited after the equation evaluates and remains true before the equation state is officially declared and actions are taken. [0]
Clear Qualification Delay	Time in minutes that is waited after the equation evaluates and remains false before the equation state is officially cleared and actions are taken. [0]
Term Matrix	Enter term. ({/}{L C}{S} [Port IA RP].{SubDev}address.DispRng.PntRng). Ranges are allowed. See the following pages for a more detailed explanation of Derived Alarm syntax and term evaluation.
Soft Alarm	Internal alarm point to set when the equation evaluates true (or to clear when the equation evaluates false). (PORT.ADD.DISP.PNT) Ranges are not allowed. An asterisk can be used as a wild card in the address field only. This will correspond with an asterisk entered in the address field of the Term Matrix. This permits a derived alarm to work with ASCII Templates, which define common displays and points that can be applied across multiple addresses.
Soft Alarm Desc	Description of the Soft Alarm. Changing this field will alter the description of the User Internal Alarm Point. If the User Internal Alarm is not defined, then this field will default to the value of the Derived Alarm Description field.
Call Type	Call to make when soft alarm is set. Valid call types are: None: Don't call. DPM: Call a DPM (Discrete Point Module). ALP: Call an ALP (AlphaMax 82A). KDA: Call a KDA 864. KDA: Call a Time-Stamp KDA KDA: Call a KDA 832-T8 D10: Call a Datalok 10D. ASC: Call an ASCII device.

**Table 12.H - Fields in the Derived Definition screen (continued)**

Field	Description
Site	Site number specified in your dial up device. Only active if you are using a dial-up call. (Refer to Call Type.)
Clr	Call when equation clears. [N] (Refer to Call Type and Site.)
Control Type	Select the type of control (if any) to issue. Valid controls are: None: Don't do anything. RLS: Release. OPR: Operate. MON: Momentary.
Port	This is the Port to issue command. [0]. Valid entries are: 1-500: Device on port 1-500. NG = NetGuardians N2 = Building Access System K1 = VIRTUAL PORT (base and satellite KDAs with relay exp. card) K2 = VIRTUAL PORT (relay and other expansion cards in base KDA's) RP = REMOTE PORT (Modem port) RC = RELAY CARD (102 card - local controls only) AV = AUDIO/VISUAL CARD (108 Card -Only relays 9-12 can be used.) 1-29 = Port Number. IAM Users - Relays 9-12 are not available on AV Card.
Sub	Sub Device Type. Valid types are C (CPM) and S (SBP). (DCM only)
Add	Address of control. Valid addresses are protocol and device dependent.
Disp	Display of control. Valid displays are protocol and device dependent.
Point	Point of control. Valid points are protocol and device dependent.

**Table 12.I - Key commands Available in the Derived Definition Screen**

Function Key	Description
F1	Skips to the next term (group of OR statements) in the Term Matrix.
F2	Options - Issue momentary control on true only; Y/N?
F3	English translation of the term matrix
F6	Read. Load an existing display of alarm point definitions into the Internal Alarms Point Definition Screen. May be further edited.
F8	Saves the Derived Definition database.
F9	Online help.
F10/Esc	Exit.

**Note:** For aid in control point definition refer to the point mapping information in Section 10.

Defining Term Syntax - The syntax for creating a term is as follows:

```
{/} {L/C} {S} PORT.ADDRESS.DISPLAY RANGE.POINT RANGE
or
TIME<HH:MM or TIME>HH:MM
or
DATE>MM-DD-YYYY or DATE<MM-DD-YYYY
or
{/} DAY={SUNDAY:MONDAY:TUESDAY:WEDNESDAY:THURSDAY:FRIDAY:
SATURDAY:WEEKDAYS:WEEKENDS}
```

**Table 12.J - Rules for creating a term**

Term	Definition
/	Logical Not. Reverses the state of the term evaluation.
L	All elements in the term evaluated from the Standing Alarms. (default)
C	Selected points in the term are evaluated from the "Failed COS" list.
S	Ignore silenced alarms. Silenced alarms will be evaluated as false.
PORT	This can be either a single port or a range of ports
Special Ports	IA: Internal alarms (Device/on-off line & Derived). RP: Rac Port. K1 and K2: Virtual ports.
TIME	Time variable in 24 hour format. The time statement <ENTER>ed will be either later than (>) or earlier than (<) the specified time.
DAY	Day of week. Specify SUNDAY, MONDAY, TUESDAY, WEDNESDAY, THURSDAY, FRIDAY, SATURDAY, WEEKDAYS, WEEKENDS. Specify only one day or expression in each term.
DATE	Date variable in DD-MM-YYYY format (e.g. 02-14-2002). Specify only one day or expression in each term. The date statement entered will be either later than (>) or earlier than (<) the specified time.

DISPLAY and POINT can reference a single item or a range of items. The values in the RANGE are grouped together with "OR" operators. Please see the examples below. ADDRESS can also be a wildcard (\*) to accommodate use with ASCII Templates.

**Table 12.K - Term syntax examples**

Term	Definition
1.2.3.4	Port 1, Address 2, Display 3, Point 4
1.*.2.3	Point 3 of Display 2 in any Address on Port 1
2.1.1-32.64	Port 2, Address 1, Point 64 in Displays 1-32
3.2.1-7,9.64	Port 3, Address 2, Point 64 in Displays 1-7 and 9
3.7.5-10, 12-14	Address 3, Display 7, Points 5-10 and 12-14
IA.11.4.1-3	Internal Alarm, Address 11, Display 4, Points 1-3
TIME>13:00	Time of day is after 13:00 (1:00PM)

**Note:** To improve processing efficiency when the same time qualification is used on multiple occasions, use only a single time equation that sets an internal alarm. This can be used in other more detailed terms. This has the added benefit of being able to change such time terms as "daylight" or "first shift" in a single place.

Example: The base time qualification is between 5 AM and 5 PM, Monday through Thursday. The point to be set during this time is internal alarm address 11, display 15, point 1. The statement in the derived definition screen is:

>TIME>5:00	>TIME<17:00	>MONDAY
>TUESDAY	>WEDNESDAY	>THURSDAY
>	>	>
Soft Alarm: 11.15.1		

This time qualification is used in a derived alarm as follows:

>1.2.3.7	>IA.11.15.1	>
>	>	>
>	>	>
Soft Alarm: 11.5.5		

This derived definition will produce an internal alarm at address 11, display 5, point 5 between the hours of 5 AM and 5 PM, Monday thru Thursday, whenever a live alarm exists at port 1, address 2, display 3, point 7.

### How an Equation is Evaluated

Each equation consists of up to three OR statements. Each OR statement contains up to nine terms that are put together using the AND statement (the between each field). Therefore, each OR statement will only be true if all terms in that statement (up to nine) evaluate true. Blank terms evaluate true. The entire equation is considered true if any of the three OR sections are true.

You don't have to fill in each group of OR statements. You can have as few as 1 term and as many as 27 (9 per OR statement with 3 groups of OR statements).

To summarize, T/MonXM first looks at each statement independently, then each AND is evaluated. Finally, the ORs are checked to see if there is a true statement among them. If there is, the equation is true.

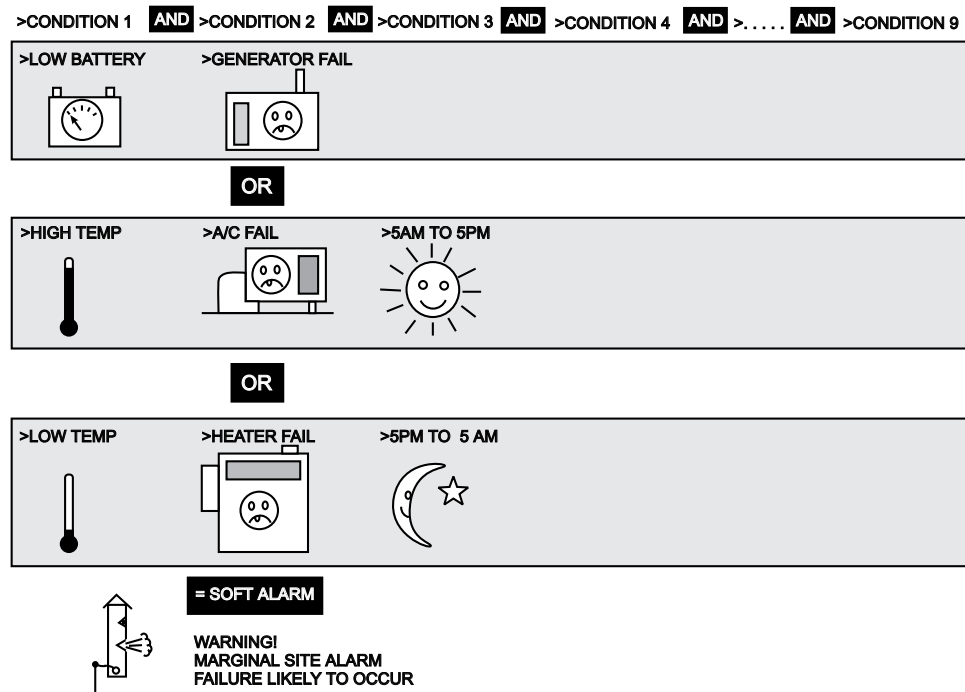


Fig. 12.7 - Diagram of derived alarm logic in T/MonXM.

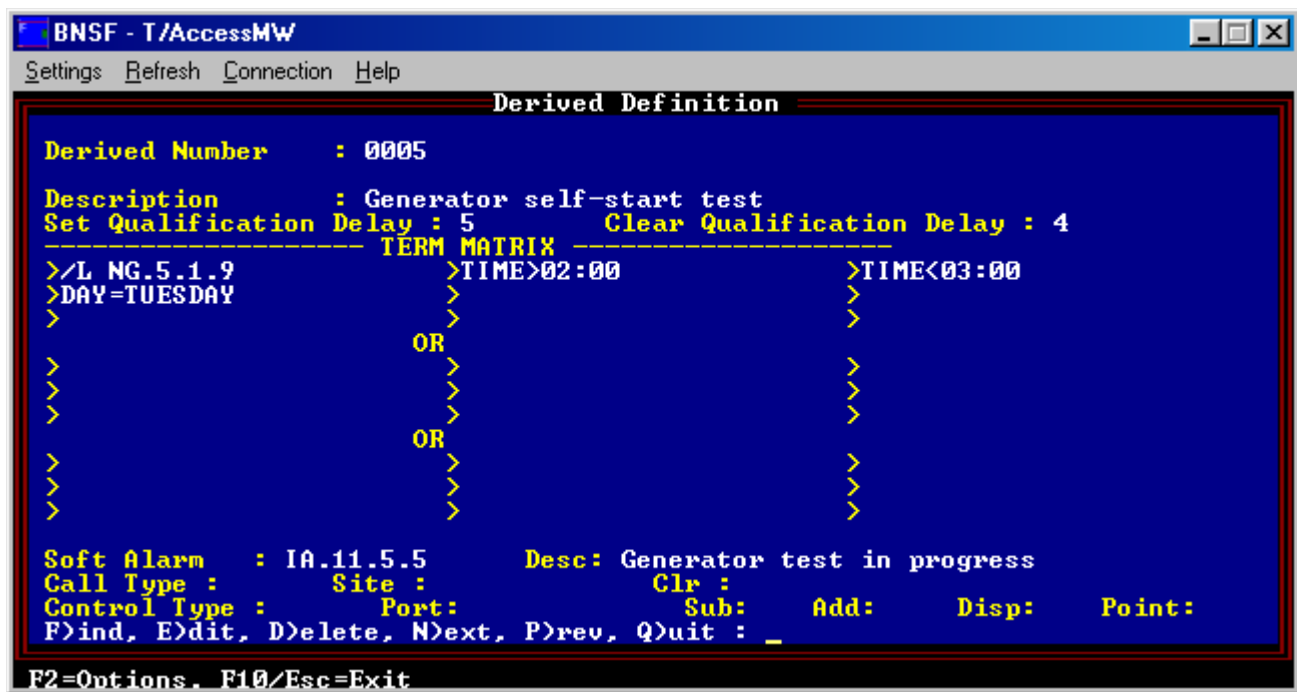


Fig. 12.8 - An alarm that's set only if the specified event *doesn't* happen

## Creating Derived Alarms for Events That Don't Happen

An interesting and useful application of derived alarms is creating alarm formulas that alert you when events do *not* happen. These alarms can inform you of failures where equipment should start and run automatically but does not.

This is particularly useful for maintaining visibility of recurrent background events, such as periodic equipment tests. A weekly alarm informing system operators that all is well is a nuisance alarm that will be ignored, and no one will notice when the alarm doesn't happen. A negative derived alarm will instead inform system operators only when the equipment test fails.

For example, let's say a generator is supposed to run a self-start test early every Tuesday morning, and you want to know if the generator doesn't self-start. When the generator starts, it sends an alarm signal to a NetGuardian, which is mapped in T/MonXM to the alarm point NG.5.1.9.

So you could create the alarm formula shown in Figure 12.8, which states: `/L.NG.5.1.9` and `TIME>02:00` and `TIME<03:00` and `DAY=TUESDAY`.

Translated into English, this says, "Declare an alarm if no alarm signal is received at NG.5.1.9 between 2:00 and 3:00 A.M. on Tuesday."

By adding the `/` (NOT) symbol before the alarm point, you have defined the derived alarm to occur when the alarm at the NetGuardian point doesn't happen.

The time and day terms are important, because they define when the test should happen. The NetGuardian alarm point will, of course, be inactive all other times as well, but you're only interested in the alarm point's inactivity during the time the test should take place.



**This page intentionally left blank.**

## Section 13 - Define Building Status Unit Controls



**Fig. 13.1 - The Building Status Unit (BSU) shows overall facility alarm status.**

BSU fields and key commands are defined in Table 13.A and Table 13.B.

### Introduction

The Building Status Unit (BSU) mounts near the door of a remote site facility to provide personnel with a “last chance out the door” view of how the site is functioning. If there is an alarm condition, the lamps on the BSU will indicate the level of the alarm. A red lamp indicates a critical alarm, an amber lamp indicates a major alarm, and a green lamp indicates a minor alarm. A flashing indicator and audible alarm signals a change of state. A Line On/Line Off or Sanity indicator is Green when all is well, Red when communications fail between the workstation and the BSU and Off when power fails. There is no indicator for alarms defined as status level.

A local BSU can also be used at the location of the T/MonXM WorkStation to provide summary alarm information to personnel located away from the screen.

Alarm points are assigned to windows under the Remote Ports sub-menu of the Parameters Menu. For an alarm to cause a BSU to be activated it must be assigned to a window which has that BSU defined.

### BSU Activation Overview

The BSU is activated through a window. It will respond to all alarms defined for that window. Thus, if there is a window assigned to Fire Alarms, a BSU located at the fire station could be activated through that window. This gives the fire department instantaneous notification of alarms.

The BSU’s indicators are operated by contact closures. Four are required (Critical, Major, Minor and Sanity or Line On/Line Off.) There are two ways T/MonXM can activate them (see Figure 13.2):

1. Locally by either a 108 Card (included with T/MonXM - also called an Audible Alarm Card or AV Card) or by a 102 Card.
2. Remotely by issuing controls via protocols which are converted into relay closures by a Remote Telemetry Unit. For example, DCP(F) protocol could be used to control 4 relays on a KDA. The outputs of the KDA relays would operate the BSU indicators.

**Note:** In many cases it is possible to use the BSU window/relay interface to drive existing light panels.

Once you have defined the window name, pressing F2 (BSU) from the Window Definition screen takes you to the BSU Definition screen (see Figure 13.2). Because the BSU is tied to a window, when there is an alarm in that window it will be sent to the BSU. For a local BSU you must also define a 102 or 108 Relay Card.

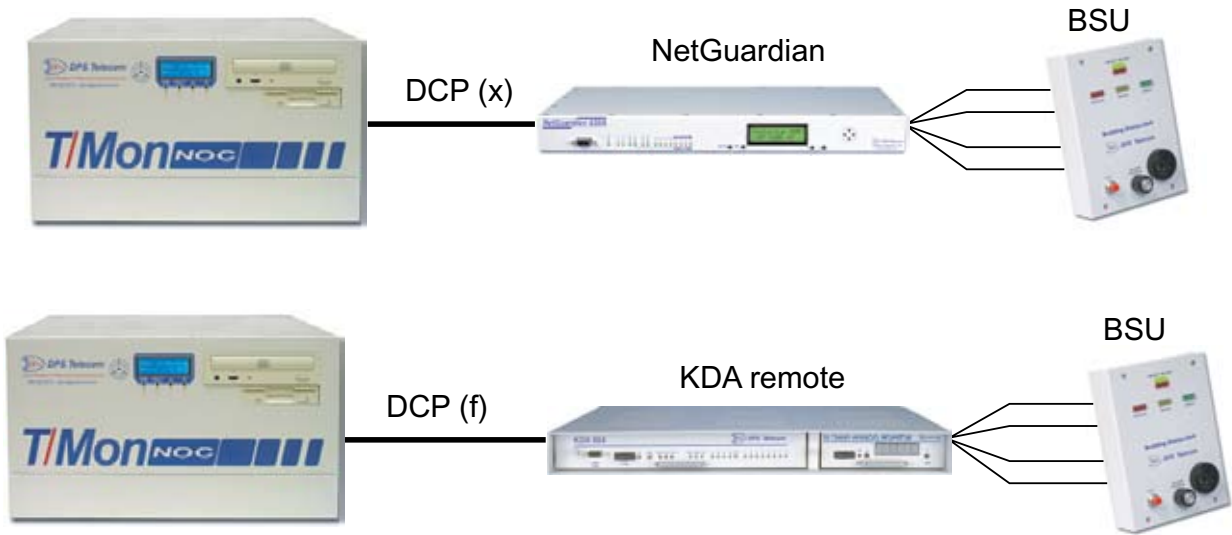


Fig. 13.2 - Two BSU applications

# Assign Controls

Control relay assignments depend on how the RTU is wired to the BSU.

If you enter a port number for remote operation, the protocol of the interrogator on the port selected will automatically appear in the protocol field. The cursor will jump to the next required field, depending on the protocol. Then type in the required entries to activate the control relays for Critical, Major, Minor and Sanity (On Line/Off Line).

If you enter RC or AV for local operation, the cursor will jump to the point field. Type in the number of the relay that will activate the BSU for Critical, Major, Minor and Sanity (On Line/Off Line).

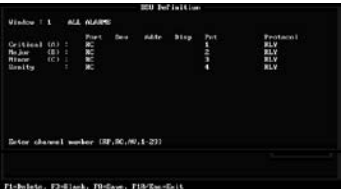


Fig. 13.3 - The BSU Definition screen

**Note:** Later in the data basing procedure when you select the BSU option from the Parameters menu, it will take you to the BSU Frequency screen. The Sanity Frequency field is set so T/MonXM can pulse the sanity point. This pulsing tells the BSU it is in contact with T/MonXM. When pulses do not occur faster than the rate selected by DIP switches in the BSU, the Sanity light will turn Red, indicating that the alarm display is not current. Sanity only works on BSU devices. You can also define the Update Frequency for all BSU relays to be refreshed. For more details see the following pages.

Interrogator Ports must be defined under the Parameters Menu before using the BSU Definition screen.

**Table 13.A - Fields in the the BSU Definition screen**

Field	Description
Port	Identify local relay card or remote port number controlling the BSU. Valid entries are: RC = 102 Relay Card AV = Audio Visual Card (108 card) 1-500 = Remote port number <b>NOTE:</b> The selected port's protocol will appear in the Protocol field.
Dev	Cursor goes to DEV only for DCM protocol devices. Enter the device type. The only valid device for a BSU is CPM (Control Point Module). While the SBP (Smart Bypass Card) is offered, it is used only with the Building Access Unit (BAU).
Addr	Cursor goes to Addr only for DCM & DCP/DCP(F)/DCP(X)
Disp	Cursor goes to Disp only for TBOS & DCP/DCP(F)/DCP(X)
Pnt	Enter the point number. Valid points are: 1-64 for remote ports
Protocol	The protocol of the interrogator on the port selected will automatically appear in the Protocol field.

**Note:** The 102 Card is not the standard audio/video card. It is another relay card with 12 control points that are available for general use.

**Table 13.B - Key commands available in the BSU screen**

Function Key	Description
F1	Delete BSU definition. This will delete the entire BSU Definition from the screen. This option does not delete just one line.
F3	Blanks all the fields in the current row.
F8	Saves the BSU Definition database and returns to the Window Definition screen. <b>NOTE:</b> Define points for Critical, Major and Minor before saving.
F10/Esc	Exit

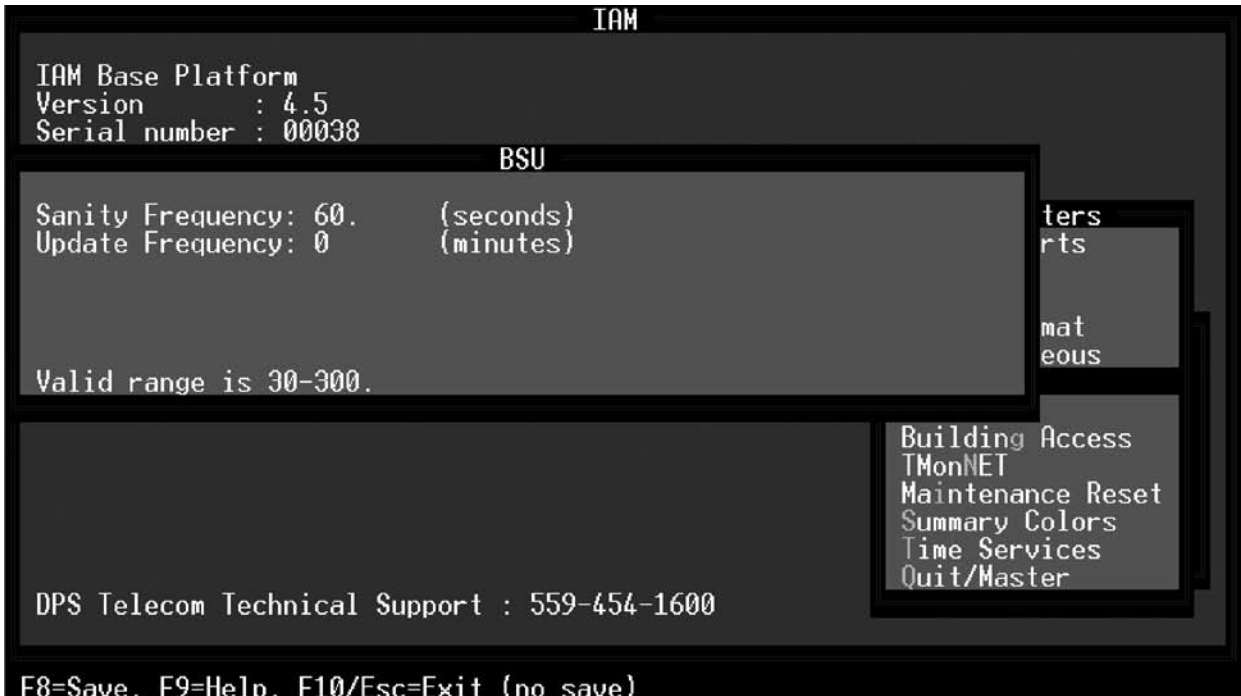


Fig. 13.4 - The building status definition screen

# Configure Sanity Frequency

Selecting BSU from the Parameters menu (press B to select BSU and press Enter) will allow you to configure the Sanity Frequency (how often the BSU is polled for online status) and the Update Frequency (how often all BSU relays are refreshed.)

Table 13.C lists of screen options for the BSU screen:

Table 13.C - Fields in the BSU screen

Field	Description
Sanity Frequency	The Sanity Frequency field is set so T/MonXM can pulse the sanity point. This pulsing is the mechanism by which the BSU knows it is in contact with T/ MonXM. When pulses do not occur faster than the rate selected by DIP switches in the BSU, the BSU Sanity light will turn Red, indicating to the observer that the alarm display is not current. Sanity only works on BSU devices. Valid range is 30-300 seconds.
Update Frequency	The Update Frequency is the frequency that all BSU relays will be refreshed. Valid range is 5-60 minutes. A 0 entry indicates never update.

Table 13.D - Key commands available in the BSU screen

Function Key	Description
F8	Saves the BSU parameters settings
F9	On-line help
F10/Esc	Exit

BSU Definition is available from the File Maintenance menu by selecting the Windows command and pressing F2 for BSU.

## Section 14 - Define Internal Alarms

Selecting the Internal Alarms option from the Files Maintenance menu will bring up the Internal Alarms menu. From this menu, you will be able to edit Standard Alarms and User Defined Alarms.

Internal Alarms are handled by T/MonXM to report events developing within the system environment. There are two (2) types of Internal Alarms, Standard and User-Defined (see Figure 14.2).

Standard Alarms are pre-defined alarms processed exclusively by T/MonXM. Standard Alarms use address 0, display 1, points 1-64, display 2, points 1-7, and address 13, Display 1, points 1-2 — see Table 14.A and 14.B

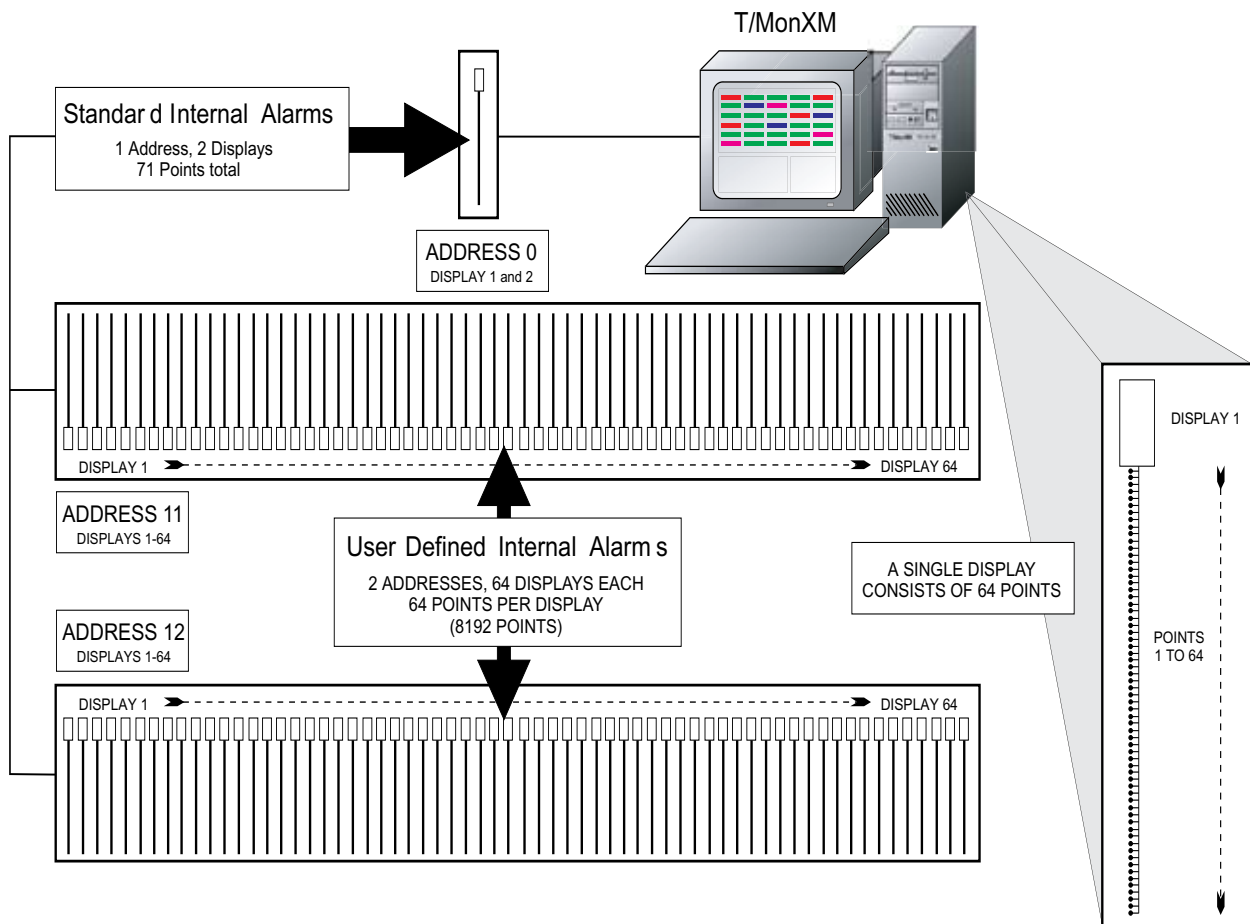
System Health Alarms are predefined alarms. System Health Alarms use address 14, display 1, points 1-64

User Defined Alarms are defined by the user and are activated either by a device going online or offline, or by a user defined equation (derived alarm). User Defined Alarms occupy 2 addresses (11 and 12) with 157 displays, each with 64 points for a total of 8,192 addressable points. This expendability makes the management of such alarms very flexible.

ASCII template users may use Local Displays to store internal (derived) alarms. See the ASCII Templates in Software Module 6.



Fig.14.1 - The Internal Alarms menu



**Fig. 14.2 - Standard and user defined internal alarms layout**



Fig. 14.3 - Standard alarms are configured in the point definition screen

# Internal Alarms Point Definition Screen

Internal Standard Alarms always have Address 0. User Defined Internal Alarms always have either address 11 or 12. Port related internal alarms have address 13.

The Point Definition screen is used to define alarm points for the Standard and User Defined Internal alarms. For more detailed information on Point Definition and editing procedures — see Section 10 (Point Definition Tutorial).

Internal alarms are reported on the screen in the following format:  
**IA Address. Display. Point**

For example, IA 0. 1. 7 refers to an Internal Alarm in internal address 0, display 1, point 7. Because it is in address 0, this is a Standard Internal Alarm. IA 11.1.2 would refer to an Internal Alarm in internal address 11, display 1, point 2. Because it is in address 11, this is a User Defined Internal Alarm.

# Standard Internal Alarms

Every time certain system specific actions are performed with T/MonXM, a standard alarm is reported. For example, when T/MonXM goes offline, the standard alarm point 7 “T/MonXM OFFLINE” is reported.

Standard alarms are pre-defined for use with T/MonXM and are activated internally. These internal alarms are reported on address 0 and display 1 and 2. Port-related internal alarms are reported on address 13 (Only two alarms are reported on address 13 and they apply to Alt Path and Teltrac Mux only). Selecting Standard Alarms from the Internal Alarms menu will bring up the Point Definition screen for Standard Internal Alarms (Figure 14.3).

This screen permits you to assign the editable options and window



for a particular alarm. Press E to edit. Editable options include Log, History, Levels, Status, Fail, Clear, Windows and Message.

Standard Alarms in display 1 are listed in Table 14.A. Standard Alarms in display 2 are listed in Table 14.B.

**Table 14.A - Standard Internal Alarms in display 1**

1 GOING ACTIVE	34 REMOTE TERMINAL HAS FAILED [6]
2 GOING PASSIVE	35 REMOTE TERMINAL HAS FAILED [7]
3 NO ACTIVITY ONLINE*	36 REMOTE TERMINAL HAS FAILED [8]
4 ACTIVITY DETECTED	37 PWR FAILURE; SWITCH TO BATTERY
5 ADDRESS TAKEN OFFLINE	38 LOW BATTERY CONDITION DETECTED
6 DEVICE FAILURE	39 UPS TIMEOUT OCCURRED
7 T/Mon (or IAM) OFFLINE*	40 LED BAR OFFLINE
8 T/Mon (or IAM) ONLINE*	41 BLDG ACCESS LOG ON
9 TASK CARD NOT FUNCTIONING	42 BLDG ACCESS LOG OFF
10 HST COM ERROR WITH D/TASK CARD	43 RCVD CTL:
11 UNABLE TO RESTART TASK CARD	44 WORKSTATION RESET ATTEMPTED
12 Unassigned	45 REMOTE 3 CARD NOT FUNCTIONING
13 REMOTE CARD 1 NOT FUNCTIONING	46 STANDBY IS ACTIVE
14 REMOTE CARD 2 NOT FUNCTIONING	47 REMOTE LOG IN:
15 ASCII DATABASE IS FULL - PORT	48 AUTO RESTART OCCURRED
16 DIAL-UP DEVICE FAILURE	49 REMOTE 4 CARD NOT FUNCTIONING
17 AUTO-CUTOFF ENABLED (LPT1)	50 MAS DATABASE ERROR
18 AUTO-CUTOFF ENABLED (LPT2)	51 REMOTE LOG OUT:
19 PRINT AUTO-CUTOFF ENABLED [1]	52 REMOTE LOG OUT:
20 PRINT AUTO-CUTOFF ENABLED [2]	53 REMOTE LOG OUT:
21 PRINT AUTO-CUTOFF ENABLED [3]	54 REMOTE LOG OUT:
22 PRINT AUTO-CUTOFF ENABLED [4]	55 ASCII LOG STOPPED: DISK FULL
23 PRINT AUTO-CUTOFF ENABLED [5]	56 DURESS LOG IN:
24 PRINT AUTO-CUTOFF ENABLED [6]	57 REMOTE 5 CARD NOT FUNCTIONING
25 PRINT AUTO-CUTOFF ENABLED [7]	58 DATABASE NEEDS TO BE BACKED UP**
26 PRINT AUTO-CUTOFF ENABLED [8]	59 REMOTE 6 CARD NOT FUNCTIONING
27 PRINTER HAS FAILED (LPT1)	60 NO DIAL TONE ON PAGER PORT
28 PRINTER HAS FAILED (LPT2)	(Alpha, 2-Way, and Logger paging)
29 REMOTE TERMINAL HAS FAILED [1]	61 UNEXPECTED ENTRY:
30 REMOTE TERMINAL HAS FAILED [2]	62 UNAUTHORIZED ENTRY:
31 REMOTE TERMINAL HAS FAILED [3]	63 UNABLE TO ACCESS TIME SERVICE
32 REMOTE TERMINAL HAS FAILED [4]	64 NO DIAL TONE ON THE ASCII PORT
33 REMOTE TERMINAL HAS FAILED [5]	

\*Change of State (COS) alarm only.

\*\*Set the number of days in Parameters/Misc.

The Pol, Rvs and Description fields cannot be edited for Standard Internal Alarms. See the following pages for more information.

The ADDRESS TAKEN OFFLINE (Point 5) and DEVICE FAILURE alarm (Point 6) alarms will report the site name (obtained from the database).

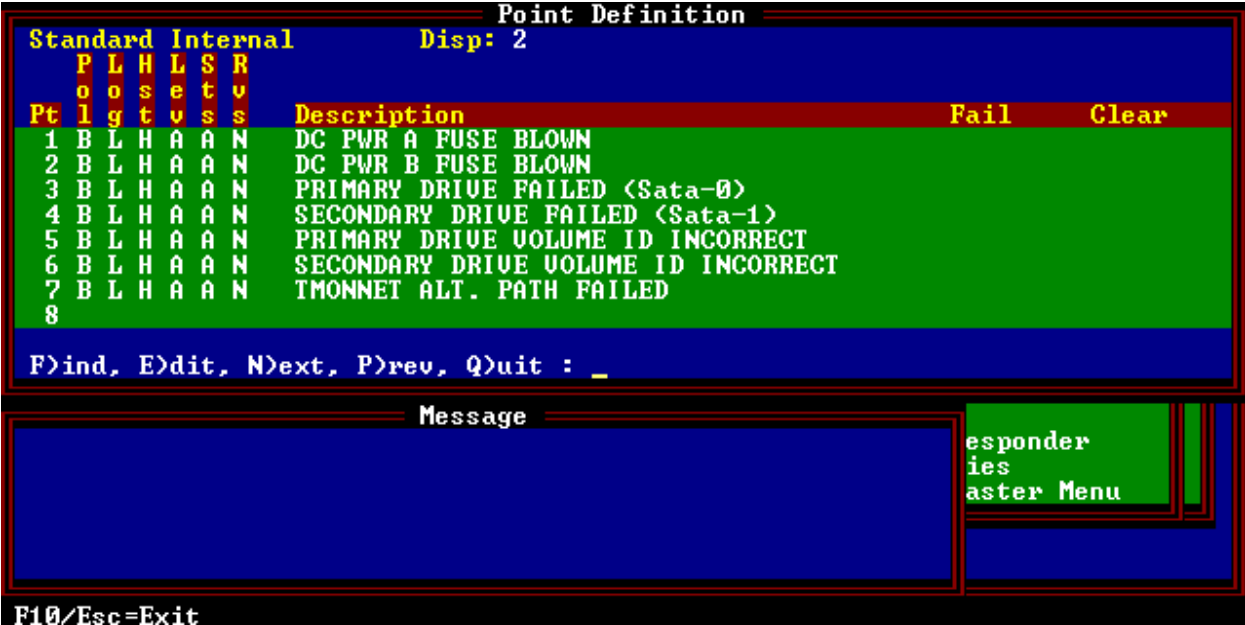


Fig. 14.4 - Standard alarms in display 2

To edit standard alarms in display 2, press N (Next) and then press E (Edit). For alarm descriptions, see the following pages.

**Table 14.B - Standard internal alarms in display 2**

Point Number	Description
1	DC PWR A FUSE BLOWN
2	CD PWR B FUSE BLOWN
3	PRIMARY DRIVE FAILED (Sata-0)
4	SECONDARY DRIVE FAILED (Sata-1)
5	PRIMARY DRIVE VOLUME ID INCORRECT
6	SECONDARY DRIVE VOLUME ID INCORRECT
7	TMONET ALT. PATH FAILED
8	NIC IRQ UNDEF - LEGACY MODE ACTIVE
9	PCI SERIAL CARD 1 FAILED
10	PCI SERIAL CARD 2 FAILED
11	PCI SERIAL CARD 3 FAILED
12	SERIAL PORT FAILED
13	SERIAL PORT TX BUFFER OVERFLOW
14	DEVICES AVAILABLE LESS THAN 10%
15	POINTS AVAILABLE LESS THAN 10%
16	POINTS AVAILABLE EXCEEDED
17	CANNOT CONNECT TO SNPP SERVER
18	CANNOT CONNECT TO SNMP SERVER
19	CANNOT CONNECT TO DNS SERVERS
20	CPU TEMPERATURE OUT OF TOLERANCE
21	AMBIENT TEMPERATURE OUT OF TOLERANCE
22	CPU FAN SPEED OUT OF TOLERANCE
23	AUXILARY FAN SPEED OUT OF TOLERANCE
24	LOW DISK SPACE DETECTED
25	PAGER CONNECTION ERROR
26	CANNOT CONNECT TO EXP VOICE DIALER
27	CONNECTION ERROR WITH PROXYIP
28	CONNECTION ERROR WITH PROXYIP DATA
29	CONNECTION ERROR WITH PROXYIP SERIAL
30	CONNECTION ERROR WITH PROXYIP FP
31	LOW MEMORY DETECTED

Internal alarms exist within T/MonXM for the purpose of indicating the status of the system. T/MonXM internal alarms are not directly generated from the outside environment. Internal alarms are created within the software when T/MonXM or its hardware have switched its mode or status of operation.

Below is a list of the internal alarms that may be generated from T/MonXM and a description of each. These alarms will show up while in monitoring mode just like a point alarm would.

**Note:** Internal alarms marked with an asterisk will only show up in the Change Of State window and will not show up in the Live Alarms window.

---

## Address 0 Display 1 Alarms

### 1 GOING ACTIVE

A Level A internal alarm that indicates T/MonXM is actively polling the channel specified. This alarm will occur when you first go into monitor mode and T/MonXM is in Master Mode. This will also occur when in combined mode and T/MonXM switches from passive to active polling.

### 2 GOING PASSIVE

A Level A internal alarm that indicates T/MonXM is passively monitoring the channel specified. This alarm will occur when you first go into monitoring mode and T/MonXM is set to Passive Mode. This alarm will also occur when in combined mode and T/MonXM switches from active polling to passive monitoring.

### 3 NO ACTIVITY ON LINE

A Level D internal alarm that occurs when monitoring, and the period of Warning Threshold seconds expire, without any activity being detected on the line.

### 4 ACTIVITY DETECTED

A Level D internal alarm that is the complement of internal alarm number 3. It occurs if alarm number 3 has failed and activity is detected on the Line.

### 5 ADDRESS TAKEN OFFLINE

A Level D internal alarm that occurs when an address is manually taken offline.

### 6 DEVICE FAILURE

Occurs when a device has been determined to be non-responsive.

### 7 T/MonXM OFFLINE

A Level D internal alarm that occurs when the system returns to the Master Menu from Monitor Mode. Note: Each address can have its own internal alarm of this type.

### 8 T/MonXM ONLINE

A Level D internal alarm that occurs when Monitor Mode is selected from the Master Menu.

**Note:** The Offline and Device Failure alarms are system default alarms that share the same internal alarm point. DPS Telecom recommend you use user-defined device failure and offline alarms for improved granularity and control. For details, see section 14-11.

#### **9 TASK CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Task Card. Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm of type 11 will be declared. Type: COS only.

#### **10 HST COM ERROR WITH D/TASK CARD**

Dtask report communication error

#### **11 UNABLE TO RESTART TASK CARD**

Occurs after an internal alarm of type 9 has occurred and activity still cannot be detected from the card. Type: COS only.

#### **12 UNASSIGNED**

#### **13 REMOTE 1 CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Remote 1 card (Intelligent Controller Card for ports 1-4). Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm of type 15 will be declared. Type: COS only. Port related internal alarms are reported on address 13.

#### **14 REMOTE 2 CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Remote 2 card (Intelligent Controller Card for ports 5-8). Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm of type 16 will be declared. Type: COS only.

#### **15 ASCII DATABASE IS FULL - PORT**

An auto ASCII port is full.

#### **16 DIAL-UP DEVICE FAILURE**

A dial-up address has failed (mat shelf).

#### **17 AUTO-CUTOFF ENABLED (LPT1)**

Occurs when the printer buffer for LPT1 is full or there is not enough disk space to expand the buffer. Type: COS and Standing alarms.

#### **18 AUTO-CUTOFF ENABLED (LPT2)**

Occurs when the printer buffer for LPT2 is full or there is not enough disk space to expand the buffer. Type: COS and Standing alarms.

#### **19 PRINT AUTO-CUTOFF ENABLED [1]**

Occurs when the printer buffer for Remote 1 is full or there is not enough disk space to expand the buffer. Type: COS and standing alarms.

#### **20 PRINT AUTO-CUTOFF ENABLED [2]**

#### **21 PRINT AUTO-CUTOFF ENABLED [3]**

#### **22 PRINT AUTO-CUTOFF ENABLED [4]**

#### **23 PRINT AUTO-CUTOFF ENABLED [5]**

#### **24 PRINT AUTO-CUTOFF ENABLED [6]**

**25 PRINT AUTO-CUTOFF ENABLED [7]****26 PRINT AUTO-CUTOFF ENABLED [8]**

Internal Alarms numbering 20 through 26 occur when the printer buffer for Remotes 2 through 8 are full or there is not enough disk space to expand the buffer. Type: COS and standing alarms.

**27 PRINTER HAS FAILED (LPT1)**

Occurs when the printer connected to LPT1 fails. Type: COS and Standing alarms.

**28 PRINTER HAS FAILED (LPT2)**

Occurs when the printer connected to LPT2 fails. Type: COS and Standing alarms.

**29 REMOTE TERMINAL HAS FAILED [1]**

Internal Alarms numbering 30 through 36 occur when Remotes 2 through 8 have failed.

**30 REMOTE TERMINAL HAS FAILED [2]****31 REMOTE TERMINAL HAS FAILED [3]****32 REMOTE TERMINAL HAS FAILED [4]****33 REMOTE TERMINAL HAS FAILED [5]****34 REMOTE TERMINAL HAS FAILED [6]****35 REMOTE TERMINAL HAS FAILED [7]****36 REMOTE TERMINAL HAS FAILED [8]****37 PWR FAILURE; SWITCH TO BATTERY**

Occurs when system power fails and the WorkStation switches to battery power.

**38 LOW BATTERY CONDITION DETECTED**

Occurs after an internal alarm of type 37 has occurred and line power still cannot be detected from the WorkStation. Occurs when a low battery condition is detected and UPS shutdown is imminent.

**39 UPS TIMEOUT OCCURRED**

Occurs after an internal alarm of type 37 has occurred and line power still cannot be detected from the WorkStation. Occurs when Uninterruptible Power System shutdown is imminent because of a user preset timeout.

**40 LED BAR OFFLINE**

Occurs when T/MonXM can't communicate with the LED Bar and it goes offline.

**41 BLDG ACCESS LOG ON**

Occurs when T/MonXM acknowledges a building access Log On.

**42 BLDG ACCESS LOG OFF**

Occurs when T/MonXM acknowledges a building access Log Off.

**43 RCVD CTL**

Occurs when any of the responders receives a control. The port.address.display.point of the control that was received follows the colon. For example: RCVD CTL : 6.1.3.2

**44 WORKSTATION RESET ATTEMPTED**

CTRL-ALT-Delete reset attempted.

**45 REMOTE 3 CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Remote3 card (Intelligent Controller Card for ports 9-12). Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm will be declared. Type: COS only.

**46 STANDBY IS ACTIVE**

Indicates secondary master is active.

**47 REMOTE LOG IN**

Occurs when a DTMF or BAU Log In occurs. The initials of the person logged in follows the colon.

**48 AUTO RESTART OCCURRED**

Occurs when T/MonXM automatically returns to Monitor Mode after a power failure.

**49 REMOTE 4 CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Remote 4 card (Intelligent Controller Card for ports 13-16). Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm will be declared. Type: COS only.

**50 MAS DATABASE ERROR**

MAS database checksum error.

Internal Alarms numbering 51 through 54 occur when a Remote Log Out occurs.

**51 REMOTE LOG OUT:**

Internal Alarm number 51 occurs when a Level A alarm is the highest standing alarm at the time of the remote log out.

**52 REMOTE LOG OUT:**

Internal Alarm number 52 occurs when a Level B alarm is the highest standing alarm at the time of the remote log out.

**53 REMOTE LOG OUT:**

Internal Alarm number 53 occurs when a Level C alarm is the highest standing alarm at the time of the remote log out.

**54 REMOTE LOG OUT:**

Internal Alarm number 54 occurs when a Level D alarm is the highest standing alarm at the time of the remote log out. The initials of the person logged out follows the colon.

**55 ASCII LOG STOPPED: DISK FULL**

Occurs when there is not enough disk space to save the ASCII data.

**56 DURESS LOG IN**

Occurs when a Duress Log In occurs. The initials of the person logged in follows the colon.

**57 REMOTE 5 CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Remote 5 card (Intelligent Controller Card for ports 17-20). Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm will be declared. Type: COS only.

**58 DATABASE NEEDS TO BE BACKED UP****59 REMOTE 6 CARD NOT FUNCTIONING**

Occurs when the program cannot detect activity from the Remote 4 card (Intelligent Controller Card for ports 21-24). Immediately after this alarm is declared, the program will reset the card. If activity is still not detected then an internal alarm will be declared. Type: COS only.

**60 NO DIAL TONE ON PAGER PORT**

Applies to alpha, 2-way and logger paging.

**61 UNEXPECTED ENTRY**

BAU at a remote site has a log in, but there is no door alarm.

**62 UNAUTHORIZED ENTRY**

BAU at a remote site has a door alarm with no log in.

**63 UNABLE TO ACCESS TIME SERVICE**

Occurs when the time synchronization is turned on and the system is unable to communicate with the time service. Can be caused by no phone line, no dial tone or wrong phone number. This applies to both the Dial-up and NTP time services.

**64 NO DIAL TONE ON THE ASCII PORT**

Applies to ASCII Dialup.

---

## Address 0 Display 2 Alarms

**1 DC PWR A FUSE BLOWN**

Fuse A has blown on a DC powered T/Mon NOC.

**1 DC PWR B FUSE BLOWN**

Fuse B has blown on a DC powered T/Mon NOC.

**3 PRIMARY DRIVE FAILED (Sata-0)**

The primary hard drive on a T/Mon NOC has failed. Contact DPS Telecom Technical Support for a new hard drive.

**4 SECONDARY DRIVE FAILED (Sata-1)**

The secondary hard drive on a T/Mon NOC has failed. Contact DPS Telecom Technical Support for a new hard drive.

**5 PRIMARY DRIVE VOLUME ID INCORRECT**

Primary hard drive volume ID incorrectly named for hard drive mirroring. Contact DPS Telecom Technical Support.

**6 PRIMARY DRIVE VOLUME ID INCORRECT**

Secondary hard drive volume ID incorrectly named for hard drive mirroring. Contact DPS Telecom Technical Support.

**7 TMONNET ALT PATH FAILED**

The TMonNet alternate communication path has failed.



#### **8 NIC IRQ UNDEF - LEGACY MODE ACTIVE**

Your system is configured to run in enhanced mode and the TCP Agent cannot detect the IRQ of the network adapter. This is probably due to your system having an ISA network adapter that does not support the PCI BIOS. You will need to configure your system to run in legacy mode. This can be done from the W/Shell > Network Setup menu by setting the legacy mode field to “Y” and rebooting your system. If you would like to run your system in enhanced mode, contact DPS Technical Support and ask about upgrading your network adapter.

#### **9 PCI SERIAL CARD 1 FAILED**

#### **10 PCI SERIAL CARD 2 FAILED**

#### **11 PCI SERIAL CARD 3 FAILED**

System detected a parity error on serial card. The PCI card may need to be reseated to make sure connections are secure.

#### **12 SERIAL PORT FAILED**

Failed to transmit data out of serial port buffer. Try reseating the PCI card or reinitialize.

#### **13 SERIAL PORT TX BUFFER OVERFLOW**

Transmit buffer is full for serial port. When this alarm is created, it had already flushed out the current buffer. This indicates that the transmit buffer was full and was flushed out to make room for new data that needs to be transmitted.

#### **14 DEVICES AVAILABLE LESS THAN 10%**

Only applies to T/Mon SLIM. Gives warning if available devices are running low.

#### **15 POINTS AVAILABLE LESS THAN 10%**

Only applies to T/Mon SLIM. Gives warning if available points are running low.

#### **16 POINTS AVAILABLE EXCEEDED**

Only applies to T/Mon SLIM. Gives warning that all available points has been used up.

#### **17 CANNOT CONNECT TO SNPP SERVER**

Failed to connect to SNPP server.

---

## Address 13

### Display 1

### Alarms

#### 1 ALTERNATE PATH ACTIVE

Teltrac Mux alternate path is in use. The main polling path has been disrupted.

#### 2. ALTERNATE PATH FAILED

The Teltrac Mux alternate path connection failed.

#### 1. T/MON NRI QUEUE FULL

The T/Mon NRI Queue has reached its maximum capacity.

Everything that needs to be sent will be dumped. This could indicate that NRI units are now out of sync.

---

## Address 14

### Display 1

### Alarms

Entering F3 (Int Alarms) from the Remote Device Definition screen for defined Interrogators will bring you to the Device Internal Alarm Assignment screen — see Figure 14.5.

It's very important to define the internal alarms for each of your devices. If internal alarms are not defined for a device, any failure of that device will be reported by the default device failure alarm.

Undefined device failures are reported by the default device alarm, which always reports to the same point, IA.0.1.6. This default alarm simply informs you that an undefined device failure has occurred, and does not specify the device or the nature of the failure.

Internal device alarms are extremely useful for having better control of your devices, better descriptions of your alarms, and are essential for derived alarm applications.

The fields on the Device Internal Alarm Assignment screen are as follows:

---

## Internal Alarms

## Assignments

Device Internal Alarm Assignment				
Port : 9				
Address	Dev	Description	Fail	Offline
1	DCPf	Sites 1-11	11.1.3..	11.1.4
Enter internal point (addr.disp.pnt) (blank=none) (address range: 11-13)				
F8=Save, F10/Esc=Exit				

Fig. 14.5 - Device Internal Alarm Assignment screen

Table 14.C - Fields on the Device Internal Alarm Assignment screen

Field	Description
Port	The port used by the remote device.
Address	The address used by the remote device.
Dev	The remote device.
Description	The display description (optional).
Fail	This is the internal alarms point that is generated if it doesn't answer or is failed. Enter the internal point (address.display.point) for Fail. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.
Offline	Manually takes an address offline using line mode. This the alarm you would see. If you don't type anything here you get a standard alarm. Enter the internal point (address.display.point) for Offline. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.

**Note:** You can see the Internal Alarm Assignment from File Maintenance/Internal Alarms/User Defined Alarms. To do this, from the User Defined Internal Alarms screen, define the address and display if not already defined. Press F1 (Points) to see the Internal Alarm on the Point Definition screen.

## User Defined Internal Alarms

**Note:** User Defined Internal Alarms originate from remote port device failures or derived alarms. These alarms must first be assigned in Remote Ports - Device Definition or in Derived Alarms. Next, the alarm is further defined on the screens described on the following page. This procedure creates the point and gives it a default description (which may be modified).

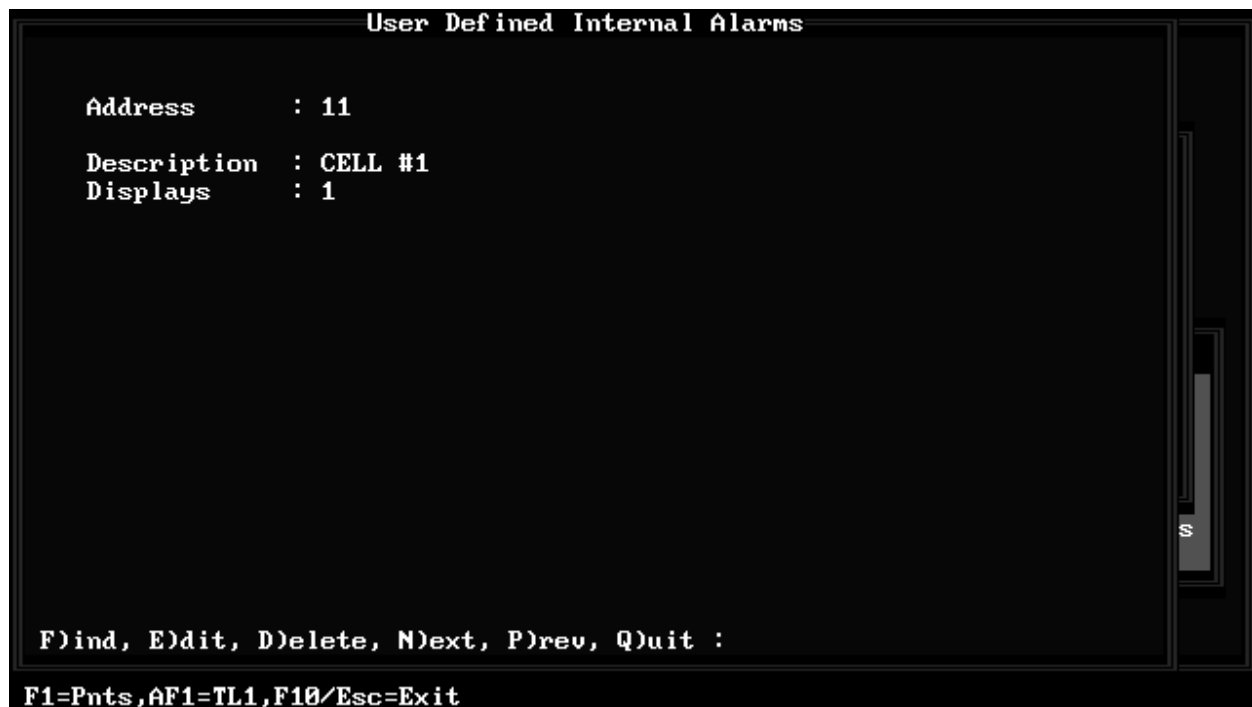


Fig. 14.6 - The user defined internal alarms screen

The POL and RVS fields cannot be edited for User Defined Internal Alarms.

When the User Defined Alarms option is executed the User Defined Internal Alarms screen appears. enter either Address 11 or 12. Enter an optional description and the displays (1-64) to use. Selecting Points (F1) from the User Defined Internal Alarms screen takes you to the Point Definition screen for User Defined Internal Alarms. The pre-assigned internal alarms can be further defined from this screen. Refer to Section 10 for information on point definition.

Typing Alt-F1 takes you to the Sid Definition screen for TL1 Alarms. Refer to Software Module 13 (TL1Responder) for details.

**Note:** Recommended pattern for internal alarm assignment:

- Address 11, Display 1 = first 64 device failures;
- Address 11, Display 2 = first 64 Off Line;
- Address 11, Display 3 = next 64 device failures
- Address 11, Display 4 = next 64 Off Line
- Address 11, Display 21 = Derived Alarms; etc.

T/MonXM notes the alarms origin in the upper right corner so you'll know where it originated after editing its description.

### How To Create User Defined Internal Alarms

User Defined Internal Alarms are created by assigning a derived alarm, device failure or device offline alarm. These are assigned in either the Remote Ports - Device Definition screen (see Figure 14.7) or the Derived Alarms screen. Then go to the Internal Alarms Point Definition screen to further define the alarm (refer to section 14-3). Note that the description for the alarm will already be in the Description field but can be edited.



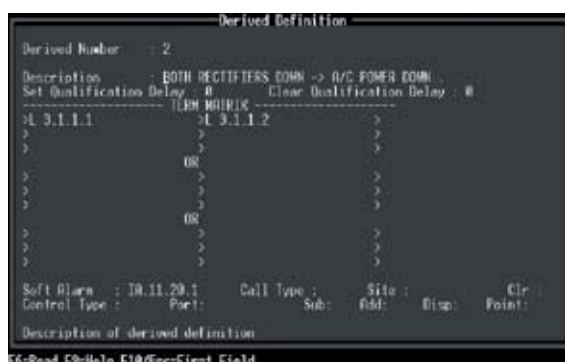
Device Failures and Offlines Alarm Definition



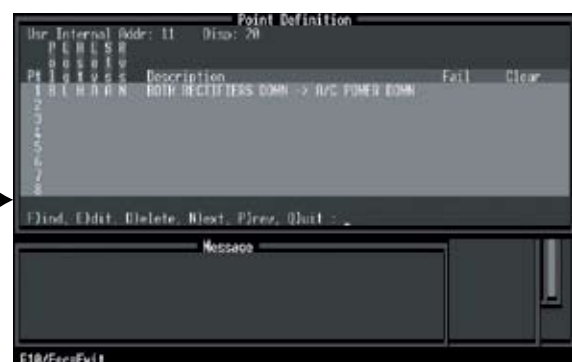
Internal Alarms Point Definition

**Fig. 14.7 - User defined alarms mapped from device failures and offlines**

Notice how the User Defined Alarms are mapped in both figures. In Figure 14.7 the alarm (11.1.2) comes from the device failure defined on Port 1, address 2. In Figure 14.8 the alarm (11.20.1) comes from the derived alarm defined as derived number 2.



Derived Alarm Definition



Internal Alarms Point Definition

**Fig. 14.8 - User defined alarms mapped from derived alarms**

# Section 15 - Root Groups

## Root Groups

Root Groups provide a mechanism for suppressing alarms as a direct consequence of another alarm. This allows the user to filter alarms to get at the root of a problem when a large number of points fail. (eg. A DS3 or Fiber fails causing an excessive number of T1 points to set irrelevant alarms.)

Root Groups are defined by a RootGroupID up to 12 characters in length. Alarms within the group are designated root alarms or member alarms. In the event of a root alarm failure, all member alarms will automatically be acknowledged and silenced until the failed root alarm clears. In the absence of a root alarm, member alarms will report as normal.

You are not limited to a specific number of root groups or alarms per root group.

You can assign individual alarm points to root groups from the point definition screen (see section 10) or edit whole groups from the Master Menu > Files > Root Alarm Filter. You cannot edit individual points from the Root Alarm Filter screen.

Root Alarm Filter						
Root Group ID		: DS3-FRESNO				
Description		: DS3 Fresno root filter				
Root alarms:						
ID	Port	Addr	Disp	Pnt	Site	Point Name
1	200	0	1	1	root alarms	DS3-1
2	NG	193	1	49	CBH Rack	DS3-1 Failed
3						
4						
Root members:						
ID	Port	Addr	Disp	Pnt	Site	Point Name
1	200	0	1	2	root alarms	DS3-1_T1-1
2	200	0	1	3	root alarms	DS3-1_T1-2
3	200	0	1	4	root alarms	DS3-1_T1-3
4	NG	193	1	50	CBH Rack	DS3-1 T1-1 LOS
5	NG	193	1	51	CBH Rack	DS3-1 T1-2 LOS
6	NG	193	1	52	CBH Rack	DS3-1 T1-3 LOS
F)ind, E)dit, D)elete, N)ext, P)rev, Q)uit : _						
F9=Help, F10/Esc=Exit						

Fig. 15.1 - The Root Alarm Filter Screen

The Following are descriptions of the fields in the Root Alarm Filter area:

### Root Group ID.

The name of the root alarm filter group, maximum 12 character alphanumeric entry.

### Description

Provide a description for the root alarm group.

**ID**

The system provides a unique numerical value for each alarm in the group. This field is not editable.

**Port**

The port of the alarm point. Valid values include 1-500, IA, RP, K1, K2, K3, NG, N2

**Addr**

The address of the alarm point

**Disp**

The display of the alarm point

**Pnt**

The alarm point

**Site**

Provides the sitename of a given alarm point. This field is not editable from the root alarm filter. To edit the site name, see the point definition tutorial, section 10.

**Point Name**

Provides a description of the given alarm point. This field is not editable from the root alarm filter. To edit the point name, see the point definition tutorial, section 10.

**Root Alarms**

This table provides a list of all the alarms in the filter with the RGType “root”. Any alarm in this table will silence member alarms upon failure.

**Root Members**

This table provides a list of all the alarms in the filter with the RGType “member”. All alarms in this table will be silenced if any root alarm in the group fails.

## Root Group Commands

**Table 15.A - Commands for the Root Alarm Filter screen**

Function Key	Command
F2	Adds a blank line to the Root Alarm or Root Members table for new entries
F3	Clears a line in the Root Alarms or Root Members table, removing the point from the root group
F5	Toggles between the Root Alarms and Root Members tables
F8	Save
F9	Help
F10/Esc	Exit

## Section 16 - Define Miscellaneous Parameters



Fig. 16.1 - The miscellaneous parameters screen.

### Define Miscellaneous Parameters

Selecting Miscellaneous from the Parameters menu (press M to select Miscellaneous and press Enter) will allow you to setup the miscellaneous operating parameters. An example of the Miscellaneous Parameters screen appears in Figure 16.1.

The Miscellaneous Parameters are used to set various system settings not covered elsewhere.

Table 16.A continues on the following pages.

Table 16.A - Fields in the Miscellaneous Parameters screen

Field	Description
Default Level	Defines the default level of points on the Point Definition section. Valid values are: A (most critical), B, C and D (least critical). [A] The order (A-D) is important for the relay cards to function properly.
Use Display Desc	Answering Y will enable the user to enter a display description when editing the point definitions. Pressing F2 in the Point Definitions screen prompts for a display description. Valid answers are Y and N. This feature has been included in this menu for backward compatibility with older versions of T/MonXM. You are now able to enter a display description from any alarm formatting point screen.
Use Alarm Qual	Y = alarms report after the qualification time (Point Definition screen). N = report the alarm immediately (good while testing). When returned to Y after setting to N, all defined times are reactivated. <b>Note:</b> Select "N" if alarm qualifying not used. (Speeds up operation).



**Table 16.A - Fields in the Miscellaneous Parameters screen (continued)**

Field	Description
Aud Rly Polarity	Audible Relay Polarity - Determines whether audible relays will operate only when an alarms occurs or both when an alarm occurs and when it is restored to normal. U = Unipolar (failed COS alarms only) B = Bipolar (all COS alarms).
Aud Rly Release	Audible Relay Release - Determines whether audible relays will release only when an alarm is acknowledged or when an alarm is either acknowledged or cleared. A = Ack alarm C = Ack alarm or alarm clear.
Auto Scroll Alarms	Determines if alarm display in the monitor mode will automatically scroll to show newest alarms or scroll only by manual operation of the cursor keys. Y = Yes (auto scroll) N = No (manual scroll).
Live Path	This is the path (drive and directory) where T/MonXM will keep the Standing Alarms file. [C:\TMONXM], [C:\IAM], (or drive/directory you specify when installing T/MonXM software). The Standing Alarm File stores data on all alarms that have not been cleared, regardless of whether they have been acknowledged.
History Path	This is the path (drive and directory) where T/MonXM will keep the History file. [C:\TMONXM], [c:\IAM], (or drive/directory you specify when installing T/MonXM software).
Hist Auto Purge	With your cursor at this field, the description line at the bottom of the window will display the minimum value (which is the current total) of entries allowed. The maximum allowed is 999,999 entries. [75000] Once this is reached the oldest entries will be overwritten. 75,000 entries will last over a year in the typical system.
Full Display	Selecting Y (show all points in the display) will allow all undefined alarms to be displayed along with the defined alarms. Selecting N (show only defined points) will ignore all undefined alarms to be reported. <b>NOTE:</b> Y is recommended to help find points that were not previously defined.
Undef Polarity	Selecting B (bipolar) will allow COS undefined alarms to be reported and selecting U (unipolar) will only report failed undefined alarms. [B]
Undef Reverse	Selecting R (reverse) will process undefined alarms reversed (open relays) and selecting N (no reverse) will process undefined alarms normally (closed relays).
Screen Saver	Sets the number of minutes of keyboard inactivity before the screen saver will activate. (0 - 10 minutes, 0 to disable) If the Screen Saver is active while monitoring, new alarms will cancel the Screen Saver and return you to the Monitor Mode screen. The Screen Saver also displays the current Unacknowledged and Live Alarm count on the screen while it is active. Affective on T/MonXM Work Station display only.

**Note:** All values in [ ] are examples or defaults.

**Table 16.A - Fields in the Miscellaneous Parameters screen (continued)**

Field	Description
Pulse Aud Relays	Selecting Y (pulse audio relays) will open and close the relay every time a new alarm comes through. Selecting N (do not pulse audio relays), will keep the relays closed until there are no more alarms. [N] Mainly used for support with equipment connected with DPS' alarm monitoring equipment via the Audible Alarm Card.
System Name	The name (up to 30 characters) that will be displayed during Remote Log On. [BLANK] Typical names use the company name , division or department.
Disable Audio	Selecting Y (yes) allows the user to disable audio while in the monitor mode with Ctrl F4. The audio will remain disabled until manually re-enabled. Selecting N (no) will not allow the user to disable audio. Entering the number of minutes (1-60) allows the user to temporarily disable the audio, which will be automatically re-enabled after the specified time passes. (This is a safeguard feature so if the sound was disabled by the user and they forgot to turn it back on again, the audio will be enabled again after the set number of minutes.)
Alm Pan Time-out	Pans Alarm Monitor screen back to the left after a set number of seconds (0-180). This serves to keep the screen on the most critical part in case it has been panned left and forgotten. Entering 0 will disable this time-out feature. [16]
Debug Port	Used by DPS Technical Support to analyze abnormal protocol or line conditions. Enter port number for analyzer file capture (1-28) (0 = None). Note: save to the file protanal.rep.
Edit Aux Desc	The auxiliary description is a 30 character "bonus" field in the alarm description that can be used for additional information about the alarm point. This field appears on a third page in the alarm display. If an auxiliary description field is not being used, turning it off here will eliminate display of the third page, which may cause confusion. Y = Can edit Aux Desc. N = Cannot edit Aux desc.
Max COS Entries	Number of COS alarms before auto acknowledge. (200 to 3000) [200]
DB Backup Alarm	Threshold for database backup internal alarm (7 to 90 days) [30]
Strict Passwords	Enforces policy for strict system user passwords. When enabled, the following rules will be enforced: <ol style="list-style-type: none"> <li>1. Passwords must be at least 7 characters.</li> <li>2. Passwords must not contain the same consecutive character (two of the same characters in a row.)</li> <li>3. Three of the following character classes must be used: <ul style="list-style-type: none"> <li>• Uppercase alphabetic (A, B, C...)</li> <li>• Lowercase alphabetic (a, b, c...)</li> <li>• Numbers (0-9)</li> <li>• Punctuation (!, @, #...)</li> </ul> </li> <li>4. Password cannot be the same as any of the last four passwords.</li> </ol>

**Note:** All values in [ ] are examples or defaults.

**Table 16.A - Fields in the Miscellaneous Parameters screen (continued)**

Field	Description
Password Reset	Number of days before System Users must enter a new password. This will automatically prompt for a new password when the user attempts to login. (1 to 255 days.) [0]
Normal Analog History Period	Periodic analog history interval that applies when no analog threshold alarms exist. Takes snapshot of the existing analog values. Visible in History and Export Analog History Reports. (10 to 1440 min. 0 to disable) [0]
Alarm Analog History Period	Analog history interval that applies when analog threshold alarms do exist. Takes snapshot of the existing analog values. Visible in History and Export Analog History Reports. (10 to 1440 min.) (0 = disabled) [0] NOTE: Set this time shorter than the normal period to get a greater sampling rate when problems occur.
Preserve Stats	If set to Y, Site Statistics will be preserved when initializing. Setting to N will reset the stats on init. Stats will also be preserved when the software exits and starts up again.
Fast menus	Toggle menu command selection by single keystroke of hot key.

# Section 17 - Monitor Mode Tutorial

## Monitor Mode Overview

View alarm databasing while in monitor mode — see section 17-11.

T/MonXM now features an intelligent help file to provide targeted information to what you are currently databasing, as opposed to the previous comprehensive summary.

This section generally applies to T/RemoteW and T/Windows monitoring T/MonXM screens. Differences are noted in underlined text where appropriate.

After all of the hardware has been installed properly and the software databases have been set up, most of your time will be spent in Monitor mode. Monitor mode is the heart of T/MonXM. While in this mode, T/MonXM begins the polling process and displays the status of the alarms. If an alarm is activated you'll receive visual and (optional) audio indication that an alarm has failed, allowing you to take action as soon as possible. You will be able to view the alarm's location, the type of alarm, and a description of the problem.

Operating within Monitor Mode is very simple. With a press of a key, you will be able to view the alarm and take care of it immediately depending on the severity of the alarm. T/MonXM provides three basic alarm viewing screens: Alarm Summary screen, COS (Change of State) Alarm screen and Standing Alarm screen. Each of these screens is explained in greater detail over the next few pages, but here is a quick overview.

The Alarm Summary screen allows you to see the big picture. You can view all your sites, devices, and alarm types from this display. This ability to consolidate data in one centralized location is what makes T/MonXM so useful.

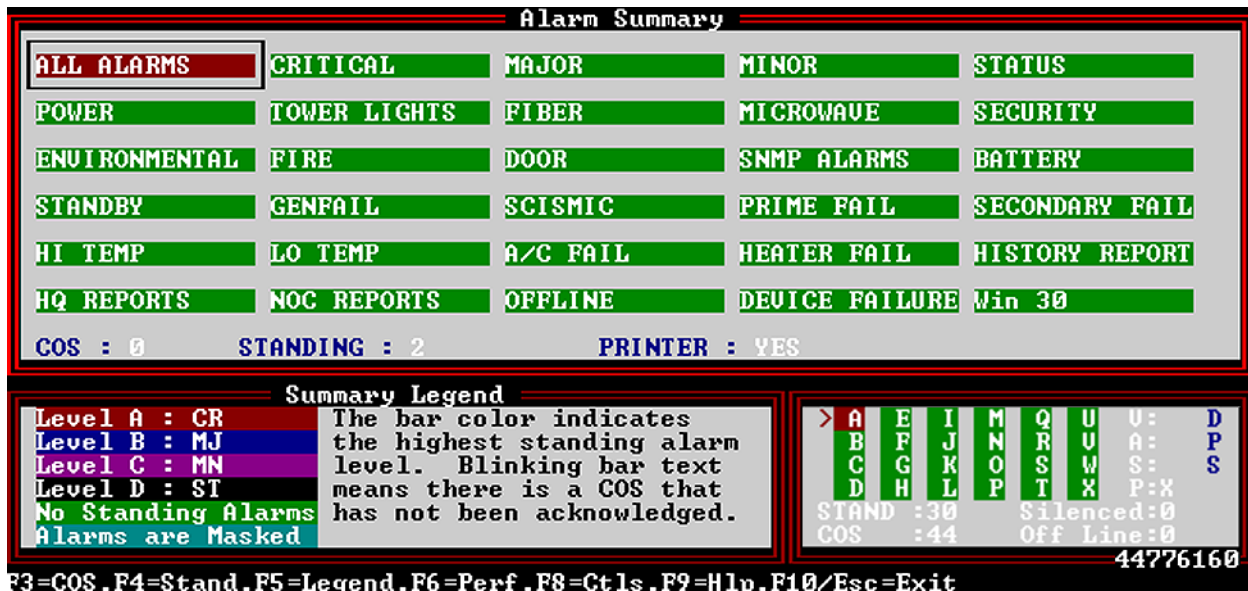


Fig. 17.1 - Monitor mode begins with the alarm summary screen.

The COS Alarm screen (press F3) allows you to view any alarms that have had a change of state whether they've failed or cleared.

The Standing Alarms screen (press F4) allows you to view any alarms that are currently active. The alarms will stay on this screen as long as they are active, regardless of whether they've been acknowledged.

The hierarchical format for viewing the windows is shown below:



**Fig. 17.2 - Monitor mode shows alarm details in COS and standing alarm screens.**

Page Index shows alarm levels for the entire network

The standing and COS screens automatically switch between trouble logs and text messages as alarms are browsed.

Entering Monitor Mode for the first time will automatically initialize the system. .

The Alarm Summary screen has a smaller window at the lower right called the Page Index window. This window uses color to show the highest order alarm existing on each of the pages in the Alarm Summary. Since T/MonXM can accommodate up to 720 Alarm Windows, it wouldn't be realistic to try and fit them all on the same screen. This window represents each block of 30 Windows, a page, by a square of its own. The illustration on the next page shows the different parts of the display.

Note the relationship between the Alarm Summary and Page Index Windows. The Page Index Window represents groups of 30 Alarm Windows (another full screen). If you've purchased additional Alarm Windows the Page Index window will contain the appropriate number of squares. When adding additional windows, System User Accounts need to be updated to view the new windows.

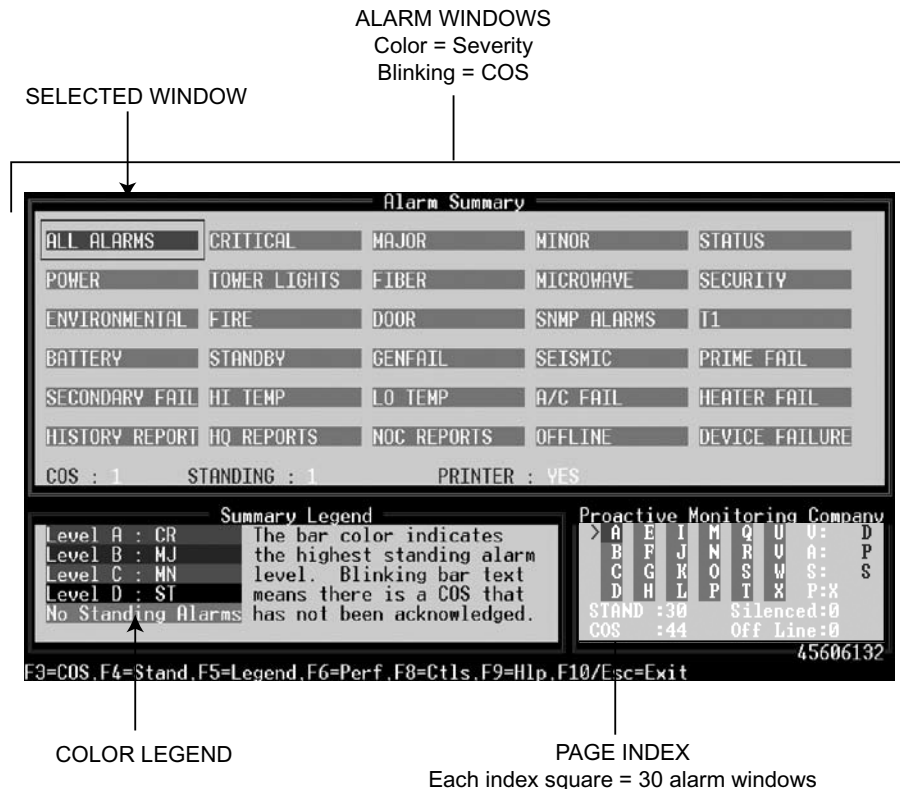
From a selected window, access to the COS Alarms screen or to the Standing Alarms screens is gained by a single key stroke (F3 or F4).

Both the COS and Standing Alarms screens have their own windows for more detailed information. Either screen can display the Text Messages or Trouble Log windows at the lower left portion of the screen (where the Summary Legend window was in the Alarm Summary screen).

Initialize from the Master Menu before entering Monitor Mode when logging on or after changing the database. This is necessary so the system can read the databases and prepare for monitoring.

## Alarm Summary Screen

The Alarm Summary screen is the first alarm viewing screen T/MonXM displays when Monitor Mode is initiated. The Alarm Summary screen presents status information for the entire network on one screen. This screen is comprised of three separate status windows: the Alarm Summary window, the Summary Legend window and the Page Index window. Each is explained in greater detail on the following pages.



**Fig. 17.3 - The alarm summary screen presents three status windows.**

**Table 17.A - Commonly used key commands available in the Alarm Summary screen**

Field	Description
F3	COS. Show Change of State Alarms for selected window. See section 17-15 for more information.
F4	Show Standing Alarms for selected window. See section 17-18 for more information.
F5	Summary Legend. See section 17-8 for more information.
F6	Performance/Statistics Mode. See section 17-30 for more information.
F8	Site Controls for selected window. See section 17-34 for more information.
F9	Online help. Full description of all function keys.
Alt+F2	Manual disconnect for remote access connections (if remote access job has a connection but the user hasn't logged in yet).
F10/Esc	Exit Monitor mode.



## Alarm Summary Window

Fewer windows may be displayed for users with fewer security access permissions

The Alarm Summary window is located in the upper portion of the Alarm Summary Screen. It displays up to 30 alarm grouping windows per page. A total of 90 windows (or any increment of 90 windows up to 720 windows total) can be viewed in this window by using the PgDn/PgUp keys or the keyboard letter (A-X) corresponding to the page index letter. You will notice a box around one of the windows. This is the window selection box. It can be moved across the screen to the various windows using the editing keys listed in the table below.



Fig. 17.4 - Upper portion of alarm summary screen shows 30 alarm windows.

Table 17.B - Editing key commands available in the Alarm Summary Window

Function Key	Description
Left Arrow/Right Arrow	Move left or right one window.
Up Arrow/Down Arrow	Move up or down one window.
PgUp/PgDn	Move up or down one page of windows.
Home	Go to first page of alarm windows.
End	Go to last page of alarm windows.
A-X	View alarm page that corresponds to the letter (30 Windows per page). See section 17-6 (Page Index Window) for more information.

Window titles blink when COS alarms appear.

When the box is over a particular window and you wish to view more information on the alarms in that window, press F3 to access the COS Alarm screen or F4 for the Standing Alarm screen. These are explained on the next few pages.

Window titles will blink when unacknowledged COS alarms appear in that window. An unacknowledged COS Alarm is one that you have not acknowledged previously as being active. When a window is blinking, you can move the window selection box to the window and press F3 to zoom in on the COS alarm.

Acknowledging indicates the alarm has been seen

**Acknowledging alarms.** The act of acknowledging an alarm simply indicates that the alarm has been seen by someone and that it is

noted or that some form of action has been started. When an alarm is acknowledged it is no longer displayed in a manner intended to attract attention, such as blinking. (Acknowledging is done while in the COS Alarms screen — see Section 17-25.)

### Colors denote severity

The priority or level of the most severe alarm can be easily determined by looking at the color of the window. (The color is the background color under the window title.) For example, if most of the alarm windows are green and one is red (the most severe alarm status), you know there is at least a critical alarm (Level A) in the alarm window that is red. The colors used on the Alarm Summary window coincide with the colors listed in the Summary Legend window located at the bottom left of the Alarm Summary screen (see Section 17-8).

Toward the bottom of the Alarm Summary window are three fields which give you additional information about the alarm window currently selected. The COS and Standing fields show the alarm count of the window you are currently positioned on. This is different from the Page Index window's Standing and Alarm fields which give alarm counts for all of the windows that you are authorized to access (see next page).

The Printer logging field is always Yes when you are logged on to the main system — see Figure 17.5. The printer logging field shows whether or not alarms for a window will be logged to the printer. Printer logging can be toggled off by pressing Ctrl-F1 (see Page Index window on section 17-6 for more information).

**Note:** There is a yes/no option for printer logging on remote systems if, for example, you didn't want your remotes to log alarms.

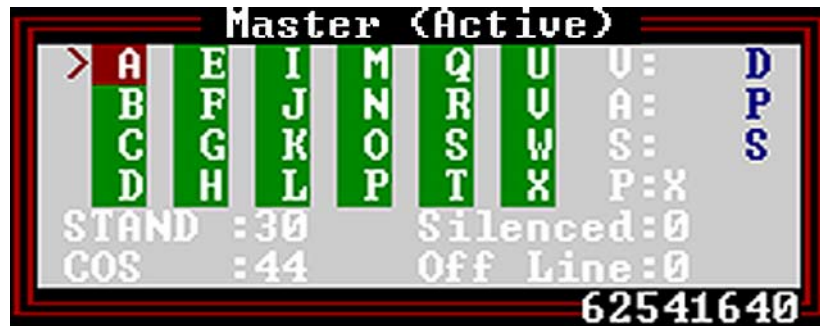


**Fig. 17.5 - COS, Standing, and Printer fields**



## Page Index Window

Page Index displays > next to the current alarm page number.



**Fig. 17.6 - Page index shows page and status**

The Page Index window is located at the lower right portion of the Alarm Summary screen. It is the only window that is always displayed when in Monitor mode. This window will display a “>” symbol next to the alarm page letter you are currently viewing. Each illustrated page represents one (A) full page of Alarm Summary windows. For example, page A allows you to view the first 30 windows, page B you would see windows 31-60, etc.

Users can only view as many windows as they are authorized to access, regardless of how many windows are installed. Therefore, if you only see a few pages in the Page Index window but know you have more windows installed, you may want to check the View Alm Windows setting in the System Users screen from the Files menu to see if all installed windows are available.

The Page Index window also displays monitoring statistics and conditions as listed in Table 17.C.

Live status reports of your master and slave units also appear above the Page Index Window screen if you are using a network of T/Mons or IAMs. You’ll see the name of your unit and whether it’s active or passive, so you’ll always know whether your master or slave units are polling your remotes — see Figure 17.6.

**Table 17.C - Fields in the Page Index window**

Field	Description
Stand	Displays the alarm count of the total number of standing alarms for the windows in the system that you are authorized to access.
COS	Displays the alarm count of the total number of unacknowledged COS alarms for the windows in the system that you are authorized to access.
Off Line	Displays the count of the total number of addresses that have been manually taken offline. This reminds you if any addresses are now off line.
V	Visual Cutoff (VCO) status of the Audible Alarm Card. “X” indicates disabled. Alt F1 opens the Alarm Indicator Control window where the VCO is controlled. (See section 17-39 for further information.)

**Note:** Table 17.C continues on following section.

**Table 17.C - Fields in the Page Index window (continued)**

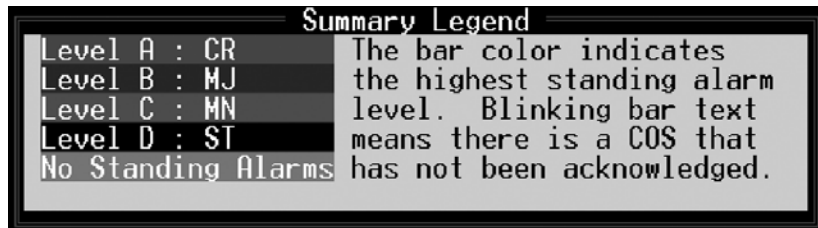
Field	Description
A	Audible Cutoff (ACO) status of the Audible Alarm Card. "X" indicates disabled. Alt-F1 opens the Alarm Indicator window where the ACO is controlled. (See section 17-26 for further information.)
S	Sound status of the Audible Alarm Card (refers to the on-board speaker on the Audible Alarm Card that emits warning sounds for different level alarms). "X" indicates disabled. Ctrl-F4 toggles.
P	Printer Logging status. "X" indicates disabled. Ctrl-F1 toggles.
Silenced	Shows number of silenced items in the system. That is, the number of entries in the list when Alt-F4 is pressed.
R	Indicates that the Report resource is in use.

**Note:** ACO and VCO control external devices that are connected to relays on the audible alarm card.

The Page Index window uses the same color scheme as the Alarm Summary window. The Page Index window colors, however, show the status of the entire set of windows on a page-by-page basis, rather than on a window-by-window basis. The highlight color indicates the level of the highest standing alarm on the page. If there is an unacknowledged COS alarm the page number will blink.

The initials of the person logged on are displayed vertically on the right side of the Page Index Window. In the example in Figure 17.6 the person logged in is "DPS."

## Summary Legend Window



**Fig. 17.7 - Summary legend window shows color scheme.**

The Summary Legend window is located at the lower left portion of the Alarm Summary Screen. It shows the alarm color coding scheme that indicates alarm status/severity for the alarm summary and page index. The default colors are described in Table 17.D.

**Table 17.D - Default colors in the Alarm Summary screen**

Field	Description
RED	Indicates a level "A" alarm is the highest standing alarm.
BLUE	Indicates a level "B" alarm is the highest standing alarm.
MAGENTA	Indicates a level "C" alarm is the highest standing alarm.
BLACK	Indicates a level "D" alarm is the highest standing alarm.
GREEN	Indicates that there are no Standing alarms.
BLINKING	Indicates that there are unacknowledged COS alarms.
CYAN	Indicates masked alarms.
YELLOW	Indicates an alarm in the process of being qualified

**Note:** These colors can be changed in the Alarm Summary Colors window under the Parameters menu — see section 17-23.

**Table 17.E - Key commands available in the Alarm Summary screen**

Function Key	Description
F3	Activates the Change-Of-State Alarm screen (COS) (see section 17-25) for the current alarm window selected.
F4	Activates the Standing Alarm screen (see section 17-28). This screen will only show alarms that are standing (failed) for the current alarm window selected.
F5	Selects the Summary Legend window to display T/MonXM's color coding scheme for indicating alarm levels. This window will be displayed by default until you've selected one of the other sub-mode windows.
F6	Selects the Performance/Statistics window (see section 17-31) which shows a variety of information on the quality of alarm equipment's communication link to T/MonXM.

**Note:** Table 17.E continues on following page.

Table 17.E - Key commands in the Alarm Summary screen (continued)

Function Key	Description
F8	Activates the Site Controls screen (see section 17-34) for the selected window.
F9	Displays on line help for the Alarm Summary Mode.
F10/Esc	Exit monitor mode or logoff. Press Y to logoff but continue monitoring alarms. Press R to logoff and quit monitoring alarms. <b>Note:</b> This selection can be activated only if security authorization has been given in the System Users screen — see Section 7, System Users Press N to continue monitoring and stay logged on.
Alt-F1	Allows editing of the Audible/Relay card configurations from the Alarm Indicator Control window (see section 17-39).
Alt-F2	Resets the statistics in the Performance/Stats window (see section 17-31).
Alt-F3	Silences the selected alarm window — see section 17-30 (Silence Alarm/Window).
Alt-F4	Displays list of silenced items and their expiration dates/times (see section 17-30).
Alt-F5	Activates the English Analyzer window. Displays protocol traffic to and from the alarm equipment in English. (see section 17-42)
Alt-F7	Enables you to print a report by displaying the Report Mode menu (see section 17-44).
Alt-F8	Activates the Protocol Analyzer window to display protocol traffic to and from the alarm equipment in hexadecimal, decimal or ASCII format. (see section 17-46) <b>Note:</b> The Protocol Analyzer is available only from the Main Console, not from a remote access application.
Alt-F9	Activates the Channel Summary window (see section 17-35) to display the polling mode, status, error percentage and current polling of four channels at a time.
Ctrl-F1	Toggles printer logging in the Page Index window (see section 17-6). The printer which is connected on the main T/MonXM system will, if enabled, print all alarms that are displayed in the All Alarm window. On DPS T/Remote and T/Windows the user can select a Single alarm window to print an alarm from. <b>Note:</b> Do not enable this feature unless a printer is connected to the parallel printer port or an alarm will be reported.
Ctrl-F2	Activates the TL1 Observation screen if you have the TL1 Responder Software Module installed. For more information, see Software Module 13 — TL1 Responder.
Ctrl-F3	Activates the Building Access Site Status screen if you have the Building Access Software Module installed. For more information—see Software Module 22 — Building Access System.
Ctrl-F4	Controls the Audible/Relay card local sound cutoff (see section 17-39). Current status is displayed in the page index window.
Ctrl-F5	Activates English Filter window (see section 17-42). Use in conjunction with English Analyzer window to view data traffic from specific equipment.

**Table 17.E - Key commands in the Alarm Summary screen (continued)**

Function Key	Description
Ctrl-F6	Displays the System Information window (see section 17-51). This screen shows the current Standing Alarm Memory Threshold number, COS Auto Acknowledge Threshold number and history.
Ctrl-F7	Activates the Craft Mode screen (see section 17-53). Enables you to communicate with XM ports, typically ASCII and Craft.
Ctrl-F8	Activates the Labeled Controls screen (see section 17-55). This allows you to operate control equipment within your network using English-based look-up tables.
Ctrl-F9	Activates the Remote Access Chat Mode window (see section 17-45). Selects a communication chat mode that allows remote terminal users to communicate with each other and the T/Mon.
Shift-F2	Activates the X25 Statistics screen — see Appendix C for configuration information.
Shift-F3	Activates the Pager Status screen. For more information see section 17-60.
Shift-F4	Activates the Dialup Site Monitor screen (see section 17-49) if you have a dial-up remote connection. T/MonXM comes standard with TRIP software support. For more information see Software Module 3 (Standard Dial-Up Remotes).
Shift-F5	Activates the VDM Voltages screen if you have the VDM Software Module installed.
Shift-F6	Activates the Site Statistics screen. This screen gives you general statistics about a particular site. Allows you to take devices on/off line as well as other address specific special functions. (See section 17-62.)
Shift-F7	Activates the ASCII Analyzer screen if you have either Direct or Dial Up ASCII Software Module installed. For more information, see Software Module 6 -ASCII Interrogator.
Shift-F8	Activates the Datalok 10 Voltages screen if you have the Pulsecom Datalok Software Module installed. For more information, see Software Module 17 – Pulsecom Datalok.
Shift-F10	Activates the DCP(F) Network screen. For more information, see Software Module 1 – DCP(F) Interrogators/Responders. (This module is standard in T/MonXM.)
PgUp	Select the previous page of alarm widows.
PgDn	Select the next page of alarm windows.
Home	Positions first page (windows 1-30) of alarm windows on the screen.
End	Positions the last page of alarm windows on the screen.

**Note:** Appendix I provides helpful quick reference sheets.

## Monitor Sub-Mode Descriptions

T/MonXM's Monitor Mode allows a multitude of sub modes to be activated while polling. These include modes such as English Analyzer, Protocol Analyzer, and Report mode. Alarm equipment polling will continue in the background.

Monitor sub-modes are explained in greater detail throughout this section.

## Monitor Alarm Point Descriptions

First, press Shift-F6 to monitor the status of your devices (see Figure 17.8). Select a device, and then press Alt-F1 to monitor your alarm point descriptions (see Figure 17.9).

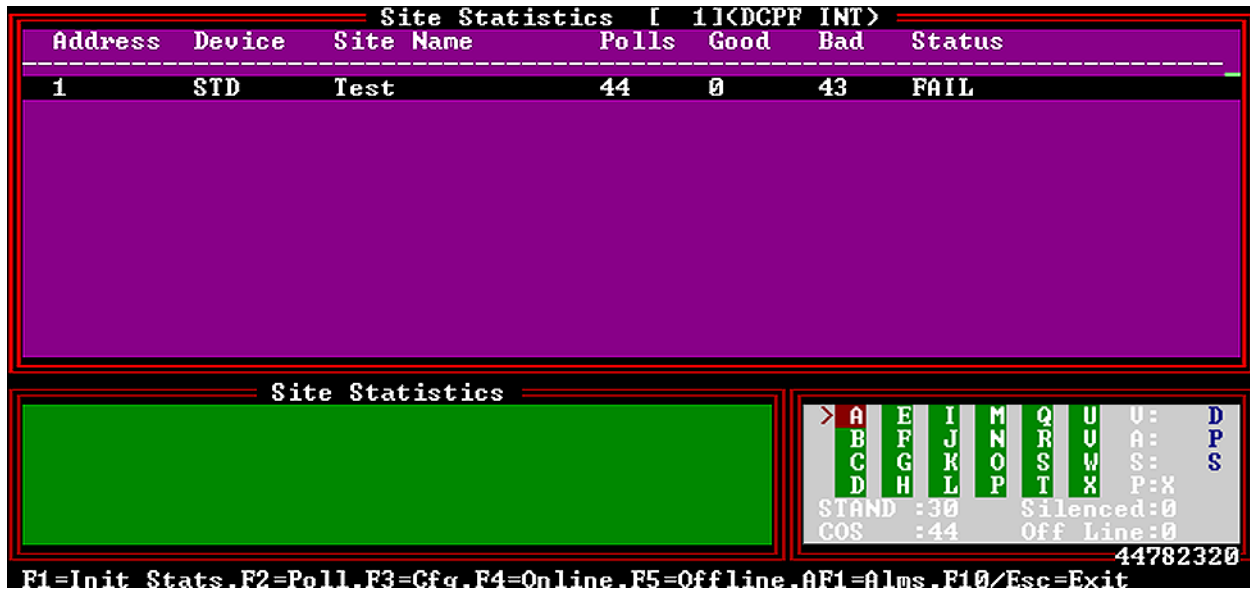


Fig. 17.8 - Monitor Site Statistics in the Monitor Mode by pressing Shift-F6

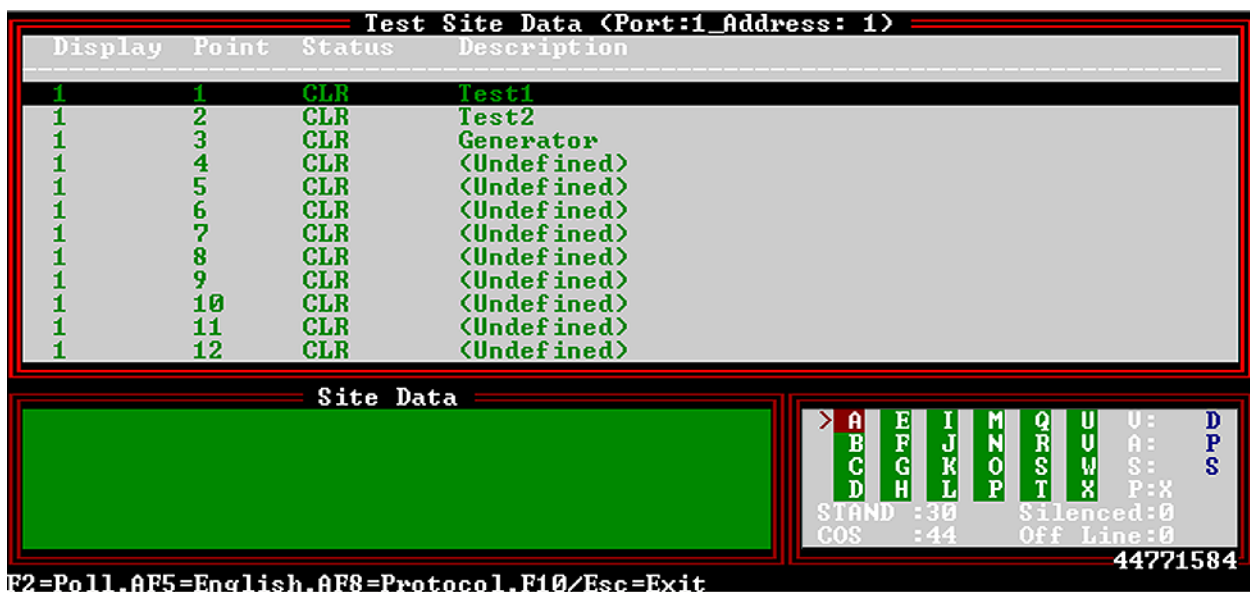


Fig. 17.9 - Monitor alarm points in the Monitor Mode by pressing Alt-F1

## Monitor Mode Operation Notes

Monitor Mode is a conglomeration of many individual operations. Because of memory and storage limitations and the effect it has on the computer's speed of operation, T/MonXM uses every chance possible to conserve memory and disk storage. This conservation enhances the program's speed of execution.

When many large databases are defined and there are great amounts of data that must be polled or monitored, program speed of execution becomes crucial. T/MonXM uses the following techniques to increase the program's speed of execution and performance:

### Automatic History Purging

T/MonXM will automatically purge History file entries based on the number of entries in the file. The selected level can be no less than the current number of entries in the history file (the exception being an absolute minimum level of 100). The default level is 75,000 entries. Entries are automatically purged if there is less than 200K of free disk space. The Auto History Purging option can be disabled by selecting a really large value (more entries than would fit on a hard disk). This option is called Hist Auto Purge and is located in Miscellaneous command on the Parameters menu.

**Note:** this is a first in, first out setup (i.e. oldest entry is deleted first).

### Standing Alarm Virtual Mode

Standing alarms will be logged to disk when the total number of standing alarms is greater than the threshold computed at the time the system is initialized. The threshold is computed based on the amount of available memory after initialization. The threshold can be viewed by pressing Ctrl-F6 while in Monitor Mode. The oldest standing alarms are always stored in the computer's memory. Any other standing alarms will be stored on disk. There must be at least 100K of free disk space available for a standing alarm to be logged to disk. An alarm will not be logged if there is insufficient disk space. The standing alarm count will blink when alarms are not being logged.

### Automatic Alarm Acknowledging

Change of state alarms will be automatically acknowledged in the order of occurrence, from the oldest to the newest, as needed. This is done to be sure that there is always sufficient computer memory available to log new alarms.

Alarms will be automatically acknowledged when the total number of occurrences of alarms in the change of state alarm windows is greater than the user-defined COS threshold. This option is set in the Parameters > Miscellaneous Parameters menu option when Offline, and has a maximum value of 3000.

If the Initials option is active, then the initials of an alarm that has been automatically acknowledged will be reported as @@@. (The initials are only displayed in Standing Alarm mode.)

## Initialization

Selecting Initialize from the Master menu will bring you to the Core Prep screen and start system initialization. Initialization and Core Prep makes ready all data structures and files Monitor mode uses. Any database changes you've made will not take effect until you've initialized after making the changes.

As of T/MonXM 4.2, it is no longer necessary to manually initialize the system before entering Monitor Mode. Choosing Monitor from the Master menu will automatically initialize the system.

However, you must manually choose Initialize from the Master menu after making database changes for your changes to take effect.

**Note:** Always initialize after making Database changes as certain changes may cause problems if not initialized first.

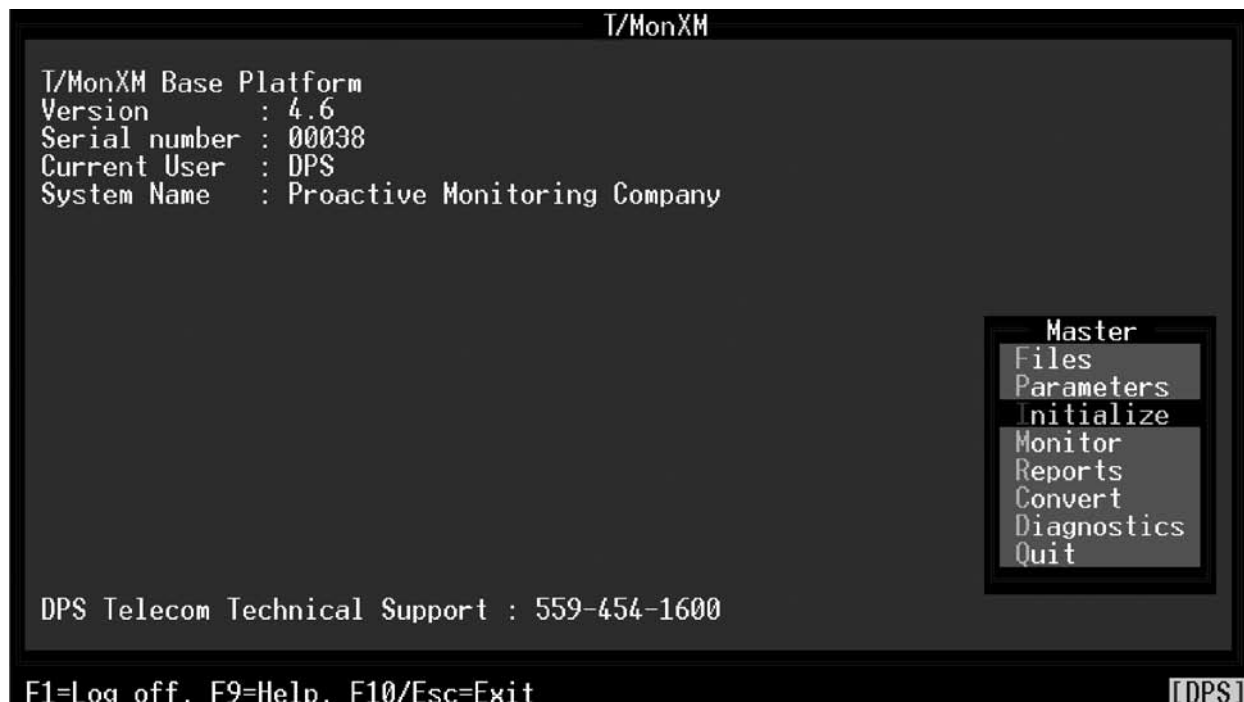


Fig. 17.10 - The initialize function is selected from the master menu.





**Fig. 17.11 - The Core Prep screen appears during the initialize function.**

### **Core Prep**

This mode runs automatically upon selecting the Initialize function from the Master menu. Core Prep will automatically run the first time Monitor Mode is entered.

It must also be run again if you make any changes to database files or they will not take effect in the monitoring system.

When used with a large database, this function can be time intensive (on the order of a few minutes).

# Alarm Formatting

Configure Monitor  
Screen format with Edit  
Alarm Format Screen



**Fig. 17.13 - Alarm Format menu command**

The Alarm Formatting screen allows you to configure the screen format for the alarm displays that will be shown in monitor mode. This allows formatting the alarm message so it is most useful for alarm system attendants. The Alarm Formatting screen is similar in operation to the Alphanumeric Pager Formats screen in the File Maintenance Section.

Alarm Format Definition allows the user to customize which alarm fields are defined, their position, and the colors used when an alarm is reported on the screen. The T/Mon system has a default alarm format to display the most common data, but can be customized to fit a user's information needs. Field position, width and color are all user definable. The text displayed for each alarm level is user definable.

The text displayed for the Status field is definable on an alarm-by-alarm basis. (Both a fail status description and a clear status description can be defined for each alarm. If a status description is not defined for a particular alarm, a global default description is displayed).

Special color options called FOLLOW STATUS, FOLLOW LEVEL and FOLLOW MATRIX allow the color of a field to be derived from the alarm's state or combination of states (failed, cleared, level A, etc.).

The width of the Alarm Format Definition may be up to 2 screens wide (a total of 153 characters). Pressing Tab while in Monitor mode toggles the format between being left justified and right justified. (A parameter in the Miscellaneous Parameters section called Alarm Pan Time-out determines when a right justified screen will



**Fig. 17.12 - Alarm formatting screen**

automatically be restored to being left justified. This is safety feature designed to prevent confusion when reading the alarm display.)

To access the Alarm Formatting screen select Alarm Formatting from the Parameters menu and press Enter. The Edit Alarm Format screen will appear.

The screen presents status information at the top and two example format bars below that. The status information includes the page, status, level and total width. This information tells you what the format bars are showing. The upper format bar illustrates the message that will be shown on the screen as a highlighted window. The lower format bar illustrates the message that will be shown on the screen as an un-highlighted window. This simulates the two backgrounds as you would see them in Monitor mode. Do not pick one of these background colors as an alarm color because the alarm will not be visible.

Table 17.F explains how the format bar and associated function keys can be used to quickly pre-view a message.

**Table 17.F - Status information fields in the Edit Alarm Format screen**

Function Key	Description
Page	Portion of the format bar being shown. Page 1 always shows character columns 2 through 77. Page 2 shows the balance of the columns (up to 153). F7 toggles between the two pages.
Status	What alarm status (F = Failed, C = Clear) is represented on the format bar. If the status is changed by stepping through with F6 the status characters in the format bar will change to show how the message changes when status changes. The actual words used to describe the status can be changed by using the F4 key. (See additional information in the table that follows.)
Level	What alarm level (A, B, C, D) is represented on the format bar. If the level is changed by stepping through with F6 the level characters in the format bar will change to show how the message changes when alarm level changes. The actual words used to describe the level can be changed by using the F4 key. (See additional information in the table that follows.)
Total Width	Number of characters the message occupies at its present state of configuration. This number will increase as further fields are defined.

Fields allow you to keep track of what is being simulated.

By default, the first field starts at character 6.

When the Edit Alarm Format screen is opened the cursor will be located in the Name field. Up to 14 fields can be defined with a total of up to 153 characters. For each field you will enter a name, width and whether a space is to separate it from the following field. The name of the field must be selected from an established list that can be viewed by pressing the Tab key while the cursor is in the name column. Each item on the list also has a default value for the field width, which can be edited while the cursor is in the width column. The following table provides details.

The screen captures in this alarm formatting sub-section reflect the DPS default settings.

New systems will default to DPS recommendations. When creating an alarm format, always put the most important information on the first screen.

**Table 17.G - Fields in the Edit Alarm Format screen**

Field	Description
FLD	Field position.
START	The starting column of the field. Note that this item cannot be edited. (Start is automatically calculated based on field position and width).
NAME	The name of field. Use the Tab key to bring up a list of names. Then use the Tab key to move the highlight bar and press Enter to select the highlighted item. Options available include:
	Alarm ID Port.Address.Display.Point
	Alarm Status Fail and clear description
	Level Severity (CR, MJ, MN, ST)
	Description Alarm description
	Disp Desc Display description
	Date-1 [MM/DD/YY] Month/Day/Year
	Date-2 [MM/DD] Month/Day
	Date-3 [JAN 12, 1992] Date (text description)
	Date-4 [JAN 12] Date (text description, year omitted)
	Time-1 [12:34:56] Time (hour:minute:second)
	Time-2 [12:34] Time (hour:minute)
	Site Name Site name as defined in Parameters > Remote Ports > Device Definition screen.
	Protocol Port type description
	Device Type Device type description
	Aux Desc Auxiliary description <b>Note:</b> you must enable this feature in the Parameters > Miscellaneous screen option.
	System Name T/Mon system name as defined in Parameters > Miscellaneous screen option.
	Ack Label "ACK:" (optional)
	Ack Initials Initials of user who acknowledged alarm.
	Ack Date-1 [MM/DD/YY] Date of Ack (Month/Day/Year)
	Ack Date-2 [MM/DD] Date of Ack (Month/Day). No year shown.
	Ack Date-3 [JAN 12, 2003] Date of Ack (text description)
	Ack Date-4 [JAN 12] Date of Ack (text description, year omitted)
	Ack Time-1 [12:34:56] Time of Ack (hour:minute:second)
	Ack Time-2 [12:34] Time of Ack (hour:minute)

**Note:** Table 17.G continues on following section.

**Table 17.G - Fields in the Edit Alarm Format screen (continued)**

Field	Description	
NAME	Time Stamp	Time alarm was collected by remote unit.
	Ats Status	Absolute Status. A = Alarm C = Clear
	Event ID	Unique number associated with an alarm event.
	Pager Prof	Pager profile associated with alarm.
WIDTH	Width of the field. If the width is set to be less than the amount of data in the field then the right-hand part of the field will be truncated.	
COLOR	Color of the text. The following color choices are available: Black, Blue, Green, Cyan, Red, Magenta, Brown, Lt Gray, Drk Gray, Lt Blue, Lt Green, Lt Cyan, Lt Red, Lt Magenta, Yellow, and White. The entries FOLLOW STATUS, FOLLOW LEVEL and FOLLOW MATRIX are colors that are derived based on the state of the alarm. Use function keys F4 and F5 to set these up. See details in Level and Status Attributes and Level and Status Matrix on the following pages.	
BLINK	Determines whether the text will blink. This field does not apply to the derived colors. This is because BLINK is part of the derived definition.	
SPACE	Determines whether a trailing space follows the field. Use the Tab key to select Yes or No.	

**Table 17.H - Key commands available in the Edit Alarm Format Screen**

Function Key	Description
Tab	List. This key displays optional entries in the field.
F1	Ins. Inserts a blank field entry at the current cursor position.
F2	Del. Deletes the field entry that the cursor is under.
F4	Lv&St. Allows editing of the Level and Status and Attributes — see details in section 17-19 (Level and Status Attributes).
F5	Mtx. Allows editing the color and blinking attributes of level and status matrix — see section 17-20 (Level and Status Matrix).
F6	Sim. Cycles through all combinations of level and status to allow pre-viewing the message in the format bar.
F7	Pan. Toggles the page number and format bar to show the portion not currently on the screen.
F8	Save. Saves the Alarm Format definition.
F9	Help. Online Help.
F10/Esc	Exit. Exits without saving any changes that may have been made.

## Level and Status Attributes

Press F4 in the Edit Alarm Format screen to edit the Level and Status Attributes window.

This window allows editing level text, level colors, (used by the FOLLOW LEVEL color option), default status text (text used by the status field if no status description is defined on Point Definition screen), and status colors (used by the FOLLOW STATUS color option).

**Edit Alarm Format**

PAGE : 1    STATUS : F    LEVEL : A    TOTAL WIDTH : 95

1 1 2 2 3 3 4 4 5 5 6 6 7 7 7

2..5...0...5...0...5...0...5...0...5...0...5...0...5...0...5...7

3/13 10:47 FAIL SITE NAME-----! THIS IS THE POINT DESCRIPTION -----

3/13 10:47 FAIL SITE NAME-----! THIS IS THE POINT DESCRIPTION -----

**Level and Status Attributes**

FLD	ST	TEXT	COLOR	BLINK	
1	6	LEVEL A	CR.....	LT RED	NO
2	12	LEVEL B	MJ	LT BLUE	NO
3	18	LEVEL C	MN	MAGENTA	NO
4	23	LEVEL D	ST	YELLOW	NO
5	39	CLEAR	NORM	GREEN	NO
6	79	FAIL	FAIL	LT RED	NO
7	82	TAGGED	TAG	BROWN	NO
8					
9					
10					

Enter Text

F8=Save, F10/Esc=Exit

Fig.17.13 - Level and status attributes screen

Table 17.1 - Fields in the Level and Status Attributes screen

Function Key	Description
TEXT	Default text you would like displayed in the Alarm Status window. This lets you reason T/MonXM's alarm severity message text, and global default for fail and clear terminology.
COLOR	The text color for CLEAR or FAIL alarms. The following color choices are available: black, blue, green, cyan, red, magenta, brown, lt. gray, drk gray, lt blue, lt green, lt cyan, lt red, lt magenta, yellow, and white. Recommended defaults are: Crit: LT RED Maj: LT BLUE Min: MAGENTA Stat: YELLOW Norm: GREEN Alm: LT RED
BLINK	Determines whether the text will blink.

## Level and Status Matrix

Press F5 on the Edit Alarm Format screen to edit the Level and Status Matrix window.

The Level and Status Matrix window allows you to define a color matrix based on the combination of Alarm Levels and Alarm Status. This is the matrix the system is going to use if you select as color FOLLOW MATRIX. (On the Edit Alarm Format screen)

T/MonXM is going to look at the alarm level status for the alarm and color those fields based on this matrix table. You can have a different color for failed alarms and cleared alarms for each level. i.e.: Use red for a critical failure, but color a critical normal green so that when the point returns to normal it does not appear to be another alarm. This takes advantage of the mind-set that red is bad and green is good.

**Edit Alarm Format**

PAGE : 1    STATUS : F    LEVEL : A    TOTAL WIDTH : 95

1 1 2 2 3 3 4 4 5 5 6 6 7 7 7  
2..5...0...5...0...5...0...5...0...5...0...5...0...5...7

3/13 10:10 FAIL SITE NAME-----! THIS IS THE POINT DESCRIPTION -----  
3/13 10:10 FAIL SITE NAME-----! THIS IS THE POINT DESCRIPTION -----

**Level and Status Matrix**

FLD	ST	CLEAR	FAIL
		COLOR	BLINK
1	6		
2	12	LEVEL A    GREEN.....	NO
3	18	LEVEL B    GREEN	NO
4	23	LEVEL C    GREEN	NO
5	39	LEVEL D    GREEN	NO
6	79		
7	82	Enter color for CLEAR	
8			
9			
10			

Tab=List, F8=Save, F10/Esc=Exit

Fig. 17.14 - Level and status matrix screen.

Table 17.J - Fields in the Level and Status Matrix screen

Function Key	Description
COLOR	The text color for CLEAR or FAIL alarms. The following color choices are available: Black, Blue, Green, Cyan, Red, Magenta, Brown, Lt Gray, Drk Gray, Lt Blue, Lt Green, Lt Cyan, Lt Red, Lt Magenta, Yellow and White.
BLINK	Determines whether the text will blink.

## Alarm Message Forwarding

The purpose of Alarm Forwarding is to send selected T/MonXM alarm data to another alarm master or master of masters in an easily parsed format.

Alarm message forwarding allows T/MonXM alarm information to be output in ASCII format via T/MonXM's remote access ports. To do this, the user selects a port as the forwarding output port. Then, after assigning the baud, parity, word length and stop bits the user assigns an alarm window to follow in T/MonXM as a forwarding window. All alarms that are assigned to the forwarding window will be displayed in that window. The alarms will also be set out the selected port in the same format as they appeared on the screen. The last parameter in the number of characters to transmit the field. This is the number of characters to transmit per message.

For example: All of the power related alarms from each central office are assigned to window 8. The, window 8 is set to alarm forward to one of the remote ports. This port is tied to a printer in another location. At that time, all of the alarms in the forwarding window are output to the printer while all other alarms are only seen at the main workstation.

## Basic Operation and Setup

Installation of the optional alarm message forwarding software module is required to define or access a port for the Alarm Forward option. Refer to Section 2 (Software Installation) for installation procedures.

When the software module is installed, selecting Remote Ports from the Parameters menu will allow you to select and define the alarm forward port and parameters.

An example of the Remote Parameters screen defined for Alarm Forward is on the next page.

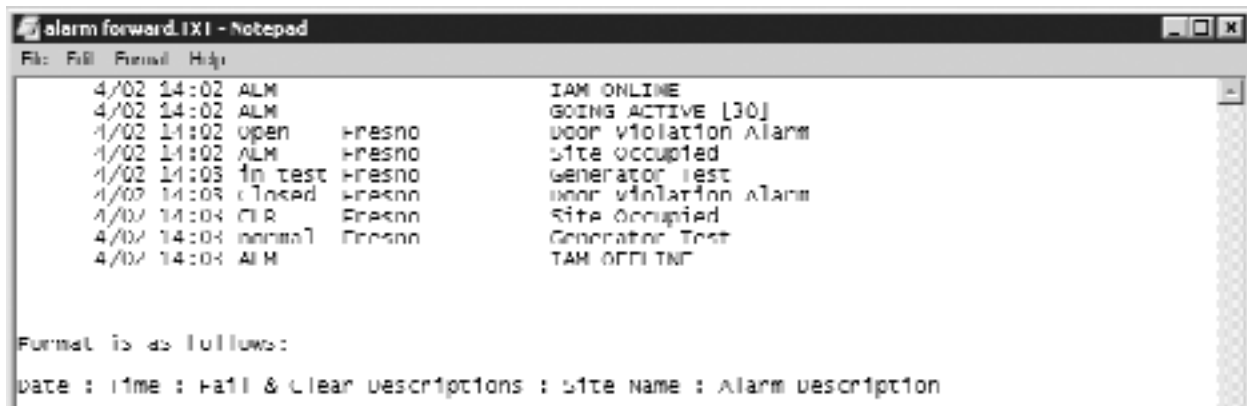


Fig. 17.15 - Example alarm forwarding text



## Alarm Forward Parameters

**Note:** Alarm Forwarding can be assigned only to Intelligent Controller Card Ports (Ports 1-20).

### Port Usage

Enter Alarm Forward in the port usage field. Use Halted (default) in Alarm Forward is not used.

**Note:** The fields on the Remote Parameters screen vary according to port usage.

### Serial Format

Baud rate, word length, parity, and stop bits settings. Default values are 9600 baud, 8 bits, none, and 1.

### Window to Follow

Standard features allow 29 windows plus the All Alarms window. When you install the optional alarm window software modules, you will be able to access additional windows. Default value is Window 1 (All Alarms).

Note: A System User account can assign windows to Alarm Message Forwarding without having security access to those windows.

### Number of Characters to Transmit

The valid range of characters to transmit per message is 10-200. Default value is 77.

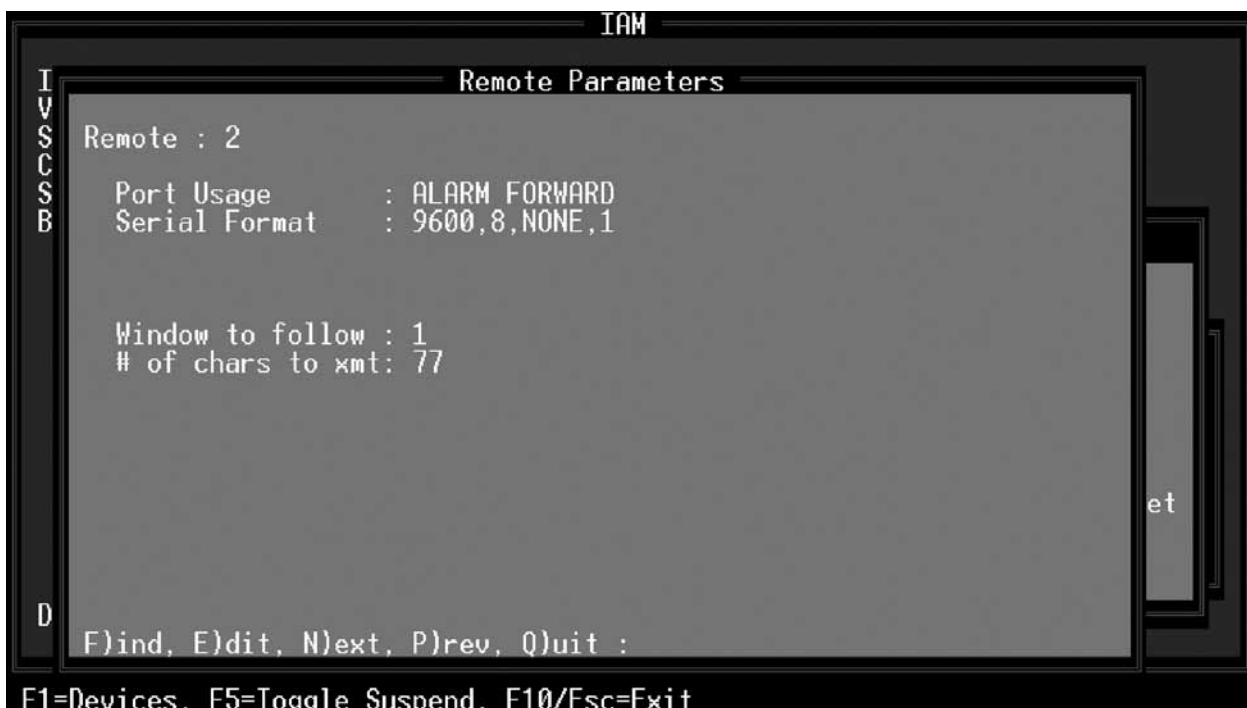


Fig. 17.16 - Remote Parameters screen defined for Alarm Forward

## Alarm Summary Colors

Selecting Summary Colors from the Parameters menu (press S to select Summary Colors and press Enter) will allow you to define colors used in backgrounds of the Alarm Summary screen.

Table 17.K lists screen options for the Alarm Summary Colors screen:



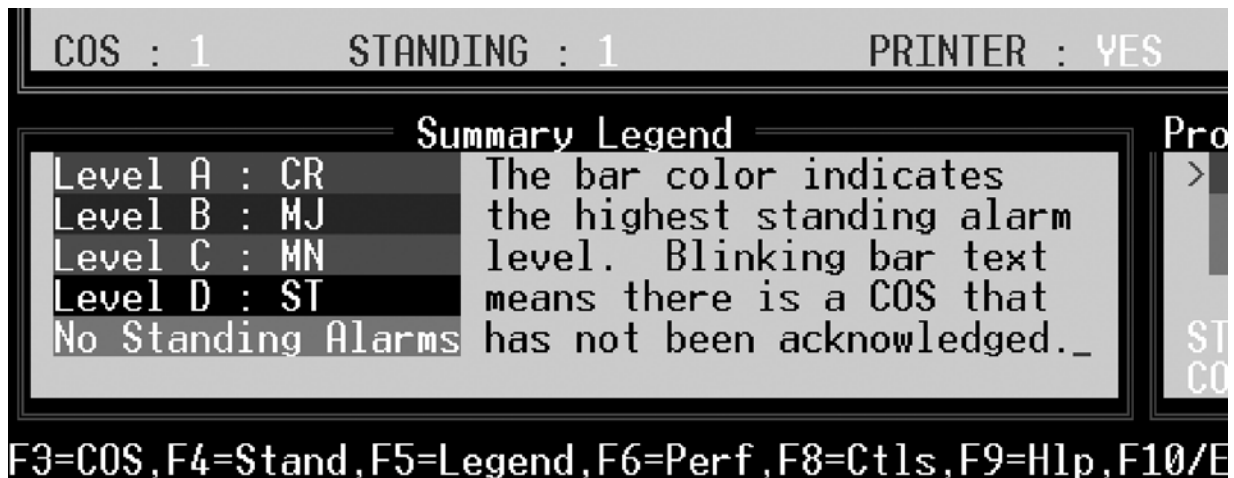
Fig. 17.17 - The Alarm Summary Colors screen

Table 17.K - Fields in the Alarm Summary Colors screen

Function Key	Description
Level A, B, C, D	Respective alarm level. Color choices for each field can be selected by hitting Tab and the arrow keys and Enter to select the color you'd like. Choices are BLACK, BLUE, GREEN, CYAN, RED, MAGENTA, BROWN and GRAY. <b>Note:</b> Recommended colors are shown in Figure 17.18.
No Alarms	Sets color for a no alarm (clear) condition window. Use the same method as above to select colors. <b>Note:</b> Using Gray for No Alarm makes sites with no alarms blend into the background which helps increase the visibility of sites with alarms.
Masked	Sets color for a masked window. Use the same method as above to select colors. (Masked windows represent sites where someone has logged on using one of the building access methods.)

**Table 17.L - Key commands available in the Alarm Summary Colors screen**

Function Key	Description
F8	Saves the Alarm Summary Colors settings
F9	On-line help
F10/Esc	Exit without saving



**Fig. 17.18 - The Summary Legend in the lower left corner of the Alarm summary screen shows the meaning of the color codes**

# Change Of State (COS) Alarms

What is COS and why do I need it?

Unlike standing alarms which show all the alarms that are failed, COS alarms answer the question “what has changed in my network since the last time I looked at it?” This screen will tell you when an alarm occurred and will also tell you when it cleared.

How does T/MonXM know which alarms you already took action on? You tell it by acknowledging the alarm condition in question by moving the highlight bar to that alarm and pressing the Enter key. Assuming you have the appropriate security authorization, the alarm will disappear from the COS page. If you acknowledged an alarm that failed, you won’t lose the alarm because it will remain in the standing alarm screen until the alarm clears.

COS Alarm Window shows details of unacknowledged alarms.

The COS Alarm Screen is activated by pressing F3 from either the Alarm Summary Screen or the Standing Alarms Screen. The COS Alarm Window displays the alarm detail lines of unacknowledged alarms.

COS alarms are reported every time the state of the alarm changes. This means that the alarm is reported when it fails and also when it clears. These alarms are also known as audible alarms due to the user-defined sound that indicates the level of alarm. By default, alarms are reported in the following format:



Fig. 17.19 - COS screen shows details of latest changes.

**SCREEN 1**

(left-most or first page portion of screen):

Date/Time	Alarm Status	Site Name	Description
-----------	--------------	-----------	-------------

**SCREEN 2**

(right-most or second page portion of screen, reached by pressing Tab):

Alarm ID	Level
----------	-------

**Note:** This formatting is user-definable via the Alarm Formatting screen under the Parameters menu — see section 17-15.

**First Column Descriptions**

The first four character columns in each alarm display line of COS screens are reserved. They are used as follows: Column 1 is always blank on a T/Mon. (At remote terminals there may be a > character here. It indicates a highlighted alarm line). Column 2 will have an exclamation point (!) if the alarm point has a Text/Message. Column 3 will have a pound sign (#) if the alarm point has an open Trouble Log. Column 4 will have an at sign (@) indicating an ASCII alarm that has an associated text fragment. (A text fragment is the portion of an ASCII alarm message that actually triggers the alarm. This text can be viewed by pressing F7 while in the Standing Alarms screen.)

The Text/Messages Window appears at the lower left portion of the screen (in place of the Summary Legend Window), displaying the text message associated with the alarm under the selection (highlight) bar. If there is a text message on the line it may be viewed by pressing F5 to select text mode (this is the default) and then moving the highlight bar to the line containing the “!”. To view a trouble log, press F6 and move to the line containing the “#”.

**COS shows Messages and Trouble Logs**

After receiving a COS alarm some action should be taken, then it should be acknowledged by pressing Enter. Your logon initials along with the alarm information will then be logged. If the alarm is still active then it will remain in the Standing Alarms window along with the initials of the user who acknowledged the alarm.

CALL alarm occurrences send pages when the T/Mon Smart Paging is turned off in the Files > Paggers > Parameters menu option.

If the alarm is set to dial a pager and you acknowledge the alarm before T/MonXM dialed the pager, then the pager call will be aborted.

The maximum number of COS entries can be set in Parameters > Miscellaneous

**Note:** COS Alarms Window can hold up to 3000 COS alarms. Once full and another COS alarm is logged, then the oldest COS alarm will be automatically acknowledged with the initials @@@.

Table 17.F on the next page lists function keys for the COS Alarms window.

## ACK Alarms

An operator acknowledges an alarm after he or she has initiated the proper response action. Acknowledgment indicates to other system observers that the alarm is being attended. Therefore acknowledged alarms no longer appear on the COS screen or generate other alerting functions, such as paging (with Smar Paging enabled) or audible indication.

**Table 17.M - Key commands available in the COS Alarms window**

Function Key	Description
Enter (ACK)	Acknowledges the selected alarm. Once this is done, the selected alarm will be removed from the COS Alarms window and from any other window that it may be displayed in. <b>Note:</b> If the alarm is still standing (Failed) it will remain in the Standing Alarms window. It will not be reported to the COS Alarms window again until it changes state (Cleared).
Home	Go to the first page of COS alarms.
End	Go to the last page of COS alarms.
PgUp/PgDn	Go to the previous or next page of COS alarms.
Tab	Pans the screen from left to right to view extended definition of alarms.
F1	Go to the previous alarm window.
F2	Go to the next alarm window.
F4	Activates the Standing Alarms screen (see Page 17-28).
F5	Displays the text message box for viewing additional alarm information if attached to the currently highlighted alarm.
F6	Activates the Trouble Log window for viewing or creating trouble logs for individual alarms.
F8	Activates Site Controls.
F9	Displays online help for the COS mode in the lower left window (where Text/ Messages normally appear).
Alt-F1	Lists the COS alarms for the first alarm window.
Alt-F2	Lists the COS alarms for the last alarm window.
Alt-F4	Acknowledges ALL the COS alarms for the current window. (Requires additional security authorization.)
Alt-F7	Prints out a hard copy report of all COS alarms in the current window.
Ctrl-F1	Lists the COS alarms for the previous window that contains COS alarms.
Ctrl-F2	Lists the COS alarms for the next window that contains COS alarms.

**Note:** The Ctrl-F1 and Ctrl-F2 functions are very useful in routine operation

## Standing Alarms

Standing Alarms shows failed alarms

The Standing Alarms screen is enabled by pressing F4 from either the Alarm Summary screen or the COS Alarms screen. The Standing Alarms window displays a real-time image of all alarms that are currently failed (for the selected window). New alarms will automatically appear as they occur and disappear as they clear. Alarms are always listed in chronological order, with the newest alarm at the bottom of the screen.

By default, alarms are reported in the following format:

### SCREEN 1

(left-most or first page portion of screen):

Date/Time	Alarm Status	Site Name	Description
-----------	--------------	-----------	-------------

### SCREEN 2

(right-most or second page portion of screen, reached by pressing Tab)

Alarm ID	Level	Ack	Label	Ack Initials	Ack Date-2	Ack Time-2
----------	-------	-----	-------	--------------	------------	------------

**Note:** This formatting is user-definable via the Alarm Formatting screen under the Parameters menu.

The first four character columns in each alarm display line of Standing Alarms screens are reserved. They are used as follows: Column 1 is always blank on a T/MonXM WorkStation. (At remote terminals there may be a > character here. It indicates a highlighted alarm line). Column 2 will have an exclamation point if the alarm point has a Text/Message. Column 3 will have a pound sign (#) if the alarm point has an open Trouble Log. Column 4 will have an at sign (@) indicating an ASCII alarm that has an associated text frag-



Fig. 17.20 - Standing alarm window shows details of existing alarms.

## Standing Alarms shows Messages and Trouble Logs

ment. (A text fragment is the portion of an ASCII alarm message that actually triggers the alarm.) Press F7 to view this text.

The Text/Messages Window appears at the lower left portion of the screen (in place of the Summary Legend Window), displaying the text message associated with the alarm under the selection (highlight) bar. If there is a text message on the line it may be viewed by pressing F5 to select text mode (if you are not already there) and then moving the highlight bar to the line containing the “!”. To view a trouble log, press F6 and move to the line containing the “#”. Table 17.N lists function keys for the Standing Alarms window:

**Table 17.N - Key commands available in the Standing Alarms window**

Function Key	Description
Home	Go to the first page of standing alarms in current window.
End	Go to the last page of standing alarms in current window.
PgUp/PgDn	Go to the previous/next page of standing alarms in current window.
Tab	Pans the screen from left to right to view extended definition of alarms.
F1	Go to the previous alarm window.
F2	Go to the next alarm window.
F4	Activates the Standing Alarms screen (see Page 17-28).
F5	Displays the Text/Message window for viewing additional alarm information if attached to the currently selected alarm.
F6	Activates the Trouble Log window for viewing or creating trouble logs for individual alarms.
F7	View ASCII text fragment.
F8	Activates Site Controls.
F9	Displays online help for the standing mode in the lower left window (where Text/Messages normally appear).
Alt-F1	Lists the alarms in the first alarm window.
Alt-F2	Lists the alarms in the last alarm window.
Alt F7	Prints out a window report of all standing alarms in the current window.
Ctrl-F1	Lists the alarms in the previous alarm window with standing alarms.
Ctrl-F2	Lists the alarms in the next alarm window with standing alarms.
Ctrl-F9	Acknowledge all SNMP alarms in the standing alarm screen. Requires user rights.
Shift-F10	TAG/UNTAG alarm. Suspends alarm point from continued status change reporting. Use to control “nuisance” alarms.



**Note:** Standing alarms are always displayed until the condition causing the alarm is corrected, which clears the alarm and causes it to be automatically removed from the standing alarm list. Alarms will appear and disappear from the Standing Alarms screen without user intervention, regardless of acknowledgment. The alarm status changes are recorded in the COS Alarms screen, and must be acknowledged there.

## Root Alarm Filter Status

The root alarm filter status screen can be accessed by pressing Alt+F6 from the alarm summary screen. From here, you can view alarms silenced due to root alarm filtering.

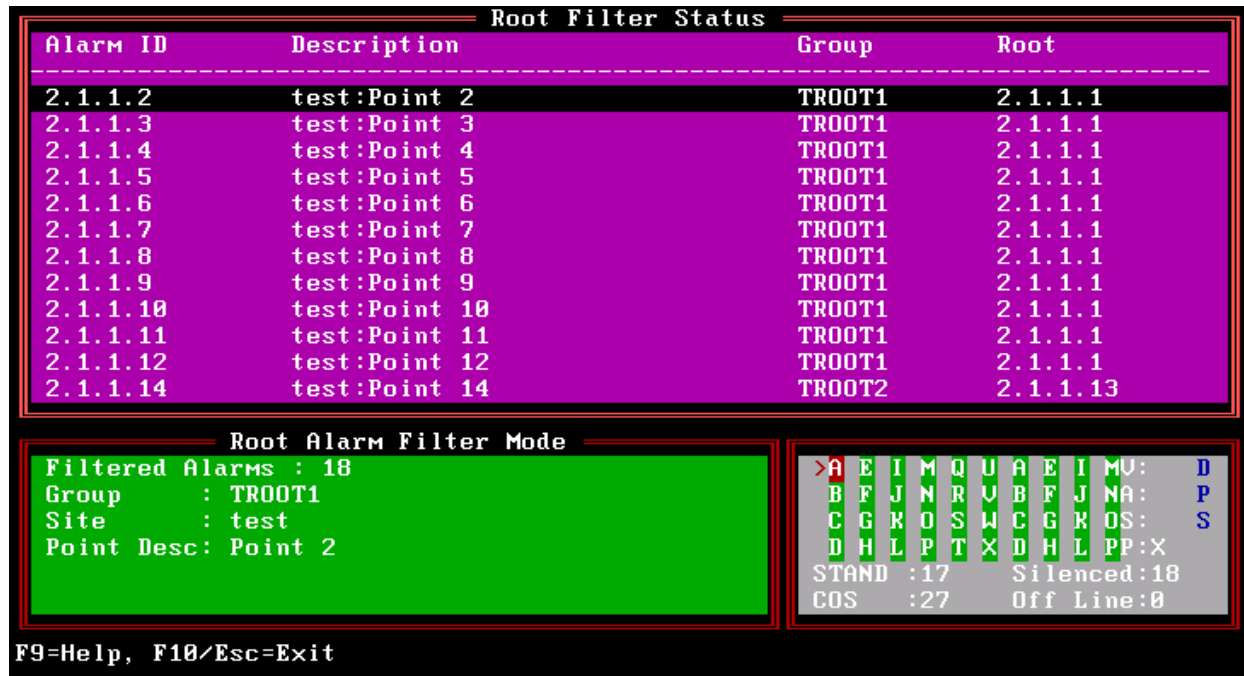


Fig. 17.21 - From the Root Filter Status window, you can silenced member alarms for each group.

Each line on this screen contains the suppressed alarm ID (port, address, display, point), a description of the point (site name and description entered in the point definition screen), the root filter group ID, and the alarm ID of the first failed root alarm that suppressed the member.

You can generate reports for each root alarm filter group from the report menu under Alarm Database > Root Alarm Filter. For more information on reports, see “Reports” later in this section.

## TAG Alarms

Tagging and silencing are different ways of doing the same thing. Most users prefer silencing.

An operator can Tag a nuisance alarm point that is cycling between alarm and clear to prevent the COS screen from filling with repeating alarms and to silence repeated pages to on-call personnel. In the Standing Alarm screen, highlight the point and press Shift-F10. When an alarm point has been tagged, the alarm status field in both the COS and Standing alarm screens will change to say "TAG." Pressing F10 again will remove the Tag and return the point to normal operation.

## Silence Alarms/Windows

Silencing allows selected alarms to be suspended for a specified period of time. When an alarm is silenced, it does not generate any COS entries and it does not appear in the standing alarm list. Each



Fig. 17.22 - Silence/alarms windows allows a nuisance alarm to be suspended for a limited time.

Single alarms can be silenced for a limited time.

Entire windows can be silenced for a limited time.

system account must have the Tag/Silence alarm field set to yes to enable the Silence Alarm Window Function

There are two ways to silence alarms: An individual alarm may be silenced or a window may be silenced. When a window is silenced, all alarms in that window are silenced.

To silence an individual alarm, highlight it in the COS or standing window and press Alt-F3. You will then be prompted for the date and time that the silenced condition will expire (Figure 17.21).

To silence a window, select it on the Alarm Summary screen and press Alt-F3. You will then be prompted for the date and time that the silenced condition will expire (similar to Figure 17.21).

To view the list of items (alarms and windows) that have been silenced, press Alt-F4 from the alarm summary (Figure 17.22). You can manually un-silence an item by highlighting it and pressing F2.

Silenced Status			
Type	ID	Description	Expires
Alarm	2.7.1.5	DENVER:RCV SQUELCH ALM "B" RADIO	06/23/00 16:00
Alarm	2.20.1.1	LOS ANGELES:TOWER BEACON #1	06/23/00 16:00
Alarm	2.1.1.3	FRESNO:TECH ON SITE	06/23/00 16:00
Alarm	1A.11.10.2	:LR24 FAILURE FOR FRESNO	06/23/00 16:00

Fig.17.23 - Pressing Alt-F4 in the alarm summary screen displays a list of silenced items and their expiration dates/times.

Silenced alarms status can be checked for each window.

To view the list of items (alarms and windows) that have been silenced, press Alt-F4 from the alarm summary (Figure 17.22). You can manually un-silence an item by highlighting it and pressing F2.

## Performance/Statistics Mode

The Performance/Statistics window is enabled by pressing F6 while in the Alarm Summary screen. It appears in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window. This window shows statistical information accumulated by T/MonXM on the quality of communication links to each communication/polling port. This window differs for each port's protocol.

Full alarm monitoring operations are available while the Performance/Statistics Window is active. If you wish to reset the statistics in this window, press Alt-F2.

You will notice a number in brackets: "[7]". This is the port number currently being viewed. You can change to a different port by using the plus, minus, and numeric keys described later.

The protocol for the current port is displayed in parentheses "(" after the port number. If SUSPENDED is displayed then the current port is suspended and can only be activated in the Remote Ports window from the Parameters menu. If HALTED is displayed then the current port is halted and no protocol is defined for this port.

The time and date appear in the lower left corner of the window.

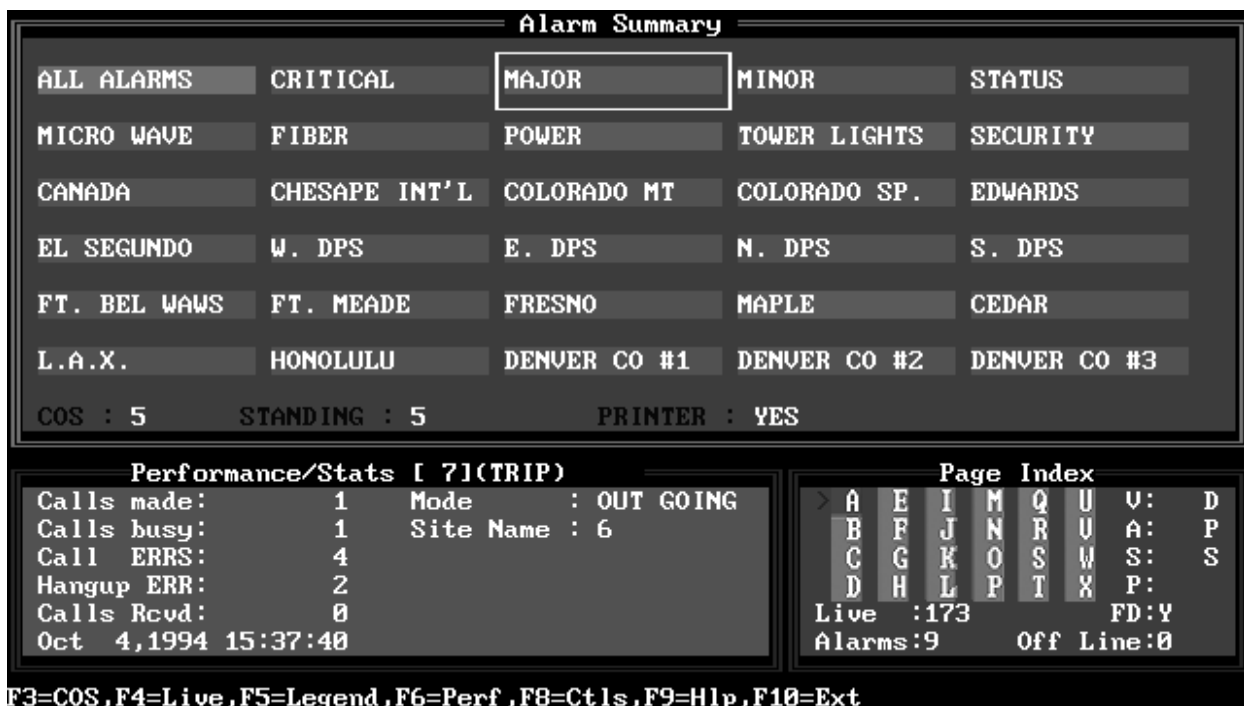


Fig. 17.24 - Performance/statistics window replaces summary legend window

**Note:** Table 17.O continues on following page.

**Note:** The only protocols with performance/statistics standard with T/MonXM are TRIP (T/Mon Remote Interface Protocol) and DCP(F). Ports that are defined for remote access will also provide information in the performance/statistics window. The performance/ statistics fields associated with these protocols are explained in the table below. If you have other protocols available refer to the appropriate Software Module for an explanation of the performance/statistics fields.

**Table 17.O - Fields in the Performance/Statistics window, Standard Protocols**

Field	Description
<b>TRIP Protocol</b>	
Calls made	The total number of outgoing calls made.
Calls BUSY	The total number of attempted outgoing calls made but the line was busy.
Call ERRS	The total number of errors on outgoing call attempts.
Hang-up ERR	The total number of hang-up errors.
Calls Rcvd	The total number of incoming calls received.
Mode	Shows current port activity. This will display one of three messages: Waiting (waiting to make an outgoing or to receive an incoming call) Outgoing (placing an outgoing call) Incoming (receiving an incoming call).
Site Name	The name of the site connected.
<b>DCP(F) Protocol</b>	
Pol Cmds	Number of polling commands sent since last reset.
Polls OK	Number of polls that resulted in good responses.
Ctrl Cmds	Number of control commands sent since last reset.
Ctrl OK	Number of control commands resulting in confirmed responses.
Noise Chars	Number of characters received as unexpected data ("noise").
No Response	A running statistic on alarm equipment that failed to respond when polled.
Time Out	Data time out. Only a partial response was received from the alarm equipment.
BCH Errors	The data frame failed the BCH data integrity check. (This is data transfer error checking.)
New CMD Err	A premature new command was received or data overflow (too much data was received).
Dsp Not Mon	Number of times a device responded with information for a display not defined in the T/MonXM database. <b>WARNING:</b> If this number is greater than zero then you may not be monitoring all the data from your RTUs.
Active/Passive	Shows polling status. Active = port is polling. Passive = port is listening only. The polling status is followed by a number indicating the address being polled. That is followed by letters and numbers indicating the type of polling (U = Upset, G = Group) and the number of the group. SKP indicates a skip in polling.

**Table 17.O - Fields in the Performance/Statistics window, Standard Protocols continued**

Field	Description
<b>Remote Access Ports</b>	
User	Log on initials of person using remote access.
Log On Date	Date of last log on.
Log On Time	Time of last log on.
Modem	Y = Modem present on port. N = Modem not present on port.

**Table 17.P - Key commands available in the Performance/Statistics window**

Function Key	Description
-	Minus key. Displays the previous port.
+	Plus key. Displays the next port
]	Advances 10 ports forward.
[	Returns 10 ports back.
1-0	Displays port numbers 1-10. If you're using your numeric keypad to select, make sure NUM LOCK is on.
Shift-1 ... Shift-0	Displays port numbers 11-20. <b>Note:</b> Not to be used with the numeric keypad.
Alt-F2	Reset contents of Performance/Statistics window for the current port. <b>WARNING:</b> Each port has one set of statistics that is shared by all users of the system (the remote access terminal and T/MonXM WorkStations). Resetting a port from one remote access location resets that port on all other locations.

**This page intentionally left blank.**

## Site Controls

Site Controls operate the controls for a window

The Site Controls screen can be accessed by pressing F8 from the Alarm Summary, COS or Standing Alarms screens. Site Controls allow the user to operate the controls for a whole window, usually defined by site, thus the name Site Controls. Site Controls can also be defined by status, by device or by any other category assigned to a window.

Before Site Controls can be operated they must be predefined. For more information on defining Site Controls see Section 12 (Configure Controls).

T/MonXM provides three methods of operating control points at RTUs: Site Controls, Labeled Controls and Derived Controls. Site Controls, described here, are operated through windows, by site or other window category. Labeled Controls, described later in this section, are very similar to site controls, but are operated from a type of control grouping rather than from a site window. Derived controls are automatically operated by T/MonXM from user-defined formulas that evaluate certain alarm points to determine if an automatic control point operation is appropriate.

Issuing Site Controls is a two step process. You must first select the category. Up to 40 categories of control groups can be defined in the data base, each containing up to 200 control point entries. Each of those entries can contain multiple points or ranges of points to give you great flexibility in issuing controls. To select a category, position the highlight bar on the line you want and press Enter. This is part of the first screen you'll see (Figure 17.24). The second screen, Site Controls Point Selection allows you to issue the individual controls. Several controls can be grouped into a batch for simultaneous operation. Both individual point operation and batch operation are explained on the following pages.

Table 17.Q lists the field definitions for the Site Controls screen.

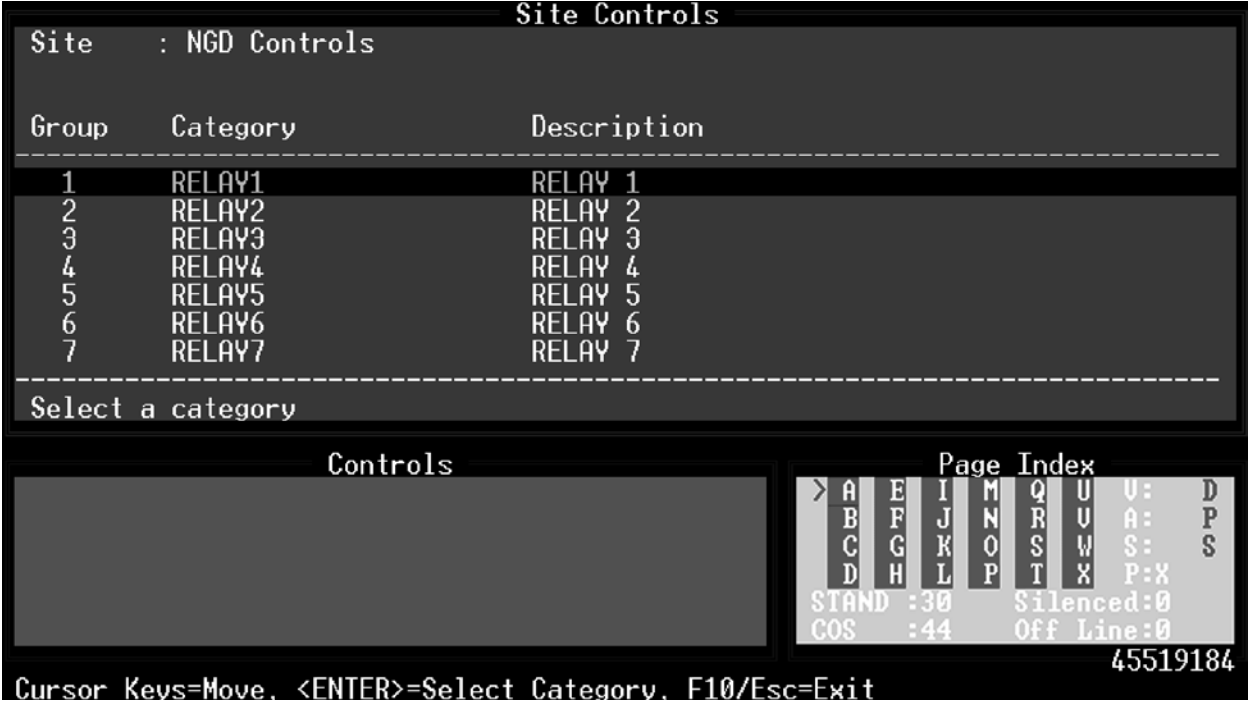


Fig. 17.24 - Site controls begins with the category selection screen.

Table 17.Q - Fields in the Site Controls screen

Field	Description
Category	The title for the category.
Description	A description for the category.



# Site Controls Point Selection

Issue controls from the Site Controls Point Selection screen.

After you’ve selected your category, you can issue the individual or batch controls to the devices. This is done from the Site Controls Point Selection screen. The Control Points must also be predefined, just as the Categories must, from the File Maintenance menu.

## Individual Point Operation

From Site Controls Point Selection screen, select the desired control entry based on description and press Enter. A verification window appears asking the you to press “C” to confirm the control command. After you confirm the command, another verification window appears (illustrated below) which shows the total points ‘Okay’ and the total points ‘Failed’. If a control point fails, this window will allow you to either: A (Abort), R (Retry) or C (Continue to the next control point).



Fig. 17.25 - Verification window shows controls sent.

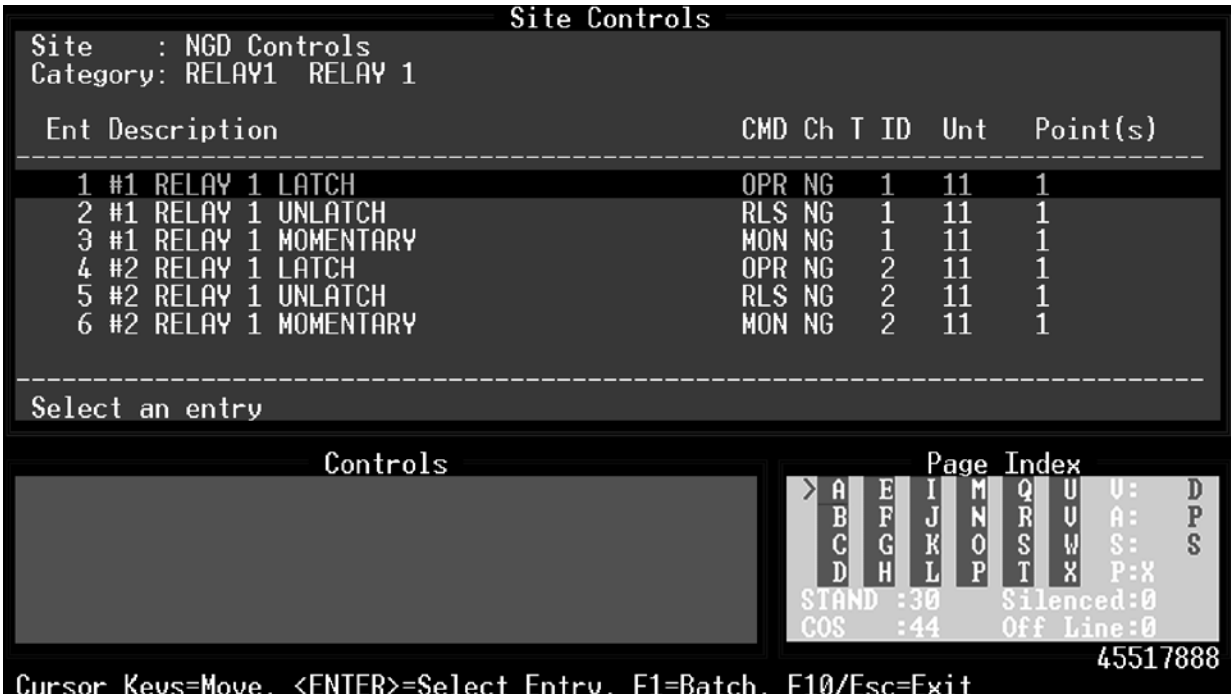


Fig. 17.26 - Control details are provided on the site control point selection screen.

The following tables list the field names, function keys and descriptions for the Site Controls Point Selection screen.

**Table 17.R - Fields in the Site Controls Point Selection screen**

Field	Description
Ent	The entry number within the group selected (200 entries per group).
Description	The description of the control points. Up to 40 characters.
*CMD	The command that will be used to activate the control point. OPR = Operate Relay RLS = Release Relay MON = Momentary On MOF = Momentary Off SBO = Select Before Operate SBL = Select Before Release SMO = Select Before Momentarily Operating EXE = Execute Select Before Operate/Release Commands CLR = Clear all Select Before Operate/Release Commands
*Ch	Channel number to issue controls to. RP = Remote Port (Modem port) RC = Relay Card (102 Card) AV = Audio/Visual Card (101 or 108) 1-500 = Port number K1-K2 = KDA Shelf NG, N2 = NetGuardian NW = NetWatchman
*D	Device Type C = CPM S = SBP (Smart Bypass Card)
*Add	The device's address.
*Unt	Unit. This varies depending on the protocol and serves as a data index. Typically a display or group.
*Point(s)	Control point(s) that control will be sent to.

\*These fields are for system administrator troubleshooting and most users need not be concerned with them. The description field should contain all the necessary information to identify the proper control point.

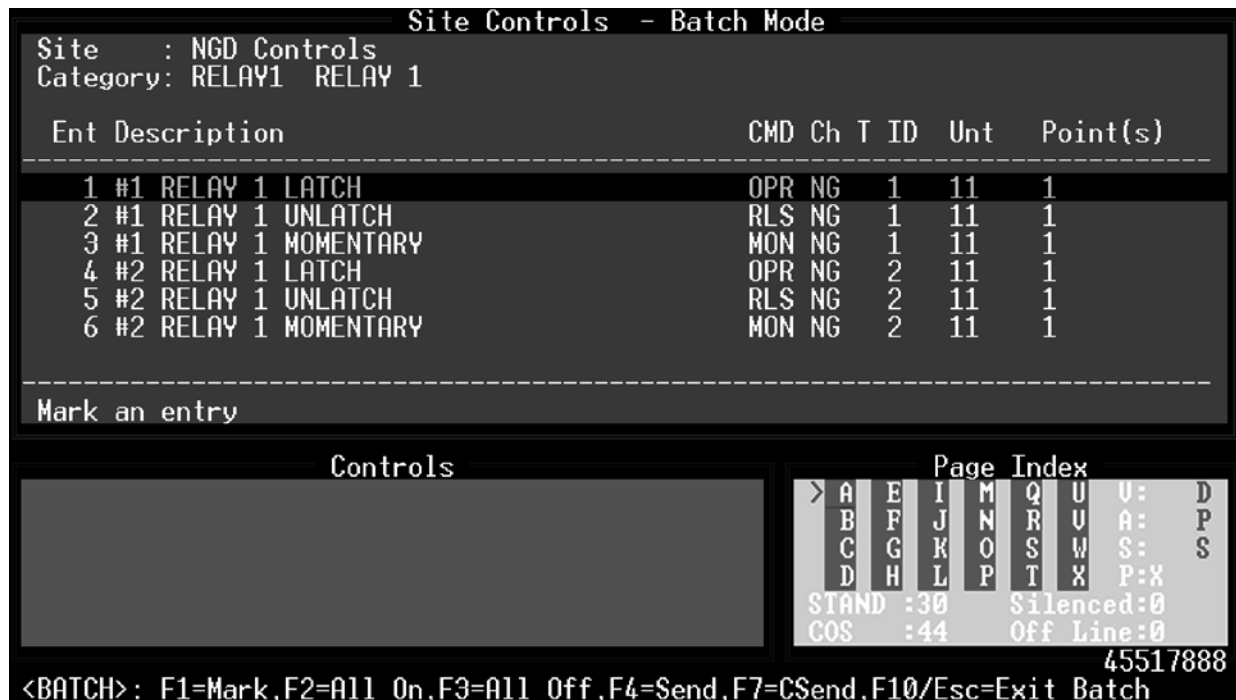


Fig. 17.27 - Operate site control points in batches from the batch mode screen.

#### Batch Point Operation

From the Site Controls Point Selection screen press F1 to select the Site Controls - Batch Mode screen. The prompt line will display the commands in the table below. Highlight and mark points with F1. Execute control point operation with F4.

Table 17.S - Key commands available in the Site Controls - Batch Mode screen

Function Key	Description
Up Arrow/Down Arrow	Moves highlight bar up or down through the fields.
F1	Mark. Press to mark highlighted point. An asterisk (*) will appear at the left end of each marked line. Toggles mark on or off.
F2	All On. Marks all points in the category.
F3	All Off. Un-marks all points in the category.
F4	Send. Verification window asks you to press "C" to confirm sending the control command. After command is sent the window will show the results, as in individual point operation.
F7	Confirm Send. Use with Select Before Operate (SBO) points. Verification window will be presented a second time, after the initial operate command is sent.
F10/Esc	Exit Batch Mode.

**Note:** After control points are operated, points will remain marked in case additional operations are needed. To clear marks use F3 or F1.

## Alarm Indicator Control

The 108 Audible Alarm Card supports external audible and visual alarm devices, 4 general purpose relays and a watchdog timer.

On the T/MonXM WorkStation, the Alarm Indicator Control window options only work if the DPS 108 Audible Alarm Card is installed. On the IAM-5, the Alarm Indicator Control is supported without the 108 card. For more information about the card, refer to Appendix M - Hardware Installation, Section M-17 Audible Alarm Card.

The DPS 108 Audible Alarm Card is standard in all T/MonXM systems, version 2.0 and later. This card supports external audible and visual alarm devices such as bells or lights or a DPS Building Status Unit. Up to four (4) audible and four (4) visual devices may be independently controlled. These devices are usually programmed to correspond to the four levels of alarm (A, B, C and D) used by T/MonXM. There are also four general purpose relays, a watchdog timer and an internal audible device that provides 3 distinctive sounds for different alarm levels.

The Alarm Indicator Control window is enabled by pressing Alt F1 while in the Alarm Summary screen. It appears in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window. This window allows you to turn the audible and visual devices on or off and to define the internal audible device sounds for the different levels of alarms.

The eight (8) relays each have an associated software switch, which, when turned on, suspends operation of the relay. Those associated with the visual control relays are called visual cut off (VCO) and those associated with the audible relays are called audible cut off (ACO).

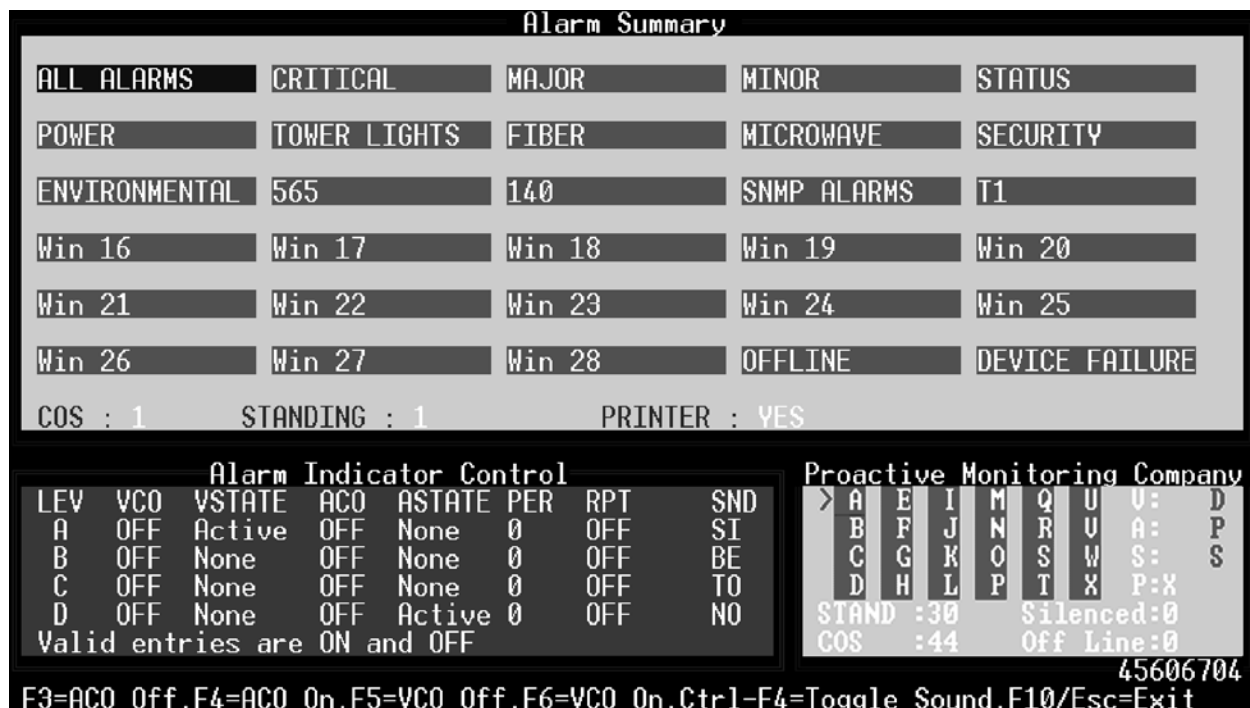


Fig. 17.28 - Alarm indicator control window replaces summary legend window.

The relays are either opened or closed, depending on the state of the associated alarm level. When the relay is closed, the state field in the Alarm Indicator Control Window becomes Active (an alarm failed). When the relay is opened, the state field changes back to None (the alarm cleared).

**Table 17.T - Fields in the Alarm Indicator Control window**

Field	Description
LEV	Level. Displays the alarm level you are editing.
VCO	Visual Cut Off. If set to "ON" the relay is opened regardless of the state of the alarm level (the relay is disabled). If set to "OFF" the relay will function normally.
VSTATE	Visual State. Displays the visual state of the alarms for the current alarm level. If there are any standing alarms for this level then it will display "Active", otherwise it will display "None."
ACO	Audio Cut Off. If set to "ON" the relay is opened regardless of the state of the alarm level (the relay is disabled). If set to "OFF" the relay will function normally.
ASTATE	Audio State. Displays the audio state of the alarms for the current alarm level. If there are any COS alarms for this level then it will display "Active", otherwise it will display "None". <b>Note:</b> This shows you what the relay would have been doing if the cutoff were active. If the cutoff is not active, it shows the actual state of the relay.
PER	Period. The amount of time (in seconds from 1-100) that the relay will remain closed before automatically opening. If this is set to 0 the relay will remain closed until the alarm is acknowledged. If it is not set to 0, acknowledging the alarm will still cause the relay to open.
RPT	Repeat. If set to "ON" the relay will alternately open and close for the set period. If period is set to 0, this option will have no effect.
SND	Sound. This setting is independent of the relays. It sets the internal audible device sound for each alarm level. There are four possible settings: SI Siren [Default for Critical or "A" level alarms] BE Beep [Default for Major or "B" level alarms] TO Tone [Default for Minor or "C" level alarms] NO No sound [Default for Status or "D" level alarms]

**Table 17.U - Key commands available in the Alarm Indicator Control window**

Function Key	Description
Arrow Keys	Moves up, down, left and right, respectively, through the fields.
F3	Sets all ACOs to OFF. (Enables all external audible devices.)
F4	Sets all ACOs to ON. (Disables all external audible devices.)
F5	Sets all VCOs to OFF. (Enables all external visual indicators.)
F6	Sets all VCOs to ON. (Disables all external visual indicators.)
Ctrl F4	Toggles (enables/disables) the internal audible device. NOTE: Depending on how your T/MonXM has been configured by the system administrator this feature may do one of three things: 1. It may disable the sound until toggled back on. 2. It may temporarily disable the sound until an internal timer turns it back on. In this case it can still be manually toggled back on. 3. It may have no effect at all.
F10/Esc	Exit

**NOTE:** Two external switches can be wired to the DPS Audible Alarm Card. This will allow you to cutoff the alarm relays for level A and/or B with a flip of a switch. These switches take precedence over the software cutoffs and cannot be overridden.

## English Analyzer Mode/English Filter

English Analyzer is primarily a diagnostic mode that is not part of typical system operations.

This window shows protocol traffic in ordinary English. Text varies according to protocol type—not all protocols support English descriptions.

An English Analyzer Mode can be activated from any of the alarm monitoring screens to provide an easy to read analysis of the protocol communications between T/MonXM and any remote device. The analysis is displayed in the English Analyzer window. This mode is port specific, and may be made address specific by using the English Filter window.

The English Analyzer window is enabled by pressing Alt F5 while in the Alarm Summary, Dialup Site Monitor, Site Statistics, COS or Standing Alarms screens. It appears in the lower left portion of the screen, in place of the Summary Legend window or Text/Messages window. This window displays protocol traffic in an English form. When the English Window is activated, protocol commands are translated and displayed. Function keys may be used to select a specific port for analysis.

To select a specific address for analysis, enter the English Filter window from the Alarm Summary screen. Press Ctrl F5 to enable the English Filter window. (This window may also be selected directly while in the Alarm Summary screen.) It appears in the lower left portion of the screen, in place of the Summary Legend window. Enter the desired information in the fields, as described in the second table on the following page, and press Enter. The English Filter window will change to the English Analyzer window, displaying data from the selected address.

The data that appears in the English Analyzer window will differ for each protocol in use. The Appendix lists the commands that will be seen for each of the common protocols. If you are debugging over the phone with a DPS technician you may be asked to read the

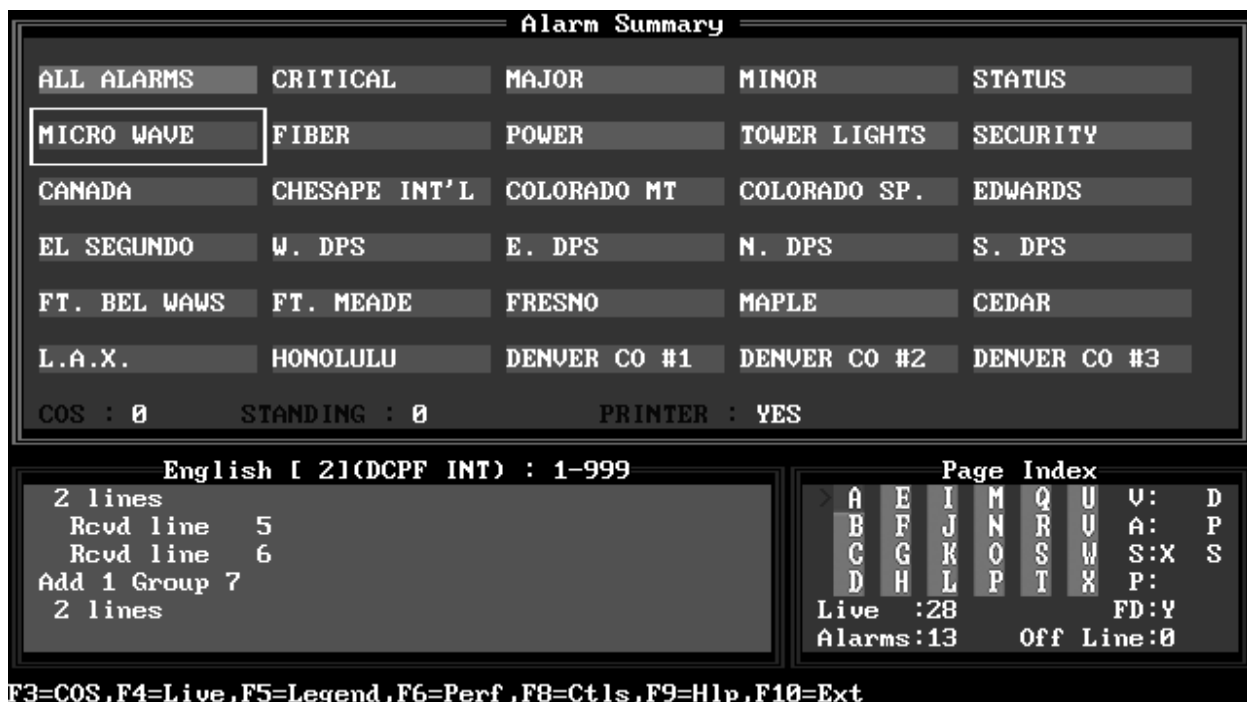


Fig. 17.29 - English analyzer window replaces summary legend window.

data in this window. The line at the top of the window displays the following information:

English	[<Port#>:Module Number_<Protocol>]	(Protocol:Addresses)
---------	------------------------------------	----------------------

NOTE: Alarm polling will continue while in either of these windows and alarms will still be displayed on the screen, but polling speed may be affected. Therefore, you should not leave this mode constantly enabled.

English	[Port#: Protocol Number_Protocol Name]	(Addresses)
---------	--	-------------

The following tables list the function keys and descriptions for the English Analyzer and English Filter mode windows.

**Table 17.V - Key commands available in the English Analyzer window**

Function Key	Description
Space	Space bar. Freezes (pauses) the window for you to inspect the information (monitoring still continues in the background). Press space bar again to continue viewing new data.
-	Minus key. Displays the previous port.
+	Plus key. Displays the next port
]	Advances 10 ports forward.
[	Returns 10 ports back.
1-0	Displays port numbers 1-10.
Shift 1-Shift 0	Displays port numbers 11-20.
F5	Leave English Analyzer mode and restore the Summary Alarm Legend window.
F10/Esc	Exit



**Fig. 17.30 - English filter window.**

**Table 17.W - Fields in the English Filter window**

Field	Description
Addresses	Enter the addresses (1-999) that you wish to include in the English Analyzer window.
Cmds Only	Enter Y for viewing only polling commands or N for viewing both polling commands and responses from the monitored alarm equipment.



## Report Mode

See Section 19 (Managing Reports) for additional information.

The Report Mode window is enabled by pressing Alt-F7 while in the Alarm Summary screen. This window shows a menu listing the available reports. Reports give a print out or file record of data base information. To select a report, type the number and press Enter. Table 17.X lists a summary of available reports.

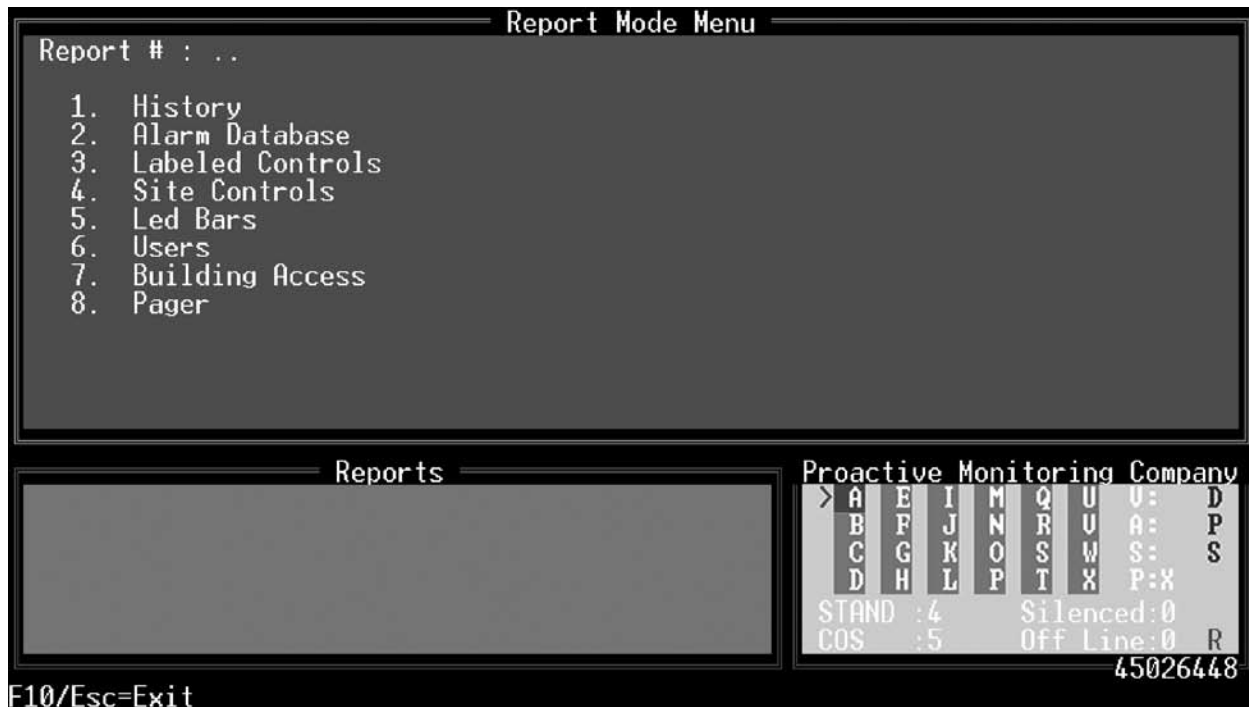


Fig. 17.31 - Report mode window

Table 17.X - Reports available in the Report Mode menu

Report	Description
History	Report for a selected period of time (or other criteria) that alarms occurred.
Alarm Database	Report on selected alarm items in the Alarm Database.
Labeled Controls	Report on labeled controls defined in the database. Corresponds with information on Labeled Controls editing screens.
Site Controls	Report on site controls defined in the database. Corresponds with information on Site Controls editing screens.
LED Bars	Report on LED Bars defined in the database. Corresponds with information in LED Bars editing screens.
Users	Report on users and security access privileges defined in the database.
Building Access	Report on building access sites defined in the database.
Pagers	Report on pager information in the database. Select from Pager Carriers, Pager Schedules or Pager Exceptions.

Some reports require additional information. This information will be requested in the window after a report number is selected. If you selected Reports from either the COS or Standing Alarms screens, you can generate a report for the specific window you're positioned in. See section 19 (Managing Reports) for more information on reports and report formatting.

When reports are created from monitor mode, T/MonXM is still actively monitoring the alarm equipment. The report can either be sent to the printer or saved to the hard drive. Only one report can be in progress at any one time. If you attempt to enter Alt F7 while a report is running, an error message will be displayed. As soon as the printer stops printing, you may start the next report. (If your printer has a large buffer, you may be able to start sooner).

User interaction may be a bit sluggish when reports are being processed.

Reports can be generated from console access, T/Remote, and T/Windows, but reports cannot be generated from the Web Browser Interface

Reports generated in the Monitor Mode allow monitoring to continue while the report is produced. Report selections 1 through 8 listed in the Report Mode Menu menu are available. In addition, by pressing Alt-F7 while in the COS or Standing Alarms screens you can generate a report of the COS or Standing alarms for a specific window. In this mode you cannot view the reports on screen.

Reports generated in the Reports screen under the Master Menu are produced while T/MonXM is off line (not monitoring alarms). In this mode you cannot generate a report for a specific window. In this mode you can view reports on screen. (Refer to Section 19 - Reports, for more information.

**Technical note:** Remote access users can also run reports. However, only one user can run a report at the same time.

T/RemoteW and T/Windows users can send reports directly to their local or network printer or save reports to a file on their PC.

## Protocol Analyzer

**Note:** The protocol analyzer is available only at the main workstation or through T/Access. It is not available at remote terminals.

Protocol traffic is displayed in hexadecimal or ASCII form

The Protocol Analyzer window is enabled by pressing Alt F8 while in the Alarm Summary, COS or Standing Alarms screens. It appears in the lower left portion of the Alarm Summary Screen, in place of the Summary Legend window or Text/Messages window. This window is used as a debugging tool for monitoring protocol traffic between the polling port of your computer and the alarm equipment. When the Protocol Analyzer is activated, protocol traffic commands are translated into hexadecimal or ASCII form and displayed in the window. This mode is port specific only. Function keys may be used to select a specific port for analysis.

The data that appears in the Protocol Analyzer window will differ for each protocol in use. If you are debugging over the phone with a DPS technician you may be asked to read the data in this window. Transmitted characters are displayed in yellow and are prefaced with a "T" when viewed in HEX mode. Received characters are white. The line at the top of the window displays the following information:

Protocol	[Port Number:Protocol Number_Protocol Name]
----------	---

**Note:** Alarm polling will continue while in this window and alarms will still be displayed on the screen, but polling speed may be affected. Therefore, you should not leave this mode constantly enabled.

Alarm Summary

ALL ALARMS	CRITICAL	MAJOR	MINOR	STATUS
MICRO WAVE	FIBER	POWER	TOWER LIGHTS	SECURITY
CANADA	CHESAPE INT'L	COLORADO MT	COLORADO SP.	EDWARDS
EL SEGUNDO	W. DPS	E. DPS	N. DPS	S. DPS
FT. BEL WAWS	FT. MEADE	FRESNO	MAPLE	CEDAR
L.A.X.	HONOLULU	DENVER CO #1	DENVER CO #2	DENVER CO #3

COS : 0
STANDING : 0
PRINTER : YES

Protocol Analyzer [ 21(DCPF INT)

```

0 T00 TFF T01 T40 T03 T02 T00 T01 T17 00 FF 01 0
2 01 00 FF 03 40 00 01 80 20 3A 00 FF 04 08 00 0
2 20 41 T00 TFF T01 T06 T30 00 FF 01 06 30 T00 T
FF T01 T40 T05 T02 T00 T01 T05 00 FF 01 02 01 00
FF 05 00 03 22 46 00 FF 06 00 03 20 65 T00 TFF
T01 T06 T30
          
```

Page Index

```

> 1 5 9 13 17 21 U: D
  2 6 10 14 18 22 A: P
  3 7 11 15 19 23 S: X S
  4 8 12 16 20 24 P:
Live :29 FD:Y
Alarms:14 Off Line:0
          
```

F3=COS,F4=Live,F5=Legend,F6=Perf,F8=Ctl's,F9=Hlp,F10=Ext

Fig. 17.32 - Protocol analyzer window replaces summary legend window

Table 17.Y lists the function keys and descriptions for the Protocol Analyzer window.

**Table 17.Y - Key commands available in the Protocol Analyzer window**

Function Key	Description
Space	Space bar. Freezes (pauses) the window for you to inspect the information (monitoring still continues in the background). Once you pause the display, you can select between hexadecimal or ASCII output by pressing either the H or A keys respectively. <b>Note:</b> ASCII output is limited to output that is between 32 and 127. Any data less than 32 or greater than 127 will continue to display in hexadecimal, even if you've selected ASCII. Protocol Analyzer shows characters as they are processed, therefore if paused, the display will not resume at the same place.
-	Minus key. Displays the previous port.
+	Plus key. Displays the next port
]	Advances 10 ports forward.
[	Returns 10 ports back.
1-0	Displays port numbers 1-10.
Shift 1-Shift 0	Displays port numbers 11-20.
F5	Leave Protocol Analyzer mode and return to the Summary Legend or Text/ Messages window.
F10/Esc	Exit

**Protocol Analyzer is a turnup/diagnostic tool that requires specific protocol knowledge. It is not intended for general use.**

## Channel Summary

The Channel Summary window is enable by pressing Alt F9 while in the Alarm Summary screen. It appears in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window. This window shows the status of remote ports, four ports at a time.

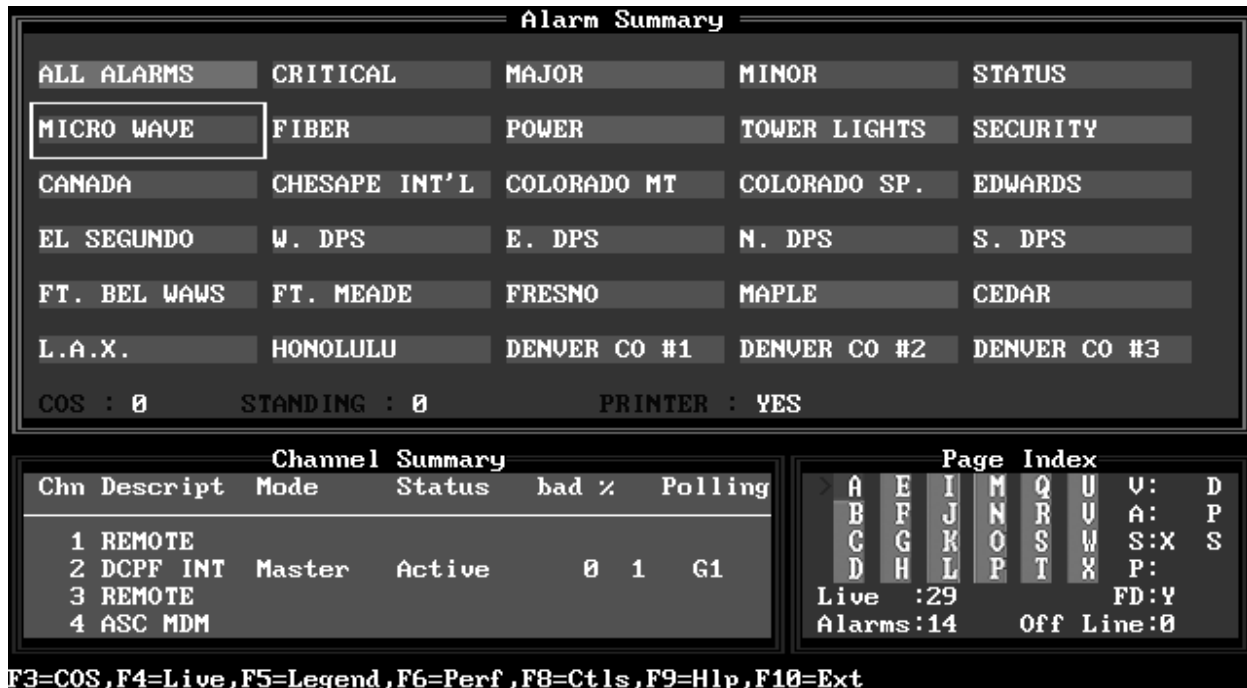


Fig. 17.33 - Channel summary window replaces summary legend window

Table 17.Z - Fields in the Channel Summary window

Field	Description
Chn	Channel/Port. Displays the channel number. An asterisk (*) displayed in front of the number the channel indicates a communication link failure between the port and the equipment.
Descript	Displays the protocol description.
Mode	This field is only active with DCPf or E-Telemetry ports. It indicates either a Master, Combined or Passive configuration designation for the E2A and DCPf protocols. It shows what the port can do, not necessarily what it is doing. i.e.: In combined mode the port may be either active or passive at a particular time.
Status	Displays the status of the port. Indicates Stopped, Active or Passive.
bad %	Displays percentage of successful polls versus unsuccessful polls.
Polling	Displays a cryptic polling message. Refer to the appropriate section in the manual which describes the protocol being polled.
+/-	Press the + or - key to scroll up or down in this window.

## Dialup Site Monitor

The Dialup Site Monitor screen is opened by pressing Shift F4 while in the Alarm Summary screen. It appears as a Dialup Site Monitor window in the upper portion of the screen, in place of the Alarm Summary Window, and as a Dialup Statistics window in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window. This screen shows the status of all currently defined dialup sites. From here you can tell T/MonXM to call the device next to gather alarm data, configure/re-configure or take the device on or offline.

Tables 17.AA and 17.AB List the field names and function key descriptions for the Dialup Site Monitor screen.

Dialup Site Monitor						
Dev	Site Name	Call	Type	Status	Last Call	
ASC	TNDS #1 FTS-2K	Waiting		OK		
DPM	PACKING SHED #2	Dialing	Standard	OK	Sep 21,2002 10:26:07	
DPM	EAST TOWER	Waiting		OFFLINE		
ALP	PACKING SHED #1	Waiting		OK		
ALP	WEST TOWER	Waiting		RETRY	Sep 21,2002 10:26:06	
D10	AMES NASA	Waiting		OK		
D10	BAY ST LOUIS	Waiting		OK		
D10	BELV ES	Waiting		OK		
D10	BELV WAWS	Waiting		OK		
D10	BWI ES	Waiting		OK		

Dialup Statistics		Page Index	
		A	E
		B	F
		C	G
		D	H
		I	M
		J	N
		K	O
		L	P
		Q	U
		R	V
		S	W
		X	P
		Live :3 FD:Y	
		Alarms:1 Off Line:1	

F1=Call,F2=Undo Call,F3=Reconfig,F4=Online,F5=Offline,F8=Lock,F10/Esc=Exit

Fig. 17.34 - Dialup site monitor and statistics windows replace alarm summary.

Table 17.AA - Fields in the Dialup Site Monitor screen

Field	Description
Dev	Device type.
Site Name	Site name assigned to device.
Call	Incoming or outgoing call status.
Type	Indicates source of the outgoing call - user dial out (User), normal dial out (Standard) or Labeled Controls dial out (Lbl Ctrl).
Status	Status of the site. Indicates whether it OK, failed or offline. Retry indicates the initial contact was unsuccessful. Redial will occur after approximately one minute. After repeated re-dials the status is failed.
Made	How many calls have been made to that site.
Revd	How many calls have been received from that site.
Last Call	Last time site was called.

**Table 17.AB - Key commands available in the Dialup Site Monitor screen**

Function Key	Description
F1	Call Next. This function key allows you to immediately check on a site by assigning the site selected as the next site called. An asterisk appears to the left of the site selected when the Call Next option is chosen.
F2	Undo Call Next. This function key cancels the Call Next selection, if it is not already in progress.
F3	Reconfig. Instructs T/MonXM to re-send configuration to device. This is normally only done when T/MonXM first communicates with the device. <b>Note:</b> This function is applicable only to DPS KDA and Pulsecom Datalok 10D remote telemetry units. For further information refer to Module Section 15 - Dial Up Remotes or to Module Section 15 - Pulsecom Datalok Notes.
F4	Online. Put device online. Alarm data will be transmitted and received by the unit.
F5	Offline. Takes device offline. Alarm data will not be transmitted or received by the unit. T/MonXM will not continue to call the device for alarm data until it is put back online.
F6	Analogs. Brings up the KDA Analogs screen. Press F5 to cause the modem to dial the site for the latest analog data. The modem remains on line monitoring the analog values until F5 is pressed again to hang up the modem. During this function no other alarms can be received via the dial port. Other ports will continue to be monitored. The Page Index Window will indicate if any new alarms are received.
F8	Lock. Lock device. This is used to lock out alarms for maintenance, etc. <b>Note:</b> This function is applicable only to Datalok 10D units. For further information refer to the Datalok 15 Module section.
F10/Esc	Exit

## System Information

The System Information window is enabled by pressing Ctrl F6 while in the Alarm Summary screen. It appears in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window. This window shows a general overview of Monitor mode resources.

Table 17.AC lists the field names and descriptions for the System Information window.

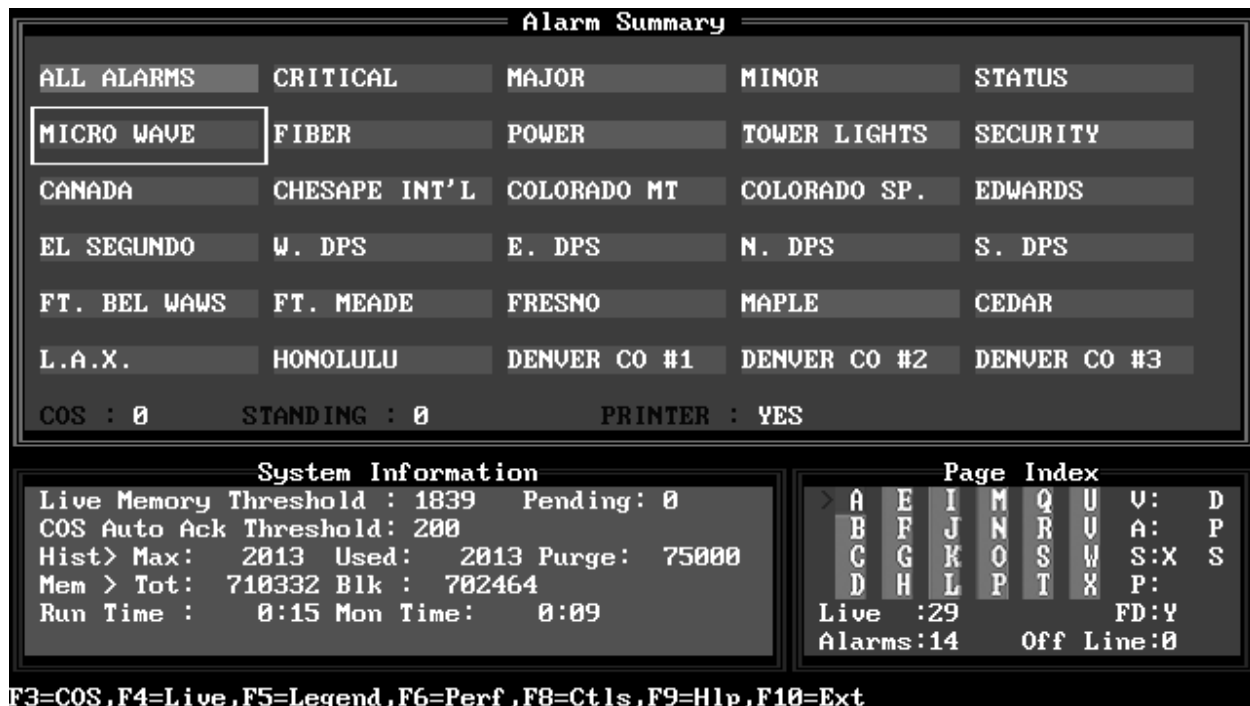


Fig. 17.35 - System information window replaces summary legend window.

Table 17.AC - Fields in the System Information window

Field	Description
Live Memory Threshold	Number of live alarms that can be stored in memory before T/MonXM begins sending data to the hard drive.
Pending	Number of alarms with a qualification time that have not yet qualified.
COS Auto Ack Threshold	Maximum number of COS Alarms that can be active before they are automatically acknowledged is 200.
Hist Max	Total number of records defined in History file.
Used	Total number of records actually being used in History file.
Purge	Maximum number of records that will be kept on the T/MonXM hard drive before they are purged and new records begin writing over the old ones. This setting can be adjusted from the History Auto Purge setting in the Miscellaneous Parameters screen from the Parameters menu.



**Table 17.AC - Fields in the System Information window (continued)**

<b>Field</b>	<b>Description</b>
Mem Tot	Device type.Free system memory.
Blk	Largest contiguous block of free system memory.
Run Time	Time in T/MonXM since starting program.
Mon Time	Elapsed time since entering Monitor mode.

**Table 17.AD - Key commands available in the System Information window**

<b>Function Key</b>	<b>Description</b>
F3	Device type.Free system memory.
F4	Largest contiguous block of free system memory.
F5	Time in T/MonXM since starting program.
F6	Elapsed time since entering Monitor mode.

# Craft Mode

Craft Mode allows communications with another network device

The Craft Mode screen is enabled by pressing Ctrl F7 while in the Alarm Summary screen. It appears as a Craft Mode Dialog window in the upper portion of the screen, in place of the Alarm Summary Window, and as a Craft Interface Mode window in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window.

Craft Mode allows the keyboard and screen to be used for communications via ASCII text with another device in the alarm network. One use of this mode is to obtain data from the craft port of a remote PABX. The Craft Mode Dialog window shows the dialog text being returned from the remote device. The Craft Interface Mode window shows the port in use. This mode can be entered from either the main terminal or from a remote terminal. Highlight the desired port. Press Enter to establish the connection (Figure 17.36).

Craft Mode Interface parameters can be set from the Parameters menu > Remote Ports option — see Section 9 (Remote Ports and Virtual Jobs) for more information.

**Note:** Do not confuse Chat Mode with Craft Mode. While both are ways to communicate text between the T/MonXM and remote devices, Chat Mode is intended for communication between individuals using terminals and Craft Mode is for communication between devices.

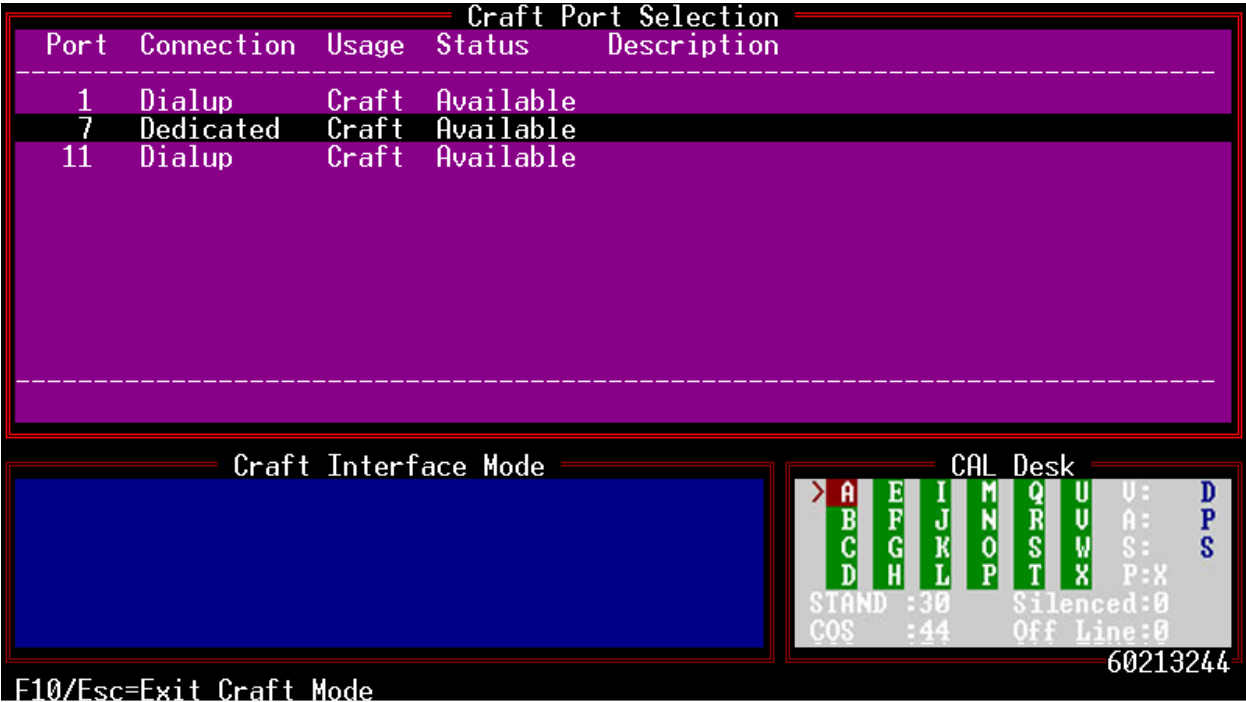


Fig. 17.36 - Craft mode dialog and craft interface mode windows replace alarm summary

Craft mode supports VT100 terminal emulation (default), WYSE 50 terminal emulation or no terminal emulation. VT100 emulation provides a full-screen display. If a half-screen display is preferred (so that the Page Index window is visible) emulation should be turned off. (Press F6, press F1.)

**Note:** Remote Access Terminals will show a half screen display with no terminal emulation.

**Table 17.AE - Key commands available in the Craft Mode screen**

Function Key	Description
F1	RTS on. Turns RTS on (low).
F2	RTS off. Turns RTS off (high).
F5	Half. Goes to half screen display. NOTE: Does not work with VT100 emulation.
F6	Driver. Select emulation. F1 = None,, F2 = VT100,, F3 = Wyse 50,,F10 = Exit.
End	Escape. Sends a break code to devices that make use of it.
F9	How many calls have been made to that site.
F10	Exit.

\*The Esc key will not function as an exit key from this part of T/MonXM. This allows Escape key sequences to be sent to the remote terminal, if required.

Craft is also available for ASCII and TRIP jobs for debug purposes. Also craft job on network port call allows you to telnet to a device.

```

1 - Show Current Port Settings
2 - Change Current Port Settings
3 - Save Current Port Settings
4 - Load Port Settings From NURam
5 - Config Protection Switch
Cmd -> 1

Running in Protection Switch Mode

12 Port Router & Protection Switch - Version 1.1 rev C

Configuration Menu

1 - Show Current Port Settings
2 - Change Current Port Settings
3 - Save Current Port Settings
4 - Load Port Settings From NURam
5 - Config Protection Switch
Cmd ->
[VT100] F1=RTS On, F2=RTS Off, F5=Half, F6=Driver, End=Break, F10=Exit

```

**Fig. 17.37 - A craft mode connection in progress with a DPS 12-port router.**

# Labeled Controls Mode

Labeled Controls operate the controls for a group of devices.

This feature allows users to operate control equipment from within the alarm network by referring to English look up tables that are accessed from within Monitor Mode. Labeled Controls differ from Site Controls, discussed earlier in this section, in that they will always bring up the same template, no matter which window you are positioned in. Labeled Controls give you the ability to issue network-wide controls as opposed to the site or device-based controls issued from the Site Controls screen.

The Labeled Controls screen can be accessed by pressing Ctrl F8 while in the Alarm Summary, COS or Standing Alarms screens. Labeled Controls allow the user to operate the controls for equipment types, usually defined by device, thus the name Labeled Controls.

Before Labeled Controls can be operated they must be predefined. For more information on defining Labeled Controls, see Section 12-6 (Labeled Controls Definition).

T/MonXM provides three methods of operating control points at RTUs: Site Controls, Labeled Controls and Derived Controls. Site Controls, described earlier in this section, are operated through windows, by site or other window category. Labeled Controls, described here, are very similar to site controls, but are operated from a type of control grouping rather than from a site window.

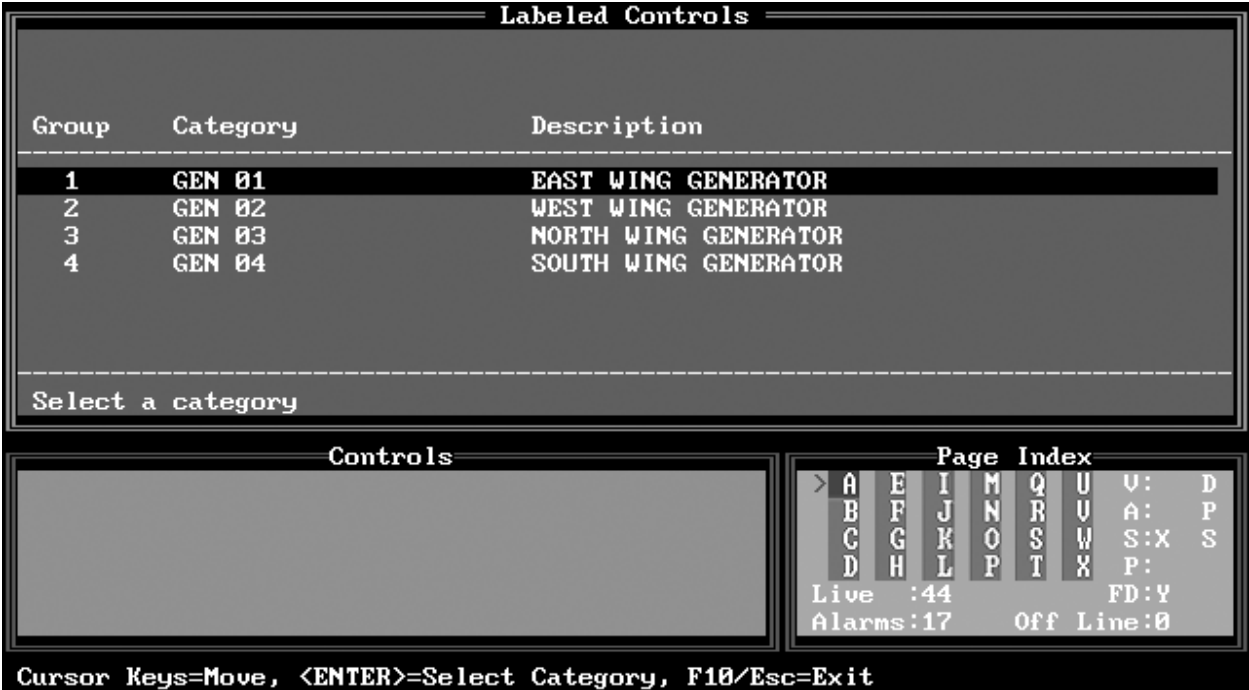


Fig. 17.38 - Labeled controls begins with the category selection screen.

Derived controls are automatically operated by T/MonXM from user-defined formulas that evaluate certain alarm points to determine if an automatic control point operation is appropriate.

Issuing Labeled Controls is a two-step process. You must first select the category. Up to 40 categories of control groups can be defined in the data base, each containing up to 200 control point entries. Each of those entries can contain multiple points or ranges of points to give you great flexibility in issuing controls. To select a category position the highlight bar on the line you want and press Enter. This is part of the first screen you'll see — refer to Figure 17.38. The second screen, Labeled Controls Point Selection allows you to issue the individual controls. Several controls can be grouped into a batch for simultaneous operation. Both individual point operation and batch operation are explained on the following pages.

The following tables list the field names, function keys and descriptions for the Labeled Controls screen.

**Table 17.AF - Fields in the Labeled Controls screen**

Field	Description
Category	The title for the category.
Description	A description for the category.

# Labeled Controls Point Selection

Issue controls from the Labeled Controls Point Selection screen.

After you've selected your category, you can issue the individual or batch controls to the devices. This is done from the Labeled Controls Point Selection screen. The Control Points must also be predefined, just as the Categories must, from the File Maintenance menu.

## Individual Point Operation

From Site Controls Point Selection screen, select the desired control entry based on description and press Enter. A verification window appears asking the you to press "C" to confirm the control command. After you confirm the command, another verification window appears (illustrated below) which shows the total points 'Okay' and the total points 'Failed'. If a control point fails, this window will allow you to either: A (Abort), R (Retry) or C (Continue to the next control point).



Fig. 17.40 - Verification window shows controls sent.

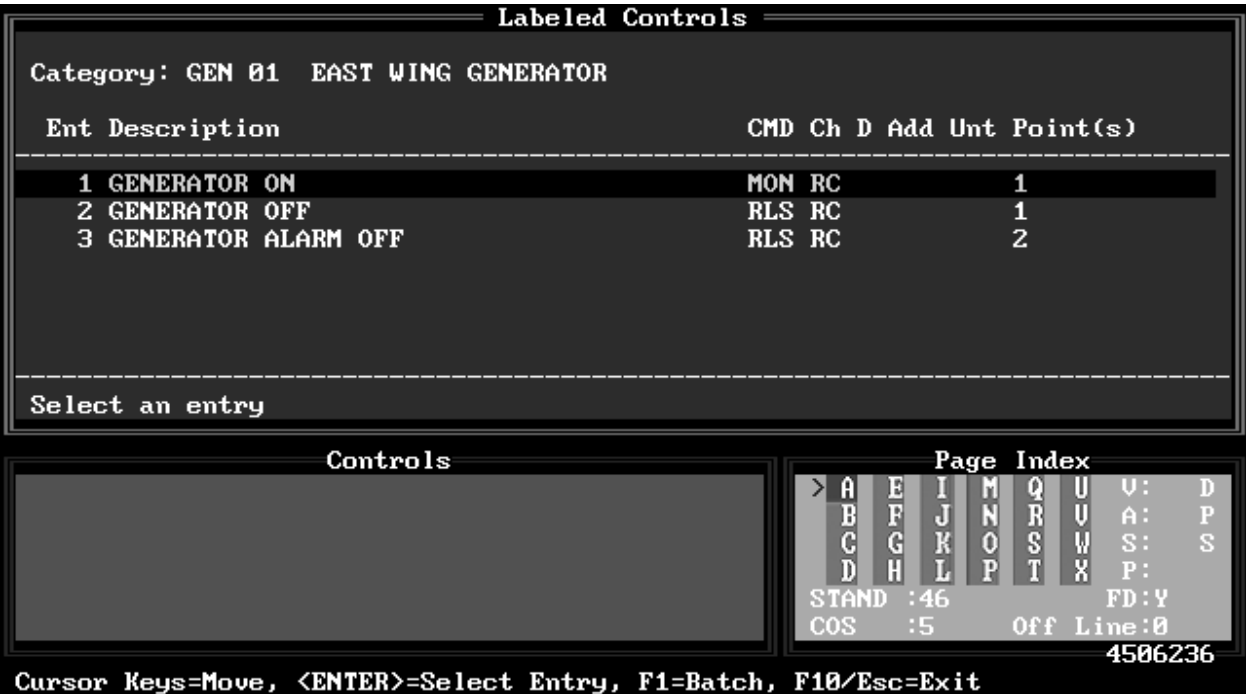


Fig. 17.39 - Control details are provided on the labeled controls point selection screen.

The following tables list the field names, function keys and descriptions for the Labeled Controls Point Selection screen.

**Table 17.AG - Fields in the Labeled Controls Point Selection screen**

Field	Description
Ent	The entry number within the group selected (200 entries per group).
Description	The description of the control points. Up to 40 characters.
*CMD	The command that will be used to activate the control point. OPR = Operate Relay RLS = Release Relay MON = Momentary On MOF = Momentary Off SBO = Select Before Operate SBL = Select Before Release SMO = Select Before Momentarily Operating EXE = Execute Select Before Operate/Release Commands CLR = Clear all Select Before Operate/Release Commands
*Ch	Channel number to issue controls to. RP = Remote Port (Modem port) RC = Relay Card (102 Card) AV = Audio/Visual Card (101 or 108) 1-500 = Port number K1-K2 = KDA Shelf NG, N2 = NetGuardian NW = NetWatchman
*D	Device Type C = CPM S = SBP (Smart Bypass Card)
*Add	The device's address.
*Unt	Unit. This varies depending on the protocol and serves as a data index. Typically a display or group.
*Point(s)	Control point(s) that control will be sent to.

\*These fields are for system administrator troubleshooting and most operators need not be concerned with them. The description field should contain all the necessary information to identify the proper control point.

```

===== Labeled Controls - Batch Mode =====
Category: GEN 01 EAST WING GENERATOR

Ent Description                                CMD Ch D Add Unt Point(s)
-----
  1 GENERATOR ON                               MON RC              1
*  2 GENERATOR OFF                             RLS RC              1
*  3 GENERATOR ALARM OFF                       RLS RC              2

-----
Mark an entry

Controls
[Empty Box]

Page Index
> A E I M Q U V: D
  B F J N R V A: P
  C G K O S W S: S
  D H L P T X P:
STAND :46          FD:Y
COS   :5          Off Line:0
                                4506236

<BATCH>: F1=Mark,F2=All On,F3=All Off,F4=Send,F7=CSend,F10/Esc=Exit Batch

```

Fig. 17.41 - Operate labeled control points in batches from the batch mode screen

**Batch Point Operation**

From the Labeled Controls Point Selection screen press F1 to select the Labeled Controls - Batch Mode screen. The prompt line will display the commands in the table below. Highlight and mark points with F1. Execute control point operation with F4.

**Table 17.AH - Key commands available in the Site Controls - Batch Mode Screen**

Function Key	Description
Up Arrow/Down Arrow	Moves highlight bar up or down through the fields.
F1	Mark. Press to mark highlighted point. An asterisk (*) will appear at the left end of each marked line. Toggles mark on or off.
F2	All On. Marks all points in the category.
F3	All Off. Un-marks all points in the category.
F4	Send. Verification window asks you to press "C" to confirm sending the control command. After command is sent the window will show the results, as in individual point operation.
F7	Confirm Send. Use with Select Before Operate (SBO) points. Verification window will be presented a second time, after the initial operate command is sent.
F10	Exit Batch Mode.



## Pager Status in Monitor Mode

### Lock Function

Pager status mode can be entered by pressing Shift-F3 (Pager Status) from the Monitor Mode Alarm Summary screen. The Pager Status screen is used to assign a pager carrier (initials and phone number) to pager operators. The Pager Statistics window (lower left) displays the amount of pager notifications in the pager queue (Queue Count) and shows the current phone number that is being dialed (Dialing field).

Pager Status					
Opr	On Call	Operator Description	Lock Status	Lock Call	Locked Until
1	DJM	on call and group 1	NOT LOCKED		
2	ERB	ERB Test	NOT LOCKED		
3	TL	Ted's Email	NOT LOCKED		

Pager Statistics		Page Index
Queue Count : 0		> A E I M Q U V : D
Dialing :		B F J N R V A : P
		C G K O S W S : S
		D H L P T X P : X
Jun 13, 2000 17:02:10		STAND : 30 Silenced : 0
		COS : 44 Off Line : 0

F1=Set Lock, F2=Remove Lock, F3=Flush, F4=Send, F6=Override, F10/Esc=Exit

17.42 - Pager status screen

Table 17.AI - Fields in the Pager Status screen

Field	Description
Opr	Operator number. T/MonXM automatically lists all assigned operator schedules.
On Call	Initials of the pager carrier that would normally be called for the associated OPR (operator).
Operator Description	Description from the description field in the Weekly Operator Schedule screen
Lock Status	Indicates operator's current pager carrier status (locked or unlocked).
Lock Call	Initials of the pager carrier that will be called if the operator is locked.
Lock Until	Date and time the lock will expire.

Table 17.AJ - Fields in the Set Lock screen

Field	Description
OPR	Enter the operator number. Valid OPR numbers are 1-99.
PGR	Initials of the pager carrier.
DATE	Enter expiration date. (MM/DD/YY)
HOUR	Enter the lock expiration hour. Valid entries are 0-23.

**Flush Pager Queue**

The queue of pagers to be dialed can be cleared by pressing F3 (Flush Pager Queue) from the Pager Status screen.

**Sending Pager Messages**

To send free form pager messages, press F4 (Send) from the Pager Status screen. A pager carrier list is displayed. To use this screen, highlight the pager carrier that you want. You have the option of pressing Enter to select the highlighted pager carrier or press F1 (Manual) to enter the information manually.

**Note:** In T/MonXM Version 4.5 and later, you can also send messages to pager groups and email addresses.

Pressing Enter selects the highlighted pager carrier and the highlighted pager information is automatically entered in the Pager Message window on the bottom left of the screen.

Pressing F1 (Manual) activates the Pager Message window on the bottom left of the screen. From this screen you can manually enter the Phone, Type, ID/Dly and Data fields.

A N (numeric) entry in the Type field will result in one 7 number data line being sent in a numeric page.

An A (alphanumeric) entry in the Type field will result in a maximum of 27 alphanumeric characters being sent per data line. Up to a maximum of 81 alphanumeric characters can be sent in a alphanumeric page.

## Site Statistics

Site Statistics shows the quality of communication to each site.

Site Statistics also serves as a site selection tool for specific device-related operations

The Site Statistics screen is enabled by pressing Shift-F6 while in the Alarm Summary screen.

For HDLC Stats see Appendix C (Configuring a X.25 Port Card).

The Site Statistics window appears in the upper portion of the screen, in place of the Alarm Summary Window. A Site Statistics window appears in the lower left portion of the Alarm Summary screen, in place of the Summary Legend window. This screen allows you to view general performance statistics for individual sites on the selected port. Site Statistics are on a port basis. The line at the top of the window displays the following information:

Site Statistics	[Port #]	(Protocol)
-----------------	----------	------------

Tables 17.AK and 17.AL list the field names and function key descriptions for the Site Statistics screen.

Site Statistics [ 81(DAT10A)						
Address	Device	Site Name	Polls	Good	Bad	Status
27	STD	KENNEDY ES	1	0	1	ACTIVE
38	STD	BLDG 3/14A	1	0	0	ACTIVE
39	STD	BLDG 3/14B	0	0	0	ACTIVE
40	STD	BLDG 3/14C	0	0	0	ACTIVE
73	STD	GODDARD 1	0	0	0	ACTIVE

Site Statistics

> A E I M Q U V: D

B F J N R V A: P

C G K O S W S: S

D H L P T X P:

Live :46 FD:Y

Alarms:3 Off Line:0

F1=Init Stats,F2=Poll,F3=Config,F4=Online,F5=Offline,F8=Lock,F10/Esc=Exit

**Table 17.AK - Fields for the Site Statistics screen (continued)**

Field	Description
Polls	Site Address Number of times the site has been polled since entering Monitor mode or stats have been reset.
Good	Number of successful polls.
Bad	Number of unsuccessful polls.
Status	Current status of the site. Options are as follows: FAILED: Unable to communicate with device. Device could be malfunctioning or transmission path may be disrupted. ACTIVE: Device is currently transmitting data. ONLINE: Device is currently online. OFFLINE: Device is not currently online.

**Table 17.AL - Key commands available in the Site Statistics screen**

Function Key	Description
F1	Init Stats. Reset stats on screen to 0 settings.
F2	Poll. Instructs T/MonXM to perform a full status poll next time through the polling loop. A full status poll gets all the alarm information from the remote, as opposed to getting only the alarms that have changed status since the last poll. T/MonXM will normally do this type of poll periodically to ensure that alarms are in sync.
F3	Config. Sends configuration to device. This would be useful if you had powered down the device while logged on via T/MonXM and you didn't want to reinitialize T/MonXM. This function is applicable only to Datalok 10As.
F4	Online. Put device online. Alarm data will be transmitted & received.
F5	Offline. Takes device offline. Alarm data will not be transmitted or received by unit. T/MonXM will not poll the device until it is back online.
F6	Analogs. Analog values will be displayed. During this function other alarms can be received via the dedicated port being used for the analog values. Other ports will continue to be monitored. The Page Index Window will indicate if any new alarms are received.
F8	Lock. Lock device. This is used to lock out alarms for maintenance, etc. <b>Note:</b> This function is applicable only to Datalok 10D units. For further information refer to the Datalok 10D Module section.
F9	View help screen.
F10/Esc	Exit
Alt-F1	Show database for the remote that is highlighted.
Alt-F3	Force a dedicated connection to a Teltrac device.
Alt-F4	Force a dialup connection to a Teltrac device.
Alt-F5	View English Analyzer
Alt-F6	View Protocol Analyzer
Alt-F9	View accumulator values of DS5000 device.

Alt+I	Accesses the LNX IP Stack Debug screen.
Ctrl-F3	Force device time synchronization with T/Mon. This will signal T/Mon to set the device's time to match its own. This only applies to devices that support their time settings to be set remotely.
Shift-F1	Flag ALL NetGuardian devices for a firmware download. (Firmware download to flagged devices will begin when user presses Shift-F5.)
Shift-F4	Toggle firmware download flag for the selected NetGuardian device. This will flag or unflag the selected NetGuardian device to receive a firmware download.
Shift-F5	Begin download to flagged NetGuardian units. If the user presses Shift-F5 while a NetGuardian unit is highlighted, T/Mon will immediately begin downloading firmware to the selected unit AND all other units which have been previously flagged for download.
Shift-F9	Unflag ALL NetGuardian devices for a firmware download. This will unflag all NetGuardian devies that are flagged for download.
Shift-F10	Toggle priority polling for the selected device. When flagged, the selected device will be polled multiple times during each poll cycle, greatly increasing its responsiveness, for diagnostic purposes.
-	Minus key. Displays the previous port.
+	Plus key. Displays the next port
1-0	Displays port numbers 1-10.
Shift 1-Shift 0	Displays port numbers 11-20.

## View Analogs

Poll type automatically changes from upset to full update when viewing a dedicated analog value.

Analog values are displayed in native units, e.g., degrees.

To read analog values from a (dedicated line) KDA remote equipped with an Analog Expansion Card or a 400-type analog card, or from a NetGuardian, press shift-F6 while in the main monitor screen. The Site Statistics screen will be displayed. Select the address/ device / site name for the desired remote.

Press F6 to see the View KDA Analogs or View NetGuardian screen. During this function other alarms will be received via the dedicated port being used for the analog values. Other ports will also continue to be monitored. The Page Index Window will indicate if any new alarms are received.

To read analog values from a (dial-up) KDA remote equipped with an Analog Expansion Card or a 400-type analog card, press shift-F4 while in the main monitor screen. The Dialup Site Monitor screen will be displayed. Select the address/ device / site name for the desired remote. Press F6 to see the View KDA Analogs screen. Press F5 to cause the modem to dial the site for the latest analog data.\* The modem remains on line monitoring the analog values until F5 is pressed again to hang up the modem. During this function no other alarms can be received via the dial port. Other ports will continue to be monitored. The Page Index Window will indicate if any new alarms are received. You must press F5 again to cause the modem to hang up.

Points in alarm will display the severity (alarm level) color behind the point value, plus an arrow pointing up for over threshold alarms and an arrow pointing down for under threshold alarms.

\*Does not work for a 400-type analog card.

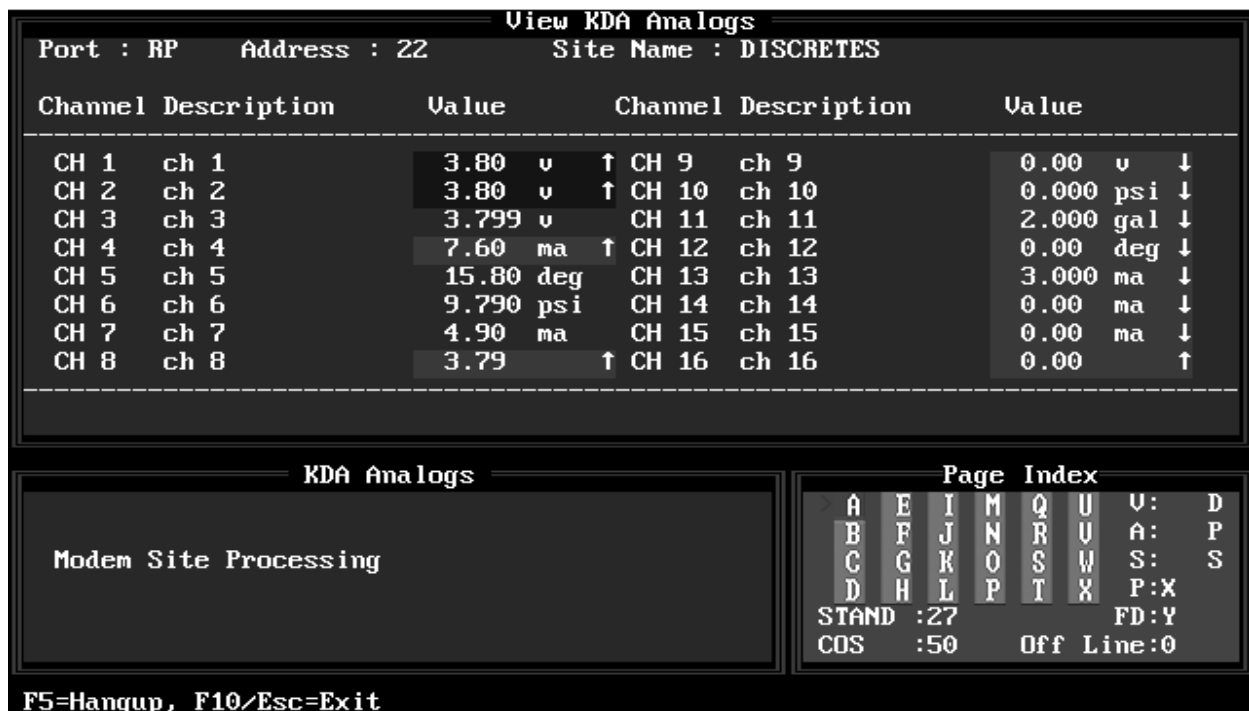


Fig. 17.44 - View KDA analogs screen shows each channel in converted value and units.

## Exit Monitor Mode (Log Off/On)

To exit or log out of Monitor Mode press F10/Esc. The System Query window appears in the bottom left corner. Once you've logged out, the system will either return to the Master menu or continue to monitor for alarms without a user logged on, depending on how you exit. If you press Y, the system will continue to monitor but will log you out (see Figure 17.45). If you press R, the system will log out and return to the Master menu. (The R key will only appear if you have exit monitor privileges in the system user file and you are on the main console.)

NOTE: If you are using Remote Access on a port with auto logon inits defined and no one has logged back in within 60 seconds, your Remote Access user(s) will be logged in automatically with the initials defined for that Remote Access port. The initials used are set via the Auto Logon field in the Remote Access port definition under the Parameters menu. Refer to the Remote Access section (Section 5) for more information on Remote Access Log On/Off.

Table 17.AM explains the key choices available. Differences for remote access are noted in underlined text.

Alarm Summary				
ALL ALARMS	CRITICAL	MAJOR	MINOR	STATUS
POWER	TOWER LIGHTS	FIBER	MICROWAVE	SECURITY
ENVIRONMENTAL	FIRE	DOOR	SNMP ALARMS	T1
BATTERY	STANDBY	GENFAIL	SEISMIC	PRIME FAIL
SECONDARY FAIL	HI TEMP	LO TEMP	A/C FAIL	HEATER FAIL
HISTORY REPORT	HQ REPORTS	NOC REPORTS	OFFLINE	DEVICE FAILURE
COS : 1      STANDING : 1      PRINTER : YES				

System Query	
Log Off? (Y/N/R) : .	
Y=Log off (Monitoring Continues)	
N=Don't log off (Monitoring Continues)	
R=Return to master menu (Monitoring Stops)	

> A	E	I	M	Q	U	V	D
B	F	J	N	R	V	A	P
C	G	K	O	S	W	S	S
D	H	L	P	T	X	P	X
STAND :30				Silenced:0			
COS :44				Off Line:0			
45605164							

F10/Esc=Exit

Fig. 17.45 - System query window replaces summary legend window.

**Table 17.AM - Key commands available in the Exit Monitor Mode**

Field	Description
Y	Log off the user from the system. Monitoring Continues and the Monitor Mode Log on screen will appear or the next user to log on.
N	Abort the log off and return to Monitor mode.
R	Return to Master menu. Monitoring stops and you are returned to the Master menu. This is often used to get to the database editing section. <b>Note:</b> <u>This key will only be visible (and available) if you gave authorization to leave monitor mode. Not available at dial-up or direct connect Remote Access Terminals.</u>
D	Disconnect. <u>Used only at dial-up Remote Access Terminals.</u>

**Fig. 17.46 - The monitor mode log on screen.**



**This page intentionally left blank.**

# Section 18 - Web Browser Interface

---

## Features Overview

The HTTPS Software Module enables secure encryption of all your traffic over IP — ensuring extra security of web connections to your T/Mon will be secure.

**Note:** The HTTPS Software Module does not come standard with T/Mon. Contact DPS Telecom (1-800-622-3314) for more information.

- View/Manage alarms via LAN using Internet Explorer™ or Netscape Navigator™.
- Permits Alarm Management from Windows and non-Windows environment
- COS Alarms
- Standing Alarms
- Tag Alarms
- Silence Alarms and Windows
- Issue Controls
- Acknowledge Individual Alarms or All Alarms
- View Text Messages
- View, Add and Close Trouble Logs
- Alarm Index and Alarm Summary can be set up to automatically refresh. (Can have up to 18 concurrent sessions. [Dependent on remote access options that you have installed.]).

### Browser Compatibility

The software has been tested with Internet Explorer 5.5, Internet Explorer 6, and Netscape Navigator 4.

---

## Set Up Procedure Overview

**Note:** It is highly recommended that you use port 443 for HTTPS TCP type connections — see Figure 18.4.

There are three main things that need to be setup.

1. If necessary, increase the number of TCP connections available to the system. The HTTP server requires multiple connections to function properly. For instructions on increasing the number of TCP connections, see section 3-1, “Ethernet I/O.”
2. Set up an HTTP server. This is done by setting up a TCP-type connection for port 80 (port 80 is the standard HTTP port) or port 443 (port 443 is the standard HTTPS port) then assigning this connection to an HTTP Server job.
3. Set up remote access jobs with a HTTP port usage. When a user logs in via web browser, the session is automatically assigned to an unused HTTP remote access job.

**Note:** You can enable both HTTP and HTTPS connections (Dual Mode) on your network, but you will need to set your router to block port 80. This will ensure that no one outside of your network will be able to access data that is not encrypted.

## TCP and UDP Procedure Detail

**Note:** Perform this procedure only if necessary. You probably already have as many TCP and UDP ports as you need.

You probably will not need to change your port settings. T/Mon ships with a default setting of 40 TCP ports and 9 UDP ports. This should be sufficient for most users.

The sum of UDP and TCP connections can be no more than 49. Use the following steps to change your port settings.

1. From the W/Shell menu select Network Setup and then Run Network Setup.
2. Select Edit Settings and increase the number of TCP connections. The default setting is 40 TCP ports, which is probably sufficient. If necessary, you can add 5 more. Make a note of the network address setting. Press Enter through the rest of the fields on this page. By following the prompts you will eventually be asked to reboot.

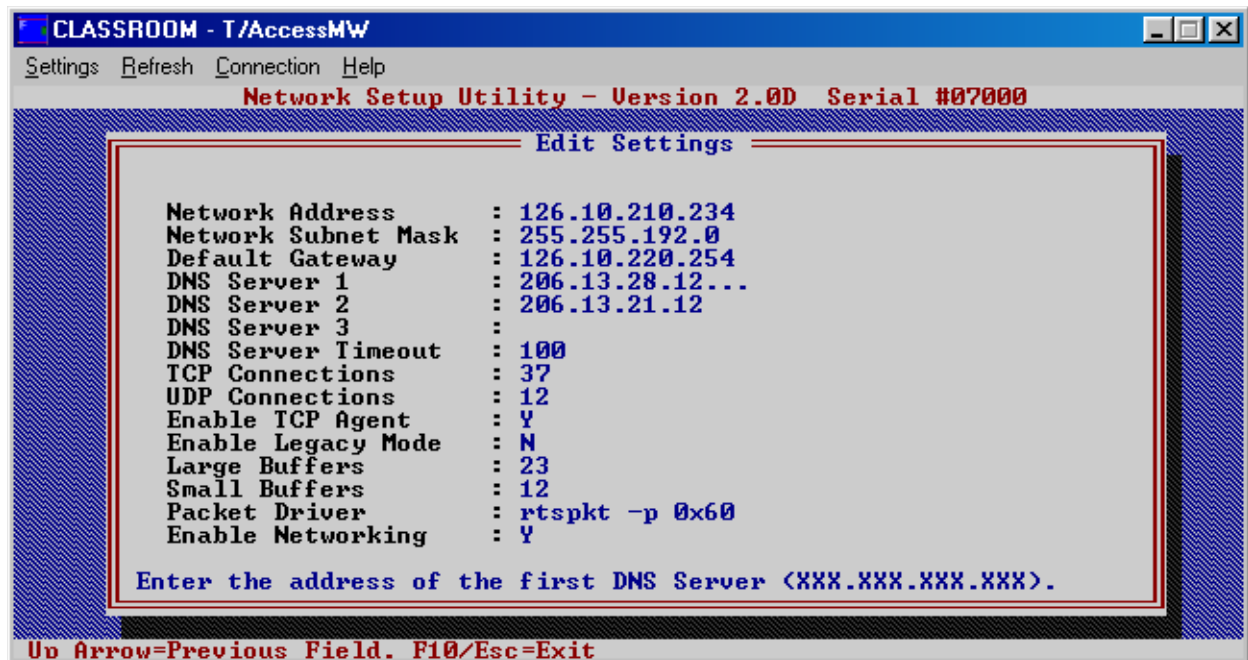


Fig 18.1 - If necessary, raise the number of TCP connections in Network Setup

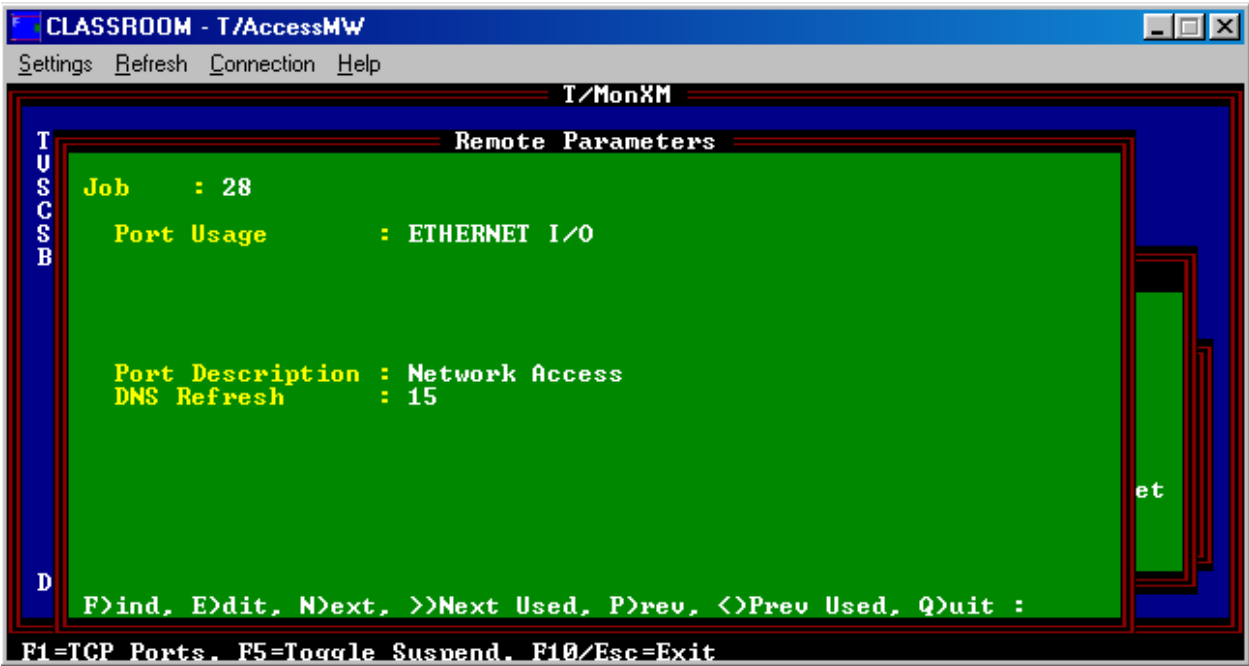


Fig 18.2 - The remote port job 28 (Ethernet I/O port).

4. After rebooting, start T/MonXM.
5. Go to Parameters > Remote Ports. Press F (Find) and enter 28 for Port Job 28. This Job should already have Port Usage set to “Ethernet I/O” — see Figure 18.2.
6. Press F1 to bring up the Ethernet TCP Port Definition screen — see Figure 18.3. Press the Tab key to select type TCP. Press Enter, and set the TCP port to 80, or 443 for HTTPS (see Figure 18.4). Press F8 to save.

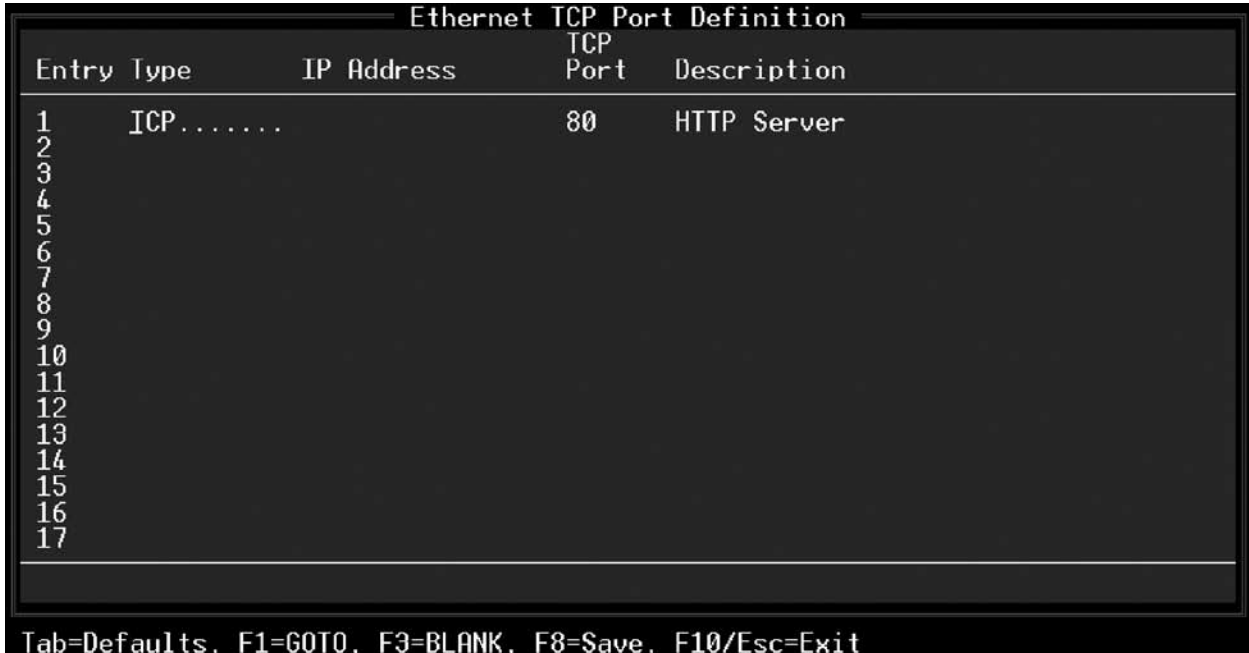


Fig. 18.3 - Press F1 from the Remote Parameters screen to go to the TCP Port Definition screen.

Ethernet TCP Port Definition			
Entry	Type	IP Address	TCP Port Description
1	TCP		443 HTTPS Server.....
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			

Enter a description for this port.

Up Arrow=Previous Field. F10/Esc=First Field

Fig. 18.4 - Use TCP Port 443 for HTTPS.

You must set up a separate Remote Access job for every simultaneous web viewing session you want to use.

**Note:** You can enable both HTTP and HTTPS connections (Dual Mode) on your network, but you will need to set your router to block port 80. This will ensure that no one outside of your network will be able to access data that is not encrypted.

7. Navigate to an open job — press N for next until you find an open port job.
8. Press “E” for Edit. In the port usage field, press the Tab key and select “HTTP Server”. Set Max Connections to 9 or the number of simultaneous web browser sessions you wish to allow. The number can be expanded to 18. See Figure 18.5 for examples of HTTP Server remote parameters and Figure 18.6 for HTTPS Server remote parameters.
9. Press F6 to assign the data connection that you created to this job — TCP 80 for HTTP Server and TCP 443 for HTTPS Server.
10. Now you will need to set up a remote access job for every simultaneous web viewing session you want to set up. Remote Access jobs can be set up on job numbers in the range of 30 to 47. The Terminal Type for the remote access job should be set to “HTTP”. When a user logs in via web browser, the session is automatically assigned to an unused remote access job that has its terminal type set to HTTP. The number of remote access jobs you set up is the number of simultaneous sessions you want to allow. (Because Remote Access jobs can only be assigned to jobs 30 to 47, the maximum number of simultaneous web browser sessions is 18.)
11. Now you can Initialize, go to Monitor Mode and attempt to connect using your browser.



Fig. 18.5 - Set up the job's Port Usage as "HTTP Server".

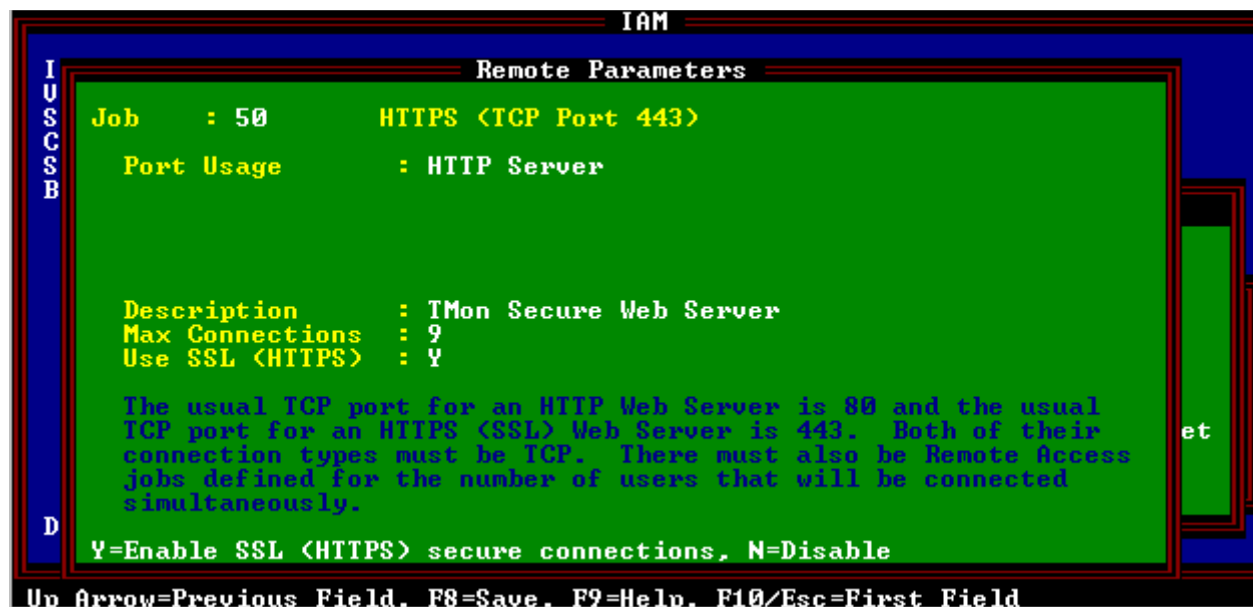


Fig. 18.6 - Remote port job settings for HTTPS.

## Connecting via Web Browser

To connect using your web browser, use the IP address of your T/Mon as the address of the page that you want to open. If you are using a HTTPS connection, enter “HTTPS://” before your IP address.

If you are using a secure HTTPS connection, Security Alert prompts will appear — press OK then Yes to continue. You may choose to view the authenticity certificate as well. The password screen prompt will appear. Enter your initials/username and password.



Fig. 18.7 - Internet Explorer Security Alert prompt.

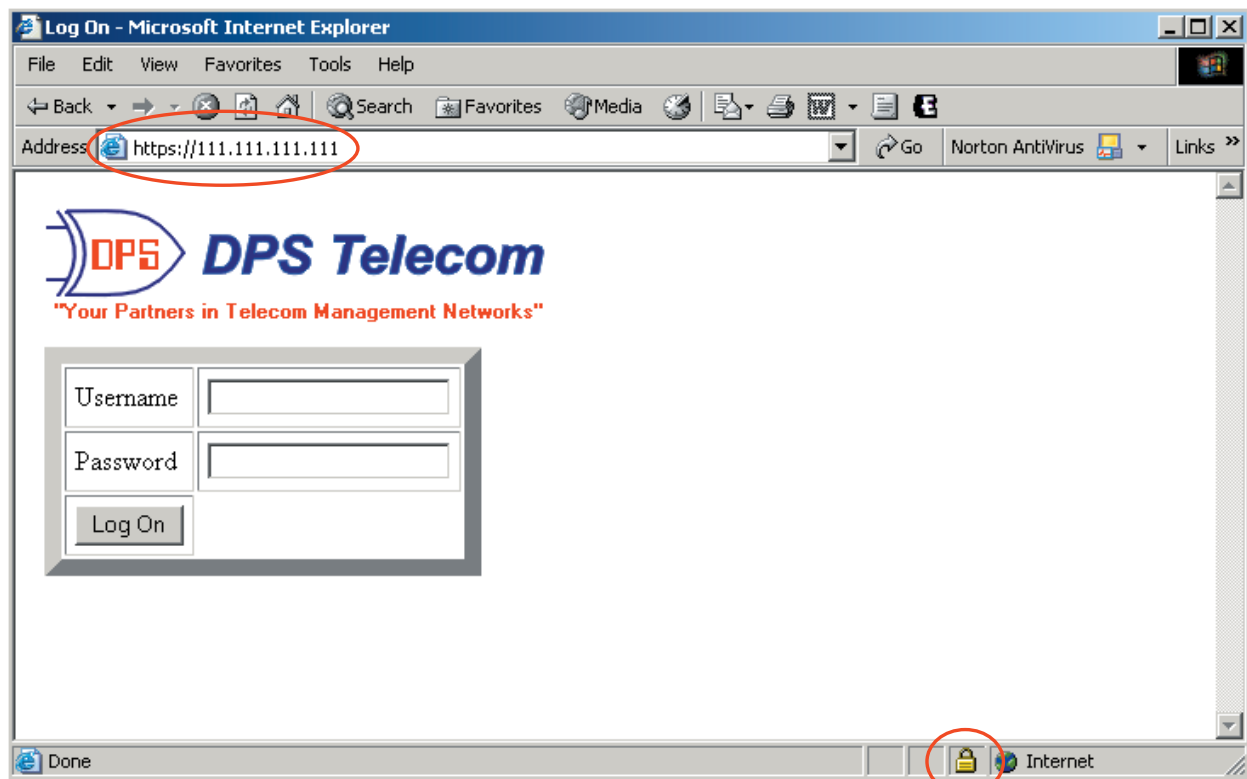


Fig. 18.8 - Enter “https” for HTTPS connection. The lock icon indicates encrypted connections for secure Web monitoring of your T/Mon.

## Using the Web Browser Interface

The Web Browser interface uses displays and conventions similar to those used in Monitor Mode. Refer to Section 16, Monitor Mode Tutorial, for additional information.

### Alarm Summary

The web browser interface is broken up into three frames. The frame at the top allows switching between the various menus. The frame to the left contains the page index and a refresh and legend link. The Page index provides a quick summary of system status. Each page number in the page index window can be clicked on to view the windows for that page. The refresh link will refresh the display when clicked. The Legend link will display the meanings of the colors of windows and alarms.

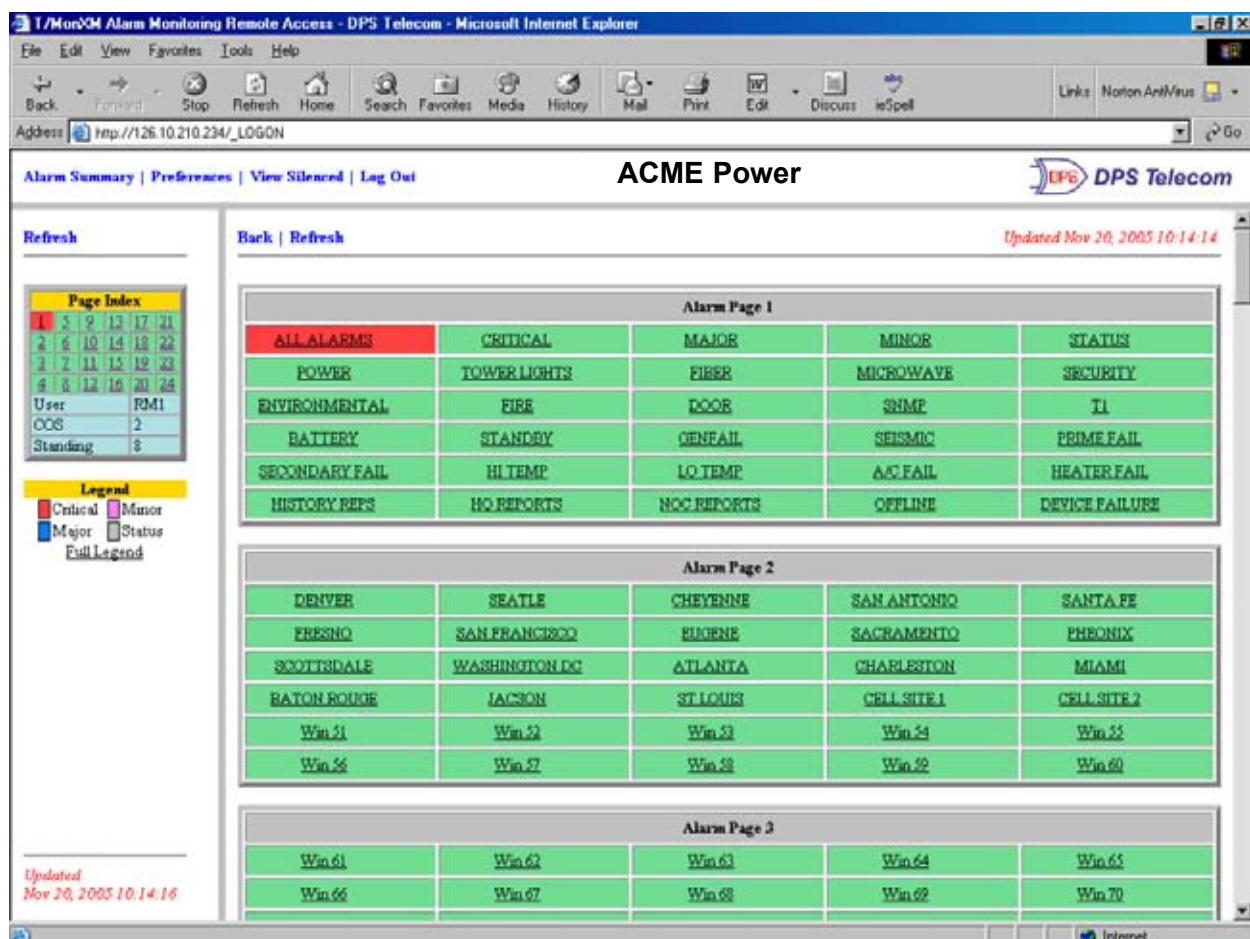


Fig. 18.9 - Web browser alarm summary window.\*

**Note:** Windows in the web browser interface behave just like windows in T/MonXM, i.e. blinking = COS, color = severity, etc.

\*This is not an HTTPS connection example. A secure HTTPS connection is indicated by the lock icon in the Web Browser's Status bar — see Figure 18.8.



Alarm Summary | Preferences | View Silenced | Log Out

ACME Power

DPS Telecom

Refresh

View Standing | Ack All | Controls | Silence This Window | Back | Refresh

Updated Nov 20, 2005 10:33:50

Page Index

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

User: RM1

COS: 5

Standing: 2

Legend

- Critical
- Minor
- Major
- Status
- Full Legend

Updated Nov 20, 2005 10:27:49

Date-3	Time-1	Level	Alarm Status	Site Name	Description	Alarm ID-3	Command
Nov 20, 2005	10:27:39	C	C	Site 1	Disp 1 Pnt 1	2111	Ack
Nov 20, 2005	10:28:05	C	A	Site 1	Disp 1 Pnt 1	2111	Ack
Nov 20, 2005	10:28:34	C	A	Site 1	Disp 1 Pnt 2	2112	Ack
Nov 20, 2005	10:28:25	C	A	Site 1	Disp 1 Pnt 3	2113	Ack

Fig. 18.10 - Switch between COS alarm and standing alarm views by clicking on the View Standing or View COS link.

### Note to existing users:

The Web browser interface is not intended for heavy, daily use, but rather for quick access after a page, etc. The web browser is not optimized for speed the way other remote access is. Network latency and bandwidth used by the web browser is much higher and will produce slower performance.

The frame to the right is the main display area. You can click on any window to view the alarms in that window. From there you can alternate between standing and COS alarms.

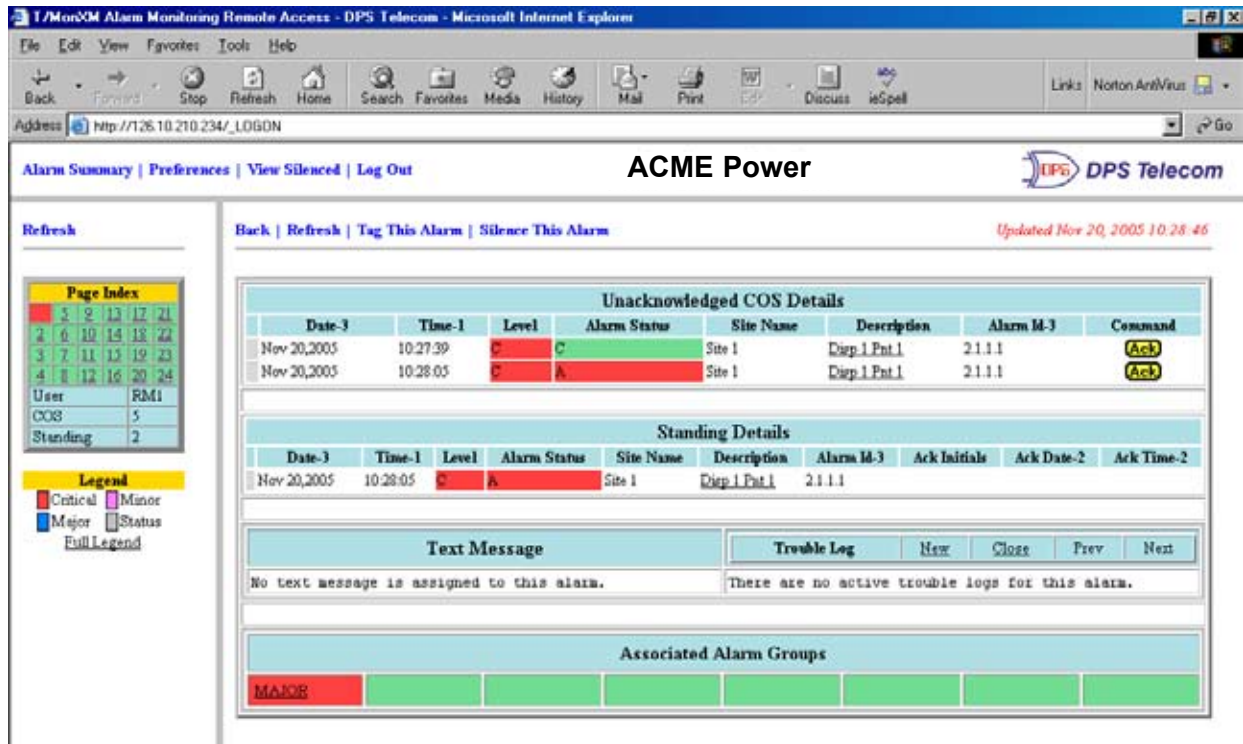


Fig. 18.11 - View alarm details by clicking on a COS or Standing alarm.

The latest versions of T/MonXM supports auto refresh of Alarm Summary, COS, and Standing Alarm screens.

## Silence Alarms/Windows

Click on the individual alarms to view the unacknowledged COS details, standing details, and other details for that alarm point. The text message and a trouble log, if any, are displayed here as well. The window groups associated with that alarm point are listed at the bottom of the window.

Silencing allows selected alarms to be suspended for a specified period of time. When an alarm is silenced, it does not generate any COS entries and it does not appear in the standing alarm list. Each system account must have the Tag/Silence alarm field set to yes to enable the Silence Alarm Window Function

There are two ways to silence alarms: An individual alarm may be silenced or a window may be silenced. When a window is silenced, all alarms in that window are silenced.

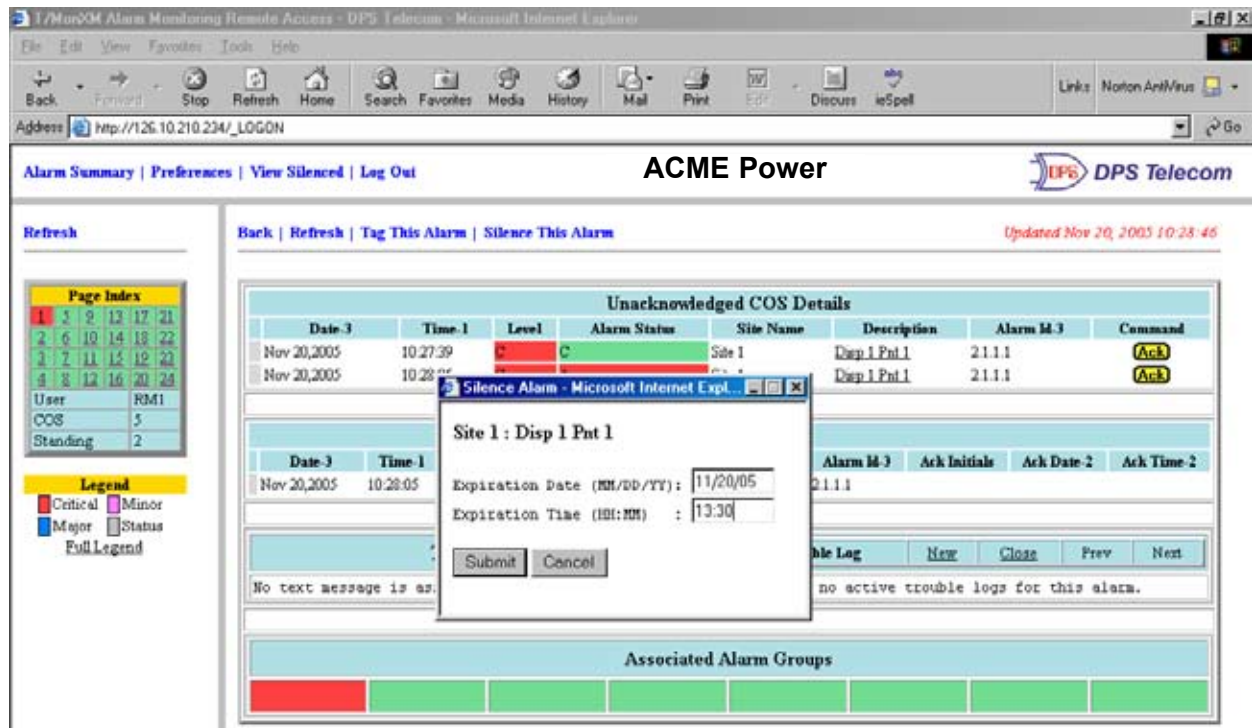


Fig. 18.12 - When silencing an alarm you will be prompted for an expiration date and time

Single alarms can be silenced for a limited time.

To silence an individual alarm, click it in the COS or standing window. When viewing alarm details you click the Silence This Alarm link. You will then be prompted for the date and time that the silenced condition will expire.

Entire windows can be silenced for a limited time.

To silence a window, select it on the Alarm Summary screen and click the Silence This Window link. You will then be prompted for the date and time that the silenced condition will expire (similar to Figure 18.12).

To view the list of items (alarms and windows) that have been silenced, click the View Silenced link on the top frame of the window. You can manually un-silence an item by clicking the Unsilence button when viewing all silenced alarms and windows.

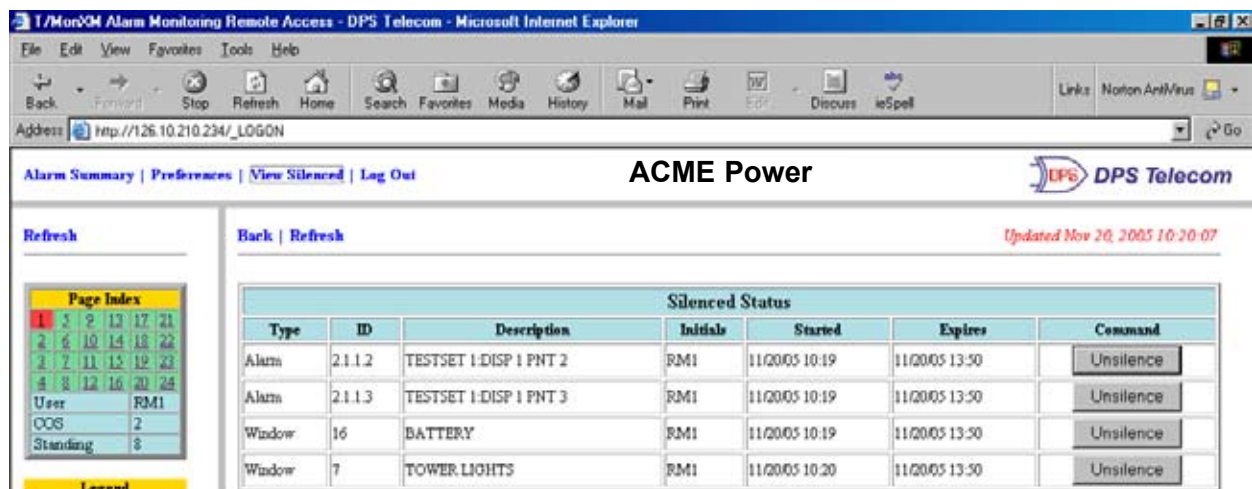


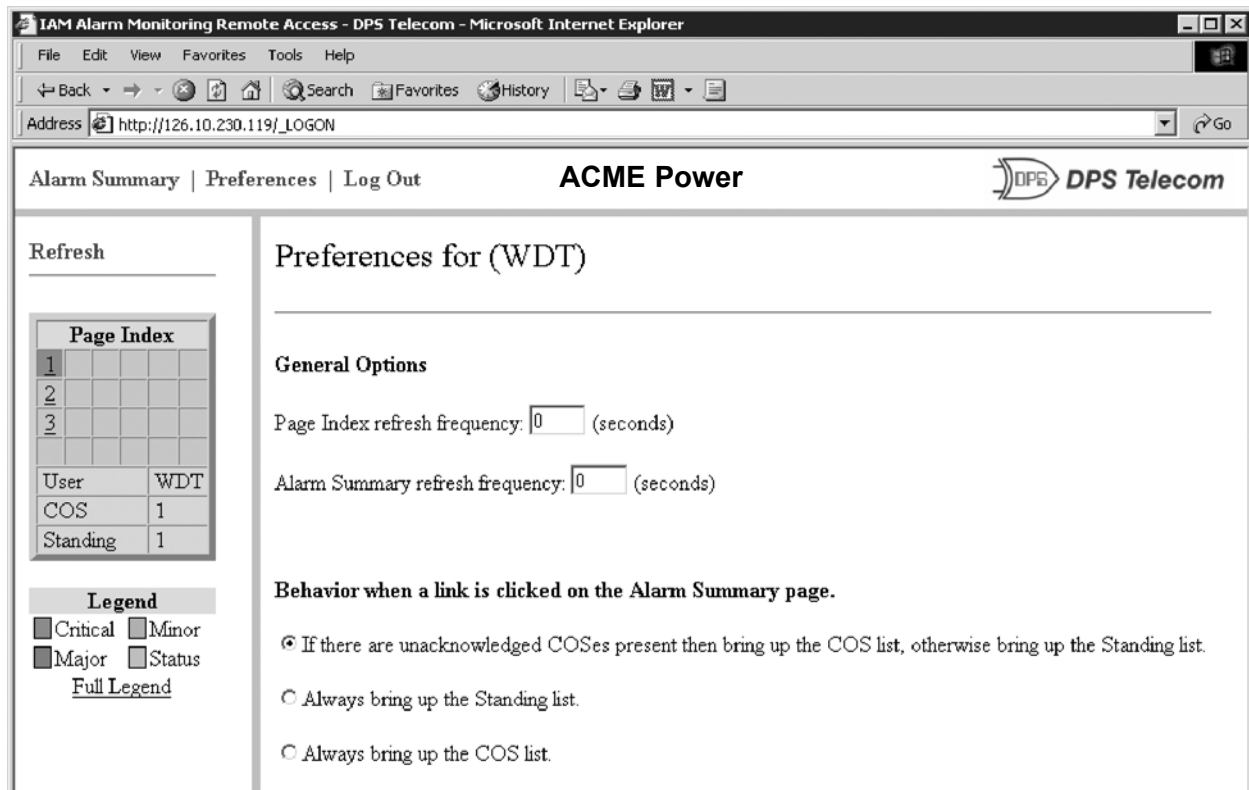
Fig. 18.13 - View all silenced items by clicking the View Silenced link

## TAG Alarms

Tagging and silencing are different ways of doing the same thing. Most users prefer silencing because it expires on a user definable date/time.

## Preferences

Set the web browser interface preferences as needed. The preferences are saved under the initials of the logged in person and are specific for each user so if you log in from a different computer, your preferences will still be displayed.



**Fig. 18.14 - Set the web browser interface preferences at this window.**

Preference screen is unique to web browser.

The **page index refresh frequency** preference determines how often, in seconds, to refresh the page index frame. Setting it to zero disables automatic refresh. You must manually update the screen by clicking on the Refresh link in the page index frame.

The **Alarm Summary refresh frequency** preference how often, in seconds, to refresh the Alarm Summary frame. Setting it to zero disables automatic refresh.

**Note:** COS and Standing Alarm screens will automatically refresh according to this setting.

The **Alarm Summary page control** is the preferences window determine the window that will be brought up when a link is clicked in the Alarm Summary page.

**This page intentionally left blank.**

## Using the Web Browser Interface

The Web Browser interface uses displays and conventions similar to those used in Monitor Mode. Refer to Section 16, Monitor Mode Tutorial, for additional information.

### Alarm Summary

The web browser interface is broken up into three frames. The frame at the top allows switching between the various menus. The frame to the left contains the page index and a refresh and legend link. The Page index provides a quick summary of system status. Each page number in the page index window can be clicked on to view the windows for that page. The refresh link will refresh the display when clicked. The Legend link will display the meanings of the colors of windows and alarms.

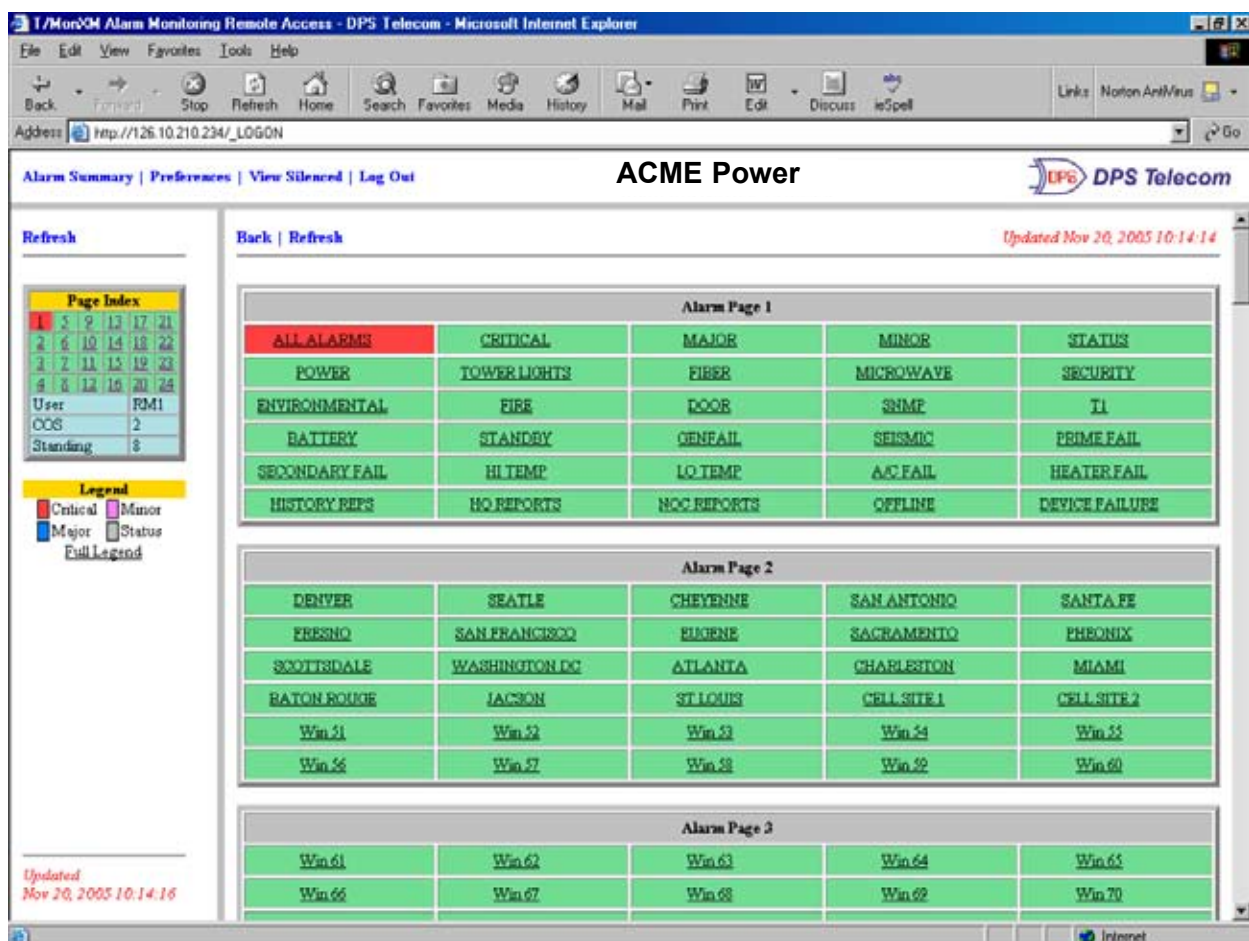


Fig. 18.9 - Web browser alarm summary window.\*

**Note:** Windows in the web browser interface behave just like windows in T/MonXM, i.e. blinking = COS, color = severity, etc.

\*This is not an HTTPS connection example. A secure HTTPS connection is indicated by the lock icon in the Web Browser's Status bar — see Figure 18.8.



Page Index

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----

User: RM1  
COS: 5  
Standing: 2

Legend

Critical	Minor
Major	Status

Full Legend

Updated Nov 20, 2005 10:27:49

Date-3	Time-1	Level	Alarm Status	Site Name	Description	Alarm ID-3	Command
Nov 20, 2005	10:27:39	C	C	Site 1	Disp 1 Pnt 1	2111	Ack
Nov 20, 2005	10:28:05	C	A	Site 1	Disp 1 Pnt 1	2111	Ack
Nov 20, 2005	10:28:34	C	A	Site 1	Disp 1 Pnt 2	2112	Ack
Nov 20, 2005	10:28:25	C	A	Site 1	Disp 1 Pnt 3	2113	Ack

**Fig. 18.10 - Switch between COS alarm and standing alarm views by clicking on the View Standing or View COS link.**

### Note to existing users:

The Web browser interface is not intended for heavy, daily use, but rather for quick access after a page, etc. The web browser is not optimized for speed the way other remote access is. Network latency and bandwidth used by the web browser is much higher and will produce slower performance.

The frame to the right is the main display area. You can click on any window to view the alarms in that window. From there you can alternate between standing and COS alarms.

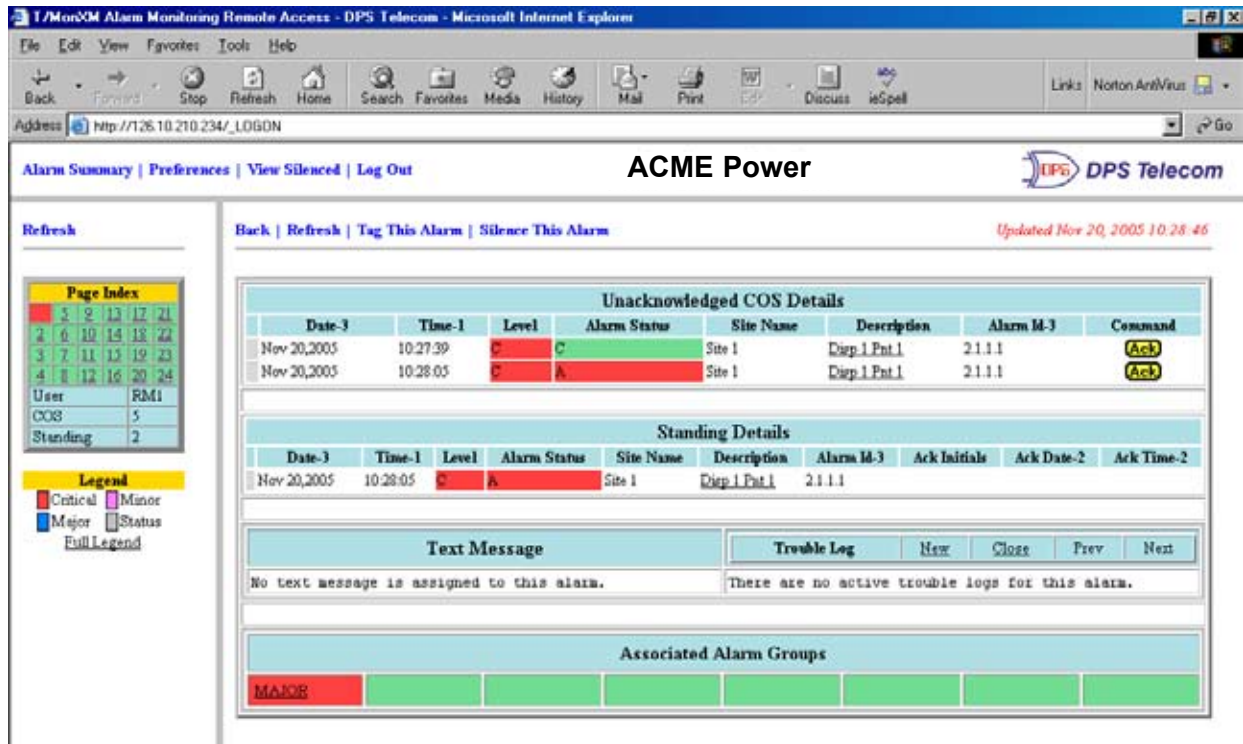


Fig. 18.11 - View alarm details by clicking on a COS or Standing alarm.

The latest versions of T/MonXM supports auto refresh of Alarm Summary, COS, and Standing Alarm screens.

## Silence Alarms/Windows

Click on the individual alarms to view the unacknowledged COS details, standing details, and other details for that alarm point. The text message and a trouble log, if any, are displayed here as well. The window groups associated with that alarm point are listed at the bottom of the window.

Silencing allows selected alarms to be suspended for a specified period of time. When an alarm is silenced, it does not generate any COS entries and it does not appear in the standing alarm list. Each system account must have the Tag/Silence alarm field set to yes to enable the Silence Alarm Window Function

There are two ways to silence alarms: An individual alarm may be silenced or a window may be silenced. When a window is silenced, all alarms in that window are silenced.



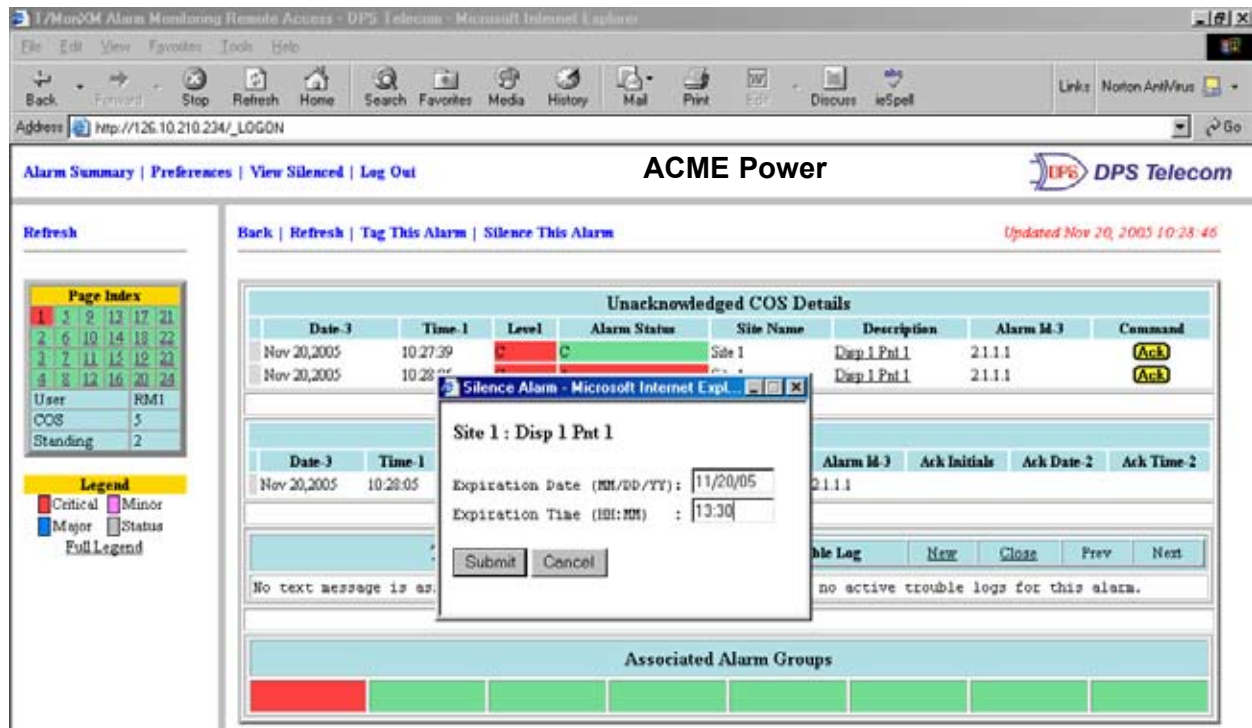


Fig. 18.12 - When silencing an alarm you will be prompted for an expiration date and time

Single alarms can be silenced for a limited time.

To silence an individual alarm, click it in the COS or standing window. When viewing alarm details you click the Silence This Alarm link. You will then be prompted for the date and time that the silenced condition will expire.

Entire windows can be silenced for a limited time.

To silence a window, select it on the Alarm Summary screen and click the Silence This Window link. You will then be prompted for the date and time that the silenced condition will expire (similar to Figure 18.12).

To view the list of items (alarms and windows) that have been silenced, click the View Silenced link on the top frame of the window. You can manually un-silence an item by clicking the Unsilence button when viewing all silenced alarms and windows.

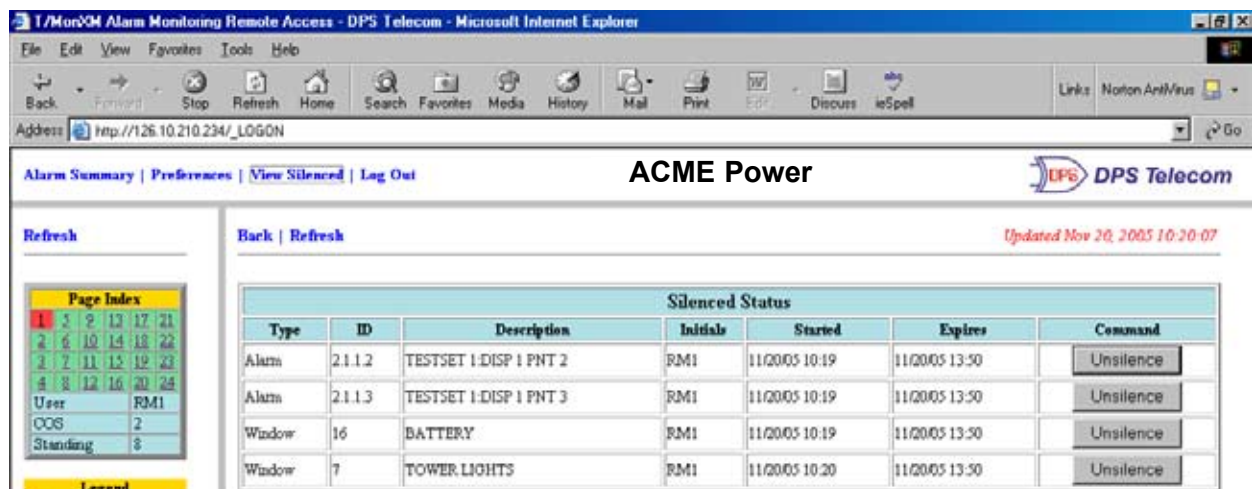


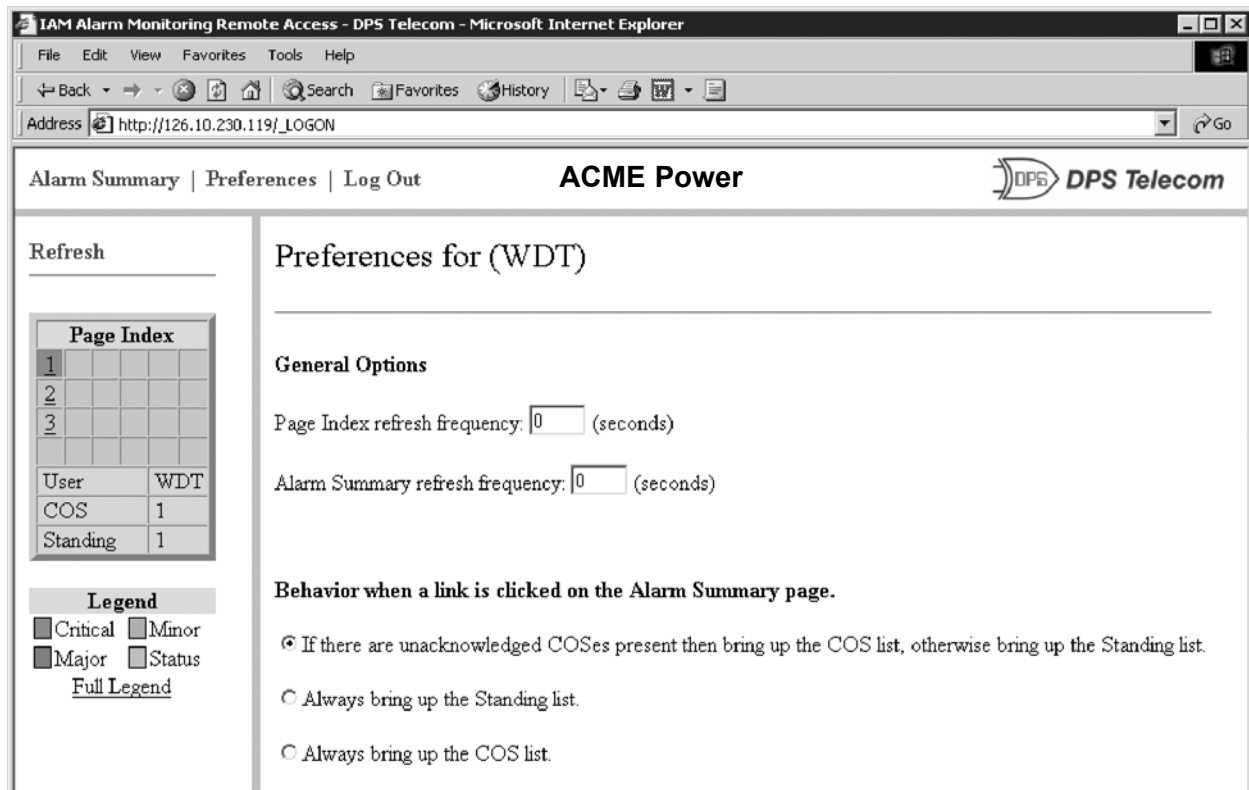
Fig. 18.13 - View all silenced items by clicking the View Silenced link

## TAG Alarms

Tagging and silencing are different ways of doing the same thing. Most users prefer silencing because it expires on a user definable date/time.

## Preferences

Set the web browser interface preferences as needed. The preferences are saved under the initials of the logged in person and are specific for each user so if you log in from a different computer, your preferences will still be displayed.



**Fig. 18.14 - Set the web browser interface preferences at this window.**

Preference screen is unique to web browser.

The **page index refresh frequency** preference determines how often, in seconds, to refresh the page index frame. Setting it to zero disables automatic refresh. You must manually update the screen by clicking on the Refresh link in the page index frame.

The **Alarm Summary refresh frequency** preference how often, in seconds, to refresh the Alarm Summary frame. Setting it to zero disables automatic refresh.

**Note:** COS and Standing Alarm screens will automatically refresh according to this setting.

The **Alarm Summary page control** is the preferences window determine the window that will be brought up when a link is clicked in the Alarm Summary page.

# Section 19 - Managing System Files

## Utilities Menu

Database should be backed up at the end of any day in which changes have been made.

In primary/secondary systems in which databasing is done on the secondary system, database backup should be done on the secondary system.

The Utilities Menu consists of disk operations for backing up, restoring, and other operations on system files. The Utilities Menu and its selections are shown in Figure 19.1.

### Back Up Data Files

Configuration files or History files can be copied or backed up.

This option will copy T/MonXM data files to diskettes. Diskettes must be preformatted and sequentially numbered. Files created on another computer using XEdit software can also be loaded under this option.

Each backup set can have a 30-character description for reference.

Upon entering the Back Up Data Files screen a reminder will show the dates of the last configuration and history archive.

**NOTE:** System configurations are not only very valuable because of the time it takes to create them, the system cannot be fully operational without them. We cannot over-emphasize the importance of having current data backups. Regular rotational backup procedures should be part of system operation. DPS recommends a MINIMUM of 4 sets of configuration backups, one of which should be located off site. If you don't want to re-enter the data you entered, BACK IT UP. Generally, backing up at the end of a day when changes were made is a good idea.



Fig. 19.1 - The File Utility menu.

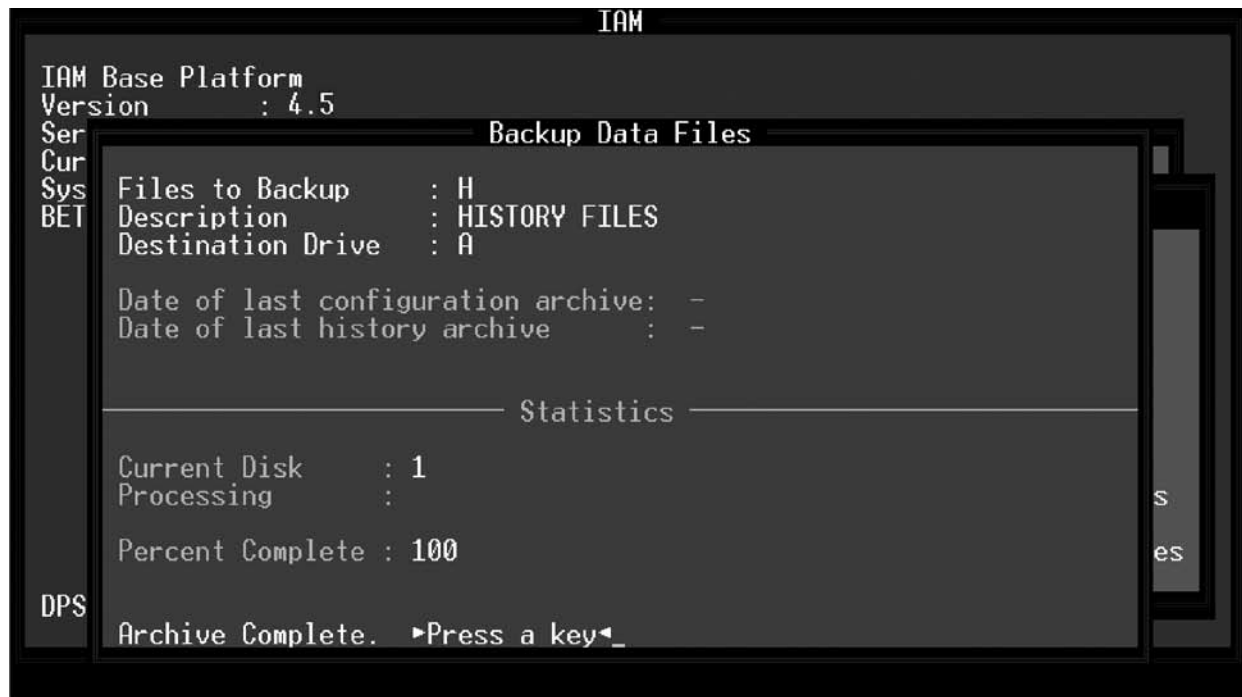


Fig. 19.2 - The data files archive screen is used to back up the data files.

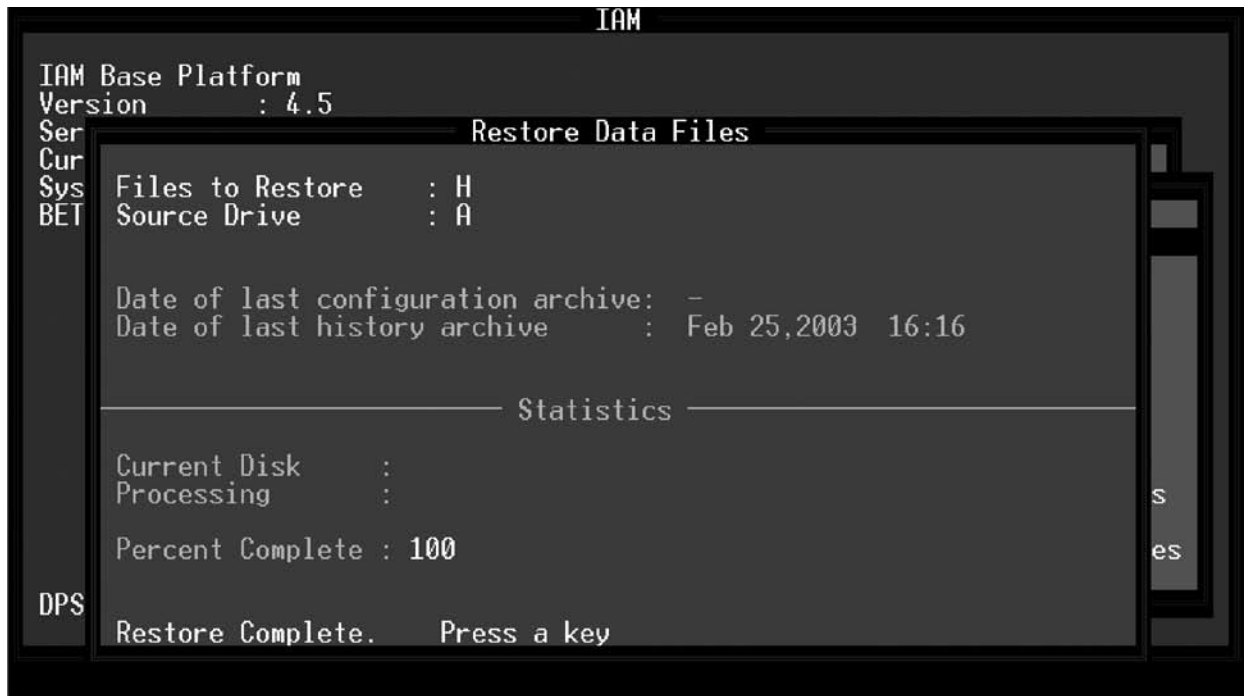
Table 19.A - Fields in the Data Files Archive screen

Field	Description
Files to Archive	Enter C to archive Configuration files or H to archive History file. (Configuration files include windows, ports, points, controls, etc.)
Description	Enter a description for the backup. Up to 30 characters are allowed. Time and date are automatically <ENTER>ed when backup is started.
Drive to Archive to	Set this option to the physical drive where the backed up files are to be stored (A-Z). <b>IAM and T/Mon users:</b> This is the drive on the IAM or T/Mon, not the PC you are running T/AccessM for Windows™ <b>All users:</b> If backup to a floppy ALWAYS remove floppy after backup is complete to ensure proper operation of Automatic Recovery function.

Changes to Backup Data Files in Version 4.2 and later:

- Configuration and History backups can share the same disk.
- Database Backup can now use drives other than A and B.
- Indexes can now be backed up, speeding restorations after file transfers via FTP. Whenever you back up configuration files, T/MonXM will ask if you want to backup indexes as well.

**Note:** DPS Telecom recommends that you back up indexes only if you are backing up via FTP. If you are backing up on floppy disks, rebuilding your indexes will be quicker than restoring them. If you have a large database it is recommended that you back up the database using index files and Auto-ASCII.



**Fig. 19.3 - The data files restore screen.**

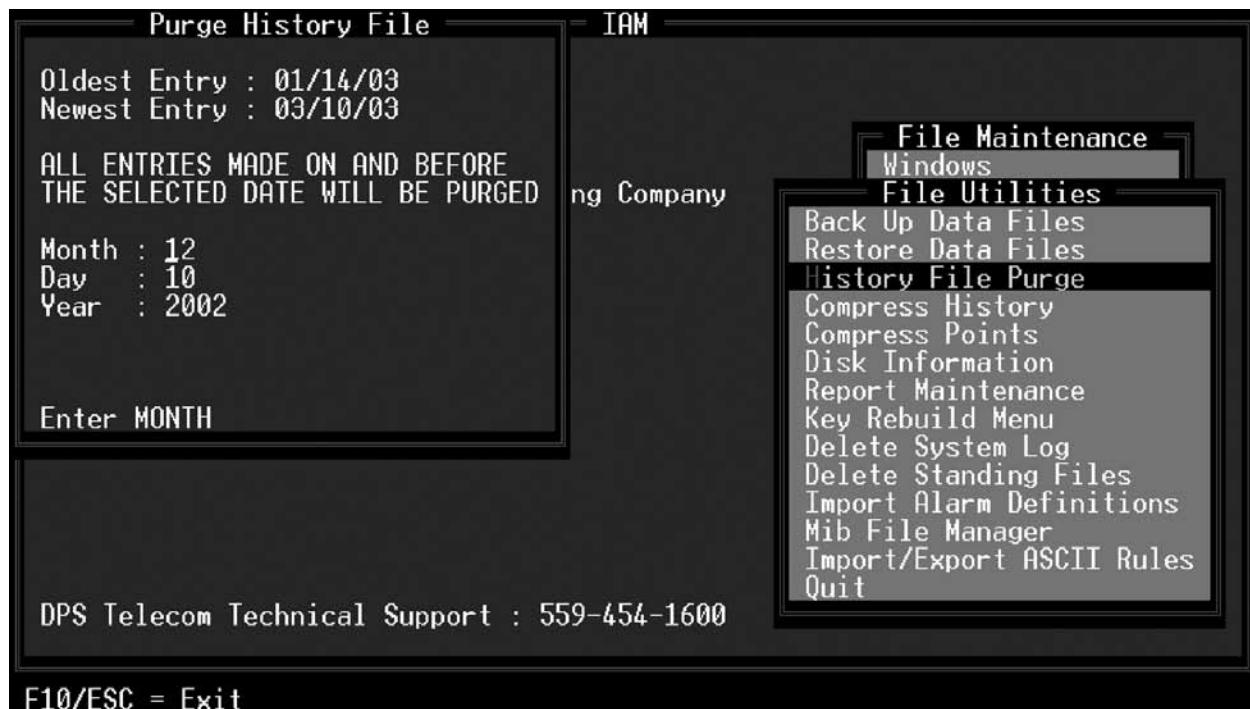
#### Restore Data Files

This option will restore the Configuration or History files that were previously backed up by the above Back Up Data Files option. Files created on another computer using XEdit software can also be loaded under this option. When executing this option, T/MonXM will first alert the user that the restore will overwrite the current system files. To restore data files, follow these steps:

- From the File Utilities menu, choose Restore Data Files.
- The Restore Data Files screen will open. You will be prompted to select the data file to restore. Choose C)onfiguration or H)istory and press Enter.
- You will be prompted to select a drive to restore from. Type the drive letter and press Enter.
- T/MonXM will test the drive and prompt you to enter the first disk of the backup series. Insert the disk and press Enter.
- T/MonXM will display the backup description and prompt you to confirm the restoration. Answer Y to begin the restore process or N to abort the restore process.

If the backup disk is correct and you answered yes to the restore prompt, the program will flash the files being read at the processing field and prompt if you need to insert the next disk of the backups-eries.

**Note:** Restoring data files will erase the current data files that are present on T/MonXM.  
T/MonXM will re-index data files if needed.



**Fig. 19.4 - The purge history file screen.**

History File Purge is not required for preventive maintenance. Older History file entries are automatically purged at the threshold set in the Miscellaneous Parameters screen — see Section 15 (Configuring Remote Access) for details.

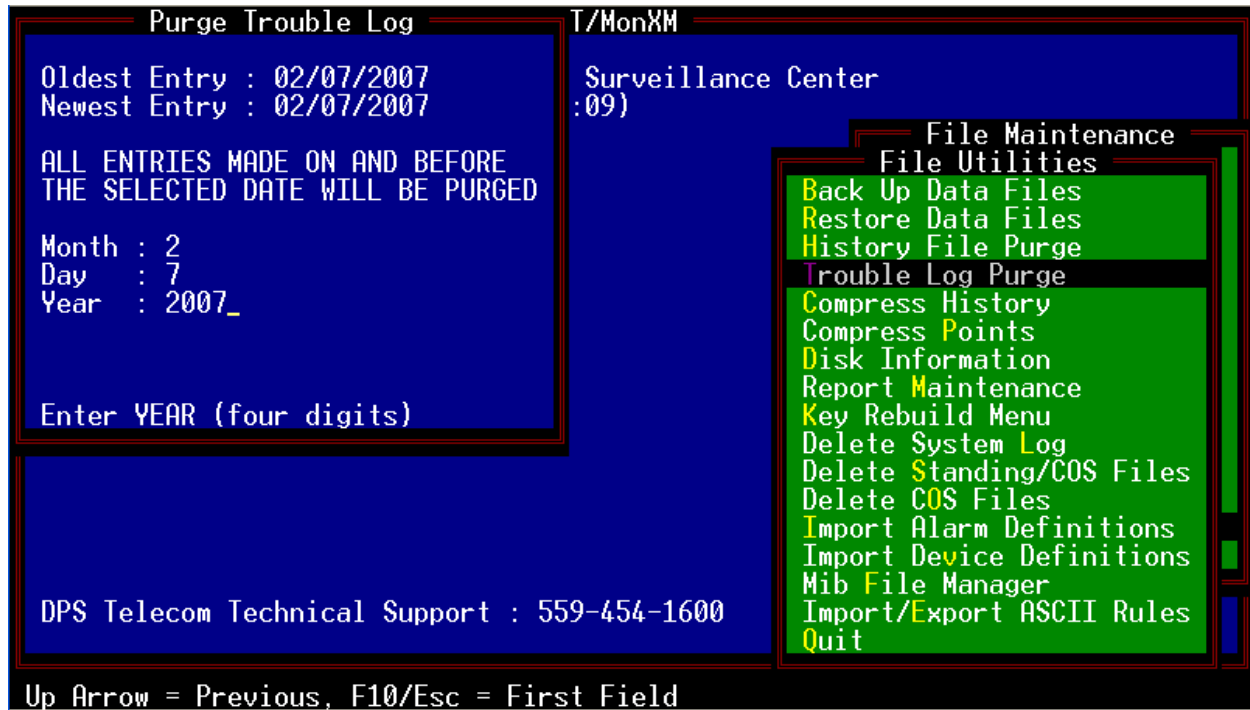
Typically the user never needs to run this utility.

#### **History File Purge**

This option lets you delete the oldest entries from the History file.

At the top of the window, the dates of the oldest and newest entries are displayed. The user selects the last day that the purge will include. All entries made on or before the selected date will be deleted. As a safety feature, the system will default to 3 months prior to today's date. In addition, you will be prompted to type the word "ERASE" after entering a date to prevent inadvertent deletions.

After the History file has been purged, its size remains the same as before the purge. The space reclaimed within the file will be reused by subsequent History file entries.

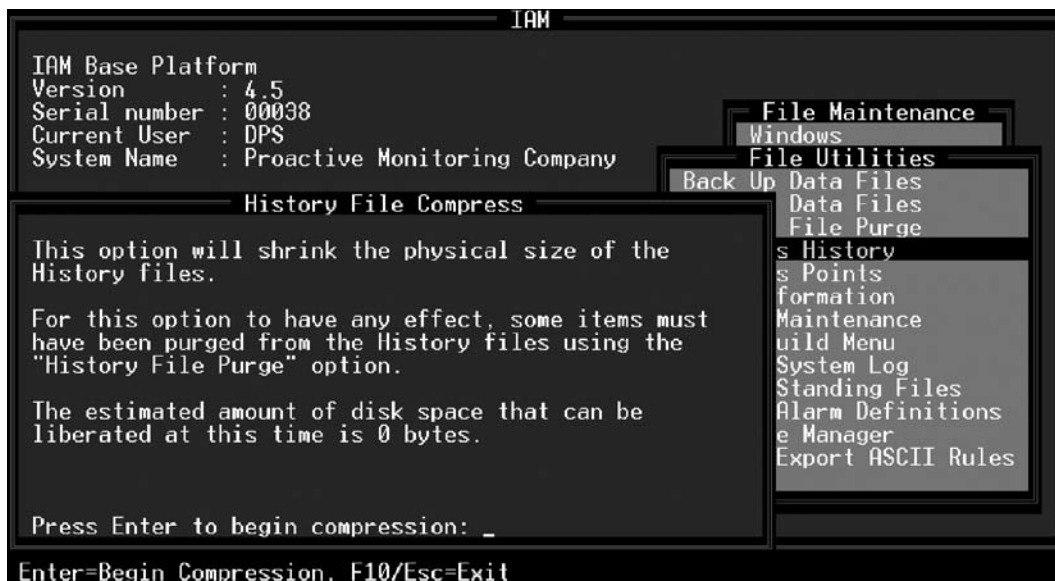


**Fig. 19.5 - The purge trouble log screen.**

#### **Trouble Log Purge**

This option lets you delete the oldest entries from the trouble log.

At the top of the window, the date of the oldest and newest entries are displayed. The user selects the last day that the purge will include. All entries made on or before the selected date will be deleted. As a safety feature, the system will default to 3 months prior to today's date. In addition, you will be prompted to type the word "ERASE" after entering a date to prevent inadvertent deletions.



**Fig. 19.6 - The history file compress screen.**

Typically the user never needs to run this utility.

#### **Compress History**

This menu option will physically shrink the size of the History file. This option will only have an effect if entries have been purged from the file using the History File Purge option. In case there is insufficient disk space available, the user will be prompted for a DOS drive and path to use as temporary storage. The user will also be informed of the amount of disk space that will be freed by the compression.





Fig. 19.7 - The compress points screen.

### Compress Points

This menu option will physically shrink the size of the Point files.

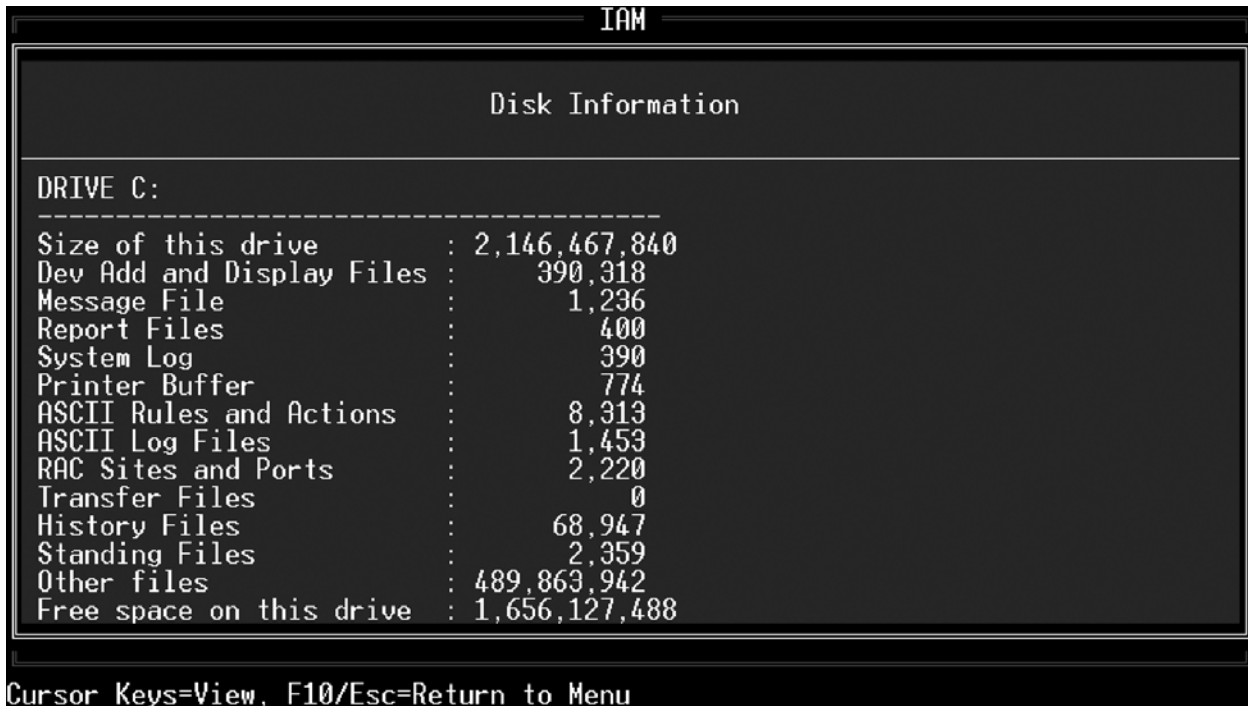


Fig. 19.8 - The disk information screen

### Disk Information

The Disk Information option generates a disk usage report displaying the number and size of configuration files on the internal hard disk.



Fig. 19.9 - The report maintenance menu.

### Report Maintenance

The three menu options on the Report Maintenance screen (see Figure 19.8) allows you to view, copy, and/or delete report files that you have previously generated.

For file viewing refer to section 19-1 in “Managing Reports.”



Fig. 19.10 - The key rebuild menu.

Preventative maintenance key rebuilds are not required.

It doesn't hurt to perform a key rebuild—no data loss will occur because of a key rebuild. However, T/MonXM will usually perform a key rebuild automatically if one is ever required.

### Rebuild Key Files

The Key Rebuild menu (see Figure 19.9) appears when you choose the Key Rebuild menu option from the File Utilities menu. The Key Rebuild menu options will rebuild an index file for the option you choose or take you to another menu of logically grouped files. It may be necessary to rebuild an index file if the data file and index file get out of synchronization. The Key Rebuild process deletes the out-of-sync index file and uses the data file to create a new index file for the chosen option.

These options will be most often used in the event of a catastrophe with T/MonXM's index files and when recommended by a DPS customer service representative. They are not used unless there is a problem. To execute the Key Rebuild menu options select an option and press Enter.

Table 19.B lists the options available under the Key Rebuild menu and sub menus. To rebuilt simply highlight the selection and press Enter

If there are over 100 keys, a progress box will appear showing the number of records restored and the total number of records.

**Table 19.B - Key Rebuild Menu selections**

<b>Key Rebuild Menu Selection</b>	<b>Sub Menu Selection</b>
Device D/B sub menu	Windows BSU Device Ports Device Address Device Point Responder Provisioning
General sub menu	History Key Security Derived Trouble Logs Labeled Control Cat Labeled Control Points Cards Data Connection
LED Bar Key	None
ASCII sub menu	ASCII Device Key ASCII Action Key ASCII Log Key
Dial Up sub menu	Dial Up Sites
T11 sub menu	Route Sid Point Tables
Building sub menu	Site Key Log Key BAS Info Key
Pager sub menu	Pager Operators Pager Exceptions Pager Carriers
VDMs	None
Indirect Analogs	None
Compiled Trap IDs	None



**Fig. 19.11 - You must confirm you want to delete the System Log**

### Delete System Log

The Delete System Log option will delete the System Log. This option should only be used when recommended by a DPS customer service representative. The Delete System Log contains vital information to correct program anomalies should they occur. To execute the Delete System Log option, simply select the option and press Enter. Then type "Y" at the warning prompt.



**Fig. 19.12 - You must confirm you want to delete the standing files**

**Note:** System must be initialized without entering Monitor mode for this to work.

This feature is also used when making rule changes for Auto ASCII databasing. See Software Module 6 for more information.

#### **Delete Live Files**

The Delete Live Files option will delete the live files which relate to live alarms and standing alarms. This option will most often be used when recommended by a DPS customer service representative. This is primarily used to delete standing alarms from the system that can never clear. (i.e.: A remote containing an alarm point that is no longer in the system).

To execute the Delete Live Files option, simply select the option and enter “Y” at the warning window (see Figure 19.11).

**CAUTION** — Deleting live alarms has two side effects:

1. Devices taken off-line will be turned back on.
2. Alarms that were previously in and possibly acknowledged will cause a new COS if they are still standing.

## Preventive Maintenance

DPS Telecom recommends the following best practices for preventive maintenance:

- Back up your Configuration files whenever changes are made.
- Use the Export History Report on a weekly/monthly basis to archive your history events.
- Periodically review System User access and remove users who are no longer employed in your organization or no longer use T/MonXM.
- Regularly check the DPS Telecom website ([www.dpstelecom.com](http://www.dpstelecom.com)) to make sure you are using the latest T/MonXM software.

## Import Alarm Definitions

### *New in 4.6*

Alarm Import Utility now has support for importing NetGuardian and KDA remotes.

**Important Note:** Alarm importation is an advanced tool for users who wish to maintain their database on another system. Most T/Mon users should use the built in point editing function.

The Import Alarm Definitions feature allows alarm point definitions to be added by importing them from a delimited text file. The general format of the file is the same as that generated by the Export Alarms report.

The default format for the import file is tab delimited with no text qualifier. This can be changed by adding directives to the import file. See the File Preparation section below for more information about directives. A text qualifier indicates that the text includes the delimiting character but you do not want it to be treated as a delimiter in that one instance. Such text would be enclosed by the text qualifier to qualify it as text, and not a delimiter.

**Note:** Files must not contain spaces, or characters such as: \, /, ?, :, ;, x, ", |, >, or <

### File Preparation

1. Before a file can be imported it must be modified to contain the following line: #ALARM:1

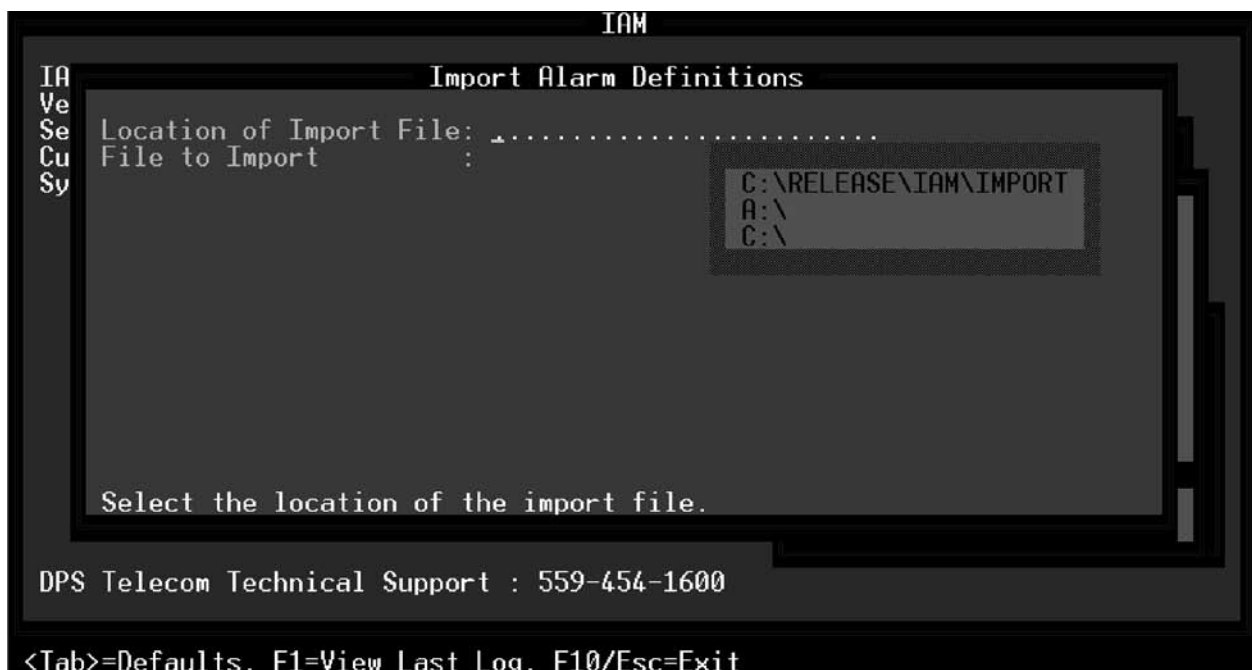


Fig. 19.13 - Import Point Database screen

Note that this line must come before the lines containing the data that is to be imported. This line tells the import processor what kind of data is being imported. (In the future the import feature may be expanded to import other kinds of records).

2. Any lines in the file that you do not want to be processed (headers for instance) may be prefixed with a pound sign (#). (However this is not absolutely necessary as lines processed that do not contain valid data will not generate fatal errors).
3. To change the delimiter, add the following line to the import file: #DELIMITER:19  
where 19 is the delimiting character.
4. To change the text qualifier, add the following line to the import file: #QUAL\_CHAR:19  
where 19 is the text qualifier.

### **Importing a File**

To begin importing a file, go to Files/Utilities/Import Alarm Definitions in the menus. Select the location of the file and the name of the file to import. Press Enter to begin importing. You may press Esc at anytime to pause.

A log file is kept of the import session. The name of this file is IMPLOG.REP. You can view it via the standard report viewing features in T/Mon or you can press F1 while the cursor is at the Location of Import File field on the Import Alarm Definitions screen.



---

## ASCII Import

The ASCII Import option allows a user to import ASCII device information from an external file. This file needs to be in a tab-delimited formatted text file or a comma-delimited formatted text file. Using the export feature and modifying the file would be the best way to make sure that it is in the right format.

Exporting ASCII device data can be done from the main T/Mon screen. Navigate to Report > 2. Alarm Database > 16. Export Devices. This will export all devices within a specified range so the output file may contain data other than ASCII-specific data.

In order to import the file, it needs to have the proper header line. The first line should be "Report Port Export Device Report". A delimiter line should also be in the first couple of lines. It should have a line of its own that says "Delimiter:" followed by the delimiter used in the file. It could be a tab or comma.

### ASCII Report Format

The Export Device Report will contain different fields and only certain fields apply to the ASCII import. These fields reflect values found on the Remote Device Definition window.

Field	Definition
<b>Port</b>	This identifies which job/remote the ASCII job is set to. The ASCII job needs to be set up prior to importing ASCII device data. (Required and cannot be left blank)
<b>Addr</b>	This identifies the address to which the line will export the data. (Required and cannot be left blank)
<b>Desc</b>	This field is not necessary. It corresponds with description field when editing an ASCII job. Please try to keep this field under 40 characters.
<b>Site Name</b>	This field is optional and corresponds with the Site Name. Please try to keep this field under 30 characters.
<b>Displays</b>	This field will need to be numerical. This field can contain dashes and commas. It would be the same data that would be typed into the display field on the actual T/ Mon screen. (Required and cannot be left blank)
<b>Poll Type</b>	Must be a numerical value. If this field is left blank, the default value of zero will be used. (Default value is zero)
<b>Refresh</b>	This is not relevant to ASCII device but must be a numerical value. If field is left blank, zero will be used. (Default value is zero)
<b>Send CMD</b>	This should be a numerical value. On an ASCII job on address zero, this would be the same field as Poll Interval. A zero value or if left blank will indicate that Poll Intervals are disabled. On an ASCII job on any address other than zero, this field would reflect the Send Cmds field. A zero (or if left blank) would indicate an N on the T/Mon ASCII Remote Device Definition screen. Anything other than a zero would display a Y. (Default value is zero)
<b>Tokens 1-5</b>	These are text strings which would display as Tokens 1 through 5 on the ASCII Remote Device Definition screen. Please try not to use more than 15 characters for these fields.
<b>ascSite Key</b>	This is another text string which can be found on the T/Mon auto-ASCII site definitions window. This field is optional but please try not to use more than 30 characters. This field can be left blank.
<b>ascSite Window</b>	This must be a numerical value and can be found on the T/Mon auto-ASCII site definition window as Site Window. Valid values for this field is 2-270 or blank for none. If this field is defined, please be sure to also define a Site Key.
<b>ascSite Win Mode</b>	This must be a numerical value and can be found on the T/Mon auto-ASCII site definition window as Window Mode. Zero corresponds with normal and 1 is row/ site. If this field is defined, please be sure to also define a Site Window and Site Key.
<b>ascDev Type</b>	This is the device type from the drop-down menu on address 0 on the Remote Device Definition window. Please make sure that the device already exists. This field currently does not validate the device type and will copy whatever is in this field into the Remote Device Definition window. Invalid devices might cause undesired results.

**The following fields are not used by the ASCII job and can be left blank:**

- Firmware
- Device
- Log Undefined
- luPol
- luHist
- luLev
- luStatus
- luReverse
- luDesc
- luWindows
- luMessage.

### **Importing the ASCII file**

From the main screen navigate to Files>Utilities>Import Device Definitions. This will allow you to select a file to import. The ASCII jobs must already be defined prior to importing. The import process checks for ASCII jobs and will only import if the job is in ASCII.

## Controls Import

The Controls Import option will allow a user to import labeled or site controls from an external file. This file needs to be in a tab delimited formatted text file. Using the export feature and modifying the file would be the best way to make sure that it is in the right format.

Exporting the Controls data can be done from the T/Mon's master menu. Navigate to Report. Select either Labeled Controls or Site Controls. Write to a file and make sure that the Export Format field is set to Y. This will format the report for export/import. Selecting N will provide a report that will be easier to read.

In order to import the file, it needs to have the proper header line. The first line should contain "Controls Export Report".

Before a file can be imported it must be modified to contain the following line:

```
#CONTROLS:1
```

Note that this line must come before the lines containing the data that is to be imported. This line tells the import processor what kind of data is being imported.

Make sure that all ports and devices are already databased on the T/Mon before importing.

### Importing a file

To begin importing a file, go to Files/Utilities/Import Control Definitions in the menus. Select the location of the file and the name of the file to import. Press Enter to begin importing. You may press ESC at any time to pause.

A log is kept of the import session. The name of this file is IMPLOG.REP. You can view it via the standard report viewing feature in T/Mon or you can press F1 while the cursor is at the Location of Import File field on the Import Control Definitions screen.

### Control Report Format

The Control Report will contain two different lines. One line is for defining Control Categories and the other is for defining the Control entry point.

A Control Category line must precede a Control Entry line. The basic structure of the import file is formatted in this manner:

```
Category Definition
    Entry Definition
    Entry Definition
    Entry Definition
Category Definition
    Entry Definition
```

All Control Entries defined after a Category Definition will fall under the last defined Category defined.

### The Category line will have this format:

```
#CATEGORY {TAB} Entry Number {TAB} Category ID {TAB} Category Desc {TAB} Category
window
```

Title	Definition
<b>Entry Number</b>	This is the entry number of the Category and must be a numerical value between 1-40.
<b>Category ID</b>	This defines the Category ID and will only use the first 6 characters defined.
<b>Category Des</b>	This is the Category description and is limited to 40 characters.
<b>Category Window</b>	This is the window if this is a Site Control Category. Enter 0 if it is a labeled control.

### Control Category Lines

All fields are necessary. The Import process will return an error if any of the fields are missing. **#CATEGORY** must be at the beginning of the line and is case sensitive.

**The Control Entry line will have this format:**

Entry Number {TAB} Desc {TAB} CMD {TAB} Chan {TAB} T {TAB} Address {TAB} UNT {TAB} Pnts

Title	Description
<b>Entry Number</b>	This is the entry number for the control point and must be a numerical value between 1-200.
<b>Desc</b>	This is the description field for the control and is limited to 40 characters.
<b>Cmd</b>	This is the control command. It should only be 3 characters long and all upper case. Valid options are: OPR, RLS, MON, MOF, SET, GET, SOP, SRL, SMO, EXE, CLR, SWI and STS
<b>Chan</b>	This is the channel or port of the device that the control is going to be issued to. Should be a numerical. The import process will check if the port is capable of sending out controls and if only certain control commands are allowed on a certain port.
<b>T</b>	This is a special field and is only used if the device on channel/port is a DCM interrogator. This is a one character value containing either S or C. C is for CPM and S is for SBP. SBP will only allow momentary on for the control command.
<b>Addr</b>	Address of the control. This is a numerical value and the range varies depending on the device defined on the channel/port. If Port is NG, this is used as the Site ID.
<b>UNT</b>	This is the display for the control. This is a numerical value and the range also varies depending on the device.
<b>Pnts</b>	This is the points that the commands will be issued to. This field can contain commas and dashes. (ex. 1-64, 66)

**Control Entry Lines**

# MIB File Manager

The MIB File Manager is used for loading, compiling, and deleting MIB files. You can also view the results of compiling a MIB by selecting View Logs or pressing V from the MIB Manager menu. To access the MIB Manager, select Files (File Maintenance) from the Master Menu, then select Utilities (File Utilities), and then select Mib File Manager.

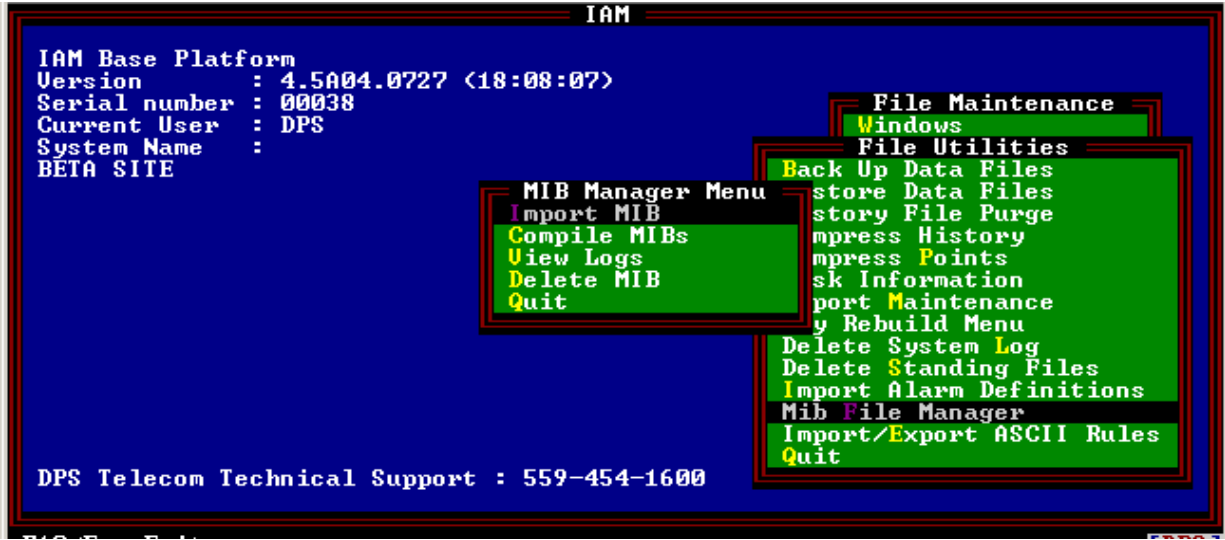


Fig. 19.14 - MIB Manager Menu.

## Import MIB

Copy your MIB files to the T/Mon or IAM by selecting Import MIB from the MIB File Manager Menu. The Import MIB File screen will appear. Place your disk into the T/Mon or IAM floppy drive and press the letter of the floppy drive. Your saved MIB files will appear as seen in Figure 19.14. Press the Tab key to highlight and select the file you wish to copy, and then press Enter.

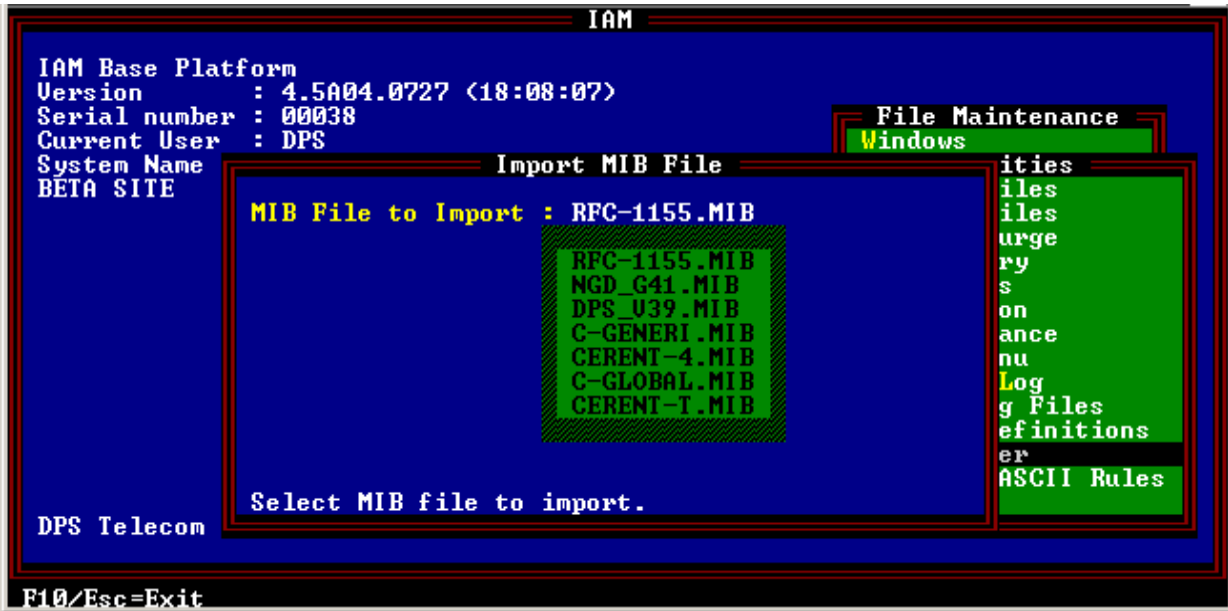


Fig. 19.15 - Press the Tab key to select the MIB file.

### Compile MIBs

This feature compiles all MIB files in the MIB directory of the T/Mon or IAM. Once compiled, you may use the TRAPS for databasing.

Select Compile MIBs from the File Utilities Menu. Then press C to compile your MIB files or press A to abort. The T/Mon or IAM will automatically compile MIB files as shown in Figure 19.15.



```

IAM
Compiler Messages
Errors Will Be Logged to MIBERR.TXT...
Parsing MIBs...
  RFC-1155.MIB ***** successful.
Parsing Complete.
Decoding Object Tree...
  *****
Compiling complete?

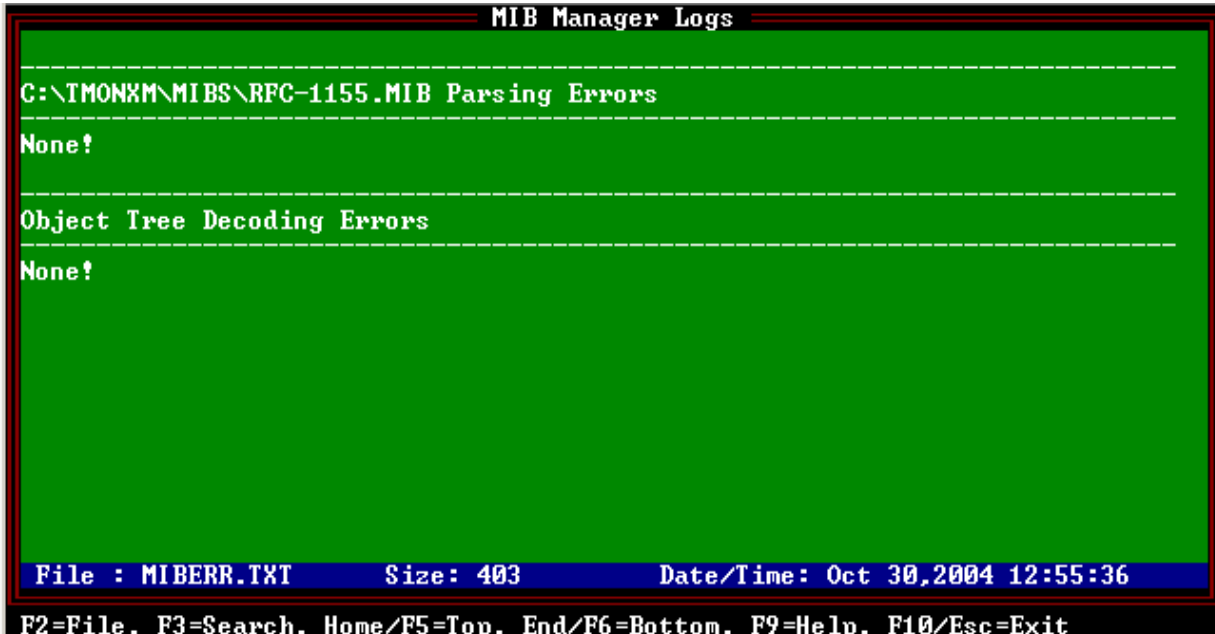
No errors!  Press a key

```

Fig. 19.16 - The Compiler Messages screen.

### View Logs

You can view the results of your compiled MIB files by selecting View Logs from the MIB Manager Menu. The Manager Log will appear as shown in Figure 19.16. Select to view a different file by pressing F2 or F3 to search for a file.



```

MIB Manager Logs
-----
C:\TMONXM\MIBS\RFC-1155.MIB Parsing Errors
None!
-----
Object Tree Decoding Errors
None!
-----

File : MIBERR.TXT      Size: 403      Date/Time: Oct 30,2004 12:55:36
F2=File. F3=Search. Home/F5=Top. End/F6=Bottom. F9=Help. F10/Esc=Exit

```

Fig. 19.17 - View compiled MIB results in the MIB Manager Log screen.



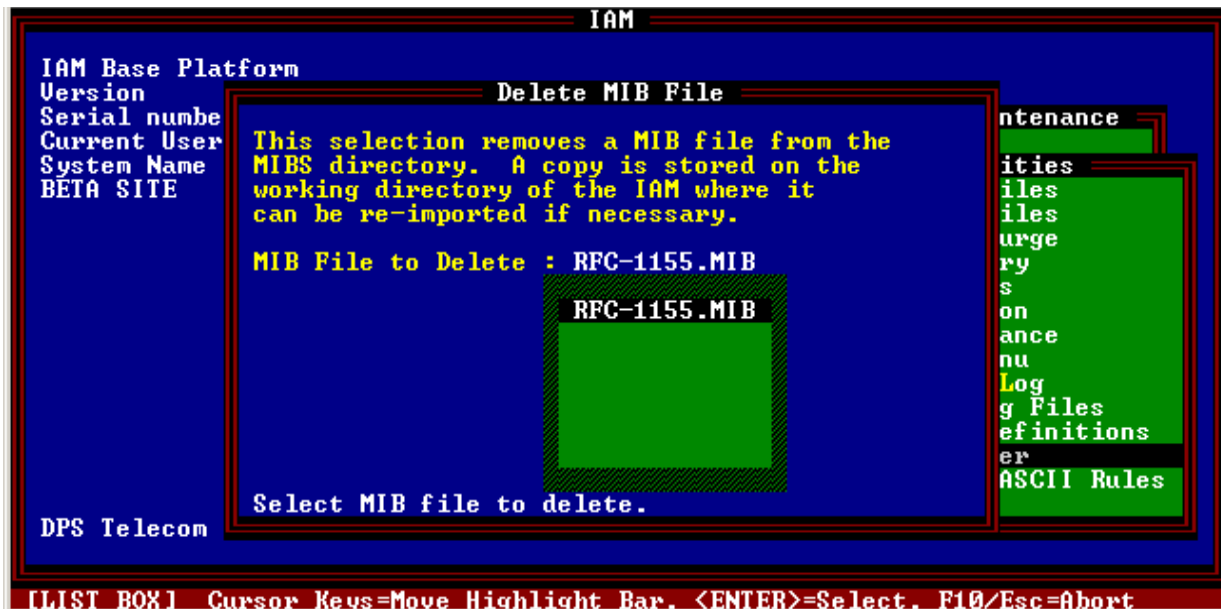


Fig. 19.18- Delete MIB files from the T/Mon or IAM internal drive.

#### Delete MIB

Delete MIB files from your T/Mon or IAM's internal drive by selecting Delete MIB from the MIB Manager Menu. Press the Tab key to select the MIB file, then press Enter.

## Import/Export ASCII Rules

Import or export your ASCII rules from your T/Mon or IAM using the ASCII Utilities Menu. To select the ASCII Utilities Menu, select Import/Export ASCII Rules from the Files Utilities Menu — see Figure 19.17.

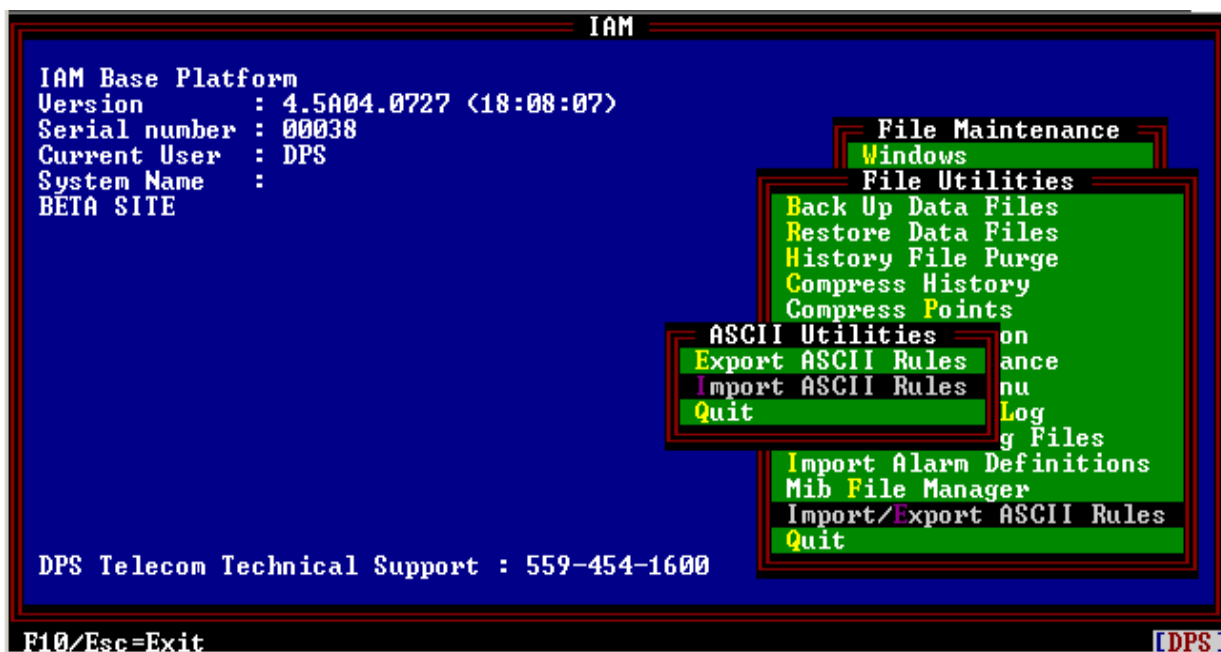


Fig. 19.19 - Select Import/Export ASCII Rules from the File Utilities Menu.



Fig. 19.20 - Press the Tab key to select the rule you wish to export.

### Export ASCII Rules

Export your ASCII rules by selecting the Export ASCII Rules feature from the Files Utilities > Import/Export ASCII Rules Menu. Use the following rules to export your ASCII rules:

1. Press the Tab key to select the rule set you wish to export from the T/Mon or IAM hard drive— see Figure 19.17.
2. Press the Tab key to select the destination you wish to export the file to.
3. Enter a rule set name, then press Enter.
4. Press E to export the rules.

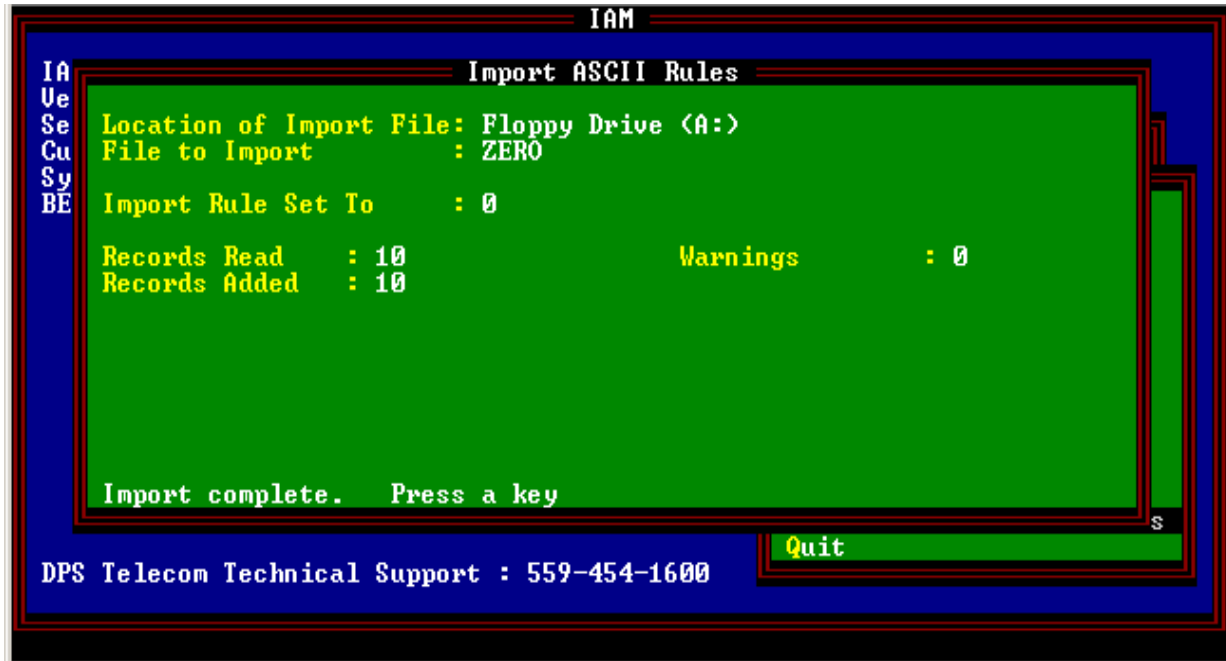


Fig. 19.21 - Select Import/Export ASCII Rules from the File Utilites Menu.

#### Import ASCII Rules

Copy your ASCII rules from a disk to the T/Mon or IAM internal drive by selecting Import/Export ASCII Rules from the Files Utilites Menu.

Use the following steps to import ASCII Rules:

1. The Import ASCII Rules screen will appear as shown in Figure 19.18.
2. Press the Tab key to select the location of the ASCII rules, then press Enter.
3. At the prompt, enter the rule set you wish to save the rules to, then press Enter.
4. You may press F1 to view the import details.

**Note:** if you make a mistake press Esc to return to the previous field.

## T/MonXM Disk Files

### Program Files

The release disk contains the following files:

TMONXM.EXE	T/MonXM executable files.
TMONXM.OVR	
TASK.TSK	
BOOT.TSK	4 Channel Communication controller file.
REMOTE.TSK	4 Terminal Controller file.
TEST.TSK	4 Channel and 4 Terminal Controller diagnostic files.
COMINT.TSK	
MLECHO.TSK	
LOOP.TSK	
IDLE.TSK	
MAIL.TSK	
HIMEM.SYS	T/MonXM memory management file.

### Database Files

As the system is used, the following files will be created in the T/MonXM account:

CTLCAT.DAT	Labeled Controls Files
CTLCAT.IDX	
CTLPNT.IDX	
CTLPNT.DAT	
DCTL2.DAT	Miscellaneous Files
DCTL2.IDX	
DEVPOINT.IDX	Point Files
DEVPOINT.DAT	
EMDEV.IDX	Address Files
EMDEV.DAT	
EMDEV2.IDX	
EMHIST2.IDX	History Files
EMHIST2.DAT	
EMLIVE.DAT	Live Files

EMLVDAT.IDX

EMLVITEM.IDX

EMMSG.DAT           Text Messages File

EMWIN.DAT           Window Files

EMWIN.IDX

TBSALM.DAT           Miscellaneous File

TMONEM.DAT           Program Data File

TRB.DAT             Trouble Log Files

TRBDATE.IDX

TRBPNT.IDX

**Note:** As the system is used, the names of the configuration files in the T/MonXM account follow the standard rule “SYSTEMNAME.EXT”.

**This page intentionally left blank.**

## Section 20 - Managing Reports

### Reports in Monitor Mode vs. Reports under the Master Menu

Reports can be run via the main T/MonXM WorkStation, T/RemoteW or T/Windows, if security access is provided. Only one user at a time can run a report.

Reports generated in the Monitor Mode allow monitoring to continue while the report is produced. Report selections 1 through 8 listed in the Report Mode Menu are available. In addition, by pressing Alt-F7 while in the COS or Standing Alarms screens you can generate a report of the COS or Standing alarms for a specific window. In this mode you cannot view the reports on screen. Reports from T/RemoteW or T/Windows can be sent directly to a local printer or hard disk.

Reports generated in the Reports screen under the Master Menu are produced while T/MonXM is offline. In this mode you cannot generate a report for a specific window. In this mode you can view reports on screen.



Fig. 20.1 - Reports mode is selected from the master menu

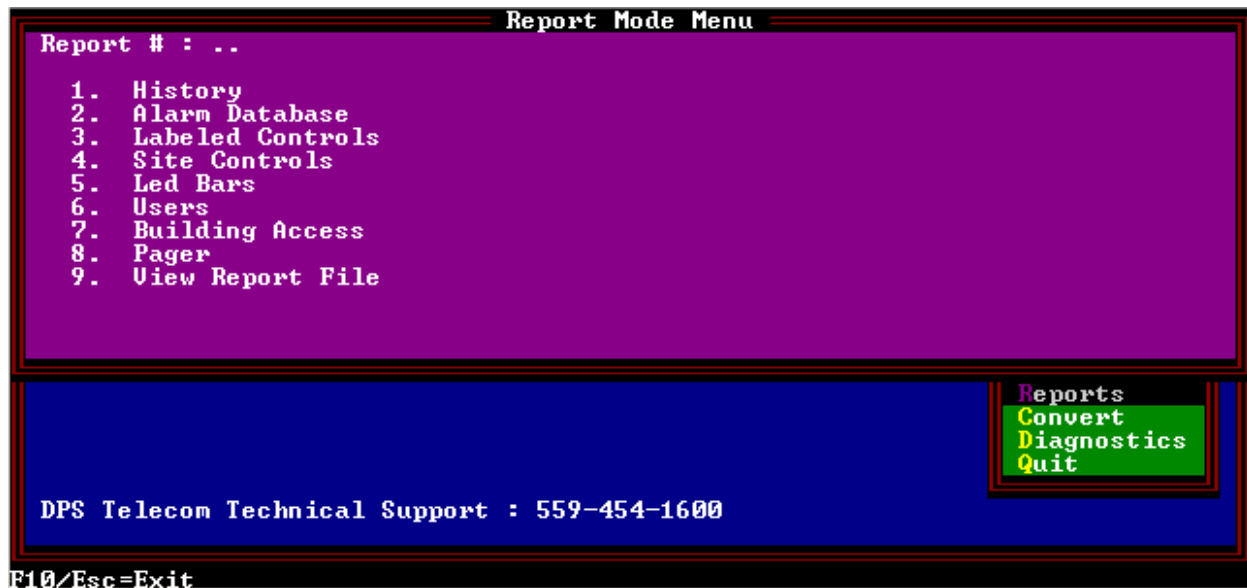


Fig. 20.2 - Report mode menu provides nine selectable options

**Note:** to view reports onscreen (option 9), you must save/output the report to a file and select it in the View Report File screen. See section 20-37 for more information.

Report mode is used to generate reports based on your T/MonXM database definitions. Report mode can be entered via the Master menu by selecting Reports (see Figure 20.1) or by pressing Alt-F7 from within Monitor mode

If Report mode is entered from Monitor mode, the window will be displayed in the main window of the screen — see Figure 20.3.

Note that the View Report File option is available only when you select Reports from the Master menu. You cannot view reports while in Monitor mode.

Reports give a print out or file record of database information. To select a report, type the number and press Enter. The table on the next page lists a summary of the available reports.



Fig. 20.3 - Report menu in monitor mode offers eight options



**Tbl 20.1 - Reports available in the Report Mode menu**

Field	Description	Options
1. History	Report for a selected period of time (or other criteria) that alarms occurred. (See Figure 20.3)	1. Standard History 2. Export History 3. Outage Summary 4. Duration History 5. Duration Summary 6. Export Analogs 7. Duration History (Incident) 8. Duration Summary (Incident) 9. Duration Detail (Incident)
2. Alarm Database	Report on selected alarm items in the Alarm Database. (See Figure 20.7)	1. Remote Ports 2. Windows 3. Text/Messages 4. ASCII Rules 5. ASCII Tables 6. ASCII Actions 7. Derived 8. VDMs 9. Site Reports <ul style="list-style-type: none"> <li>1. Sites by Address</li> <li>2. Sites by Site</li> </ul> 10. BSU 11. Cards 12. Dial Up Shelves 13. KDA Shelves 14. Net Guardians 15. Export Alarms 16. Export Devices 17. Export Ports 18. Export KDA Shelves 19. Trap Associations 20. Trouble Log By Point 21. Trouble Log by Date/Time 22. Export to NGEEdit 23. SNMP Set Commands 24. SNMP Get Commands
3. Labeled Controls	Report on labeled controls defined in the database. Corresponds with information on Labeled Controls editing screens.	
4. Site Controls	Report on site controls defined in the database. Corresponds with information on Site Controls editing screens.	
5. LED Bars	Report on LED Bars defined in the database. Corresponds with information in LED Bars editing screens.	
6. Users	Report on users and security access privileges defined in the database	
7. Building Access	Report on building access sites defined in the database.	
8. Pager	Report on pager information in the database.	1. Pager Carriers 2. Pager Schedules 3. Pager Exceptions. 4. Pager Groups
9. View Report File	View existing report files on screen. A report must have been output to file before it can be viewed on screen.	

Report menus and options will change as software modules are installed.

**Note:** you can also FTP report files from the C Drive when the FTP server is set up on the T/Mon or IAM.

Reports can be sent to the printer or to a disk file. When a report type is selected, the user will be prompted for a file name to write the report to — see Figure 20.5. The file extension of report files is .REP.

Reports that are sent to disk can be imported into spread sheets for detailed analysis or to include in other reports. You may also copy report files to floppy disks and delete them from your hard disk with the File Maintenance/Utilities/Report Maintenance menus.

Some reports require additional information. This information is explained in detail on the following pages.



Fig. 20.4 - History menu offers nine selections



Fig. 20.5 - Reports can be sent to printer or file

---

## Running Reports from T/RemoteW and T/Windows

The commands for generating reports in T/RemoteW and T/Windows are identical to those used with the T/Mon or console access to the IAM-5. However, by default, the output of the report is sent to the Report Preview window.

The report can be viewed in its entirety in the Report Preview window. The Report Preview window also has four toolbar buttons offering the following commands:

**Open:** Open any previously saved file.

**Save:** Save open report as either text file (.txt) or Rich Text Format file (.rtf). By default, T/RemoteW saves reports as text files in its own application directory.

**Print:** Print open report in any local or network printer accessible from your PC.

**Exit:** Close the Report Preview window.

---

## History Report

History reports provide the means for tracking trends and determining problem areas in your network. By running a history report for suspected trouble spots you can obtain the data needed to support revision of maintenance schedules or equipment replacement plans.

Following are some events that can be entered in History Reports per the applicable configuration screens in the Parameters menu.

- When Alarms fail and/or clear.
- When pages are sent.
- When you enter and exit Monitor mode.
- When you initialize the system.
- When Control Points are issued.
- When T/MonXM goes on or off battery power.
- When the system shuts down because the UPS battery is dead.
- When the system automatically re-starts after a UPS shutdown.
- When you exit the system.

The History Report Menu includes 9 types of history reports:

1. Standard History: history report in standard format — see Figure 20.7.
2. Export History: report in comma delimited format for export to a spread sheet — see Figure 20.8.
3. Outage Summary: outages summary report for up to 33 category windows and up to 150 site windows. For more information on this feature contact DPS Telecom.
4. Duration History: outages in excess of a specified time period — see Figure 20.9.
5. Duration Summary: total time and maximum time of outages — see Figure 20.10

6. Export Analogs - Comma delimited listing of analog values recorded per the Miscellaneous Parameters screen. For more information on this feature contact DPS Telecom.
7. Duration History (Incident)-Identical to report 4, Duration History (Time) except time reports are sorted by the time an alarm occurred, and Incident reports are sorted by site/alarm — see Figure 20.11
8. Duration Summary (Incident)-Identical to report 5, Duration Summary (Time) except time reports are sorted by the time an alarm occurred, and Incident reports are sorted by site/alarm — see Figure 20.12
9. Duration Detail (Incident)-allows report to be filtered by alarm description text and site name text — see Figure 20.13.

## Standard History

The Standard History Report window (see Figure 20.6) generates an alarm activity report (see Figure 20.7) for a selected time period. This report includes only alarms that are defined to be recording to history — see Section 10 (Point Definition Tutorial).

The Standard History Report window is selected from the Report Mode Menu. Type 1 and press Enter. In the window that appears you select the output destination (File or Printer) and the file name. Once this is done the Standard History report window appears. The following table explains the fields in the Standard History report window.

An example of a Standard History report is shown in Figure 20.7.

```

Standard History
Begin: 02/07/07 00:00
End : 02/07/07 13:10
Type : A All
Port : 1-500,RP,IA,K1,K2,NG,N2
Disp : 1-99
Description Contains : .....
Win : ALL
Addr : 0-999
Point: 1-64

Enter the text that must appear in the description
  
```

Fig. 20.6 - Standard History report screen

**Tbl 20.2 - Fields in the Standard History Report window**

Field	Description
Beg Date End Date	Enter the beginning and the ending dates of the alarm history you require. Dates are entered in the format: MM/DD/YY. [TODAY'S DATE] For example, November 5, 2000 would be entered as 11/05/00.
Time	Times are entered using standard military time in the format: HH:MM, where 0:00 = midnight. [CURRENT TIME] For example 2:39 PM would be entered as 14:39.
Type	Enter the type of alarms that will be required on the report. Valid selections are: A (All) P (Points) C (Controls) U (Users).
Win	Enter the range of windows (1-720) wanted on the report. [Defaults to maximum number of windows installed.] <b>Note:</b> This field is very useful for preparing reports of alarms based on severity, equipment type or location.
Add	Enter the range of addresses (0-999) wanted on the report.
Port	Enter the range of remote ports wanted on the report. Valid entries are: 1-28 RP (Modem Devices) RC (Relay Card) IA (Internal Alarms) K1, K2, K3 (Virtual Ports) You may select more than one entry by separating them with a comma.
Disp	Enter the range of displays (1-64) wanted on the report.
Pnt	Enter the range of points (1-64) wanted on the report. <b>Note:</b> Address and Point ranges interact to select a group that contains only the specified points within the specified addresses. For example, when addresses 1 and 2, points 6-12 are specified the report will include points 6-12 at addresses 1 and 2, but not points 1-5 or 13-up from any address, nor points 6-12 from address 3 or higher.
Desc	Enter a keyword or phrase that must appear in the point description. Entering several words will look for each individual word and include to the history report if any of the words appear. Using double quotes will match everything inside the quotes.

**Note:** For an event to be reported it must pass all of the selection criteria.

**Table 20.3 - Key commands available in the History Report window**

Function Key	Description
F10	Exit
Up Arrow	Go back to previous field.

```

History Activity Report      Run Date: 6/24/04 5:05 pm      Page 1
Start of Interval: 06/24/04 16:45
End of Interval : 06/24/04 16:51
Type: All Wins: 1-720 Ports: 1-29,RP,RC,IA,K1 Addr: 0-999
Displays: 1-64 Points: 1-64
Item      Alarm date/time  S L Description
Site      Ack date/time    T V Display Desc  Initials  Status
[USER]    06/24/04 16:45:45  [ENTER MONITOR MODE]
          DPS
3. 1. 1. 1 06/24/04 16:45:52 F A A.C. Power Fail
TEST      06/24/04 16:52:05          DPS    ALARM
- 3. 1. 1. 1 06/24/04 16:45:52 PGR A.C. Power Fail
          Msg # : 1      A Dialed pager. BMS
3. 1. 1. 2 06/24/04 16:46:39 F A Backup Gen.
TEST      06/24/04 16:52:06          DPS    RUNNING
- 3. 1. 1. 2 06/24/04 16:46:40 PGR Backup Gen.
          Msg # : 1      A Dialed pager. BMS
3. 1. 1. 3 06/24/04 16:47:46 F A Backup Gen. Fuel
TEST      06/24/04 16:52:06          DPS    LOW
- 3. 1. 1. 3 06/24/04 16:47:47 PGR Backup Gen. Fuel
          Msg # : 1      A Dialed pager. BMS
3. 1. 1. 3 06/24/04 16:49:11 C A Backup Gen. Fuel
TEST      06/24/04 16:52:06          DPS    FILLED
- 3. 1. 1. 3 06/24/04 16:49:13 PGR Backup Gen. Fuel
          Msg # : 1      C Dialed pager. BMS
3. 1. 1. 1 06/24/04 16:50:33 C A A.C. Power Fail
TEST      06/24/04 16:52:06          DPS    CLEAR
- 3. 1. 1. 1 06/24/04 16:50:34 PGR A.C. Power Fail
          Msg # : 1      C Dialed pager. BMS
3. 1. 1. 2 06/24/04 16:50:46 C A Backup Gen.
TEST      06/24/04 16:52:06          DPS    OFF
History Report Ended : Jun 24,2004 17:05:03

```

**Fig. 20.7 - Example history report to file**

## Export History

Export History exports a Standard History report as a comma-delimited text file.

This file is a tremendous resource of information about network events. The exported history file can be imported into a database or spreadsheet application, where it can be graphed and analyzed.

Export History	Field2	Field3	Field4	Field5	Field6	Field7	Field8	Field9
Start of Interval:								
End of Interval :								
Type: Points V								
Ports: 1-500	RP	IA	K1	K2	NG	N2	Addresses	
Displays: 1-99								
Date	Time	State	Level	Port	Addr	Disp	Pnt	Device
2/07/03	09:46:12	F	A	IA	11	1	1	STD
2/07/03	09:46:13	F	A	IA	11	1	3	STD
2/07/03	09:59:41	F	A	IA	11	1	1	STD
2/07/03	09:59:42	F	A	IA	11	1	3	STD
2/11/03	14:24:49	F	A	IA	11	1	1	STD
2/11/03	14:24:50	F	A	IA	11	1	3	STD
2/11/03	14:43:53	F	A	IA	11	1	1	STD
2/11/03	14:43:54	F	A	IA	11	1	3	STD
2/11/03	14:51:00	F	A	IA	11	1	1	STD
2/11/03	14:51:01	F	A	IA	11	1	3	STD
2/11/03	14:59:19	F	A	IA	11	1	1	STD
2/11/03	14:59:20	F	A	IA	11	1	3	STD
2/11/03	15:01:22	F	A	IA	11	1	1	STD
2/11/03	15:01:23	F	A	IA	11	1	3	STD
2/11/03	15:04:18	F	A	IA	11	1	1	STD
2/11/03	15:04:20	F	A	IA	11	1	3	STD
2/25/03	15:20:24	F	A	IA	11	1	1	STD
2/25/03	15:20:25	F	A	IA	11	1	2	STD
2/25/03	15:20:26	F	A	IA	11	1	3	STD
2/26/03	10:34:14	F	D	32	1	1	1	STD
2/26/03	10:35:43	F	A	IA	11	1	1	STD
2/26/03	10:35:44	F	A	IA	11	1	2	STD
2/26/03	10:35:45	F	A	IA	11	1	3	STD
2/26/03	10:50:27	F	A	IA	11	1	1	STD

Fig. 20.8 - Exported history file in database application

## Duration History

The Duration History report generates a report of outages in excess of a specified time period — see Figure 20.9. This report is one-half the size of a regular history report because it correlates the alarms and clears.

The Duration History report screen is selected from the Report Mode Menu. Type 4 and press Enter. At the prompt, select the output destination — press F to save to a file and enter the file name, or press P to send the report to your printer.

Duration History (Time)		Run Date: 6/18/04 10:35 am		Page 1
Start of Interval: 03/10/04 00:00				
End of Interval : 06/18/04 10:35				
Type: Points Wins: 1 Ports: 1-157,RP,IA,K1 Addr: 0-999				
Displays: 1-99 Points: 1-64				
Alarm Date	Alarm Time	Site Name	Alarm Description	Duration HHH:MM:SS
-/-/-	-:-:-		KDA ON/OFF LINE FOR FRESNO	11:36:11
-/-/-	-:-:-		LR24 ON/OFFLINE FOR FRESNO	11:36:12
-/-/-	-:-:-		DEVICE ON/OFFLINE FOR ADDRESS 2	11:36:15
03/10/04	11:36:31	DENVER	ACPOWER	0:19
03/10/04	11:36:31	DENVER	(Undefined)	0:55
03/10/04	11:36:57		KDA FAILURE FOR FRESNO	22:16:32
03/10/04	11:37:02		LR24 FAILURE FOR FRESNO	22:17:00
03/10/04	11:37:09		KDA FAILURE FOR BOSTON	1:33:08
03/10/04	11:38:37	LOS ANGELES	FUSE SHELF 103.12	4:30
03/10/04	13:00:43	CLASSROOM	K1. 40. 33. 33	0:00
03/10/04	13:10:17	BOSTON	TOWER BEACON #1	20:30:01
03/10/04	13:10:17	BOSTON	SIDE LIGHT	20:30:01
03/10/04	13:10:17	BOSTON	HUMIDITY	20:30:01
03/10/04	13:10:17	BOSTON	RCV SQUELCH ALM "B" RADIO	20:30:01
03/10/04	13:10:17	BOSTON	(Undefined)	20:30:01
03/10/04	13:10:47		KDA FAILURE FOR BOSTON	19:55:00
03/11/04	09:06:56		KDA FAILURE FOR BOSTON	12:49
03/11/04	09:18:26		KDA ON/OFF LINE FOR FRESNO	34:59
03/11/04	09:18:27		KDA ON/OFF LINE FOR HOUSTON	7:34
03/11/04	09:18:27		LR24 ON/OFF LINE FOR FRESNO	35:11
03/11/04	09:18:28		DEVICE ON/OFF LINE FOR ADDRESS 2	7:34
03/11/04	09:18:28		KDA ON/OFF LINE FOR DENVER	7:34
03/11/04	09:18:31		MAT SLOT 1 ON/OFF LINE FOR LA	7:32
03/11/04	09:18:31		MAT SLOT 2 ON/OFF LINE FOR LA	7:32
03/11/04	09:18:31		MAT SLOT 3 ON/OFF LINE FOR LA	7:32
03/11/04	09:18:32		T/BOS SLOT 4 ON/OFF LINE FOR LA	24:45
03/11/04	09:19:52		KDA FAILURE FOR BOSTON	0:24
03/11/04	09:19:57	CLASSROOM	K1. 40. 1. 24	23:58
03/11/04	09:20:30		KDA FAILURE FOR BOSTON	1:18
03/11/04	09:21:57		KDA FAILURE FOR BOSTON	0:48
03/11/04	09:22:57		KDA FAILURE FOR BOSTON	16:26
03/11/04	09:38:06		KDA ON/OFF LINE FOR HOUSTON	5:08
03/11/04	09:38:07		DEVICE ON/OFF LINE FOR ADDRESS 2	5:08
03/11/04	09:38:09		KDA ON/OFF LINE FOR DENVER	5:06
03/11/04	09:38:12		MAT SLOT 1 ON/OFF LINE FOR LA	5:04
03/11/04	09:38:13		MAT SLOT 2 ON/OFF LINE FOR LA	5:03
03/11/04	09:38:13		MAT SLOT 3 ON/OFF LINE FOR LA	5:03
03/11/04	09:52:31		KDA FAILURE FOR BOSTON	0:32
03/14/04	16:38:33	FRESNO	LOW BATTERY	16:17
03/14/04	16:49:44		KDA ON/OFF LINE FOR DENVER	0:09

Fig. 20.9 - Example Duration History report sorted by time

## Duration Summary (Time)

The Duration Summary (Time) report generates a report of the total time and maximum time of outages — see Figure 20.10. This report is a very useful point summary.

The Duration Summary (Time) report screen is selected from the



Report Mode Menu by typing 5. At the prompt you may press F and a enter a file name to save the report to a file, or press P to print.

```

Duration Summary (Time)      Run Date: 6/18/04 10:37 am      Page 1
Start of Interval: 03/18/04 00:00
End of Interval : 06/18/04 10:37
Type: Points Wins: 1 Ports: 1-157,RP,IA,K1 Addr: 0-999
Displays: 1-99 Points: 1-64
Site Alarm
Name Description Count TotalTime MaxTime
HHH:MM:SS HHH:MM:SS
FRESNO FUSE SHELF 103.12 2 0:25 0:23
FRESNO RECTIFIER 1 2 18:05 17:42
FRESNO RECTIFIER 2 1 0:22 0:22
FRESNO RECTIFIER 3 1 0:22 0:22
FRESNO T1 ES EXCEED 1 0:22 0:22
FRESNO T1 LOS 1 0:22 0:22
FRESNO T1 BER EXCEEDED 1 0:20 0:20
FRESNO T1 OOF EXCEEDED 2 0:33 0:25
FRESNO SMOKE ALARM 2 2:04:26 2:04:01
FRESNO HALON DISCHARGE 1 0:25 0:25
FRESNO A/C POWER FAIL 2 0:27 0:25
FRESNO GENERATOR RUNNING 1 0:25 0:25
FRESNO GENERATOR FAIL 1 0:23 0:23
FRESNO OFFICE/STATION ALM MODULE FAILURE 3 0:26 0:22
FRESNO INVALID CONTROL COMMAND 2 0:27 0:22
FRESNO LOSS OFBOTH LM INPUTS LEFT SS 1 0:22 0:22
FRESNO LOSS OF DS3 INPUTS LEFT SS 1 0:22 0:22
FRESNO LOSS OF BOTH LM INPUTS RIGHT SS 1 0:20 0:20
FRESNO LOSS OF DS3 INPUTS RIGHT SS 1 0:20 0:20
FRESNO INCOMING LINE1 DS3 FAILURE LEFT S 1 0:20 0:20
HOUSTON SIDE LIGHT 1 26:20 26:20
HOUSTON HUMIDITY 3 24:12:05 23:30:19
HOUSTON MAIN DOOR LEFT OPEN 1 14:57 14:57
HOUSTON RF SW DRIVER ALM "B" RADIO 1 166:18:26 166:18:26
HOUSTON T1 OOF EXCEEDED 2 2:35 2:23
HOUSTON (Undefined) 1 2:42 2:42
HOUSTON (Undefined) 1 17:43 17:43
HOUSTON (Undefined) 1 17:45 17:45
HOUSTON (Undefined) 1 17:45 17:45
HOUSTON Detection of on-line HR monitoring 3 7:12 4:53
HOUSTON Noninsertion of LS unit 3 112:55:43 112:49:49
HOUSTON 6 MHz transmit counter failure 2 112:55:47 112:49:49
HOUSTON Low-speed transmit counter failure 1 112:55:52 112:55:52
HOUSTON Power output down 3 7:12 4:53
HOUSTON Non-insertion of HS XMT unit 3 112:55:43 112:49:49
HOUSTON Non-insertion of HS RCV unit 2 112:55:47 112:49:49
HOUSTON 45 MHz receive counter failure 1 112:55:52 112:55:52
HOUSTON Detection of off-line HS monitor e 1 112:55:52 112:55:52
HOUSTON 6 MHz receive counter failure 3 7:12 4:53
HOUSTON Low speed transmit counter failure 3 112:55:43 112:49:49
HOUSTON Loss of VCOX output clock 2 112:55:47 112:49:49
HOUSTON Detection of off-line LS monitor e 1 112:55:52 112:55:52
HOUSTON Loss of DS1C input signal 3 7:12 4:53
HOUSTON Loss of DS1 input signal 3 112:55:43 112:49:49
HOUSTON Receiving remote alarm in DS1C inp 2 112:55:46 112:49:49
HOUSTON Receiving remote alarmi n DS1 inpu 1 112:55:49 112:55:49

```

```

History Duration Report      Run Date: 8/22/04 10:06 am      Page 1
Start of Interval: 07/30/04 00:00
End of Interval : 08/22/04 10:06
Type: Points Wins: 1-720 Ports: 1-29,RP,IA,K1,K2 Addr: 0-999
Displays: 1-64 Points: 1-64
Alarm Alarm Site Alarm Duration
Date Time Name Description HHH:MM:SS
-/-/- -:-:- 16 CHL ALOG KDA Analog - Channel 9 Minor Und 55:37:35
-/-/- -:-:- 16 CHL ALOG KDA Analog - Channel 9 Major Und 55:37:35
07/30/00 13:04:41 KDA 832 8. 1. 1.10 0:24
07/30/00 13:07:35 KDA 832 8. 1. 1. 2 1:19
07/30/00 13:07:36 KDA 832 8. 1. 1. 5 1:19
07/30/00 13:07:36 KDA 832 8. 1. 1.10 1:19
07/30/00 13:09:13 KDA 832 8. 1. 1. 2 0:21
07/30/00 15:41:43 KDA 832 8. 1. 1. 2 0:41
07/30/00 15:42:07 KDA 832 8. 1. 1. 5 0:18
07/30/00 15:42:07 KDA 832 8. 1. 1.10 0:18
07/30/00 15:42:42 KDA 832 8. 1. 1. 2 0:56
07/30/00 15:45:12 KDA 832 8. 1. 33. 3 0:16
07/30/00 15:45:20 KDA 832 8. 1. 33. 7 0:09
08/01/00 07:37:35 16 CHL ALOG KDA Analog - Channel 9 Minor Ove 0:13
08/01/00 07:37:35 16 CHL ALOG KDA Analog - Channel 9 Major Ove 0:13
08/01/00 07:40:00 16 CHL ALOG KDA Analog - Channel 9 Minor Ove 2:22
08/01/00 07:43:21 16 CHL ALOG KDA Analog - Channel 9 Minor Und 0:09
08/01/00 07:43:31 16 CHL ALOG KDA Analog - Channel 9 Minor Ove 0:14

```

Fig. 20.10 - Example Duration Summary (Time) report to file

## Duration History (Incident)

The Duration History (Incident) report, like the Duration History (time) report, generates a report of the outages in excess of a specified time period sorted by site/alarm. This report is one-half the size of a regular history report because it correlates the alarms and clears — see Figure 20.11.

The Duration History (Incident) report screen is selected from the Report Mode Menu by typing 7. At the prompt you may press F and a enter a file name to save the report to a file, or press P to print.

Duration History (Incident) Run Date: 5/19/00 5:58 pm Page 1				
Start of Interval: 05/01/00 00:00				
End of Interval : 05/19/00 17:57				
Last Scan Time : 05/01/00 00:00				
Minimum Duration : 0:00:00 Windows: 1				
Alarm	Alarm	Site	Alarm	Duration
Date	Time	Name	Description	HHH:MM:SS
05/02/00	15:56:39	31. 40	31. 40. 3. 33	0:00
05/02/00	16:25:12	31. 40	31. 40. 1. 2	0:29
05/03/00	08:16:37	LOS ANGELES	SIDE LIGHT	0:02
05/03/00	08:16:37	LOS ANGELES	TOWER BEACON #1	0:02
05/03/00	08:16:39	LOS ANGELES	RCV SQUELCH ALM "B" RADIO	0:01
05/03/00	08:17:39	LOS ANGELES	SIDE LIGHT	0:03
05/04/00	10:28:09	31. 40	31. 40. 33.33	0:01
05/04/00	14:05:05	LOS ANGELES	SIDE LIGHT	0:02
05/04/00	14:05:05	LOS ANGELES	TOWER BEACON #1	2:48:07
05/04/00	16:45:35	FRESNO	TOWER BEACON	0:12
05/04/00	16:53:25	LOS ANGELES	Alarm Point 2	0:02
05/04/00	16:53:27	LOS ANGELES	Alarm Point 1	0:01
05/04/00	18:26:41		KDA FAILURE FOR DENVER	9:09
05/04/00	18:26:43		KDA FAILURE FOR BOSTON	9:07
05/04/00	18:26:53		MAT FAILURE FOR SLOT 1 L.A.	8:48
05/04/00	18:26:55		MAT FAILURE FOR SLOT 2 L.A.	8:47
05/04/00	18:27:00		MAT FAILURE FOR SLOT 3 L.A.	8:43
05/04/00	18:27:09		MAT FAILURE FOR SLOT 4 MCI L.A.	8:36
05/04/00	18:27:11		KDA FAILURE FOR FRESNO	8:35
05/04/00	18:27:16		LR24 FAILURE FOR FRESNO	8:31
05/04/00	18:27:18		KDA FAILURE FOR HOUSTON	8:30
05/04/00	18:27:25		DEVICE FAILURE FOR ADDRESS 2.6	8:24
05/04/00	18:58:08		DEVICE FAILURE FOR ADDRESS 2.6	1:52
05/04/00	18:58:10		KDA FAILURE FOR DENVER	2:11
05/04/00	19:04:07		KDA FAILURE FOR FRESNO	2:23
05/04/00	19:04:09		LR24 FAILURE FOR FRESNO	2:21
05/04/00	19:04:13		KDA FAILURE FOR HOUSTON	2:15
05/04/00	19:04:21		KDA FAILURE FOR BOSTON	2:09
05/04/00	19:04:28		MAT FAILURE FOR SLOT 1 L.A.	2:25
05/04/00	19:04:30		MAT FAILURE FOR SLOT 2 L.A.	1:58
05/04/00	19:04:35		MAT FAILURE FOR SLOT 3 L.A.	1:56
05/04/00	19:04:45		MAT FAILURE FOR SLOT 4 MCI L.A.	2:09
05/04/00	19:05:01		DEVICE FAILURE FOR ADDRESS 2.6	1:33
05/04/00	19:05:06		KDA FAILURE FOR DENVER	1:25
05/08/00	16:30:58	31. 40	31. 40. 33.33	0:01
05/08/00	16:31:06	LOS ANGELES	POWER UP	0:03
05/08/00	16:35:08	31. 40	31. 40. 33.33	0:00
05/08/00	17:05:16		LR24 FAILURE FOR FRESNO	0:36
05/08/00	17:05:22		KDA FAILURE FOR FRESNO	0:31
05/09/00	11:35:32		MAT FAILURE FOR SLOT 4 MCI L.A.	0:27
05/09/00	11:35:34		KDA FAILURE FOR FRESNO	0:26
05/09/00	11:41:19	FRESNO	AC POWER	0:09
05/09/00	11:41:19	FRESNO	TOWER BEACON	0:09
05/09/00	16:00:21	CELL 75	INTRUSION ALARM	3:15
05/09/00	16:03:48	CELL 75	INTRUSION ALARM	0:14
05/09/00	16:06:18	CELL 75	INTRUSION ALARM	0:09
05/09/00	16:06:32	CELL 75	INTRUSION ALARM	51:54
05/09/00	16:58:42	CELL 75	INTRUSION ALARM	1:47
05/09/00	17:00:37	CELL 75	INTRUSION ALARM	26:06
05/09/00	17:21:35	CELL 75	INTRUSION ALARM	3:07
05/09/00	17:26:09	CELL 75	INTRUSION ALARM	0:23
05/09/00	17:26:51	CELL 75	INTRUSION ALARM	31:51

Fig. 20.11 - Example Duration History (Incident) report to file

## Duration Summary (Incident)

The Duration History (Incident) report generates a report of the total time and maximum time of outages sorted by alarm/site — see Figure 20.12.

The Duration History report screen is selected from the Report Mode Menu. Type 8 and press Enter. At the prompt, select the output destination — press F to save to a file and enter the file name, or press P to send the report to your printer.

Duration Summary (Incident)		Run Date: 5/19/00 5:58 pm	Page 1
Start of Interval: 05/01/00 00:00			
End of Interval : 05/19/00 17:58			
Last Scan Time : 05/01/00 00:00			
Windows: 1			
Site	Alarm	TotalTime	MaxTime
Name	Description	Count	HHH:MM:SS
FRESNO	TOWER BEACON	4	0:36
FRESNO	AC POWER	3	1:00
FRESNO	TECH ON SITE	1	0:05
FRESNO	DOOR ALARM	2	0:49
FRESNO	LOW BATTERY	1	0:04
FRESNO	RF SW DRIVER ALM "B" RADIO	2	0:50
FRESNO	BB SW/XCVR CONT ALM "B" RADIO	1	0:02
FRESNO	FUSE SHELF 103.10	2	0:48
FRESNO	T1 OOF EXCEEDED	1	0:08
FRESNO	OFFICE/STATION ALM MODULE FAILURE	1	0:01
HOUSTON	TOWER BEACON #1	3	0:38
HOUSTON	T1 OOF EXCEEDED	1	0:12
DENVER	(Undefined)	1	0:13
DENVER	TOWER BEACON #1	1	0:13
DENVER	SIDE LIGHT	1	0:17
DENVER	RECTIFIER 1	1	0:02
LOS ANGELES	TOWER BEACON #1	2	2:48:09
LOS ANGELES	SIDE LIGHT	3	0:07
LOS ANGELES	RCV SQUELCH ALM "B" RADIO	1	0:01
LOS ANGELES	Alarm Point 1	2	24:47:10
LOS ANGELES	Alarm Point 2	1	0:02
LOS ANGELES	PANIC ALARM	1	0:48
LOS ANGELES	DOOR OPEN	2	1:41
LOS ANGELES	POWER UP	4	0:19
LOS ANGELES	ILLEGAL ENTRY	3	3:44
CELL 75	INTRUSION ALARM	12	8:43
CELL 75	CONTROLLER SHELF POWER CONVERTER A3	3	3:17
31. 40	31. 40. 1. 2	1	0:29
31. 40	31. 40.33.33	4	0:02
	KDA FAILURE FOR FRESNO	5	12:32
	LR24 FAILURE FOR FRESNO	3	11:28
	KDA FAILURE FOR HOUSTON	3	11:18
	KDA FAILURE FOR DENVER	3	12:45
	KDA FAILURE FOR BOSTON	2	11:16
	MAT FAILURE FOR SLOT 1 L.A.	2	11:13
	MAT FAILURE FOR SLOT 2 L.A.	2	10:45
	MAT FAILURE FOR SLOT 3 L.A.	3	11:28
	MAT FAILURE FOR SLOT 4 MCI L.A.	4	11:53
	DEVICE FAILURE FOR ADDRESS 2.6	4	12:12

Fig. 19.12 - Example Duration Summary (Incident) report

## Duration Detail (Incident)

The Duration Detail (Incident) allows reports to be filtered by alarm description text and site name text — see Figure 20.13.

The Duration Detail (Incident) report screen is selected from the Report Mode Menu. Type 9 and press Enter. At the prompt, select the output destination — press F to save to a file and enter the file name, or press P to send the report to your printer.

Duration Detail (Incident)			Run Date: 5/19/00 5:59 pm		Page 1	
Start of Interval: 05/01/00 00:00						
End of Interval : 05/19/00 17:59						
Last Scan Time : 05/01/00 00:00						
Minimum Duration : 0:00:00 Windows: 1						
Desc Text To Include : ALARM						
Desc Text To Exclude : CLEAR						
Site Text To Include :						
Site Text To Exclude :						
Alarm	Alarm	Site	Alarm	Duration		
Date	Time	Name	Description	HHH:MM:SS		
05/04/00	16:53:25	LOS ANGELES	Alarm Point 2	0:02		
05/04/00	16:53:27	LOS ANGELES	Alarm Point 1	0:01		
05/09/00	16:00:21	CELL 75	INTRUSION ALARM	3:15		
05/09/00	16:03:48	CELL 75	INTRUSION ALARM	0:14		
05/09/00	16:06:18	CELL 75	INTRUSION ALARM	0:09		
05/09/00	16:58:42	CELL 75	INTRUSION ALARM	1:47		
05/09/00	17:00:37	CELL 75	INTRUSION ALARM	26:06		
05/09/00	17:21:35	CELL 75	INTRUSION ALARM	3:07		
05/09/00	17:26:09	CELL 75	INTRUSION ALARM	0:23		
05/09/00	17:26:51	CELL 75	INTRUSION ALARM	31:51		
05/09/00	17:58:50	CELL 75	INTRUSION ALARM	0:31		
05/09/00	17:59:27	CELL 75	INTRUSION ALARM	0:31		
05/09/00	18:00:25	CELL 75	INTRUSION ALARM	0:31		
05/09/00	18:08:39	CELL 75	INTRUSION ALARM	0:38		
05/09/00	18:32:09	CELL 75	CONTROLLER SHELF POWER CONVERTER A	0:51		
05/09/00	18:33:03	CELL 75	CONTROLLER SHELF POWER CONVERTER A	0:43		
05/09/00	18:33:51	CELL 75	CONTROLLER SHELF POWER CONVERTER A	1:43		
05/10/00	14:29:48	CELL 75	INTRUSION ALARM	0:05		
05/10/00	14:31:20	CELL 75	INTRUSION ALARM	0:05		
05/10/00	14:31:28	CELL 75	INTRUSION ALARM	0:39		
05/10/00	14:32:14	CELL 75	INTRUSION ALARM	0:04		
05/10/00	14:32:20	CELL 75	INTRUSION ALARM	1:27		
05/10/00	14:34:10	CELL 75	INTRUSION ALARM	0:24		
05/10/00	14:34:51	CELL 75	INTRUSION ALARM	0:19		
05/10/00	14:35:50	CELL 75	INTRUSION ALARM	1:27		
05/10/00	14:38:28	CELL 75	INTRUSION ALARM	0:31		
05/10/00	14:39:20	CELL 75	INTRUSION ALARM	0:12		
05/11/00	11:43:38	LOS ANGELES	PANIC ALARM	0:48		
05/14/00	09:57:33	LOS ANGELES	Alarm Point 1	24:47:09		
05/15/00	10:06:13	FRESNO	DOOR ALARM	0:44		
05/15/00	10:08:21	FRESNO	DOOR ALARM	0:05		
05/15/00	10:44:07	DENVER	DOOR ALARM	-:-		
History Report Ended : May 19,2000 17:59:31						

Fig. 20.13 - Example Duration Detail (Incident) report

## Dial-Up History Report

Dialup history events have been added to the Standard History report to give the user visibility to dial-up exceptions due to POTS connectivity (for example, No Dial tone, No Carrier, Busy) or mis-configuration (Incorrect Site Number, Site Offline). The new dial-up history events apply to both TRIP and ASCII dial-up connections. A filter has also been added to the Standard History reports to allow the option of displaying only these dial-up events.

You can run the Standard History report from the Main Menu by selecting Reports->Standard History. Figure 20.14 shows an example of a Standard History report with no filters activated. The report contains two TRIP history events (of type TRP) along with several alarm events.

View Report File									
NG 115			Not Acknowledged						ALM
NG.115.	2.20		02/28/03 14:46:31	F D	<Undefined>				
NG 115			Not Acknowledged						ALM
Standard History			Run Date: 2/28/03 2:49 pm					Page 7	
Item			Alarm date/time	S L	Description				
Site			Ack date/time	T U	Aux/Disp Desc	Initials		Status	
NG.115			02/28/03 14:46:58	TRP	Call Aborted:NO DIAL TONE				
NG 115					CallType:User				
NG.115.	3. 1		02/28/03 14:48:47	F C	Analog - Channel 1	1	Minor	Under	
NG 115			Not Acknowledged					ALM	
NG.115.	3. 3		02/28/03 14:48:48	F B	Analog - Channel 1	1	Major	Under	
NG 115			Not Acknowledged					ALM	
NG.115			02/28/03 14:48:49	TRP	Call Aborted:TIMEOUT				
NG 115					CallType:User				
[USER]			02/28/03 14:48:53		[EXIT MONITOR MODE]				
							DPS		
IA. 0.	1. 7		02/28/03 14:48:57	F D	IAM OFFLINE				
			Not Acknowledged					ALM	
History Report Ended : Feb 28,2003 14:49:36									
File : HIST.REP		Size: 25036		Date/Time: Feb 28,2003 14:49:36					
F2=File, F3=Search, Home/F5=Top, End/F6=Bottom, F9=Help, F10/Esc=Exit									

Fig. 20.14 - History report with no filters activated

**Note:** The Type can be either TRP to indicate that this event occurred on a TRIP port, or ASC to indicate that this event occurred on an ASCII port.

Dialup Events: There are essentially 3 types of dial-up events

1. **CALLED REMOTE** : T/MonXM has successfully dialed out and connected to the remote. It is still possible for the call to be aborted after this point; this just means the connection was successful.
2. **RECEIVED CALL** : T/MonXM has successfully connected to a remote which has called in. It is still possible for the call to be aborted after this point, this just means the connection was successful.
3. **CALL ABORTED** : The call has been aborted due to one of the following reasons:
  - **Pre-Connection:** The following events can occur only **before** T/MonXM has successfully connected with the remote due to reasons of POTS connectivity.

- a. NO PHONE NUMBER : T/MonXM has no phone number defined for the remote.
- b. LINE BUSY : The phone line was busy.
- c. NO DIAL TONE : The phone line had no dial tone.
- d. NO ANSWER : The remote did not reply to T/MonXM's connection attempt.
- e. NO CARRIER : The phone line had no carrier.
- Post-Connection: The following events can occur only *after* T/MonXM has successfully connected with the remote.
  - f. TIMEOUT : The remote did not respond to one of T/MonXM's queries soon enough.
  - g. DID NOT RECEIVE QUERY : The remote did not query T/MonXM for its information.
  - h. NO DIAL PORT : T/MonXM does not have a dial-up port setup for the remote that is dialing in.
  - i. BASE UNIT MISMATCH : The remote calling in is not the same type as the remote databased for that port.
  - j. SITE OFFLINE : The remote dialing in is set as OFFLINE in T/MonXM.
  - k. SITE UNDEFINED : The site number given to T/MonXM by the remote did not match the site number databased for that device locally.
  - l. SITE NUMBER EXPECTED : T/MonXM did not expect to receive a site number from the remote at this time.

The Trip/ASCII Dialup Filter enables the user to run the Standard History Report and include only the dial-up history events. In order to use this filter the Type field must be set to D for Trip/Ascii Dialup — see Figure 20.15.



Fig. 20.15 - Setting the Trip/Ascii Dialup Filter

Figure 20.16 below shows a Standard History report filtered by the Trip/Ascii Dialup Filter. It is the same report as the unfiltered report shown in Figure 20.14, but with only dial-up history events displayed.

```

View Report File
Standard History                      Run Date:  2/28/03   2:50 pm                Page 1
Start of Interval: 02/28/03   00:00
End of Interval   : 02/28/03   14:50
Type: Trip/Ascii Dialup   Windows: 1-720
Ports: 1-500,RP,IA,K1,K2,NG,N2   Addresses: 0-999
Displays: 1-99   Points: 1-64

Item      Alarm date/time   S L Description              Initials   Status
Site      Ack date/time     T U Aux/Disp Desc
NG.115    02/28/03 14:46:58 TRP Call Aborted:NO DIAL TONE
NG 115                                CallType:User
NG.115    02/28/03 14:48:49 TRP Call Aborted:TIMEOUT
NG 115                                CallType:User
History Report Ended : Feb 28,2003 14:50:35

File : HIST1.REP      Size: 706      Date/Time: Feb 28,2003 14:50:34
F2=File, F3=Search, Home/F5=Top, End/F6=Bottom, F9=Help, F10/Esc=Exit

```

Fig. 20.16 - Standard History report filtered by TRIP/ASCII Dialup Filter

## Alarm Database Report

Provides users with a hard copy of your various database elements.

The Alarm Database Reports offer many different reports based on your database files. When Alarm Database is selected from the Report menu (press 2 and then Enter), a Report Alarm Menu (see Figure 20.17) will appear with all of the available reports.

Reports are useful items when databasing or reviewing your network.

This menu will vary depending on the modules you have installed.

```

Report Alarm Menu
Report # : ..

1. Remote Ports      11. Cards              21. Trouble Log By Date/Time
2. Windows           12. Dial Up Sites    22. Export To NEdit
3. Text/Messages     13. Kda Shelves      23. SNMP SET Commands
4. Ascii Rules        14. NetGuardians     24. SNMP GET Commands
5. Ascii Tables       15. Export Alarms
6. Ascii Actions      16. Export Devices
7. Derived            17. Export Ports
8. VDMs              18. Export KDA Shelves
9. Site Reports       19. Trap Associations
10. BSU               20. Trouble Log By Point

```

Fig. 20.17 - Report alarm menu

### 1. Remote Ports

Prints a report of all or a range of remote ports defined in the system. These reports reproduce the Port Parameters screen for the specified port(s). Several options can be selected to customize the report.



**Fig. 20.18 - Remote ports menu**

**Table 20.4 - Fields in the Remote Ports Report window**

Field	Description
Remote Ports	Enter the range of ports (1-500, 1A) desired in the report. [1-500, 1A]
Detail Level	Enter the detail level desired in the report. [1] Valid entries are: 1 (Minimum) Port information only 2 (Moderate) Port information and address 3 (Maximum) Port information, address, point and provisioning info
Address Range	Enter the range of addresses desired in the report. [0-999]
Display Range	Enter the range of displays desired in the report. [1-64] <b>Note:</b> Address and Display ranges interact to select a group that contains only the specified displays within the specified addresses. i.e.: A report for addresses 1 & 2, display 4 includes only display 4 at address 1 and display 4 at address 2. Address 1, displays 1-3 and 5-up are not included. Address 2, displays 1-3 and 5-up are not included. All other displays from all other addresses are not included.
Window Range (Detail Level 3 only)	Enter the range of windows desired in the report.
Min Severity (Detail Level 3 only)	Enter severity levels desired in the report. Choices are: A (Critical alarms only) B (Critical and Major) C (Critical, Major, and Minor) D (Critical, Major, Minor and Status)
Show No Log (Detail Level 3 only)	Choose if No Log points will be included in report. Choice are Y (yes) and N (no).

**Table 20.5 - Key commands available in the Remote Ports Report window**

Function Key	Description
F10	Exit
Up Arrow	Go back to previous field.



```

Remote Port Report                               Page 1
Ports : 1-29   Add: 0-999   Disp: 1-64   Det: 3

Port 1 DCP(F) INTERROGATOR
  Baud      : 1200
  Parity    : NONE
  Word Length : 8
  Stop Bits  : 1
  Time out   : 1000
  Poll Delay : 0
  DCPF Mode  : Y
  Poll Mode  : Master
  Warning Threshold: 65
  Switch Threshold: 70
  Fail Poll Cycles : 20
  Dcd Check on Rcv : N
  Immediate Retries: 1
  RTS Lead Time : 0
  RTS Tail Time : 0

-----
Remote Port Report                               Page 2
Ports : 1-29   Add: 0-999   Disp: 1-64   Det: 3
  Address   : 3   Desc : Small Hut at 1st and Oak St
  Poll Displays : 1,2,3,4,5,33
  Poll Type  : Upset
  Refresh    : 100
  Log Undefined : NO
  — Address Defaults —
  Description : (Undefined)
  Windows     : 66   Message : 0
  Polarity    : B Log : L Hst : H Lev : A Sts : A Rvs : N
  Display     : 1   Display Description :
  P L H L S R Description          Fail Clear
  o o s e t v Windows             Msg Qual
  Pt l g t v s s AUX Description
  1 B L H A A N FIRST POINT      A   C
    2,5          1   0

```

**Fig. 20.19 - Example remote port report to file**

## 2. Windows

Prints a report (see Figure 20.20) of all window names and indexes as currently defined.

```

Window Report                               Page 1
Report generated on 2/2/01 at 1:46pm by DPS
Window  Name      Description
-----
1    ALL ALARMS    All alarms go into window 1
2    IPLS - NCC    INDIANAPOLIS NCC
3    IPLS - IUPUI  INDIANAPOLIS IUPUI
4    IPLS - 1 CALL INDIANAPOLIS ONE CALL
5    IPLS - SPRINT SPRINT - DAVIDSON ST.
6    IPLS - CNI    INDIANAPOLIS CNI
7    IPLS - MCI    INDIANAPOLIS MCI
8    IPLS - SOB    INDIANAPOLIS STATE OFF. BLDG.

```

**Fig. 20.20 - Example window report to file**

## 3. Text/Messages

Prints a report (see Figure 20.21) of all the standard text/messages that were defined in the system.

```

Text/Messages Definition Report             Page 1
Msg: 1
  IPLS-NCC
  FIRE 111-1111
  POLICE 222-2222
  EQ MAINT 333-333-3333
Msg: 3
  *****      WARNING!      *****
  BATTERIES AT THIS SITE WILL FAIL IN 1 HOUR.
  DISPATCH GENERATOR NOW!!!!!!
  *****      WARNING!      *****
Msg: 24
  One or more working channels have failed and
  have not been switched to standby.
  NEC SWC
Msg: 28
  EXERCISER TEST CIRCUIT HAS DETECTED A FAULT.
  NEC SWC
Msg: 32
  Emergency override function of O-LTM equipment
  has been used to perform switching of one or
  more channels (O-LTM EOVS switch is on).
  NEC SWC

```

**Fig. 20.21 - Example text /message report to file**

**4, 5, 6. ASCII Rules, Tables and Actions**

Prints reports of all ASCII rules, tables or actions that were defined or took place in the system — see Figure 20.22.

```

ASCII Rule Report                      Page 1
Report generated on 11/05/04 at 10:31am by DPS

Device           : AQL                      HEADER
Description      : Device Header for AQL devices
Soft Separators  : <SPC>    <CR>
Hard Separators  :
Line Terminator  : 0A Hex    <LF>

Log On          : logon cbh;<CR>
CMD1            : AUTO ALARM ON;<CR>
CMD2            :
CMD3            :
```

**Fig. 20.22 - Example ASCII Rules report to file**

**7. Derived**

Prints a report (see Figure 20.23) of all derived definitions as currently defined.

```

Derived Report                      Page 1
Report generated on 3/27/01 at 6:11pm by DPS

Derived Number : 0001
Description    : FRESNO - Both rectifiers @ site failed.
Set Qualification Delay : 0 Secs  Clr Qualification Delay : 0 Secs

----- TERM MATRIX -----
L 1.1.1.2      L 1.1.1.32

Soft Alarm    : 11.5.1
```

**Fig. 20.23 - Example Derived report to file**

## 8. VDMs

Only available if the Voltage Detector Module is installed.

Generated reports include analog values for VDM devices. Refer to Figure 20.24 for example report.

```
VDM Report                               Page 1
Report generated on 11/05/04 at 1:31pm by DPS

Derived Number : 0001
Description   : FRESNO - Both rectifiers @ site failed.
Set Qualification Delay : 0 Secs   Clr Qualification Delay : 0 Secs

----- TERM MATRIX -----
L 1.1.1.2      L 1.1.1.32

Soft Alarm   : 11.5.1
```

**Fig. 20.24 - Example VDM report to file**

## 9. Site Reports

Prints a report (see Figure 20.27) giving a list of the remote devices and descriptions for the ports or sites specified. They are intended to give a list of the equipment on any port in the network.

Upon selecting this report two more selections will become available in the window:

1. Sites by Address (Numerically sorted by port and address.) — see Figures 20.26 and 20.27.
2. Sites by Site. (Alphabetically sorted by name.) — see Figures 20.28 and 20.29.



**Fig. 20.25 - The site reports window presents a menu**

**Sites By Address**

Remote Ports : 1-29,RP...

Address range:

Enter ports or range of ports (1-29,RP)

**Fig. 20.26 - Sites by address report window****Table 20.6 - Fields in the Sites by Address Report window**

Field	Description
Remote Ports	Enter the range of ports (1-29 or RP) desired on the report. [1-29]
Address Range	Enter the range of addresses desired on the report. [0-999]

Site Report (By Address)				Page 1
Ports : 1-29,RP    Add: 0-999				
Port	Addr	Site Name	Description	Dev/Unt
<hr/>				
1	3	DEL MAR	Small Hut at 1st and Oak St	
1	4	BEAR MT	Repeater on Bear Mt.	
5	2	COLD CREEK	Repeater site alarms	MAT
5	121	DPS	test sbc carrier	MAT
5	122	MADERA MAIN	Central Repeater Alarms	MAT
5	1	COLD CREEK	Repeater Controls	CPM
5	2	YALE	BAU	SBP
5	121	MADERA MAIN	Downtown Center Door Alarms	SBP
11	N/A	PORT	test for 4 port scanner	
RP	2		ASC	
RP	105	PACKING SHED #1	WEST ALLUVIAL PACKING SHED #1	ALP
RP	106	PACKING SHED #2	EAST ALLUVIAL PACKING SHED #2	DPM
RP	801	TNDS #1	FTS-2K	ASC

**Fig. 20.27 - Example sites by address report to file**

Sites By Site	
Remote Ports :	1-29,RP
Start Site :	.....
End Site :	
Enter starting site	

Fig. 20.28 - Sites by site report window

Table 20.7 - Fields in the Sites by Site Report window

Field	Description
Remote Ports	Enter the range of ports (1-29 or RP) desired on the report. [1-29]
Starting Site Ending Site	Enter the site names for the starting and ending range of sites to print on the report.

Table 20.8 - Key commands available in the Site report, Sites by Site Report window

Function Key	Description
F10	Exit
Up Arrow	Go back to previous field.

```

Site Report (By Site)                                Page 1

Ports : 1-29,RP      Start: COLD CREEK      End: ZZZZZZZZZZZZZZZZ

Port Addr Site Name  Description                      Dev/Unt
-----
5 2 COLD CREEK  Repeater site alarms          MAT
5 1 COLD CREEK  Repeater Controls             CPM
1 3 DEL MAR     Small Hut at 1st and Oak St
5 121 DPS       test sbc carrier             MAT
5 122 MADERA MAIN  Central Repeater Alarms       MAT
5 121 MADERA MAIN  Downtown Center Door Alarms   SBP
RP 105 PACKING SHED #1 WEST ALLUVIAL PACKING SHED #1    ALP
RP 106 PACKING SHED #2 EAST ALLUVIAL PACKING SHED #2    DPM
11 N/A PORT     test for 4 port scanner
RP 801 TNDS #1 FTS-2K          ASC
5 2 YALE       bau                SBP

```

Fig. 20.29 - Example sites by site report to file

**10. BSU**

Prints a report (see Figure 20.30) of all BSU definitions as currently defined.

```

BSU Report                               Page 1
Report generated on 3/28/03 at 11:21am by DPS

Window : 8   Name : POWER   Desc : LINE AC FAILURE
Port   Addr  Disp  Pnt Type
-----
Critical (A) 1   1   1   3   DCPF
Major (B)    1   1   1   4   DCPF
Minor (C)    1   1   1   5   DCPF
Sanity       1   1   1   6   DCPF

```

**Fig. 20.30 - Example BSU report to file**

**11. Cards**

Prints a report (see Figure 20.31) of all card definitions as currently defined.

```

Card Report                               Page 1
Report generated on 3/28/03 at 11:22am by DPS

Part #   Description      Address
-----
D-PC-600-00 232 ports      1
D-PC-600-00 232 ports      2
D-PC-602-00 Modular ports  3

```

**Fig. 20.31 - Example cards report to file**

## 12. Dial-Up Sites

View all your dial-up remotes from the Dial Up Sites screen, as shown in Figure 20.32.

**Dial Up Sites**

```

Site type      : KDA
Starting Site: 1
Ending Site: 6
Show Devices   : Y      Show Points:  Y   Show No-Log:  Y
Show Prov      : Y
  
```

**Include provisioning detail report (Y/N) ?**

**Fig. 20.32 - Dial-up sites window**

**Table 20.9 - Fields in the Dial-Up Sites Report window**

Field	Description
Site type	Enter the equipment type desired on the report. Report will include only those locations that use the specified device. Valid entries are: 2 = DPM 3 = DLK (Datalok) 4 = KDA 5 = ALP 12 = Netdog 6 = ASC 8 = KDS-TS 9 = KDA 832 Enter (leave blank) = All. [All]
Starting Site Ending Site	Enter the site names for the starting and ending range of sites to print on the report. Sites will be reported in alphabetical order.
Show Devices	Include device detail report? (Y/N)
Show Points	Include point detail report? (Y/N)
Show No-Log	Include no log points? (Y/N)
Show Prov	Include provisioning detail report? (Y/N)

**Table 20.10 - Key commands available in the Site Report, Dial Up Sites Report window**

Function Key	Description
F10	Exit
Up Arrow	Go back to previous field.



```

Dial Up Sites                               Page 1
Report generated on 5/8/04 at 4:52pm by DPS
Select Device : KDA Start Site: 1   End Site: 100
*****
Device type   : KDA
Site Name    : 1
Description   : DEL MAR HUT (OAK ST)
Remote Site Phone : 222344444
Polling Type  : SCHEDULE
Scheduled Days-- SUN: N MON: Y TUE: Y WED: Y THU: Y FRI: Y SAT: N
Scheduled Hours : 5,8,12,15,18,22
Scheduled Minute : 30
Output modem chan : 7

Description   : Small hut at 1st and Oak St
Site Name    : DEL MAR
Virtual Address : 1
Primary Port  : 1
Primary Address : 3
Log Undefined : YES
--- Address Defaults ---
Polarity     : B Log : L Hst : H Lev : A Sts : A Rvs : N
Description   : (Undefined)
Windows      :      Message : 0

Addr :   1 Display :   1

P L H L S R Description      Fail  Clear
o o s e t v Windows      Msg Qual
Pt l g t v s s AUX Description

1 B L H A A N DOOR          OPEN  CLOSED
   5                1  12
2 B L H A A N MAIN POWER      OFF  ON
   7                2  0

```

Fig. 20.33 - Example dial-up sites report to file

```

                                Kda Shelves

Starting Site: 1
Ending   Site: 6
Show Devices : Y      Show Points:  Y   Show No-Log: Y
Show Prov   : Y

Include provisioning detail report (Y/N) ?

```

Fig. 20.34 - KDA shelves window

### 13. KDA Shelves

This option gives you all the information associated with KDA setup.

**Table 20.11 - Fields in the KDA Shelves Report window**

Field	Description
Starting Site Ending Site	Enter the site names for the starting and ending range of sites to print on the report. Sites will be reported in alphabetical order.
Show Devices	Include device detail report? (Y/N)
Show Points	Include point detail report? (Y/N)
Show No-Log	Include no log points? (Y/N)
Show Prov	Include provisioning detail report? (Y/N)

### 14. Export Alarms

This report is similar to the Export History and Export Analogs Reports (preparing a file with delineating commas) suitable for import into a spread sheet — refer to Figure 20.36. The report lists the alarms occurring within the specified parameters.

**Export Alarms**

Remote Ports : 1-24

Address range: 0-999

Display range: 1-64

Window range : 1-720

Min Severity : D

Show No-Log : Y

Include No-Log points (Y/N)

**Fig. 20.35 - Export alarms window**

**Table 20.12 - Fields in the Export Alarms Report window**

Field	Description
Remote Ports	Enter ports or range (1-n, 1A)
Address Range	Enter address range (0-999)
Display Range	Enter display range (1-64)
Window Range	Enter window range (1-720)
Min Severity	Enter severity levels: A = Critical B = Critical and Major C = Critical, Major and Minor D = Critical, Major, Minor and Status
Show No-Log	Include no log points? (Y/N)

```

Remote Port Export Alarm Report Ports : 6 Add: 0-999  Disp: 1-64
Port,Addr,Disp,Point,Pol,Log,Hist,Lev,Status,Rvs,Descrip,AuxDescrip,FailStat,
ClearStat,Windows,Msg,QualDelay
6,1,1,1,B,L,H,A,A,N,IT A 1,,ALARM,CLEAR,,0,0
6,1,1,2,B,L,H,A,A,N,IT A 2,,ALARM,CLEAR,,0,0
6,1,1,3,B,L,H,A,A,N,IT A 3,,ALARM,CLEAR,,0,0
6,1,1,4,B,L,H,A,A,N,IT A 4,,ALARM,CLEAR,,0,0
6,1,1,5,B,L,H,A,A,N,IT A 5,,ALARM,CLEAR,,0,0
6,1,1,6,B,L,H,A,A,N,IT A 6,,ALARM,CLEAR,,0,0
6,1,1,7,B,L,H,A,A,N,IT A 7,,ALARM,CLEAR,,0,0
6,1,1,8,B,L,H,A,A,N,IT A 8,,ALARM,CLEAR,,0,0
6,1,1,9,B,L,H,A,A,N,IT A 9,,ALARM,CLEAR,,0,0
6,1,1,10,B,L,H,A,A,N,IT A 10,,ALARM,CLEAR,,0,0
6,1,1,11,B,L,H,A,A,N,IT A 11,,ALARM,CLEAR,,0,0
6,1,1,12,B,L,H,A,A,N,IT A 12,,ALARM,CLEAR,,0,0
6,1,1,13,B,L,H,A,A,N,IT A 13,,ALARM,CLEAR,,0,0
6,1,1,14,B,L,H,A,A,N,IT A 14,,ALARM,CLEAR,,0,0
6,1,1,15,B,L,H,A,A,N,IT A 15,,ALARM,CLEAR,,0,0
6,1,1,16,B,L,H,A,A,N,IT A 16,,ALARM,CLEAR,,0,0
6,1,1,17,B,L,H,A,A,N,IT A 17,,ALARM,CLEAR,,0,0
6,1,1,18,B,L,H,A,A,N,IT A 18,,ALARM,CLEAR,,0,0
6,1,1,19,B,L,H,A,A,N,IT A 19,,ALARM,CLEAR,,0,0
6,1,1,20,B,L,H,A,A,N,IT A 20,,ALARM,CLEAR,,0,0
6,1,1,21,B,L,H,A,A,N,IT A 21,,ALARM,CLEAR,,0,0
6,1,1,22,B,L,H,A,A,N,IT A 22,,ALARM,CLEAR,,0,0
6,1,1,23,B,L,H,A,A,N,IT A 23,,ALARM,CLEAR,,0,0
6,1,1,24,B,L,H,A,A,N,IT A 24,,ALARM,CLEAR,,0,0
6,1,1,25,B,L,H,A,A,N,IT A 25,,ALARM,CLEAR,,0,0
6,1,1,26,B,L,H,A,A,N,IT A 26,,ALARM,CLEAR,,0,0
6,1,1,27,B,L,H,A,A,N,IT A 27,,ALARM,CLEAR,,0,0
6,1,1,28,B,L,H,A,A,N,IT A 28,,ALARM,CLEAR,,0,0
6,1,1,29,B,L,H,A,A,N,IT A 29,,ALARM,CLEAR,,0,0
6,1,1,30,B,L,H,A,A,N,IT A 30,,ALARM,CLEAR,,0,0

```

**Fig. 20.36 - Example export alarms report to file**

### 15. Export To NGEEdit

This report allows the user to export the base alarms for a single NetGuardian into NGEEdit. To do this the user must first define a NetGuardian device in TMon, along with its Base alarm points (Figure 20.37), and then run this report against the device. Only the base alarms will be exported because NGEEdit automatically defines the System alarms when the device is created. The Tmon formats the report in a TAB delimited format which NGEEdit can parse and use to auto-populate its base alarm points for the currently loaded device.

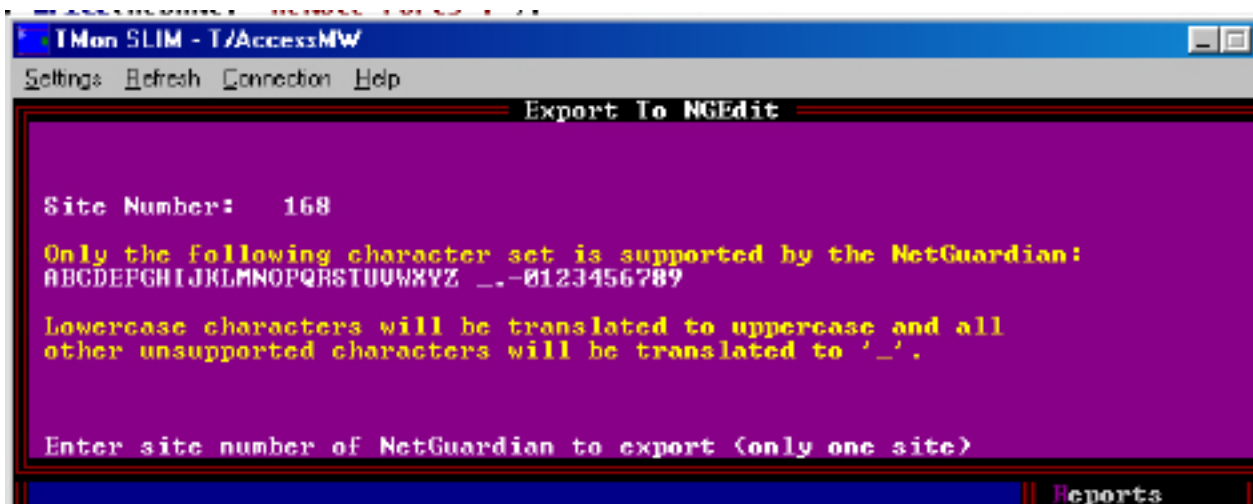


Fig. 20.37 -Export to NGEEdit window

Table 20.13 - Fields in the Export to NGEEdit window.

Field	Description
Site Number	Enter the site number of the NetGuardian to Export. Only one site can be exported per report.



## Site Controls Report

Site Controls reports are site oriented, so they are done by site and group — see Figure 20.40.

**Note:** Site controls will be linked to a specific window.

**Site Controls**

Site Numbers : 1-720.....  
Control Groups :

Enter range of Control Sites

**Fig. 20.40 - Site controls report window**

**Table 20.16 - Fields in the Site Controls Report window**

Field	Description
Site Numbers	Enter the range of control sites (1-720) desired. [1-720]
Control Groups	Enter the range of control groups (1-40) desired. [1-40]

**Table 20.17 - Key commands available in the Site Controls Report window**

Function Key	Description
F10	Exit
Up Arrow	Go back to previous field.

## LED Bars Report

There is no input window for this report. To run it select 5 from the Report Mode Menu and press Enter. It runs as soon as you select printer or file and a file name. This report is available only if the LED Display Bar Module is installed. Refer to Appendix K (LED Display Bar).

LED Bar Report		Page 1
Report generated on 3/28/95 at 11:30am by DPS		
LED Bar Alm		
Address Win	Description	
1 2	CRITICAL ALARMS	
2 8	POWER ALARMS	
3 10	SECURITY BREACH	

**Fig. 20.41 - Example led bar report to file**

## Users Report

The Users Report is useful for system administration to keep track of all users' privileges. There is no input window for this report. To run it select 6 from the Report Mode Menu and press Enter. It runs as soon as you select printer or file and a file name. The Users option prints a report of all system users and their authorization levels. The password field is left blank for security reasons. Refer to Section 7 (Managing System Users) for more information.

```

System Users Report                      Page 1
Report generated on 2/2/00 at 2:03pm by DPS
Initials : DPS  Name : T/MonXM Default User Id
Password : ***** Title :
Control Group Mask : 1-25
View Alm Windows : 1-49
Ack Alm Windows : 1-49
Alarm Ack Level : ALL ALARMS
Site Controls :
Modem Logon Access : YES
Modem Call Back :
Diagnostics : YES
Run Reports : YES
File Maintenance : YES
Edit Parameters : YES
System Operator : YES
Start Chat : YES
Device On/Off Line : YES
Exit Monitor Mode : YES
Bldg Manual Logout : YES
Configure Remotes : YES
Craft Mode : YES
Init Stats : YES
Trouble Log : MODIFY
Auto Log Off : 0
Id Number : 123
Pager Edit/Lock : YES
Site Stats : YES
Dial Up Stats : YES

```

**Fig. 20.42 - Example users report to file**

## Building Access

There is no input window for this report. To run it select 7 from the Report Mode Menu and press Enter. It runs as soon as you select printer or file and a file name. The Site option prints a report of all Building Access Unit (BAU) sites in the network giving site information and descriptions — see Figure 20.43. Use this report to obtain a complete catalog of BAUs in your network.

Site Report									
Page 1									
Report generated on 3/28/04 at 11:36am by DPS									
Site									
Entry	Id	Win	Type	Port	Dev	Addr	Disp	Pnt	Description
<hr/>									
1	123	4	B	5	SBP	2	1		Yale Office
2	456	5	B	5	SBP	121	1		Madera Office

Fig. 20.43 - Example site report to file

## Pager

The Pager option prints four different reports on pager definitions in the database. The reports are listed on the pager menu window (see Figure 20.44) when the pager option is selected from the Report Mode Menu as follows:

1. Pager Carriers
2. Pager Schedules
3. Pager exceptions.
4. Pager profiles.

Each of these reports gives a print out of their respective screen in the database. When Pager Schedules is selected a window appears for selecting the operator (1-9) to be printed (see Figure 20.45). Each operator prints on a separate page. Any or all may be selected.



Fig. 20.44 - The pager report menu presents four options





Fig. 20.45 - Pager schedules window

Pager Carrier Report			Page 1	
Report generated on 5/8/04 at 4:55pm by DPS				
Pag	Int	Name	Pager Phone	Type ID/Delay
1	SLR	SHIRLEY RAYMOND	299-4403	N 10
2	ADG	ANSEL GRIFFINS	352-2251	A 1000998
3	HHR	HANSEN RADCLIFF	448-0902	N 10
4	CRD	CLIFFORD SIMPSON	477-2152	A 4002990
5	TMC	TOMAS COLEANDER	577-2943	A 4002991
6	KTJ	KIM JACKSONS	599-0203	N 10
7	AJK	ALFONSO KAUFMAN	688-2209	A 4002562
8	TRD	TERRY DARDOWLE	299-0345	N 10
9	MRD	MACK DONALDSON	448-3020	N 10
10	PLM	PAUL MAULER	577-3386	A 6009932

Fig. 20.46 - Example pager carriers report to file

```

Pager Schedule Report                               Page 1
Report generated on 5/8/04 at 4:55pm by DPS
Operator : 1
Hour  SUN   MON   TUE   WED   THU   FRI   SAT
-----
0:00  ADG   SLR   SLR   SLR   SLR   SLR   ADG
1:00  ADG   SLR   SLR   SLR   SLR   SLR   ADG
2:00  ADG   SLR   SLR   SLR   SLR   SLR   ADG
3:00  ADG   SLR   SLR   SLR   SLR   SLR   ADG
4:00  ADG   SLR   SLR   SLR   SLR   SLR   ADG
5:00  ADG   SLR   SLR   SLR   SLR   SLR   ADG
6:00  MRD   AJK   KTJ   TRD   PLM   CRD   MRD
7:00  MRD   AJK   KTJ   TRD   PLM   CRD   MRD
8:00  MRD   AJK   KTJ   TRD   PLM   CRD   MRD
9:00  MRD   AJK   KTJ   TRD   PLM   CRD   MRD
10:00 MRD   AJK   KTJ   TRD   PLM   CRD   MRD
11:00 MRD   AJK   KTJ   TRD   PLM   CRD   MRD
12:00 MRD   AJK   KTJ   TRD   PLM   CRD   MRD
13:00
14:00
15:00
16:00

```

Fig. 20.47 - Example pager schedules report to file

```

Pager Exception Schedule Report                               Page 1
Report generated on 5/8/04 at 4:56pm by DPS
Date : 3/15/95 (WED)
Hour OPR1 OPR2 OPR3 OPR4 OPR5 OPR6 OPR7 OPR8 OPR9
-----
0:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
1:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
2:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
3:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
4:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
5:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
6:00 RAB TMC TMC TMC TMC KJ KJ ACH TRD
7:00 [TRD] TRD TRD TRD TRD TRD TRD TRD TRD TRD
8:00 [TRD] TRD TRD TRD TRD TRD TRD TRD TRD TRD
9:00 [TRD] TRD TRD TRD TRD TRD TRD TRD TRD TRD
10:00 [TRD] TRD TRD TRD TRD TRD TRD TRD TRD TRD
11:00 [TRD] TRD TRD TRD TRD TRD TRD TRD TRD TRD
12:00 [TRD] TRD TRD TRD TRD TRD TRD TRD TRD TRD
13:00
14:00
15:00
16:00
17:00
18:00
19:00
20:00
21:00
22:00
23:00

```

Fig. 20.48 - Example pager exceptions report to file

```

View Report File
Pager Profiles Report                               Page 1
Report generated on 3/20/03 at 11:22am by DPS

Profile 1: Profile 1

Pt OPR Type Delay Fmt Count Repeat Delay Alpha Pager Message
-----
1 1 ALM 0 1 0 0 PNT 1 ALM
2 2 ALM 0 1 0 0 PNT 2 ALM
3 3 CLR 0 1 0 0 PNT 3 CLR
4 4 ALM 0 1 0 0
5 5 ALM 0 1 0 0
6 6 ALM 0 1 0 0
7 7 ALM 0 1 0 0
8 8 ALM 0 1 0 0
9 9 ALM 0 1 0 0
10 10 ALM 0 1 0 0
11 11 ALM 0 1 0 0
12 12 ALM 0 1 0 0
File : PGRPROF.REP Size: 5469 Date/Time: Mar 20,2003 11:22:58
F2=File, F3=Search, Home/F5=Top, End/F6=Bottom, F9=Help, F10/Esc=Exit

```

Fig. 20.49 - Example pager profiles report to file

## View Report File

**Note:** You can view reports only from console access to the T/MonXM system.

View Report File allows you to view on screen the existing report files that were generated with the Report feature in T/MonXM. Before using this option you must choose Output to File and enter a file name.

When you select this report option a file name field appears at the bottom of the screen. Above it is a default box that lists the existing report files. To select a file to view from the default box press Tab. Then use Tab to scroll down and Shift-Tab keys to shift up, or use the up and down arrow keys, then press Enter. **Note:** You cannot view reports while in Monitor Mode.

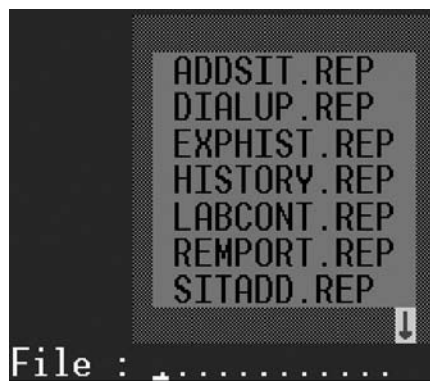


Fig. 20.50 - Select file from default box

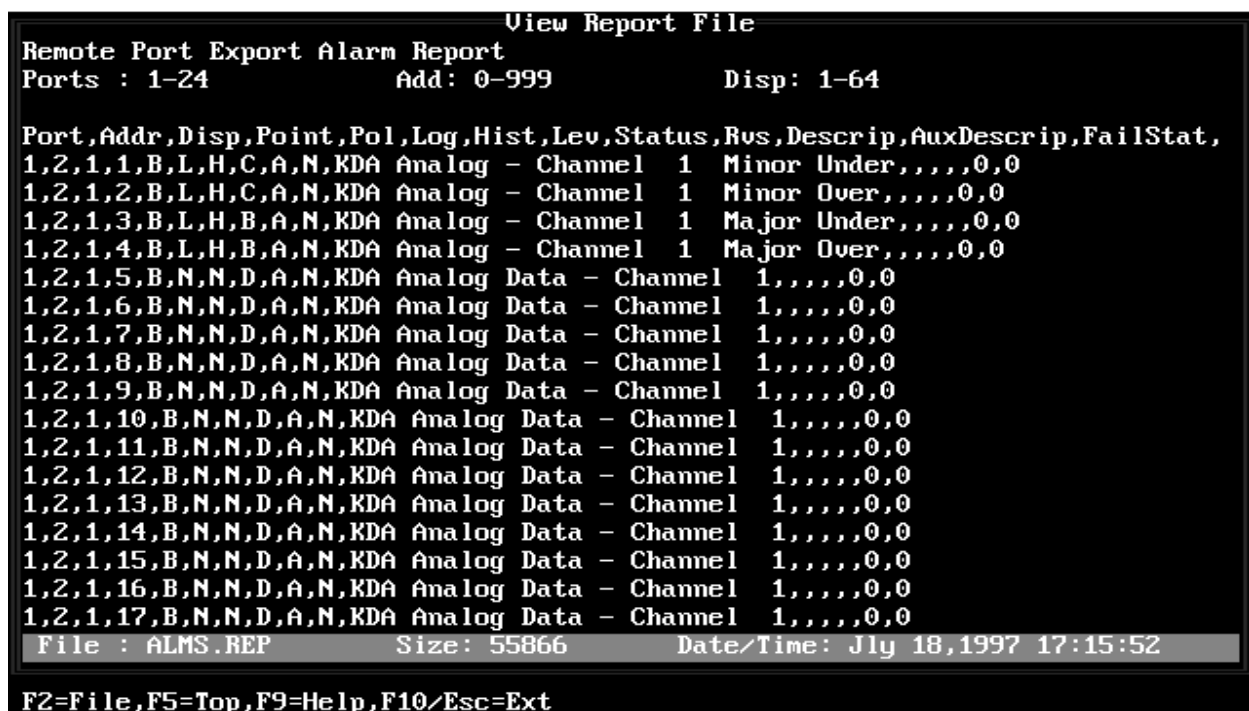


Fig. 20.51 - Example of a report shown in the view report file screen

**Table 20.18 - Fields in the View Report File screen**

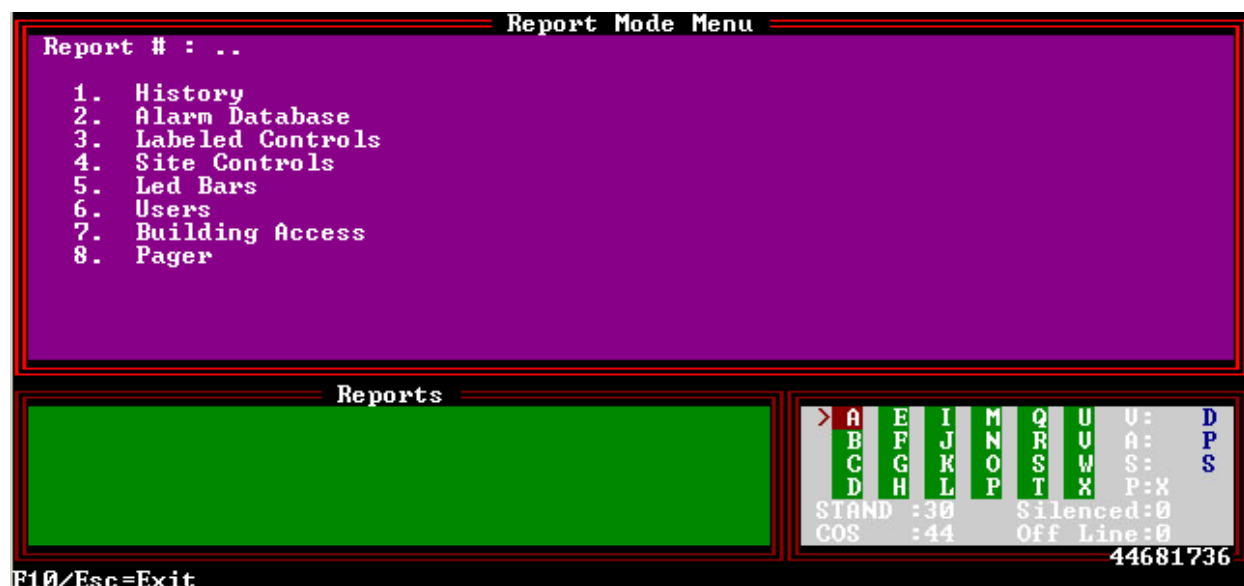
Function Key	Description
F2	Opens the file name field and default box to select a file to view
F3	Search feature
F5/Home	View the beginning of the file
F6/End	Move to the end file
F9	On line help screen
F10/Esc	Exit
PgUp	Go to previous page. <b>Note:</b> At the end of a large file it may be necessary to use F5 to return to the beginning of the file.
PgDn	Go to next page
Home	Move to the top file

**Note:** It is recommended that you review reports from T/RemoteW or T/Windows, where they can be easily pre-viewed, printed, or saved to disk. See Running Reports from T/RemoteW, section 20-5.

## Report Mode in Monitor Mode

The Report Mode window is enabled by pressing Alt F7 while in the Alarm Summary screen. This window shows a menu listing the available reports. Reports give a print out or file record of database information. To select a report, type the number and press Enter. Table 20.1 lists a summary of available reports.

Some reports require additional information. This information will be requested in the window after a report number is selected. The report will be sent to the printer.

**Fig. 20.52 - Report Mode in Monitor Mode screen**

**Table 20.19 - Reports available in the Report Mode menu**

Report	Description
History	Report for a selected period of time (or other criteria) that alarms occurred.
Alarm Database	Report on selected alarm items in the Alarm Database.
Labeled Controls	Report on labeled controls defined in the database. Corresponds with information on Labeled Controls editing screens.
Site Controls	Report on site controls defined in the database. Corresponds with information on Site Controls editing screens.
LED Bars	Report on LED Bars defined in the database. Corresponds with information in LED Bars editing screens.
Users	Report on users and security access privileges defined in the database.
Building Access	Report on building access sites defined in the database.
Pagers	Report on pager information in the database. Select from Pager Carriers, Pager Schedules or Pager Exceptions.

When reports are created from monitor mode, T/MonXM is still actively monitoring the alarm equipment. Only one report can be in progress at any one time. If you attempt to enter Alt-F7 while a report is running, an error message will be displayed. As soon as the printer stops printing, you may start the next report. (If your printer has a large buffer, you may be able to start sooner).

User interaction may be a bit sluggish when reports are being processed.

**Note:** Reports can be generated from console access, T/Remote, and T/Windows, but reports cannot be generated from the Web Browser Interface

Reports generated in the Monitor Mode allow monitoring to continue while the report is produced. Report selections 1 through 8 listed in the Report Mode Menu menu are available. In addition, by pressing Alt-F7 while in the COS or Standing Alarms screens you can generate a report of the COS or Standing alarms for a specific window. In this mode you cannot view the reports on screen.

Reports generated in the Reports screen under the Master Menu are produced while T/MonXM is off line (not monitoring alarms). In this mode you cannot generate a report for a specific window. In this mode you can view reports on screen. Refer to section 20-1 for more information.

Technical note: Remote access users can also run reports. However, only one user can run a report at the same time.

**T/RemoteW and T/Windows users can send reports directly to their local or network printer or save reports to a file on their PC.**

## Hard Copy



**Fig. 20.53 - Hard Copy menu command**

With the Hard Copy command you can:

1. Log alarms to a printer as they occur.
2. Automatically generate daily printed reports of the alarms occurring in specified windows.
3. Produce hourly printed reports of all standing alarms (Status alarms can be omitted).

This function is helpful for producing log records of things like tower light operation or cable pressure variations.

**Note:** Two printers can be in use, one for the logging feature and the other to print the periodic and manual reports (see Reports section of this manual). With only one printer, the logging function will be suspended while reports are being printed and the alarms that occur during report printing will not be printed.

Selecting Hard Copy from the Parameters menu (press H to select Hard Copy and press Enter) will allow you to setup the operating characteristics of the printer logging feature.

**Note:** With only one printer logging is suspended when reports are printed.



**Fig. 20.54 - The hard copy screen**

**Table 20.20 - Key commands available in the Hard Copy screen**

Function Key	Description
Up Arrow	Move to the previous field.
F8	Save
F9	Help
F10/Esc	Move to the first field or exit without saving if the cursor is in the first field.

**Table 20.21 Fields in the Hard Copy screen**

Field	Description
Multiple Printers	N = one printer. Y = two printers*. With one printer, no logging will occur during reports. With two printers, one printer logs and one printer reports.* [N]
Printer Logging	N = alarms will NOT be logged to the printer. Y = alarms WILL be logged to the printer. [N] Printer Logging can also be toggled while in Monitor mode using Ctrl-F1.
Printer Log Messages	Determines whether text messages will also be printed with logging. Y = Print alarm text messages. N = Do not print alarm text messages. [N] <b>Note:</b> Printer Logging will only print messages when alarms fail, not when alarms clear.
Wide Carriage	Set the Wide Carriage to Y if your printer supports up to 132 columns of text. The default setting (N) sets output at 80 columns for standard 8" paper. [N]
Page Length	Enter the page length (55 to 67 lines) [63 lines]
Daily Report Hour	Determines the hour when your alarm log will be sent to the printer. Settings are 0-23 and N for none. [N]
Daily Report Windows	Determines windows that will be sent to printer for automatic logging of standing alarms. Values are 1-720 (or maximum number of windows your T/MonXM supports). This field will be skipped if the Daily Report Hour field is set to N. [blank]
Hourly Standing Report	Y = Automatically generate standing alarm report hourly. N = Disable. [N]
Ignore Level D Alarms	Y = Level D alarms do not appear in hourly reports. N = Level D alarms do appear in hourly reports. [N]
Window Rep Messages	Y = Print text messages in COS or Live window reports. N = Don't print text messages in COS or Live window reports. [Y]
Incident Pre-Scan	The number of days prior to the start of the reporting period that the system will look for the start time of alarms that are active when the report begins. (0-99) [0]
Alarm Export Type	Standard: uses designated export delimiter, Original: always uses a comma delimiter, or Alarm Format: exports the alarms in an "onscreen" format. [STANDARD]
Export Delimiter	Either comma or tab. Using tab as the delimiter has an advantage over the comma because no text qualifier is needed since none of the T/Mon data contains tab characters. [TAB]
Export Text Qualifier	The text qualifier character used when Alarm Export Type is set to Standard. This character is used to enclose fields that contain the delimiter. It can be set to one of the following characters: double quote, single quote, or left blank. If left blank, then no text qualification is done. [blank]

\* Two printers requires a second parallel port in the T/MonXM WorkStation. This will take the space of one 600 card, which means the maximum number of serial ports will be 12 on T/MonXM or 20 on the IAM-5. LPT 1 is for printer logging and LPT 2 is for reports.

[ ] = default



## Trouble Log Mode in Monitor Mode

Trouble Logs are a record of operator reaction to alarms

Trouble Logs are ideal to bring operators up to date during shift changes

Each log is time- and user-stamped.

Multiple logs can create an action log history for an alarm.

The Trouble Log feature allows T/MonXM users to attach alarm notes or trouble tickets to individual alarm failures in the network. This allows other users of the system to access this information and know if an alarm has been purposely failed, serviced, etc. Once the problem is resolved, an operator can make a trouble log entry saying "This action is closed and has been taken care of." As part of the history file an operator can bring up all the trouble logs for a certain point for trending and analysis. You can also have multiple Trouble Logs for a point.

Trouble logs apply to all external alarms and to user defined internal alarms in addresses 11 and 12. Trouble logs cannot be prepared for standard internal alarms.

Trouble logs can be written for either standing or COS alarms, from either of their respective screens. The COS screen is recommended because when the alarm clears it will remain on the COS screen until acknowledged. This makes the trouble ticket easy to prepare by simply highlighting the alarm and pressing F6 twice. (The trouble ticket notations should be performed before the alarm is acknowledged.) However, if a trouble log is created for an alarm that is being tracked from the standing alarm screen, once the alarm clears it will no longer appear on the screen and the trouble log will have to be manually accessed by entering the address, display and point information

There are two mode levels for the trouble log window, Trouble Log mode and Trouble Log Examination mode. The trouble log window appears at the lower left portion of the COS or Standing Alarms screen, in place of the Text/Messages window. To enter Trouble

```

COS ALARMS - ALL ALARMS
9/26 8:45 FAIL DPSLAB (Undefined)
9/26 8:45 FAIL DPSLAB (Undefined)
9/26 8:45 FAIL DPSLAB (Undefined)
9/26 8:46 FAIL 8.27 DEVICE FAIL KENNEDY ES
9/26 8:46 FAIL 8.38 DEVICE FAIL BUILD 3/14 C
9/26 8:47 FAIL 8.39 DEVICE FAIL BUILD 3/14 A
9/26 8:47 FAIL 8.40 DEVICE FAIL BUILD 3/14 B
9/26 8:47 FAIL 8.73 DEVICE FAIL GODDARD ES
9/26 8:48 FAIL DPSLAB (Undefined)
9/26 8:49 FAIL T/MonXM OFFLINE
9/26 8:51 FAIL T/MonXM ONLINE
9/26 8:54 FAIL DPSLAB (Undefined)
9/26 8:55 FAIL DPSLAB (Undefined)
9/26 8:56 FAIL DEVICE FAILURE DPM: RP.106

Trouble Log - Examine
Port : IA
Device :
Address: 11
Display: 1
Point : 2
Not found. Wish to add (Y/N)?

Page Index
> 1 5 9 13 17 21 U: D
2 6 10 14 18 22 A: P
3 7 11 15 19 23 S:X S
4 8 12 16 20 24 P:
Live :47 FD:Y
Alarms:22 Off Line:0

F10/Esc=Exit

```

Fig. 20.55 - Trouble log replaces text/messages window in COS and standing screens

	Log Mode, first highlight the alarm for which you wish to start a trouble log record.
Trouble Log Mode = Green	Press F6 to enable the Trouble Log window. If a trouble log already exists it will be displayed in the window. If you are starting a new trouble log or wish to add to the existing one, press F6 again to enable Trouble Log Examination mode.
Examine Mode = Magenta	The Trouble Log Examine window appears in the lower left bottom portion of the screen. If you have highlighted the alarm that is to have a new trouble log, the address, display and point numbers will be automatically entered in the fields in the Trouble Log Examination window. If not there, or if for a different alarm, you will need to enter the address, display, and point numbers manually.
	Any trouble ticket for an alarm not shown on the screen can be accessed by pressing F3 and entering the port, address, display and point numbers manually.
	Alarms with existing, active trouble logs will have a # symbol in character column 3 of the alarm reporting line.
# Symbol designates a trouble log is open	When a trouble ticket is totally cleared up it is closed by pressing F5. The # sign will then be removed from the alarm reporting line, but the closed message will still be displayed in the trouble log window, as long as this alarm remains on the screen (unacknowledged) and is highlighted.
	The Trouble Log appears as shown in Figure 20.58 on the next page.

**Table 20.22 - Key commands available in Trouble Log windows**

Function Key	Description
F1	Previous. Select previous Trouble Log.
F2	Next. Select next Trouble Log.
F3	Select. Allows you to change the point you are on and check the message for another point.
F4	New. Allows you to create a new message.
F5	Close. Allows you to create a special kind of message called a "closed message". Once you have closed a message you will not see a "#" pound sign for a point message.
F7	Print. Allows you to access Print Trouble Log Mode and to print Trouble Log reports — see section 20-45.

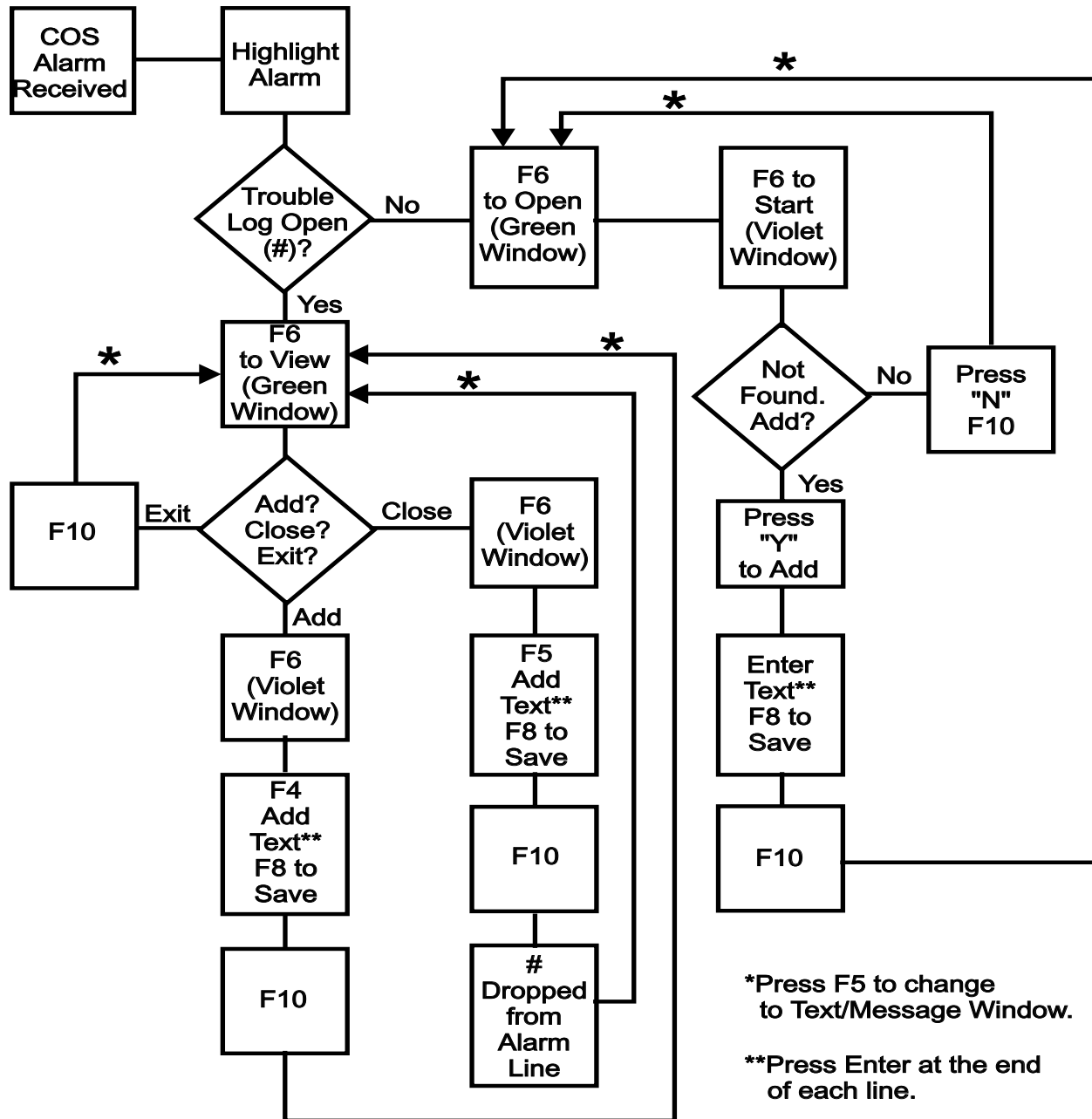


Fig. 20.56 - Trouble log sequence flow chart

```

===== Trouble Log - Examine =====
Pt:IA:11:1:2    1 of 1    9/26/94  8:58  DPS
Crew has been dispatched. No further action
is neccessary.
Tom
  
```

Fig. 20.57 - Trouble log examine window

## Trouble Log Print Mode

The Print Trouble Log screen is accessed by pressing F7 from the Trouble Log - Examine screen. (The command line at the bottom of the screen changes to show print commands.)



Fig. 20.58 - Print trouble log screen has prompt line at bottom

## Compile Trouble Log Reports

Compiling a Trouble Log report provides a summary of all trouble log entries. You can save or print a trouble log report from the Reports > Alarm Database Report Menu, or by pressing Alt-F7 in Monitor Mode to automatically go into the Reports screen.

Use the following steps to compile your trouble log entries into one comprehensive report:

1. From the Master file > Reports Mode menu, or press Alt-F7 while in Monitor Mode.
2. Enter 2 to view the Alarm Database reports
3. Enter 20 to compile trouble logs by point, or enter 21 to compile trouble logs by date/time.
4. Enter F to save a compiled report to a file or enter P to print a compiled report — see Figure 20.59.

**Note:** If saving the report to a file, you will be prompted to enter a file name. A file name can only be seven characters long.

5. Enter your report filter parameters — see Figure 20.60 for report by point filter parameters, and Figure 20.61 for report by date/time filter parameters. See Table 20.23 for field definitions in these screens.



Fig. 20.59 - Output a compiled trouble log report to a file or print a compiled trouble log

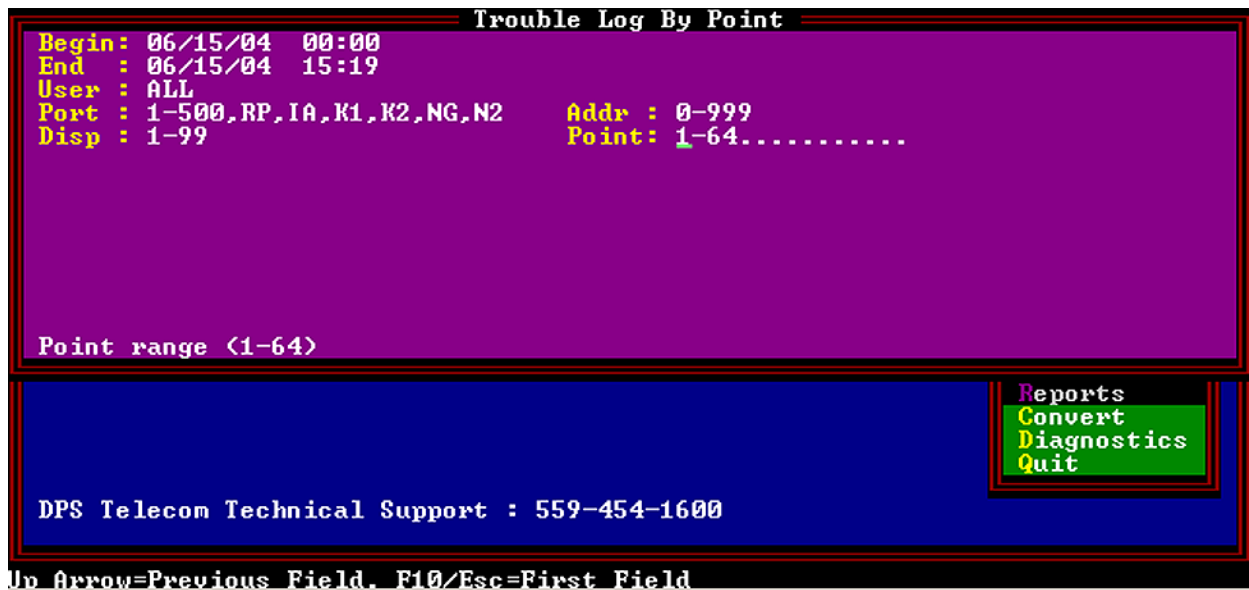


Fig. 20.60 - Compile a Trouble Log Report by point

Table 20.23 - Fields in the compile Trouble Log screen

Field	Description
Begin	Beginning date of report (mm/dd/yy). Beginning time of report (hh:mm, 00:00 = midnight)
End	Ending date of report (mm/dd/yy). Ending time of report (hh:mm, 00:00 = midnight).
User	Specify a single user or ALL
Port*	Remote Port range (1-500, RP, RC, IA, K1, K2, K3, NG, N2)
Addr*	Address range (0-999)
Disp*	Display range (0-65535)
Point*	Point range (1-64)

\* Fields only available in the Trouble Log by point screen.

```

Trouble Log By Date/Time
Begin: 06/15/04 00:00
End   : 06/15/04 15:20
User  : ALL

Specify a single user or ALL

DPS Telecom Technical Support : 559-454-1600

Reports
Convert
Diagnostics
Quit

Up Arrow=Previous Field, F10/Esc=First Field

```

Fig. 20.61 - Compile a Trouble Log Report by date/time

**View compiled Trouble Log reports.**

1. Return to the Master menu > Reports menu and select 9(View Report file).

**Note:** Reports cannot be viewed while in Monitor mode.

2. Use the Tab key to select your compiled Trouble Log report file name and press Enter.

```

View Report File
Trouble Log By Point      Run Date: 6/10/04 1:15 am      Page 1

Start of Interval: 06/10/04 00:00
End of Interval  : 06/10/04 01:15
User: ALL
Ports: 1-500,RP,IA,K1,K2,NG,N2  Addresses: 0-999
Displays: 1-99  Points: 1-64

Site: ***NO DATA FOUND***      Point Name: ***NO DATA FOUND***
- Port: IA      Address: 0      Display: 1      Point: 6
- 06/10/04 01:15 DPS  Check the LAN cable - dead line.

Trouble Log Report Ended : Jun 10,2004 01:15:54

File : ADSF.REP      Size: 496      Date/Time: Jun 10,2004 01:15:54

F2=File, F3=Search, Home/F5=Top, End/F6=Bottom, F9=Help, F10/Esc=Exit

```

Fig. 20.62 - View a Trouble Log Report by point

## Related Trouble Log Sections

Other Trouble Log sections include the following:

- **File Maintenance** - System Users  
The System Users screen has a Trouble Log access level field.
- **File Maintenance** - Utilities - File Utilities - Key Rebuild menu

The Key Rebuild Menu has a rebuild Trouble Log Key option.

- **Reports** - Alarm Database Report - Compile Trouble Log Reports menu.

**This page intentionally left blank.**



# Section 21 - Configure Redundant Dual T/Mon Backup

Primary (Master)

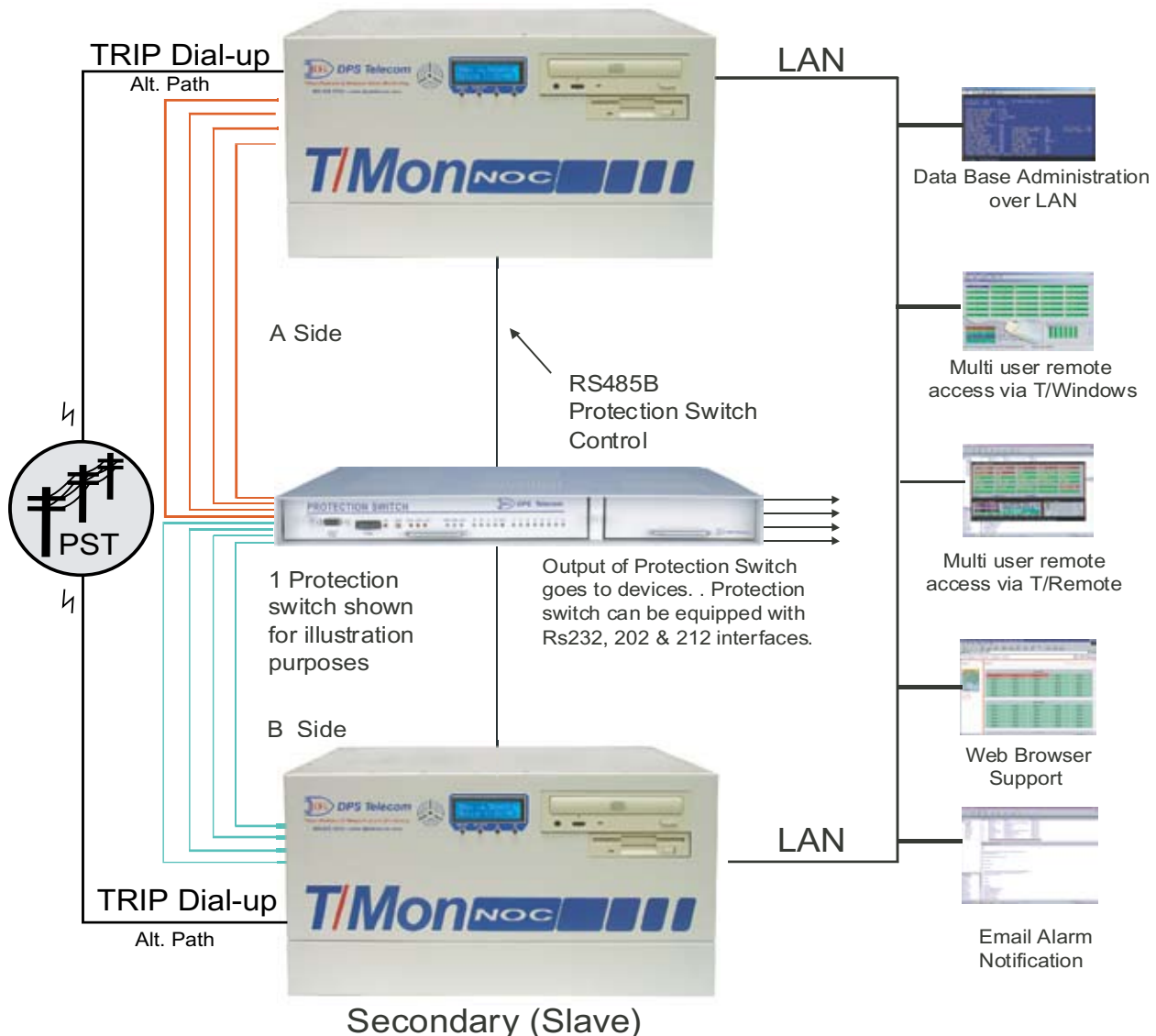


Fig. 21.1 Block diagram of dual redundant T/Mon NOCs connected by a Protection Switch

## Overview

When two or more T/Mons are used in a network, one unit can be assigned to be a secondary backup. Routers serving as protection switches are connected between T/Mons and reporting devices. If a router detects that the primary system is down, it will immediately switch all monitoring activity to the secondary system. The databases of the two systems are synchronized via a serial connection. For even greater security and redundancy, the secondary T/Mon can be placed at a different location to create a LAN-based geodiversity contingency backup.

## TMonNET

Selecting TMonNET from the Parameters menu will allow you to define settings for a network setup of T/Mon. This provides a hot standby system in another location for redundancy. This means if the primary T/Mon fails then the secondary T/Mon will take over monitoring until the primary T/Mon is restored.

In addition, having one or more T/Mon networked allows you to keep one unit monitoring while doing your databasing on the other unit. After you've defined your database, you can then transfer it to the other T/Mon via the network.

**Note:** A slave workstation in a network configuration provides redundancy at a different location than the master. The Protection Switch configuration provides redundancy at the same location.

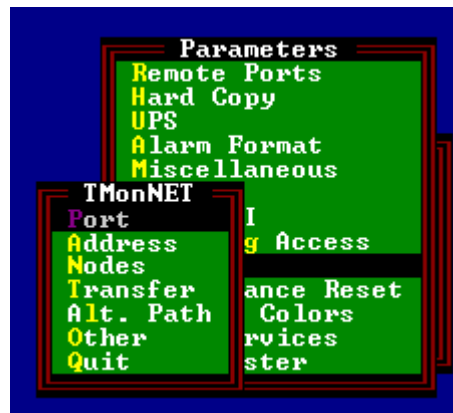


Fig. 21.2 - The TMonNET menu.

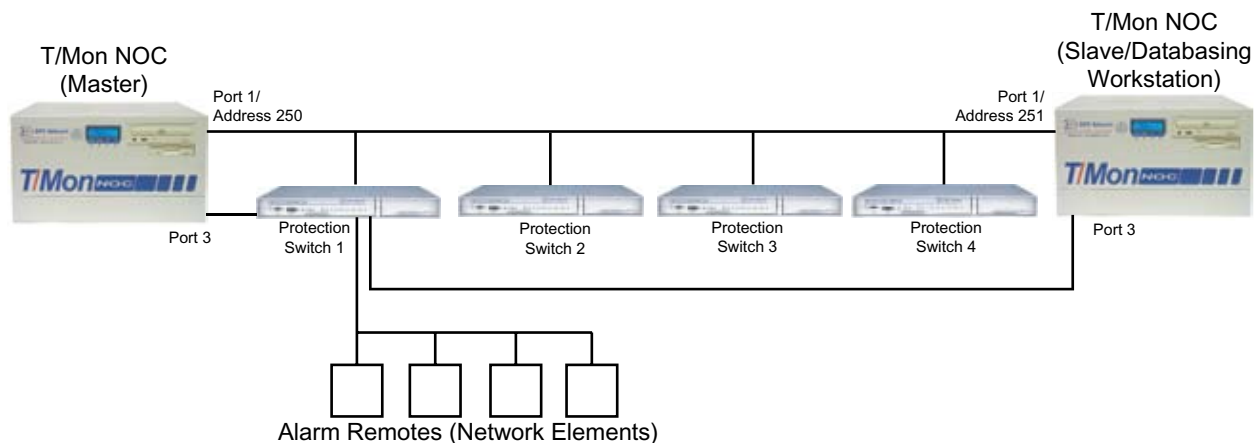


Fig. 21.3 - Slave T/Mon NOC and remotes share network port.



Fig. 2.2 - DCP(F) Remote Parameters default settings.

## Port

Use only DCP(F)  
Interrogator ports when  
connecting T/Mon NOCs  
to each other.

### Step One: Define the TMonNET Network port.

Define a port for the DCP(F) Interrogator before you can select it as your TMonNET Network Port.

**Note:** This can run on either a physical or virtual port. The following example is on a physical port.

Table 21.A - Fields in the Remote Parameters screen

Field	Description
Port Usage	Select a port from 0-500 (0 = Disabled). Valid port types are DCP(F) Interrogator and Halted. Use Halted (default) if no device is connected to the communication port. <b>Note:</b> Ports 1-24 are physical ports. Ports 30-500 are virtual ports.
Serial Format	Baud rate, word length, parity, and stop bits settings.
RTS Lead/Tail	RTS Lead is the time carrier is turned on before data is sent (0-2500 ms).(Set to 60 for 202 modems.) RTS Tail is the time carrier is left on after the last byte is sent (0-2500 ms).(Set to 40 for 202 modems.) <b>Note:</b> Setting the RTS Lead Time and RTS Tail Time both to 2500 will enable a DCP(F) constant carrier.
Path B	Enter 0 to disable Ring Polling Application (default).
Time Out	Time T/Mon will wait for response before failing the poll. Valid entries are 200-9999 milliseconds. Typical timeout is 1000.
Poll Delay	The Poll Delay is the time between polls. Valid entries are 0-9999 milliseconds. Typically this is 0.
Protocol (DCPF Mode)	Enter "F" for DCP(f) mode.
Poll Mode	These determine the way polling is performed. This should be set to "M" on both the Primary and the Secondary T/Mons.

**Note:** Table M17.A continues on the following page.

**Table 21.A - Fields in the Remote Parameters screen (continued)**

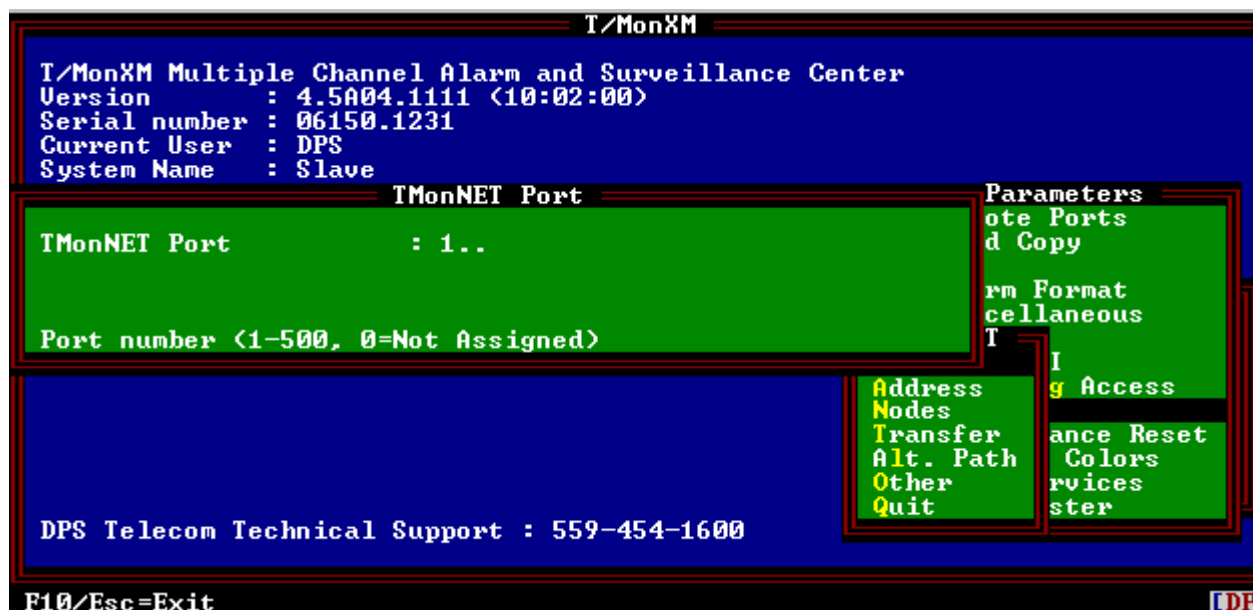
Field	Description
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Valid entries are 5-999 seconds.
Switch Threshold	The Switch Threshold is the seconds of no activity before becoming master. Valid entries are 2-999 seconds. Note: This field is only available when "Combined" is entered in the Poll Mode field.
Fail Threshold	Number of bad or failed polls before device is declared failed.
Fail Poll Cycles	The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. Valid entries are 0-255.
Check DCD on Rcv	Y = Enable DCD checking to validate Rcv. N = Disable. [N]
Immediate Retries	Number of retries after failed poll attempt before proceeding with next address. [1]

### Step Two: Select DCP(f) int. to be used for the TMonNET Port Menu.

Selecting Port from the TMonNET menu allows you to select the network port that T/MonXM will use to communicate with another T/MonXM. The network port is of type DCPF Interrogator.

1. Choose Master Menu > Parameters > TMonNET > Ports menu.
2. Enter the DCP(f) Int. being used in the TMonNET Port field.

Table 21.B lists screen options for the TMonNET Port screen.

**Fig. 21.4 - The TMonNET Port Screen**

**Table 21.B - Fields in the TMonNET Port screen**

Field	Description
TMonNET Port	Defines the network port that T/MonXM will use to communicate with remotes and other networked T/Mons. Valid values are 1-500 or 0 for not assigned. [0] The port number defined here MUST match on each T/MonXM to be networked. In other words, if your primary T/Mon is using port 1, your secondary T/Mon must also use port 1 on it's configuration. The network port must be defined in the Remote Port sub-section as "DCPF Interrogator." Type the port number and press Enter to return to the TMonNET Menu.

**Warning:** Do not use this field unless you have two T/MonXM Workstations connected together.

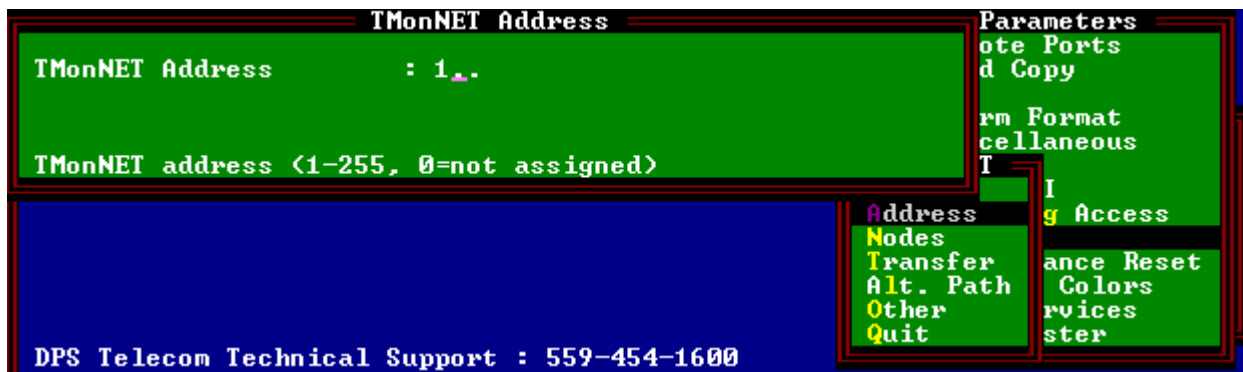
**Note:** This port can also have DCP(F) alarm remotes. This is often the case when two T/MonXM Workstations serve each end of a network as "Master-Slave"

## TMonNET Address

### Step Three: Enter the network address.

Selecting Address from the TMonNET menu allows you to enter the network address (node number) for the T/Mon or IAM.

1. Go to Parameters > TMonNET > Address.
2. Select an address (1-255). The recommended address for the Master unit is 250 and the address for the Slave unit is 251.

**Fig. 21.5 - The TMonNET address screen.****Table 21.C - Fields in the TMonNET Address screen**

Field	Description
TMonNET Address	A unique address (node number) for the T/Mon that contains the database. (i.e., The workstation you are now using.) Valid range is 1-255. Each T/Mon must have a unique address that is not duplicated (for remotes or T/Mon) elsewhere on the network port. Type the address number and press Enter to return to the Network menu.

## Node Definition

### Step Four: Enter your node definitions.

Selecting Nodes from the TMonNET menu takes you to the TMonNET Node Definition screen. This allows you to define each node (T/MonXM system) on your network.

1. Go to TMonNET > Nodes menu
2. Enter your Nodes definitions in the appropriate fields. See Table 2.C for field definitions and screen options for TMonNET Nodes screen.

**TMonNET Node Definition**

This System : 251

Entry	Addr	Site Name	Poll Mode	Warning Thresh	Switch Thresh	Time out
1	251	SLAVE	COMBINED	65	70	1000
2	250	MASTER	PASSIVE			
3						
4						
5						
6						
7						
8						

Other Quit    Colors rvice ster

DPS Telecom Technical Support : 559-454-1600

[LIST BOX] Cursor Keys=Move Highlight Bar, <ENTER>=Select, F10/Esc=Abort

**Fig. 21.6 - The TMonNET nodes screen.**

**Table 21.D - Fields in the TMonNET Node Definition screen**

Field	Description	
This System	Network node address of system you are currently using—same number that was entered for the TMonNET Address (Figure 21.3). Non-editable field.	
Entry	Entry number. This field is not editable.	
Addr	DCP(F) address of the network node you would like to define. Enter the address of the "Network Port" for each T/Mon or IAM that is on the network. Valid range is 1-255.	
Site Name	English name of the site. Limited to 30 characters.	
Poll Mode	Enter the defined polling mode for that system. Valid entries are Passive, Combined, or Master. <b>Note:</b> If set for Master Mode, the system will ask for Warning Threshold and Time out settings. If set for Combined Mode, the system will ask for Warning Threshold and Switch Threshold settings.	
	Master Mode	Will always attempt to poll RTUs. There should at most be one master in a network.
	Passive	Never polls network, but will detect alarms.
	Combined	Starts out passive, but if it senses no activity from the Master, it will become master. Will revert to passive if it detects online activity from the Master.

**TMonNET Node Definition**

This System : Not assigned

Entry	Addr	Site Name	IP Address
1			111.222.333.444
2			
3			
4			
5			
6			
7			
8			

Enter the IP address of the node <XXX.XXX.XXX.XXX>.

Other    Colors  
Quit    rvices  
ster

DPS Telecom Technical Support : 559-454-1600

Up Arrow=Previous Field, F10/Esc=First Field

Fig. 21.7 - Enter the IP address of both systems on the network (Port must be set to 50 or above)

Table 21.E - Fields in the TMonNET Node Definition screen (continued)

Field	Description
Warning Thresh	Warning Threshold. Sets the seconds of no activity before a unit set as Passive, Combined or Master issues a warning. Valid range is 5-999 seconds. [65] Note: Set warning value higher than the switch threshold to disable the warning.
Switch Thresh	Switch Threshold. Sets the number of seconds of no activity before a unit set as Combined will wait before becoming the master. Valid range is 2-999 seconds. [70]
Time Out	Amount of time a unit will wait to receive a complete poll. Valid range is 200-9999 seconds. [1000]
IP Address	The IP address of the node. This field is only valid if TMonNET is running on a virtual port.

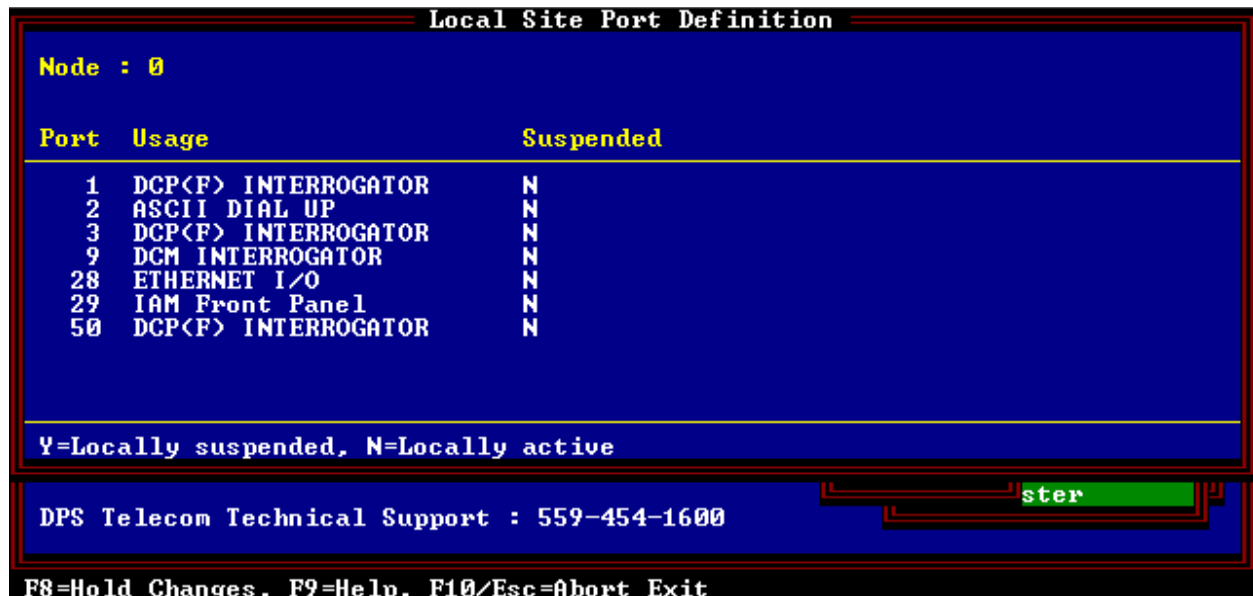


Fig. 21.8- Local site port definition window lists all defined ports and status.

Table 21.F - Key commands available in the TMonNET Node Definition screen

Function Key	Description
F2	Port Info. Shows all defined ports and suspension status. Allows suspension status to be changed. N = Locally Active Y = Locally Suspended
F3	Blank. Deletes current node entry.
F4	More. Scrolls the screen to the right to see the IP address field. (Only available if the Network Port has been set to 30 or greater.)
F8	Save Network Node Definition settings.
F9	On-line help.
F10/Esc	Exit without saving.



## TMonNET Transfer

**Note:** Unlike the Back Up Data Files command in the File Utilities menu, TMonNET Transfer does not support transferring indexes.

### Step Five: Schedule data file transfers.

Selecting the Transfer menu allows you to schedule automatic transfers of your database to or from your master and slave units.

1. Go to TMonNET > Transfer menu.
2. Enter appropriate information in each field.

See Table 21.G for field definitions.

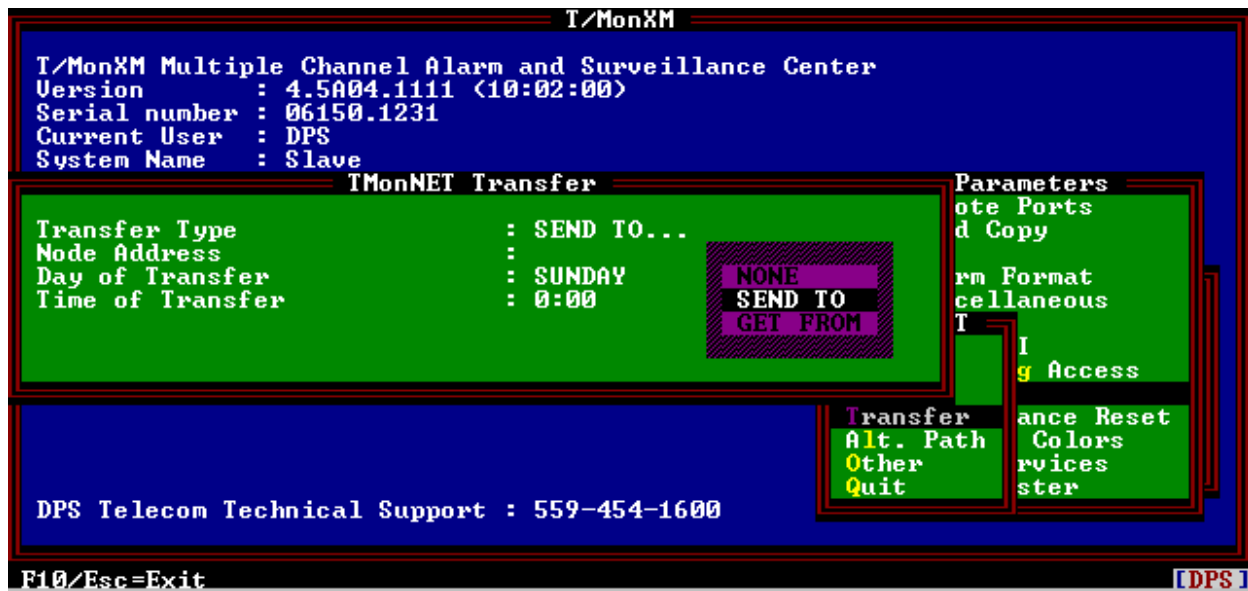


Fig. 21.9 - TMonNET transfer screen.

Table 21.G- Fields in the Network automatic transfer screen

Field	Description
Transfer Type	<ul style="list-style-type: none"> <li>• None = no automatic transfer scheduled.</li> <li>• Send To = Set this workstation as the source for the automatic transfer.</li> <li>• Get From = Set this workstation as the destination for the automatic transfer.</li> </ul> <p><b>Note:</b> Only one workstation needs to be configured. Selection of the transfer type just depends on if your workstation is the source or destination.</p>
Network Node Address	Enter the network node address of the other workstation. (1-255)
Day of Transfer	Select the day of the week from the default menu for the automatic transfer here.
Time of Transfer	Select the time that the transfer should begin here. (HH:MM)

## Other Parameters

Selecting Other from the TMonNET menu allows you to define miscellaneous settings for your network.

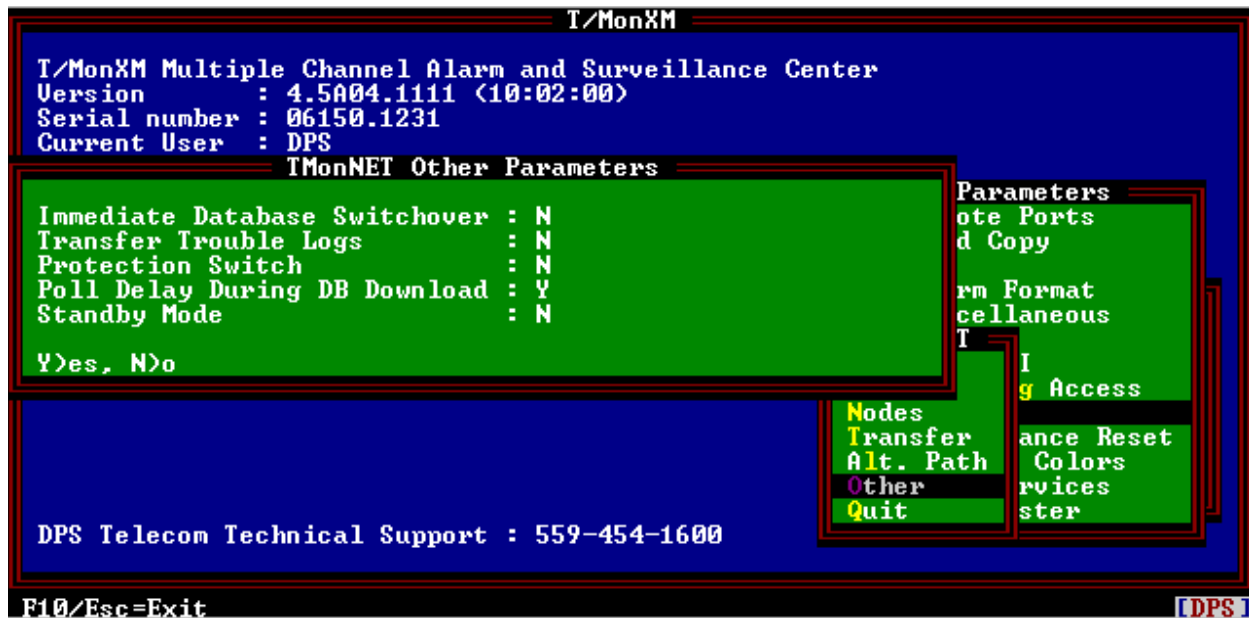


Fig. 21.10 - TMonNET Other Parameters screen

Table 21.H- Fields in the TMonNET Other Parameters screen

Field	Description
Immediate Database Switchover	Used to tell the system to switch to a new database as soon as it becomes available locally (e.g a database transfer has completed). Settings are Y (yes) or N (no). [N]
Transfer Trouble Logs	Used to tell the system to send current trouble logs along with database. Settings are Y (yes) or N (no). [N] <b>Note:</b> If you select Y the transfer may take longer.
Protection Switch	If a protection switch is used, there will be 2 T/Mons. In this field you need to define whether this T/Mon is on the A or B side of the protection switch. A = Primary, B = Secondary, N = None
Poll Delay (During DB Download)	Yes or No. Gives the option to obey or ignore the poll delay when doing a network database transfer.
Standby Mode	Yes or No. Allows secondary T/Mon to be used as a "hot standby." If Standby Mode is enabled, then the system does not poll on any port and does not make or receive calls via TRIP, with the exception of Alt. Path. The standby unit becomes active and begins polling if it loses contact with the primary unit for "Switch Threshold" number of seconds. When contact with the primary unit is re-established, the standby unit ceases polling.

# TMonNET Alt. Path

TMonNET Alt. Path is an enhancement upon the existing TMonNET Redundant Master Technology. This new feature allows a Secondary TMon to call a Primary T/Mon using an alternate communication path (TRIP Dialup) in the case that the primary communication path fails (i.e. LAN) — see Figure 21.1. If the Secondary T/Mon can reach the Primary T/Mon over the alternate communication path then the Secondary T/Mon will not go active. The Secondary T/Mon will periodically test the alternate communication path, while it is pas- sive, to make sure that it is functioning correctly.

TMonNET Alt. Path runs solely on the Secondary T/Mon and no configuration to the Primary T/Mon is necessary. All Databasing, English Messages and Housekeeping Alarms will take place only on the Secondary TMon.



Fig. 21.11 - Select Alt. Path from the TMonNET Menu

## Databasing

Databasing TMonNET Alt. Path should only be performed on the Secondary T/Mon. Databasing the TMonNET Alt. Path feature is per- formed from the following menu “Master->Parameters->TMonNET->Alt. Path” — see Figure 21.11.

The fields in the TMonNET Alt. Path screen are used to configure TMonNET Alt. Path — see Figure 21.12 and Table 21.I for a description of the fields.

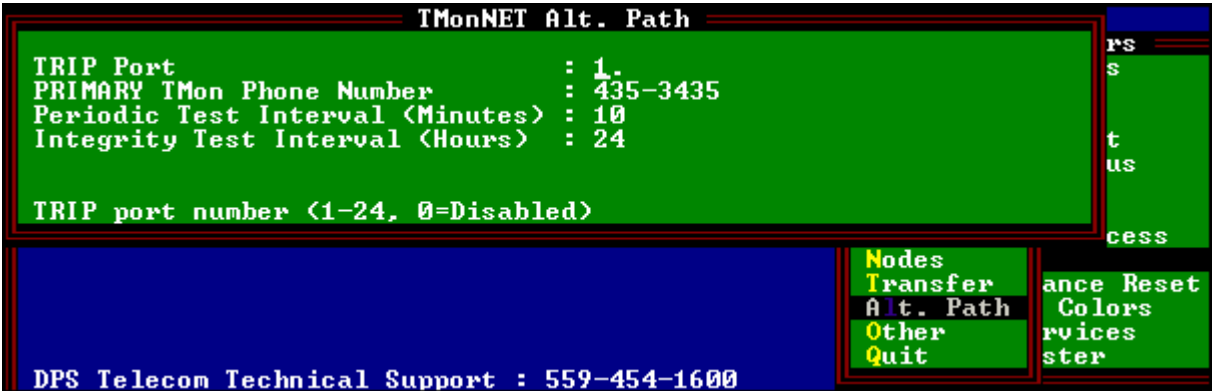


Fig. 21.12 - TMonNET Alt. Path screen

**Table 21.1 - Field descriptions for the TMonNET Alt. Path screen**

Field	Description
TRIP Port	The job number of the local TRIP Dialup port to use for calling the Primary T/Mon. This TRIP port will serve as the alternate communication path to the Primary T/Mon. Setting this field to 0 will disable TMonNet Alt. Path.
Primary T/Mon Phone Number	The phone number of the Primary T/Mon. This phone number will be used by the TRIP port
Periodic Test Interval (Minutes)	The interval in minutes with which to call the Primary T/Mon if the primary communication path fails (i.e. LAN). This test will be performed immediately if the primary communication path fails and then will be repeated periodically, based on the interval defined in this field, until the primary communication path is restored or the alternate communication path fails.  If this test fails then the Secondary T/Mon will go active and set the TMONNET ALT. PATH FAILED housekeeping alarm. If this test succeeds then the Secondary T/Mon will remain passive and clear the TMONNET ALT. PATH FAILED housekeeping alarm. This test is only performed when the Secondary T/Mon is passive.
Integrity Test Interval (Hours)	The interval in hours with which to call the Primary T/Mon to test if the alternate communication path is working. This test will be repeated periodically, based on the interval defined in this field, until the primary communication path fails.  If this test fails then the Secondary T/Mon will remain passive and set the TMONNET ALT. PATH FAILED housekeeping alarm. If this test succeeds then the Secondary T/Mon will remain passive and clear the TMONNET ALT. PATH FAILED housekeeping alarm. This test is only performed when the Secondary T/Mon is passive.

**Note:** There is a help file available by pressing 'F9' from any of the fields on this screen.

#### **Databasing Requirements**

The databasing requirements for TMonNET Alt. Path are as follows:

1. TMonNET must be configured to use one Primary TMon and one Secondary TMon on either a physical port or a virtual port. Refer to Figure 21.1.
2. Both the Primary and the Secondary T/Mon must have at least one TRIP Dialup job defined. It is ok if the TRIP job is shared by other dialup devices. Ideally the Secondary T/Mon would be configured to use the phone number of the Primary T/Mon's TRIP job with the lowest utilization to ensure maximum responsiveness.
3. The Secondary T/Mon must be configured as a "Hot Standby" (Standby Mode = 'Y' from the "Master > Parameters > TMonNET > Other" menu).

### English Messages

The messages in Table 21.I are displayed on the Secondary T/Mon in the English Window from Monitor Mode.

**Table 21.J - English message descriptions in Monitor Mode**

English Message	Description
Primary Path Failed, Testing Alt Path	The primary communication path has failed and the Secondary T/Mon is going to attempt to communicate with the Primary T/Mon using the alternate communication path. This test is only performed when the primary communication path first fails and then repeatedly until either the primary communication path is restored or the alternate communication path fails. The interval at which this test will be performed is defined in the Periodic Test Interval (Minutes) field.
Testing Alt Path	The Secondary T/Mon is performing a periodic integrity test of the alternate communication path to the Primary T/Mon. This test is only performed at the interval defined by the Integrity Test Interval (Hours) field when the primary communication path is working.
Query Master Using Alt Path	The TRIP job on the Secondary T/Mon has successfully connected to what it believes to be the Primary T/Mon. 'OK' means that the Primary T/Mon identified itself and 'FAILED' means that either no response or an incorrect response was received from the far end.
Alt Path Test Timeout, Going Active	The Secondary T/Mon was unable to complete it's alternate path communicate test with the Primary T/Mon within an acceptable amount of time and will now go active. This messages corresponds to the "Primary Path Failed, Testing Alt Path" message.
Alt Path Test Timeout	The Secondary T/Mon was unable to complete it's alternate path communicate test with the Primary T/Mon within an acceptable amount of time and will remain passive. This messages corresponds to the "Testing Alt Path" message.
Alt Path Test Failed, Going Active	The Secondary T/Mon was unable to communicate with the Primary T/Mon using the alternate communication path and will now go active. This messages corresponds to the "Primary Path Failed, Testing Alt Path" message.
Alt Path Test Failed	The Secondary T/Mon was unable to communicate with the Primary T/Mon using the alternate communication path and will remain passive. This messages corresponds to the "Testing Alt Path" message.
Alt Path Test Succeeded	The Secondary T/Mon was able to communicate with the Primary T/Mon using the alternate communication path and will remain passive. This messages corresponds to both the "Primary Path Failed, Testing Alt Path" and the "Testing Alt Path" messages.

**Note:** For more information on the English Window and Monitor Mode see Section 16.

### Housekeeping Alarms

The following housekeeping alarm (aka standard internal alarm) is available on the Secondary T/Mon for TMonNET Alt. Path:

#### TMONNET ALT. PATH FAILED

This alarm is set when the Secondary T/Mon is unable to communicate with the Primary T/Mon over the alternate communication path. This alarm is cleared when the Secondary TMon is able to communicate with the Primary T/Mon over the alternate communication path.

Refer also to Figure 21.13.

Point Definition									
Standard Internal					Disp: 2				
Pt	P	L	H	L	S	R	Description		
	o	o	s	e	t	v			
	l	g	t	u	s	s			
1	B	L	H	A	A	N	DC PWR A FUSE BLOWN		
2	B	L	H	A	A	N	DC PWR B FUSE BLOWN		
3	B	L	H	A	A	N	PRIMARY DRIVE FAILED (Sata-0)		
4	B	L	H	A	A	N	SECONDARY DRIVE FAILED (Sata-1)		
5	B	L	H	A	A	N	PRIMARY DRIVE VOLUME ID INCORRECT		
6	B	L	H	A	A	N	SECONDARY DRIVE VOLUME ID INCORRECT		
7	B	L	H	A	A	N	TMONNET ALT. PATH FAILED		

Fig. 21.13 - Housekeeping alarm available on the Secondary T/Mon for TMonNET Alt. Path

### Testing the Alternate Communication Path

The following functionality is available on the Secondary T/Mon from the Dialup Site Monitor screen (Shift-F4 from the Alarm Summary window) while in Monitor Mode. You must first highlight the TMonNET Alt Path dialup site shown below before issuing any commands. There may be multiple dialup sites, but the only one which applies to TMonNET Alt. Path is the one shown below.

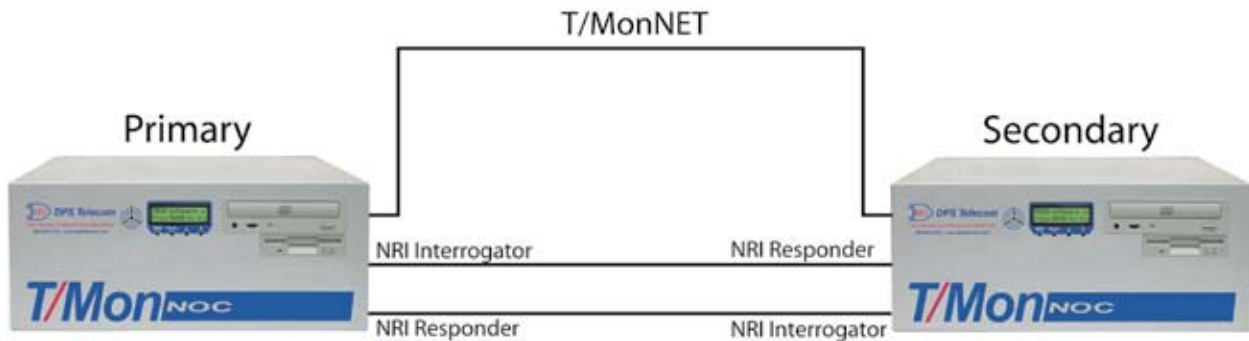
Dialup Site Monitor							
Dev	Site Name	Call	Type	Status	Made	Rcvd	Last Call
TNET	TMonNet Alt Path	Waiting		OK	1	0	Nov 11 12:15
-----							
#=No Phone Number Defined      !=Forced Calls Only							
-----							
Performance/Stats [ 11<TRIP>				Slave <Passive>			
Calls made:	1	Mode	: STANDBY	> A	E	I	M
Calls busy:	0	Site Name	:	B	F	J	N
Call ERRS:	0			C	G	K	O
Hangup ERR:	0			D	H	L	P
Calls Rcvd:	0						
Nov 11, 2004	12:16:22			STAND	:2	Silenced:	0
				COS	:2	Off Line:	0
F1=Call, F2=Hang Up, F3=Cfg, F4=Online, F5=Offline, F10/Esc=Exit				61298268			

Fig. 21.14 - Dialup Site Monitor screen

Table 21.K - Commands available in the Dialup Site Monitor screen

Key	Command	Description
F1	Call	Force a test call to the Primary T/Mon. A call can only be made if the Secondary T/Mon is passive, otherwise forcing a call will cause it to be queued up for when the Secondary T/Mon goes passive. If a call is forced when the primary path is failed then a periodic test will be performed (can cause the system to go active) else if the primary path is working then an integrity test will be performed (cannot cause the system to go active).
F2	Hang Up	Hang-up the modem after the call currently in progress has completed.
F3	Cfg	Disabled
F4	Online	Enable TMonNet Alt. Path.
F5	Offline	Disable TMonNet Alt. Path
F10/Esc	Exit	Exit back to the Alarm Summary Screen.

## TMonNRI



T/MonNRI is an enhancement to the existing T/MonNET Redundant Master Technology. T/MonNRI is designed to automatically synchronize Primary and Secondary masters (T/Mon NOC, T/Mon SLIM, IAM, T/MonXM, etc). In an NRI configuration, the Secondary will be almost instantly ready to take over monitoring after a Primary master failure. Without T/MonNRI, the Secondary can still take over monitoring, but its alarm data will not be in sync with the Primary's alarm data.

## TMonNRI Setup

Two T/Mon units are required to setup NRI. A primary system will be used to receive and poll for alarms while a secondary system will poll only the primary. The secondary will receive any alarms that the primary receives so that, if and when the primary ever goes down, the secondary is ready to take over and will have all the same data.

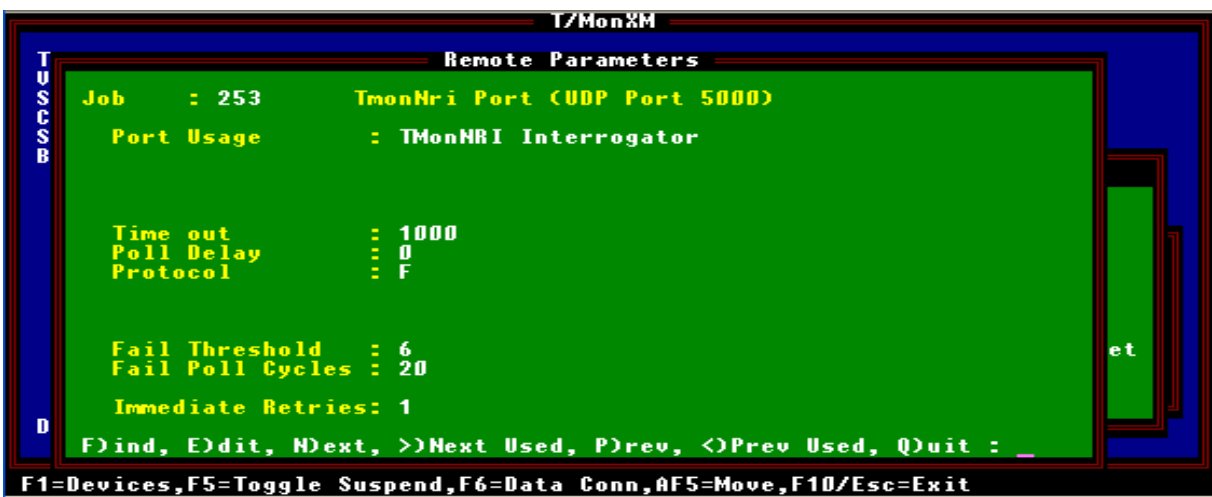
Both units will have the same database so we will only need to set it up on one and copy it to the other.

NOTE: Once your system is up and running, we recommend databasing on the secondary T/Mon and copying to the primary. For this initial setup procedure, however, it will be more convenient to database on the primary and copy to the secondary.

1. Navigate to the Parameters menu and select "Remote Ports"
2. Define a new job for T/MonNRI interrogator. The default settings are acceptable for most setups, except for Protocol and Fail Threshold. Protocol should be F for DCPF and Fail Threshold should be changed to 6 or higher.
3. Press F6 for data connection and choose the T/MonNRI interrogator data connection that we set up in step 2.
4. Back on the Remote parameters screen, while displaying the port for T/MonNRI Interrogator, press F1 to enter the device settings.

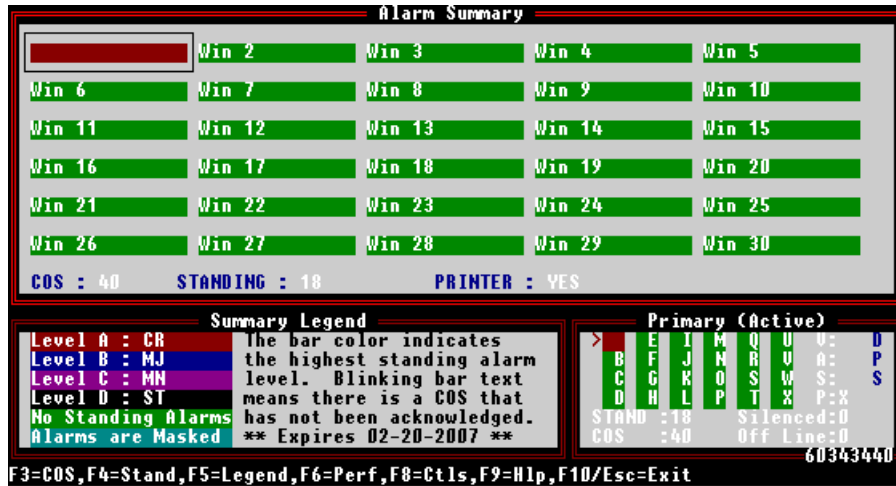


5. Press F for find and enter '1'.
6. You may be asked to create it. If you are, select 'yes'.
7. We will define the primary first. When you are asked for the IP, enter the IP of the primary unit and its responder port. We defined this is step 2, and it should be the same on both units. It is important to define the primary on device 1 and the secondary on device 2.
8. The default data will work for the rest of the settings.
9. Press F to find again but enter 2.
10. If it asks you to create, select yes.
11. Enter the IP of the secondary unit and its responder port. Use the default data for the rest.
12. Back to the Remote Parameters screen (Parameters -> Remote Ports). Define a new job for the T/MonNRI responder.



13. This one will not have as many settings as the interrogator job. Press F6 to setup the data connection and select the one you assigned for the responder job in step 2. It should be the same port that you used in steps 28 to 32.
14. The setup of the primary T/Mon is now complete. Backup the database on the primary T/Mon and restore it onto the secondary (for details, refer to pages 18-1 to 18-3 of your T/MonXM User Manual).
15. After copying, you will need to modify one item on the secondary. On the secondary unit (now loaded with the same database as the primary). Go back to Parameters -> TMonNET -> Address.
16. Enter the address for the secondary. As stated earlier, 251 is the recommended setting. This should also be the same as the one defined in Node Definitions.
17. T/Mon NRI setup is now complete. Initialize the systems and go into monitor mode. If done correctly, the secondary will say (Passive) on the bottom right corner while the primary will say (Active) in the same position.

**Note:** If the secondary ever falls out of sync with the primary, you can force synchronize the secondary (push all standing/COS alarms, silenced alarms, and device status to the secondary. To force sync, from the alarm summary screen (Master Menu > Monitor), press Shift+F10 to go to the database transfer screen, then press F3 to force the NRI sync.



18. It is a good idea to conduct a quick switching test from primary to secondary. When you exit monitor mode on the primary, the Secondary should start counting down. It will use the T/MonNET switch threshold value before it changes from (Passive) to (Active). If it has been a while and the primary is not in monitor mode but the secondary is still in monitor mode and passive, check your settings and make sure that you completed the setup procedure correctly. If the secondary unit did go Active, bring the primary back into monitor mode and the secondary should go back to passive. If the secondary switched to active when you took the primary out of Monitor Mode, then returned to passive when you put the primary back into Monitor Mode, you have completed the quick test and **T/MonNRI has been set up correctly.**

## Section 22 - DNS

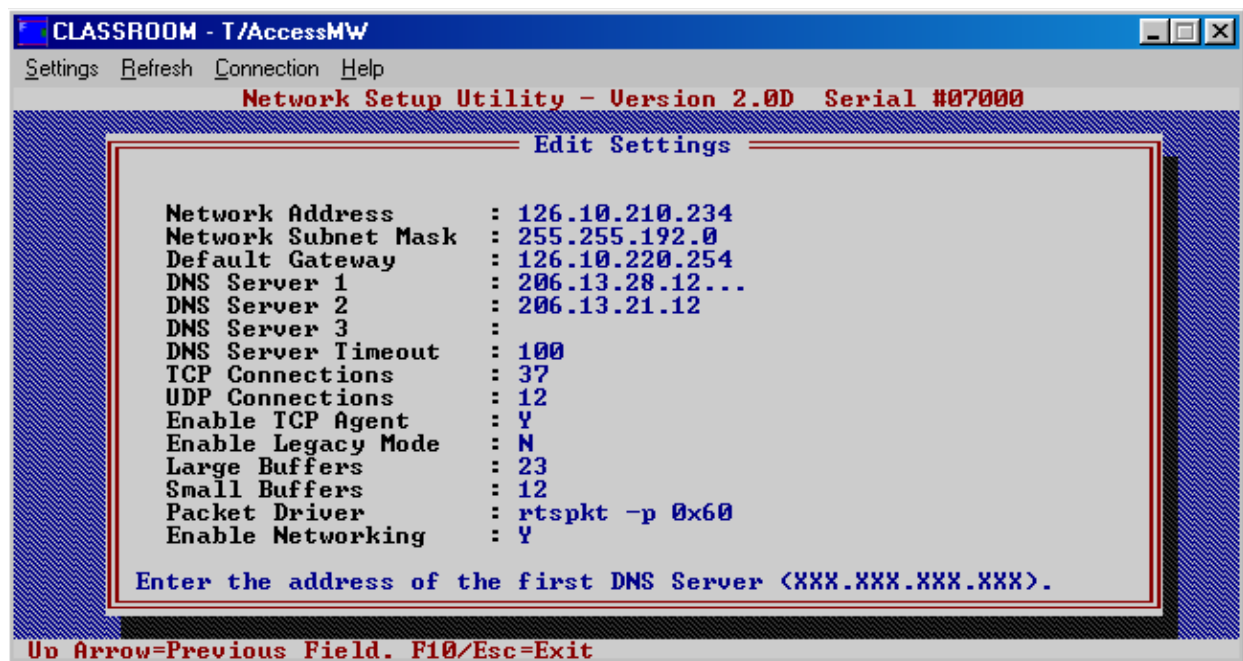


Fig. 22.1 - Assign up to 3 DNS Servers for T/Mon to use for hostname resolution

### *New in 4.7*

T/Mon now resolves hostnames into IP addresses by using DNS.

T/Mon can be setup to use a DNS Server to resolve hostnames into IP addresses. This requires that the T/Mon be configured to use anywhere from one to three DNS Servers from the WShell->Network Setup menu. The user can then enter host names in the T/Mon Data Connections screen in addition to IP addresses and T/Mon will act as a DNS Client and resolve the hostnames into IP addresses.

When the T/Mon is configured to use a DNS Server both hostnames and IP addresses can be entered into the Data Connections screen (Figure 22.3) DNS Performance stats have been added to the Performance/Stats window for the Ethernet I/O job (job 28) (Figure 22.2) Note: DNS Cmds is number of DNS refresh attempts and DNS Errors is the number of failed DNS refresh attempts.

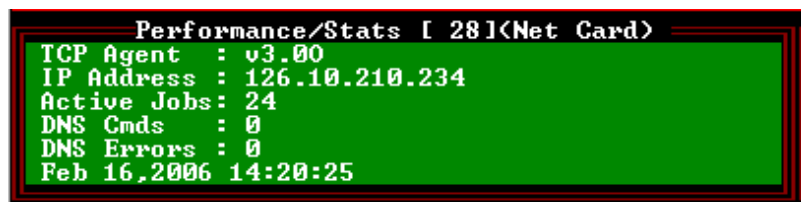


Fig. 22.2 - DNS Performance stats have been added to the Performance/Stats window

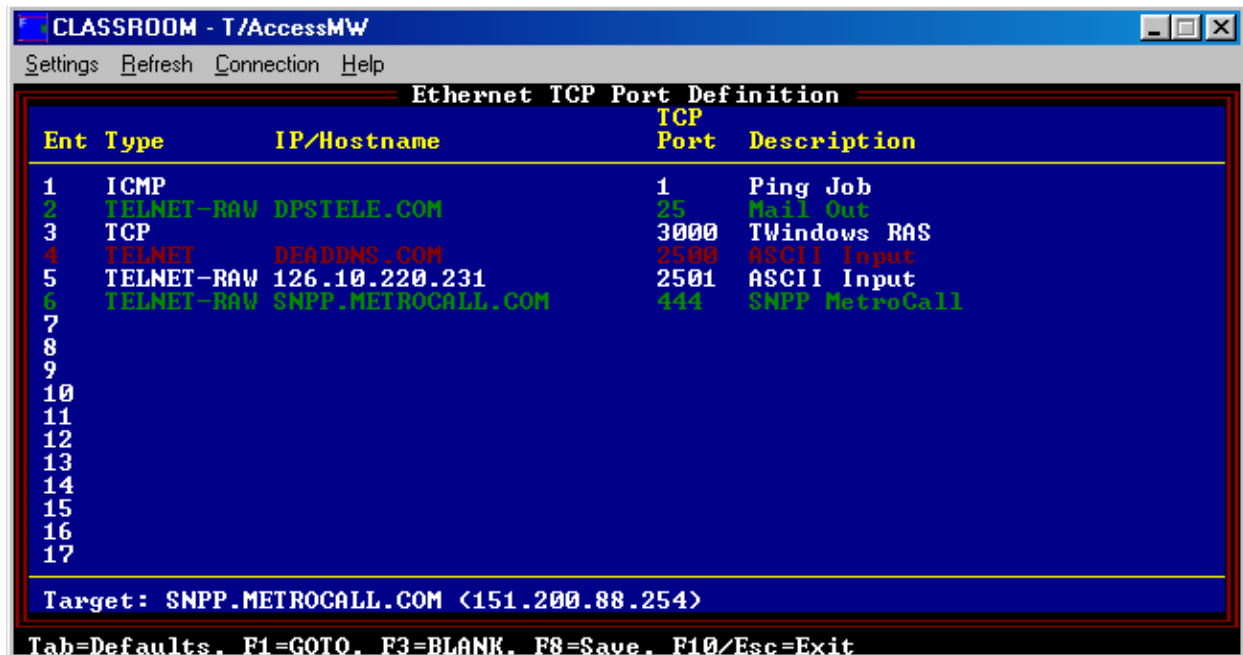


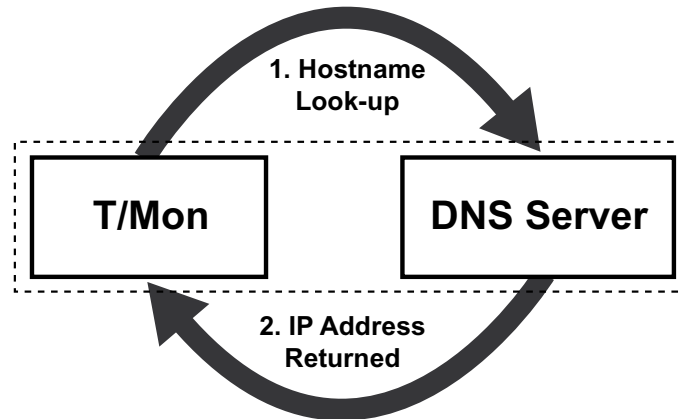
Fig. 22.3 - Both IP addresses and hostnames can be entered

## DNS Operation

Imagine today's world without address books, telephone directories, and speed dials. We would be limited to cumbersome pieces of paper with scribbled notes of telephone numbers and addresses. Furthermore, apply this lack of organization and information to business networks. Trying to remember the IP address of remote units and services would be time consuming.

With address books or scribbled down telephone numbers, loss of that address book or number makes us unable to communicate with each other. DNS allows human friendly hostnames to be mapped to computer addresses (IP Addresses). With T/Mon DNS, network technicians can now reference remote units by name and because IP addresses can frequently change, the mapping of a name to an IP Address helps confine an IP to hostname change to a single location.

Figure 22.4 shows the basics of how T/Mon interacts with a DNS Server for hostname to IP Address resolution.



**Fig. 22.4 - T/Mon functions as a DNS client, querying a DNS Server for hostname to IP Address resolutions.**

**The T/Mon will attempt to resolves hostnames into IP address under the following conditions:**

1. The user enters a hostname in the IP/Hostname field in the Data Connections screen (press Enter once). This allows for the user to immediately determine if the hostname they entered is valid. The T/Mon attempts to immediately resolve the hostname into an IP Address when it is entered. Hostnames in green were resolved and hostnames in red were not resolved. The exception to this would be if no DNS Servers were defined or if all of the DNS Servers defined were down. In either case, the user will be warned that the hostname could not be resolved, but still allowed to enter the hostname in question.
2. When the system is in monitor mode it will periodically refresh all hostnames. The interval of the periodic refresh is user configurable from the Remote Parameters screen of the Ethernet I/O job (see figure 22.5).
3. The system is in monitor mode and an error occurs on the data connection that the hostname is assigned to thereby causing an automatic refresh. An error will only cause an automatic refresh once per periodic refresh timer interval. In other words, if continuous errors were being received and the periodic refresh timer were set to 15 minutes, then an error would only cause one automatic refresh every 15 minutes. This was done to keep the system from continually refreshing under heavy error conditions, and thereby adding to the problem by causing the system to become sluggish.

Another user definable option, related to DNS, is the DNS Request Timeout. This is the time that the DNS Server will have to respond to a DNS request from T/Mon. A timeout is necessary to prevent the system from “hanging” if the DNS Server fails to respond to a request. This option is user configurable from the WShell->Network Setup menu and is defaulted to 100 msec (see figure 22.1).

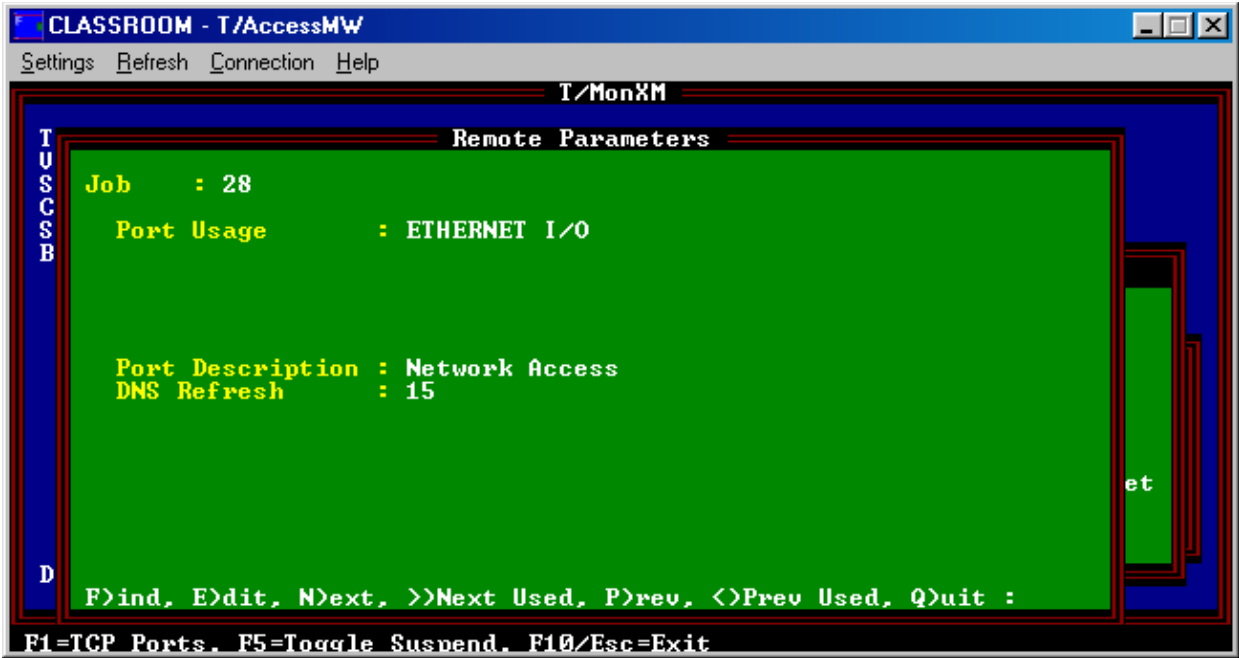


Fig. 22.5 - T/Mon Remote Parameters screen

Table 22.A - Fields in the Remote Parameters screen

Field	Description
DNS Refresh	Interval in minutes between the automatic refresh of all DNS hostnames. This field is only relevant when DNS Servers are defined and when one or more data connections are defined using a DNS hostname (not an IP address). Note: 0 = continuous refresh.

# Software Module 1

## DCP(F) Interrogators and Responders

### DCP(F) Interrogator

Interrogators allow data to be brought into the system. When you use Interrogators, you specify the display list of the items you want to have polled. You can show alarm points on the normal T/MonXM screens under COS windows and Live alarms. In addition to that, alarm points may also go out responder ports.

The DCP(F) Interrogator software module must be installed before you can access the DCP(F) Interrogator. Refer to Section 2 (Software Installation) for installation procedures.

To define a remote port for communication to DCP(F) equipment, select Remote Ports from the Parameters menu and then select DCP(F) Interrogator at the Port Usage field.

**Note:** An example of the Remote Parameters screen defined for a dedicated port for DCP(F) Interrogators is illustrated below. For instructions on defining a IP port for your DCP(F) Interrogators, see section M1-3.

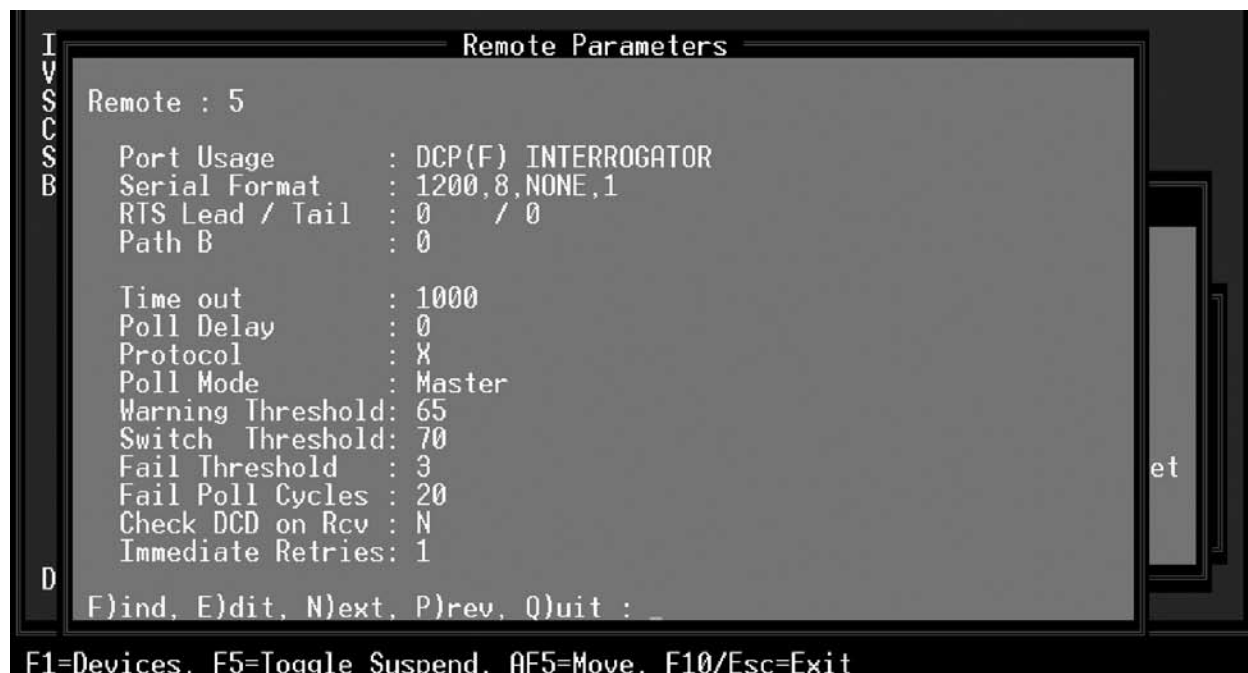


Fig. M1.1 - Example of a defined dedicated port for DCP(F) Interrogators

**Table M1.A - Remote Parameters screen field descriptions**

Field	Description
Port Usage	Select a port from 1-27. Valid port types are DCP(F) Interrogator and Halted. Use Halted (default) if no device is connected to the communication port. [DCP(F) INTERROGATOR]
Serial Format	Baud rate, word length, parity, and stop bits settings. [1200, 8, NONE, 1]
RTS Lead	RTS Lead is the time carrier is turned on before data is sent (0-2500 ms).* [0] <b>Note:</b> Set to 60 for 202 modems.
RTS Tail	RTS Tail is the time carrier is left on after the last byte is sent (0-2500 ms).* [0] <b>Note:</b> Set to 40 for 202 modems.
Path B	Port for secondary path for ring polling application. For more information about ring polling see section M1-38 (Ring Polling Application). [0]
Time Out	Time the interrogator will wait for a response before failing a poll. Valid entries are 200-9999 milliseconds. [1000]
Poll Delay	The Poll Delay is the time between polls. Valid entries are 0-9999 milliseconds. [0]
DCPF Mode	Enter “F” if you wish to use DCP(F) mode and “N” for DCP mode and “X” for DCP(X). Enter “1” for DCP1 mode. DCP(X) is better error detection. All DPS Telecom RTUs support DCP(F). Newer DPS Telecom RTUs support DCP(X). Use DCP and DCP1 when using third party RTUs. [F]
Poll Mode	These determine the way polling is performed. Valid entries are P)assive only, M)aster only, and C)ombined. Enter M if T/Mon is the only device polling the network. <b>Note:</b> If set for Master Mode, the system will ask for Warning Threshold and Time out settings. If set for Combined Mode, the system will ask for Warning Threshold and Switch Threshold settings. <b>Master Mode:</b> Will always attempt to poll RTUs. There should at most be one master in a network. <b>Passive:</b> Never polls network, but will detect alarms. <b>Combined:</b> Starts out passive, but if it senses no activity, it will become master. Will revert to passive if it detects online activity.
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Valid entries are 5-999 seconds. [65]
Switch Threshold	The Switch Threshold is the seconds of no activity before becoming master. Valid entries are 2-999 seconds. [70] <b>Note:</b> This field is only available when “Combined” is entered in the Poll Mode field.
Fail Threshold	Number of consecutive polls before device failure is declared. [3]
Fail Poll Cycles	The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. Valid entries are 0-255. [20]
Check DCD on Rcv	Y = Enable DCD checking to validate Rcv. N = Disable. [N]
Immediate Retries	Number of retries before proceeding with next address. [1]

Once you have finished entering in the parameters for the DCP(F) remote port, the function keys shown below will become available. Press F1 (Devices) to define the DCP(F) equipment addresses and displays that you wish to monitor on the remote port.

**\*Note:** Setting the RTS Lead Time and RTS Tail Time both to 2500 will enable a DCP(F) constant carrier



**Table M1.B - Key commands available in the Remote Parameters screen**

Function Key	Description
F1	Devices. Define the DCP device addresses, alarm displays, and alarm points that are on the current remote port.
F5	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
F6	Data Connection (IP/virtual port connections only)
Alt-F5	Allows you to move the port.
F10/Esc	Exit.

**Define a Virtual (IP) Port for DCP(F) Interrogators**

Defining your remote port for polling your DCP(F) remote devices via the network is a two step process. Refer to Table M1.C to complete the fields on the Remote Parameters screen. See Table M1.B for function keys available.

**Table M1.C - Remote Parameters screen field descriptions**

Field	Description
Port Usage	Select a port greater than 49 (1–27 are defined for dedicated serial ports and 30–49 are typically used for remote access). Valid port types are DCP(F) Interrogator and Halted. Use Halted (default) if no device is connected to the communication port. <b>Note:</b> Unit must have IP hardware installed and port 28 must be set for Ethernet I/O.
Time Out	Time the interrogator will wait for response before failing the poll. Valid entries are 200-9999 milliseconds. [1000]
Poll Delay	The Poll Delay is the time between polls. Valid entries are 0-9999 milliseconds. [0]
Protocol (DCPF Mode)	Enter "X" for DCPX, "F" for DCPF, "N" for DCP, or "1" for DCP1 mode. [F]
Fail Threshold	Number of unanswered polls before device is declared failed. [3]
Fail Poll Cycles	The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. Valid entries are 0-255. [20]
Immediate Retries	Number of retries before proceeding with next address. [1]

For detailed information on creating data connections see section 3-4.

**Create a Data Connection**

1. In the Remote Parameters screen press F6 to open the Data Connection screen.
2. Press F1 to open the Ethernet TCP Ports Definition screen.
3. Use the arrow keys to select a new connection.
4. Press Tab to select a port type. **Note:** Depending on your DCP remote, you may select UDP, TCP, etc.
5. Enter your IP port number and a description. See Section 3, Figure 3.5.
6. Press F8 to save your changes and return to the Data Connection Assignment screen.
7. From the Data Connection Assignment screen, press Tab to

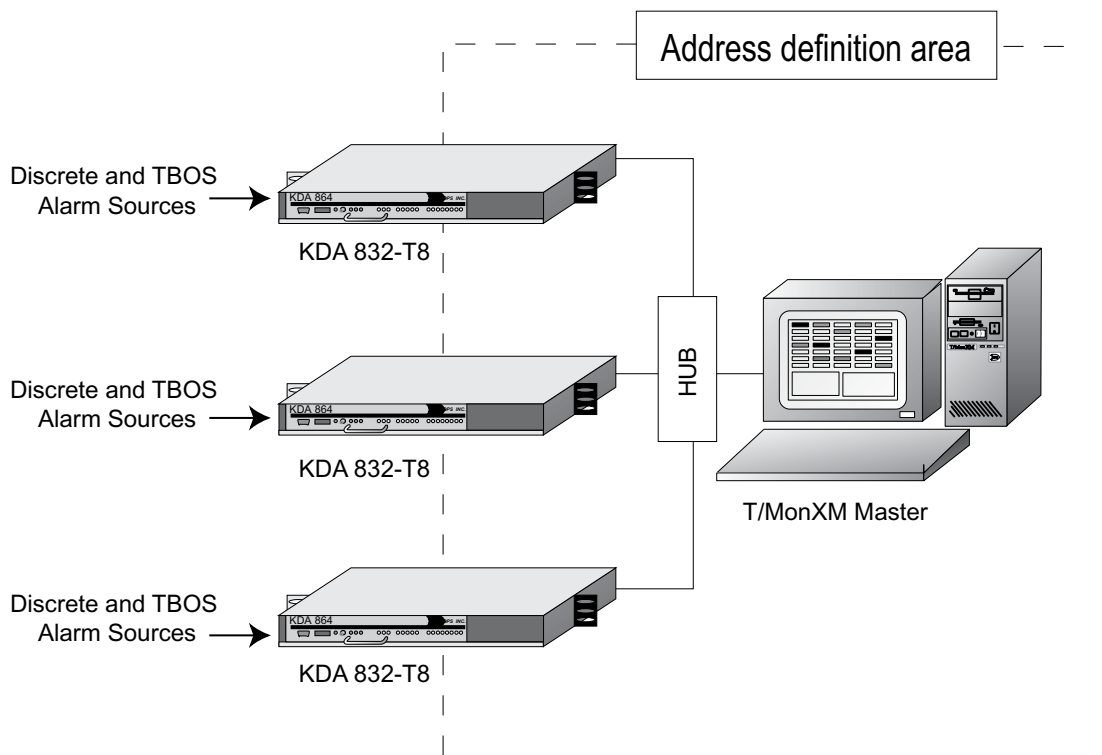
select the List Box. Select the IP port you just defined for the data connection. (See Section 3, Figure 3.7). Then return to the Remote Parameters screen.

## DCP(F) Device Definition

**Note:** DPS Telecom dial-up RTU users should refer to section M3 for Dial-Up Networks, KDA Shelves, and LAN-Based Remotes.

Pressing F1 (Devices) from a Remote Parameters screen that is defined for communicating to a DCP(F) device will bring you to the Remote Device Definition screen. The purpose of the Remote Device Definition screen is to create the alarm equipment polling list from which T/MonXM will use to gather its information. The addresses of each DCP(F) device that is to be monitored or polled within the alarm system must be entered from here. Each Address Definition represents one device.

An Address Definition consist of a DCP(F) device address, a user-definable name, device type, displays to monitored and if you are in active polling mode, the method of polling. The application drawing shown below depicts the alarm monitoring area that this definition affects:



**Fig. M1.2 - Diagram of alarm monitoring area**

Remote Device Definition		
Port	: 3	DCP(F) INTERROGATOR
Address	: 1	
Description	: KDA IN LAB	
Site Name	: DPS LAB	
Device Type	: Standard	
Displays	: 1-5	
Poll Type	: U	
Refresh Rate	: 124	
Firmware Ver	: 3.00	
Log Undefined	: N	
----- Address Defaults -----		
Polarity	: B	Windows : 0
Logging	: L	Message : 0
History	: H	
Level	: A	
Status	: A	
Reverse	: N	
Description	: (Undefined)	

Up Arrow=Previous Field. F10/Esc=First Field

Fig. M1.3 - Defined Remote Device Definition screen

**Note:** Refer to Table M1.D on the following page for field descriptions.

In the example above, the device is defined to monitor alarm information from a KDA LR24 Card addressed as #1 and will report any alarm information that is stored in alarm displays 1 through 5. The polling type is what command will be used to gather information. In the example, the polling type is set to U (upset) — see “Poll Type” on following page.

#### Defining an Address

First enter the DCP(F) address number you wish to define or edit. At this point, T/MonXM will check the system for the address entered to see if it exists. If the address is found, any previously defined information for that address will then be displayed on the screen and an option line will be displayed at the bottom of the screen. If the address isn't found, T/MonXM will ask if you want to add it to the system:

“This item is not in the database. Would you like to add it (Y/N)?”

Once added, you may then go down, line by line, making changes as needed. After the last field has been entered, the cursor will go to the “Find, Edit, Delete, Next, Prev, Quit:” prompt to get ready for another definition.

**Caution!** Deleting a unwanted Address Definition will not delete the points that were defined for that address. Therefore, you should first delete all the points contained in a DCP(F) address before deleting the DCP(F) address. The delete function was implemented this way in order to protect the user from the deletion of a large point database because of the accidental erasure of the wrong DCP(F) address.

**Table M1.D - Remote Device Definition screen field descriptions**

Field	Description
Port	The Port number used by the Remote Device.
Address	The DCP(F) address that you want to create or edit. Valid DCP(F) addresses range from 1-255. These should match the addresses assigned to KDAs or other DCP(f/x) devices.
Description	The description of the use of the address. A maximum of 50 Alphanumeric characters can be used.
Site Name	This field allows you to assign a name to all alarm information that is gathered under the DCP(F) address. A maximum of 50 Alphanumeric characters can be used.
Device Type	Enter the device type that you wish to define for the current Address Definition. Enter "S" for standard.
Displays	The alarm displays of the DCP device address that are to be monitored. Valid alarm displays range from 1-140. Sample display range inputs: 5,7,20,30 or 5-20,30-45,8 <b>Note:</b> To maximize execution speed and minimize the amount of disk space used, define only the displays that are being monitored.
Poll Type	Selects the refresh type of poll to be done for that DCP(F) address. Valid inputs are:
	"U" - Upset Polling Selects if Upset Polling (Change of State) is desired for the DCP(F) address. will assign a refresh rate.
	'G' - Group Polling Group Poll will poll two displays worth of data at a time. Group polling will start with the first group defined in T/Mon <b>Note:</b> This is the fastest polling method if the database is relatively small in size.
	'F' - Full Polling Updates every single point status on every single poll. <b>Note:</b> After a user selectable number of poll cycles, a status poll cycle will be performed to verify alarm data.
Refresh Rate	Number of poll cycles before a FUDR is issued. Refresh Rate is the rate after which a full alarm status refresh will be performed. Refresh Rate is used only with Upset Polling.
Log Undefined	Enter Y=Yes, N=No.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A (CR), B (MJ), C(MN) or D(ST) [A]
Status	Alarm(A), Status(S) [A] Defines if T/Mon internal relay will change state.
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which undefined alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

## Point Definition (F1)

**Note:** For detailed information on point definition please refer to Section 10.

This option allows the user to assign attributes and English descriptions to individual alarm points within the selected displays of the DCP(F). Defining alarm point definitions are done on a display-by-display basis. Note that you must have defined the displays previously in the Address Definition section.

1. Entering F1 (Points) from the Remote Device Definition screen will bring you to the Point Definition screen — see Figure M1.4.
2. If no display was previously entered, the cursor will be at the display number from which the DCP(F) stores the alarm point information.
3. After <Enter> has been pressed at the Display field, the database management system checks to see if any points in that display have been defined previously. If none are found, then the cursor immediately moves into the point editing area.
4. If points in the display have been defined before, then the Standard Key Entry prompt, (See Section 4), appears at the bottom of the window. To edit the points, press 'E' to select the Edit option.
5. When the cursor is in the point editing area, the Message window displays the message associated with the point that is currently being edited.
6. The Up Arrow, Down Arrow, PgUp, PgDn, Home and End keys are used to select a point for editing. Note that these keys are only active when the cursor is at the Pol (polarity) field.

**Note:** For Point Definition Field descriptions refer to Section 10.

Point Definition																									
Port	:	2	Addr:	1	Disp:	1	Display Desc :																		
P	L	H	L	S	R																				
o	o	s	e	t	v																				
					DCP(F) INTERROGATOR																				
Pt	l	g	t	v	s	s	Description																		
1	B	L	H	A	A	N	OPEN DOOR																		
2	B	L	H	A	A	N	HIGH TEMP																		
3	B	L	H	A	A	N	LOW TEMP																		
4	B	L	H	A	A	N	BEACON																		
5	B	L	H	A	A	N	EAST RADIO																		
6	B	L	H	A	A	N	WEST RADIO																		
7	B	L	H	A	A	N	PRIMARY SWITCH																		
8	B	L	H	A	A	N	SECONDARY SWITCH																		
<table border="1"> <thead> <tr> <th>Fail</th> <th>Clear</th> </tr> </thead> <tbody> <tr> <td>OPEN</td> <td>CLOSED</td> </tr> <tr> <td>HI</td> <td>NORM</td> </tr> <tr> <td>LO</td> <td>NORM</td> </tr> <tr> <td>OUT</td> <td>NORM</td> </tr> <tr> <td>FAIL</td> <td>NORM</td> </tr> <tr> <td>FAIL</td> <td>NORM</td> </tr> <tr> <td>FAIL</td> <td>NORM</td> </tr> <tr> <td>FAIL</td> <td>NORM</td> </tr> </tbody> </table>								Fail	Clear	OPEN	CLOSED	HI	NORM	LO	NORM	OUT	NORM	FAIL	NORM	FAIL	NORM	FAIL	NORM	FAIL	NORM
Fail	Clear																								
OPEN	CLOSED																								
HI	NORM																								
LO	NORM																								
OUT	NORM																								
FAIL	NORM																								
FAIL	NORM																								
FAIL	NORM																								
FAIL	NORM																								
F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :																									
<div> <div>Message</div> <div></div> </div>																									
F10/Esc=Exit																									

Fig. M1.4 - Point Definition screen

## Analog Point Definition (F5)

1. From the Remote Device Definition screen, press F5 to open the Analog Provision screen, shown in Figure M1.5. Table M1.E explains the fields in this screen.
2. Fill in the Description, Sig (Significant digits), and Unt (Units ) fields.

```

Analog Provisioning

Port: NG    Address: 1

Declare Threshold Alarms Locally : NO

(Native Unit Thresholds)
Alg Description      Sig Unt MjOvr MnOvr MnUdr MjUdr
1 Battery A.....  2  VDC 54.00 52.00 44.00 42.00
2 Battery B        2  VDC 54.00 52.00 44.00 42.00
3 Tower Lt curr    3  mA  18.00 15.00  8.000 6.000
4 Outside Temp     2  F   99.37 87.00 16.87 12.75
5 Inside Temp      2  F   78.75 74.62 41.62 33.37
6 Cable Press      2  PAL 18.00 16.00 10.00 8.000
7 Loop Current     3  mA  18.00 15.00  8.000 6.000
8

Enter description

Description : (Undefined)

E)dit, N)ext, P)rev, Q)uit :

F1=Define Scale, F2=Toggle Threshold Mode, F8=Save, F9=Help, F10/Esc=Exit

```

Fig. M1.5 - Analog Provisioning screen

Table M1.E - Fields in the Analog Provisioning screen

Field	Description
Alg	Point number (fixed field)
Description	Enter the point description. Can be up to 14 characters.
Sig	Significant digits. Enter the number of digits to display after the decimal.
Unt	Enter the Units label, e.g., VDC, VAC F, C, psi, mA, etc.
F1 - Define scale	Calculates offset and scale values for each analog point. This should be done before entering Threshold values. See description below. Press F6 to set scale and offset value to unity.
MjOvr	Major over threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
MnOvr	Minor over threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
MnUdr	Minor under threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
MjUdr	Major under threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).

## Analog Display Worksheet

**Note:** This operation is optional for users who want to change the analog reference scale so that the displayed analog values correspond to real world values.

To define your analog reference scale, press F1 from the Analog Provision screen. The Analog Display Worksheet screen is used to convert the analog voltage and current readings into meaningful measurements and units. The analog inputs actually only measure either voltage or current. The values must be converted to their actual units by determining the scale and offset for each input. By entering in a few simple values, T/Mon will make the conversion calculations automatically. Each field and its function are described below.

### Analog input type - Volts or Current (V/C)

This field is where the type of electrical input to the analog channel is selected. This is either V or C for voltage or current. Determine this by the type of sensor or input device used for each input.

### Voltage/Current value 1

This is the lowest/minimum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

### Unit value 1

This is the lowest/minimum measurement in the native units of the analog input (degrees, % relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the minimum range here.

```

Analog Provisioning
Port: NG Address: 1
De
Alg
1 Analog input type - Volts or Current (V/C) : C
2
3 Current value 1: 4.00000 Unit value 1 : -45.000 F
4 Current value 2: 20.0000 Unit value 2 : 120.000 F
5
6 Calc Scale : 10.3125 Calc Offset: -86.250
7
8
En Enter analog input type: V for Volts, C for Current
Description : (Undefined)
E)dit, N)ext, P)rev, Q)uit :
Up Arrow=Previous Field, F6=VDC, F8=Save, F10/Esc=First Field [DPS]

```

Fig. M1.6 - Analog Display Worksheet screen

**Voltage/Current value 2**

This is the highest/maximum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

**Unit value 2**

This is the highest/maximum measurement in the native units of the analog input (degrees, % relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the maximum range here.

After entering the minimum and maximum ranges in both actual voltage or current values and native units, the calc scale and calc offset will automatically be calculated. After exiting the worksheet, key through the remaining entries for that input to make the changes effective.

## Device Failures/ Offlines (F3)

Entering F3 (Int Alarms) from the Remote Device Definition screen for defined DCP(F) Interrogators will bring you to the Device Internal Alarm Assignment screen. Refer to Section 14 for more information on Internal Alarms.

Device Internal Alarm Assignment				
Port : 9				
Address	Dev	Description	Fail	Offline
1	DCPf	Sites 1-11	11.1.3..	11.1.4
Enter internal point (addr.disp.pnt) (blank=none) (address range: 11-13)				
F8=Save, F10/Esc=Exit				

Fig. M1.7 - Device Internal Alarm Assignment screen

## Control Relays

Controls that are associated with a DCP device would be configured in Label Controls or Site Controls. For detailed instructions see Section 12 "Configure Controls."



## DCP(F) Database Transfer

**Note:** Only available if multiple TMonXMs are in use — see Section 20 (Configure Redundant Dual T/Mon Backup).



Fig. M1.8 - Network menu

The DCP(F) database transfer section allows you to setup your DCP(F) database transfer menus, selections for setting up slaves and setting up the network nodes and ports.

First, Define a remote port for communication to DCP(F) equipment. Do this by selecting Remote Ports from the Parameters menu and then define a port for DCP(F) Interrogator on the Remote Parameters screen. This is explained in the previous part of this software module documentation.

### TMonNET Port

Select TMonNET from the Parameters menu, to set up the data transfer variables for T/MonXM. An example of the TMonNET menu is shown to the left.

To assign what port the job will setup select Port from the TMonNET menu. The TMonNET Port window will appear — see Figure M1.9. Enter the DCP(F) port number that you previously defined for the TMonNET Port. The TMonNET Port is the Port on both T/Mon systems that physically connect the system. It must also be set up for DCP(F) or DCP(X) protocol. This port is typically used to control protection switches. It may also be used to poll DCP(F) RTUs, though this is not recommended.



Fig. M1.9 - TMonNET Port window

Table M1.F - Field in the TMonNET Port window

Field	Description
TMonNET Port	Enter the port number for DCPF database transfer. Valid entries are 1-500. A "0" (zero) entry assigns no port for transfer

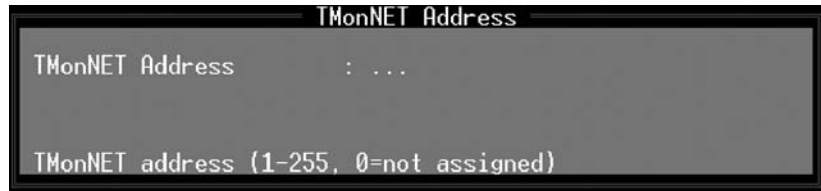
Table M1.G - TMonNET Port window key command

Field	Description
F10/Esc	Exit. Exits from this portion of the program.

**TMonNET Address**

Selecting Address from the TMonNET menu allows you to access the TMonNET Address window and define the network address.

This is the network address that you assign to **the T/MonXM system currently being edited** in the master/slave network. An example of the TMonNET Address window is shown below.



**Fig. M1.10 - Network Address window**

**Note:** *The network address can be indexed with other DCP(F) remote addresses.*

The field on the TMonNET Address window is as follows

**Table M1.H - Field in the TMonNET Address window**

Field	Description
TMonNET Address	DCP address that you are assigning to the T/MonXM system. Valid entries are 1-255. A "0" (zero) entry assigns no address. Each T/MonXM system in the TMonNET network must have a unique address.

**Table M1.I - TMonNET Address window key command**

Field	Description
F10/Esc	Exit. Exits from this portion of the program.

### TMonNET Nodes

Selecting Nodes from the TMonNET menu allows you to access the TMonNET Node Definition screen and define the network node definitions. This is where you define the master and slave addresses that are on the system. An example of the TMonNET Node Definition screen is shown below:

TMonNET Node Definition						
				This System : Not assigned		
Entry	Addr	Site Name	Poll Mode	Warning Thresh	Switch Thresh	Time out
1	255	Arco Plaza L.A.	MASTER	65		1000
2	254	Plano, TX slave	COMBINED	65	70	1000
3	253	Fresno, CA	PASSIVE	65		1000
4	...					
5						
6						
7						
8						
Enter Node Address (1-255)						

**Fig. M1.11 - TMonNET Node Definition screen**

**Note:** The fields and function keys on the TMonNET Node Definition screen are described in Tables M1.J and M1.K on the following page.

**Table M1.J - Fields in the TMonNET Node Definition screen**

Field	Description	
Entry	This is the entry reference number.	
Addr	Enter the DCPF address of the network node. Valid entries are 1-255.	
Site Name	Enter the node site name. (Maximum 15 character name.)	
Poll Mode	Enter the defined polling mode for that system. Valid entries are Passive, Combined, or Master. Note: If set for Master Mode, the system will ask for Warning Threshold and Time out settings. If set for Combined Mode, the system will ask for Warning Threshold and Switch Threshold settings.	
	Master Mode	Will always attempt to poll RTUs. There should at most be one master in a network.
	Passive	Never polls network, but will detect alarms.
	Combined	Starts out passive, but if it senses no activity, it will become master. Will revert to passive if it detects online activity.
Warning Thresh	Enter the seconds of no activity before warning is sent. Valid entries are 5-999.	
Switch Thresh	The Switch Threshold is the amount of time after the slave site sees no activity before it will switch over to active polling mode and poll the network. Valid entries are 2-999.	
Time out	Enter the communication timeout that was set on the Remote Parameters screen. Valid entries are 200-9999 milliseconds.	
IP Address	If using a port job above port 30, enter the IP Address of the secondary T/Mon unit.	

**Table M1.K - Key commands available in the TMonNET Node Definition screen**

Function Key	Description
F2	Port Information which list which ports have a job.
F3	Blank. Deletes the current entry.
F8	Save. Saves the Network Node Definition database.
F9	Help. Online Help.
F10/Esc	Exit. Exits without saving any changes that may have been made.

## DCP(F) Network Status (Monitor Mode)

Pressing Shift-F10 (DCP(F) Network) from the Monitor Mode Alarm Summary screen activates the database transfer screen. This screen displays the slave addresses and IDs in the Network Status window and shows the progress of the database transfer in the Download Statistics window. The standard Page Index window is also shown.

To perform a download, use the cursor keys to highlight the slave system that you wish to send the database (provision). Press F1 (Download) to initiate the download. Press F2 (Get Database) to retrieve a database.

**Note:** You can watch the download in the Download Statistics window. Refer to Table M1.L for field descriptions in the Network Status window. See Table M1.M for field descriptions in the Download Statistics window.

## Manual NRI Sync

If your Secondary T/Mon ever falls out of sync with the primary, you can manually synchronize your secondary with the primary, pusing the all standing/COS alarms, silenced alarms, and device status from the Primary T/Mon to your Secondary by pressing F3 from the DCP(f) Network Status Screen.

For more information about T/Mon NRI setup and function, see section 21 of this manual.

The screenshot displays the Database Transfer screen with three main sections:

- Network Status:** A table with columns 'Addr' and 'Site Name'. It shows one entry: '251 Backup System' with a 'Transfer Status' of '-----'.
- Transfer Statistics:** A list of fields for tracking the transfer: File Id, File Name, Block, Sequence, Position, and Retries.
- Page Index:** A grid of letters (A-Z) used for navigation. Below it, status indicators are shown: STAND :30, COS :44, Silenced:0, and Off Line:0.

At the bottom, a legend reads: F1=Send Database, F2=Get Database, F5=Force Master, F10/Esc=Exit.

Fig. M1.12 - Database Transfer screen

Table M1.L - Fields in the Network Status window

Field	Description
Addr	The slave's address.
Site Name	The slave's site name.
Transfer Status	Indicates the download status.

**Table M1.M - Fields in the Download Statistics window**

Field	Description
File Id	This is a description of the data is being transferred.
File Name	This is the name of the files that are being transferred.
Block	This the block number of the file name that is being transferee.
Sequence	Transfer packet information.
Position	Transfer packet information.
Retries	Indicates the number of retries because data wasn't acknowledged that it was sent correctly.

## Address Statistics (Monitor Mode)

Pressing Shift F6 (Address Statistics) from the Monitor Mode Alarm Summary screen brings up the Site Statistics screen. An example of the Site Statistics screen is illustrated below:

The fields on the Site Statistics screen are described in Table M1.O.

Site Statistics [ 2](DCPF INT)						
Address	Device	Site Name	Polls	Good	Bad	Status
1	STD	FRESNO	274	274	0	ACTIVE
2	STD	FRESNO	13	0	12	FAIL
4	STD	HOUSTON	136	136	0	ACTIVE
5	STD	HOUSTON	12	0	12	FAIL
6	STD	DENVER	136	136	0	ACTIVE
7	STD	DENVER	136	136	0	ACTIVE
8	STD	BOSTON	136	136	0	ACTIVE
9	A16	BOSTON	136	136	0	ACTIVE
20	MAT	LOS ANGELES	12	0	12	FAIL [UNKNOWN]
21	MAT	LOS ANGELES	12	0	12	FAIL [UNKNOWN]
22	MAT	LOS ANGELES	12	0	12	FAIL [UNKNOWN]
23	STD	LOS ANGELES	12	0	12	FAIL

Site Statistics				Page Index			
				> A	E	I	M
				B	F	J	N
				C	G	K	O
				D	H	L	P
				Q	R	U	V
				S	T	X	P:X
				STAND :30	Silenced:0		
				COS :44	Off Line:0		

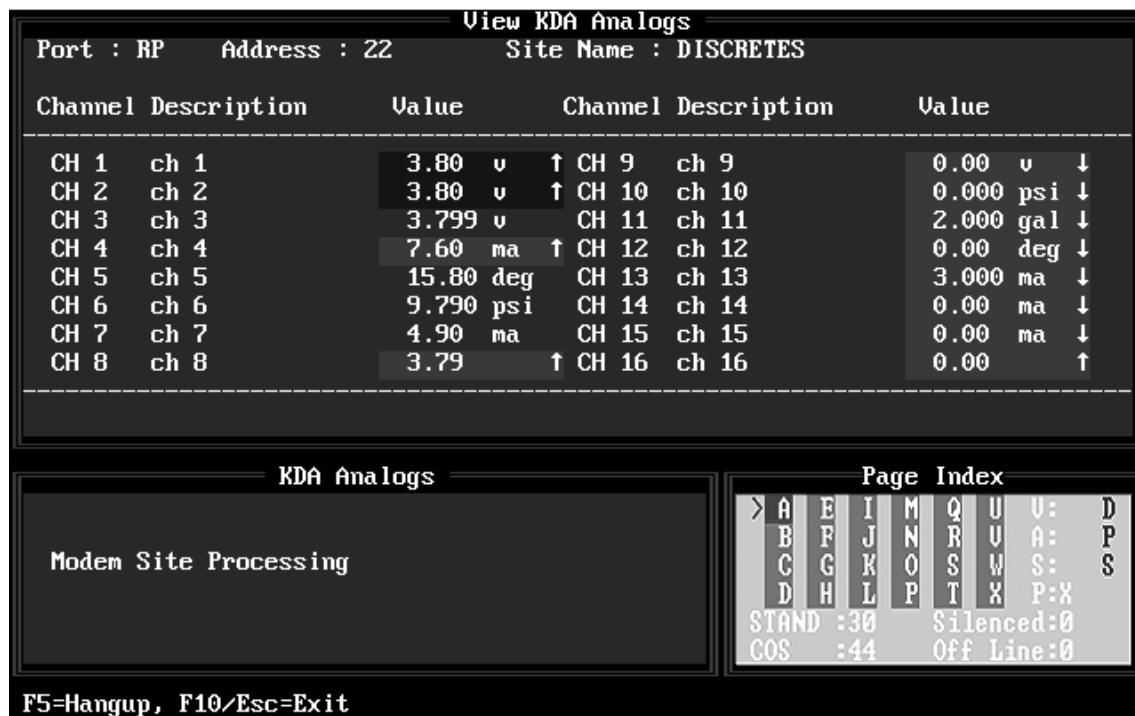
F1/AF2=Init Stats,F2=Poll,F3=Cfg,F4=Online,F5=Offline,F10/Esc=Exit

**Fig. M1.13 - Site Statistics screen****Table M1.N - Key commands available in the Site Statistics screen**

Function Key	Description
F1	Init Stats. This resets the counts back to zero to start fresh.
F2	Force poll to remote.
F4	Put unit online.
F5	Take unit offline.
F6	View analogs.
F10/Esc	Exit. Exits from this portion of the program.

**Table M1.O - Fields in the Site Statistics screen**

Field	Description	
Address	The device address that is assigned to that port.	
DCM Interrogator Devices	MAT	MAT (400)
	CPM	Critical Point Module
	VDM	Dantel™ Card
	SBP	Smart Bypass Card
DCP(F) Interrogator Devices	STD (DCPF)	Standard JACE-5XX (Modbus device) Testset
	NET	Network slaves that are on the system
	DPM	Discrete Point Module
	BVM	Battery Voltage Monitor Card
	PWS	Protection Switch
	DAS	TBOS/ASCII Expansion
	A08	8 Channel Analog (Exp)
8 Channel Analog (B) (Exp)	KDA	KDA Timestamp Base
KDA 832-T8	A16	16 Channel Analog (Exp)
16 Channel Analog (400)	A8T	8 Analog/4 TBOS
	T08	8 Channel TBOS (400)
	NG	NetGuardian
	NGC	NetGuardian C
	216	NetGuardian 216
	NW	NetWatchman
	GLD	General LED Display
	BAC	Building Access Controller
	APS	Alt Path Switch
	D5K	DS5000
	UNK	All other devices not listed
Site Name	This is the site name that was assigned to the device.	
Polls	This is a continuous count of the polls that have been sent out to the site	
Ok	This is the number of OK responses to the polls.	
Fail	This is the number of Failed responses to the polls.	
Status	Indicates whether or not the device is actively being monitored and is a good device that is answering. An OFFLINE statement occurs if the device is manually taken offline. A FAILED statement occurs if the device failed to answer in 3 consecutive polls.	



**Fig. M1.14 - View KDA analogs screen shows each channel in converted value and units.**

## View Analogs

Poll type automatically changes from upset to full update when viewing a dedicated analog value.

Analog values are displayed in native units, e.g., degrees.

To read analog values from a (dedicated line) KDA remote equipped with an Analog Expansion Card or a 400-type analog card, or from a NetGuardian, press Shift-F6 while in the main monitor screen. The Site Statistics screen will be displayed. Select the address/ device / site name for the desired remote.

Press F6 to see the View KDA Analogs or View Net Guardian screen. During this function other alarms will be received via the dedicated port being used for the analog values. Other ports will also continue to be monitored. The Page Index Window will indicate if any new alarms are received.

To read analog values from a (dial-up) KDA remote equipped with an Analog Expansion Card or a 400-type analog card, press Shift-F4 while in the main monitor screen. The Dialup Site Monitor screen will be displayed. Select the address/ device / site name for the desired remote. Press F6 to see the View KDA Analogs screen. Press F5 to cause the modem to dial the site for the latest analog data.\* The modem remains on line monitoring the analog values until F5 is pressed again to hang up the modem. During this function no other alarms can be received via the dial port. Other ports will continue to be monitored. The Page Index Window will indicate if any new alarms are received. You must press F5 again to cause the modem to hang up.

Points in alarm will display the severity (alarm level) color behind the point value, plus an arrow pointing up for over threshold alarms and an arrow pointing down for under threshold alarms.

\*Does not work for a 400-type analog card.



## DCP(F) Responder

The DCP(F) Responder software module must be installed before you can access the DCP(F) Responder. Refer to Section 2 - Software Installation for installation procedures.

To define a remote port for communication to DCP(F) equipment, select Remote Ports from the Parameters menu and then select DCP(F) Responder at the Port Usage field.

An example of the Remote Parameters screen defined for DCP(F) Responders is illustrated in Figure M1.15. Refer to Table M1.P for field descriptions.



Fig. M1.15 - Remote Parameters screen defined for DCP(F) Responders

Table M1.P - Remote Parameters screen field descriptions

Field	Description
Port Usage	Valid port types are DCP(F) Responder and Halted. Use Halted (default) if no device is connected to the communication port.
Serial Format	Baud rate, word length, parity, and stop bits settings. [1200, 8, NONE, 1]
Time Out	Time the interrogator will wait for a response before failing a poll. Acceptable values are 200-9999 milliseconds. [1000]
DCPF Mode	Enter "F" if you wish to use DCP(F) mode and "N" for DCP mode and "X" for DCP(X). Enter "1" for DCP1 mode. DCP(X) is better error detection. All DPS Telecom RTUs support DCP(F). Newer DPS Telecom RTUs support DCP(X). Use DCP and DCP1 when using third party RTUs. [F]
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds. [60]
Check DCD on RCV	Y = Enable DCD checking to validate RCV. N = Disable. [N]
RTS Lead Time	RTS on time (0-2500msec). [0] <b>Note:</b> Set to 60 for 202 modems.
RTS Tail Time	RTS on time (0-2500msec). [0] <b>Note:</b> Set to 10 for 202 modems.

## Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined DCP(F) Responders will bring you to the Remote Device Definition screen.

An example of the Remote Device Definition screen is illustrated in Figure M1.16.



**Fig. M1.16 - Remote Device Definition screen**

**Fig. M1.Q - Fields in the Remote Device Definition screen**

Field	Description
Port	Enter the Port. Valid entries are 1-500.
Address	Enter the Address of the device. Valid entries are 1-255.
Description	Enter the Description of the device.

```

Remote Device Definition
Port      : 2      DCP(F) RESPONDER
Address   : 1

Responder Definition

-----Interrogator-----
Display  PORT   DEVICE  ADDR      DISPLAY
-----
1        5      1       1         1
2        IA     11.     1         1

Enter Address Number (11-13)

Up Arrow=Previous Field, F10/Esc=First Field

```

Fig. M1.17 - Responder Definition screen

## Responder Definition

Entering F2 (Responder Displays) from the Remote Device Definition screen will bring you to the Responder Definition screen. See Figure M1.17.

Table M1.R - Fields in the Responder Definition screen

Field	Description
Display	Enter the Responding Display Number. Valid entries are 1-64.
Port	Enter the Port Number. Valid entries are Port 1-500, IA (User Internal), LC (Local Control), RP (Modem), K1, K2, NG, and N2.
Device	This field is an address modifier for applicable protocols such as DCM, ASCII, DCP.
Addr	Enter Address Number. Valid entries are 1-255. <b>Note:</b> Enter Address Number 11-12, when IA (User Internal) is selected on the port field.
Display	Enter Display Number. Valid entries for this field are relative to the device defined on the Port field

Table M1.S - Key commands available in the Responder Definition screen

Function Key	Description
F3	Blank. Deletes the current entry.
F8	Save. Saves the Network Node Definition database.
F10/Esc	Exit. Exits without saving any changes that may have been made.

## LAN-Based Remotes — NetGuardian

This section is a step-by-step guide to configuring T/MonXM to receive alarms forwarded from the LAN-based NetGuardian alarm monitoring remote. Before you can poll your remote via the LAN you will need to create a port job first.

**Note:** The NetGuardian may also be configured as a dial-up device. You will have to create a TRIP Dial-up job port. See Software Module 2.

### Step One

#### Define Port 28 for Ethernet I/O

The NetGuardian will need a LAN connection to the T/MonXM system, so your first step is to make sure Port 28 is defined for Ethernet input and output. For instructions on defining Port 28, see Section 3.

### Step Two

#### Define a job port for DCP(F) Interrogator

Next, find an unused port numbered 30 or higher, and define it for DCP(F) Interrogator port usage. Fill in the fields as shown in Figure M1.18 below.

**Note:** You must select X in the DCP(F) mode/Protocol field.



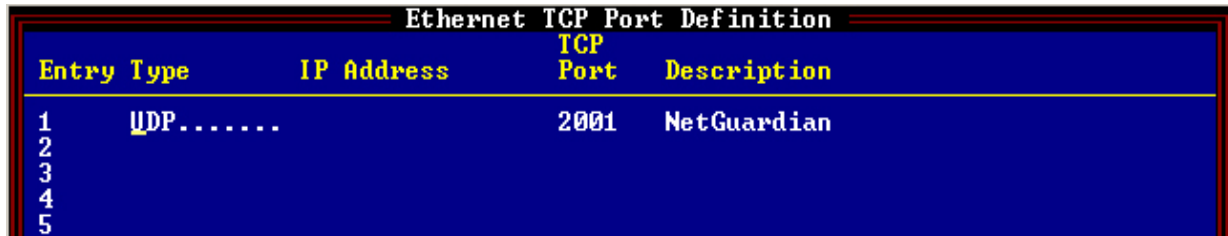
Fig. M1.18 - Define a Job for DCP(F) Interrogator

## Step Three

### Create a Data Connection

Next, create a data connection for the DCP(F) Interrogator.

1. Press F6 to open the Data Connection screen.
2. Press F1 to open the Ethernet TCP Ports Definition screen.
3. Press Tab to select a port type. **Note:** You must select UDP.
4. Enter a port number and description. See Figure M1.19 below.



Entry	Type	IP Address	TCP Port	Description
1	UDP.....		2001	NetGuardian
2				
3				
4				
5				

Fig. M1.19 - Create a UDP port for a data connection

5. Press F8 to save your changes and return to the Data Connection Assignment screen.
6. From the Data Connection Assignment screen, press Tab to select the List Box. Select the UDP port you just defined for the data connection — see Figure M1.20.

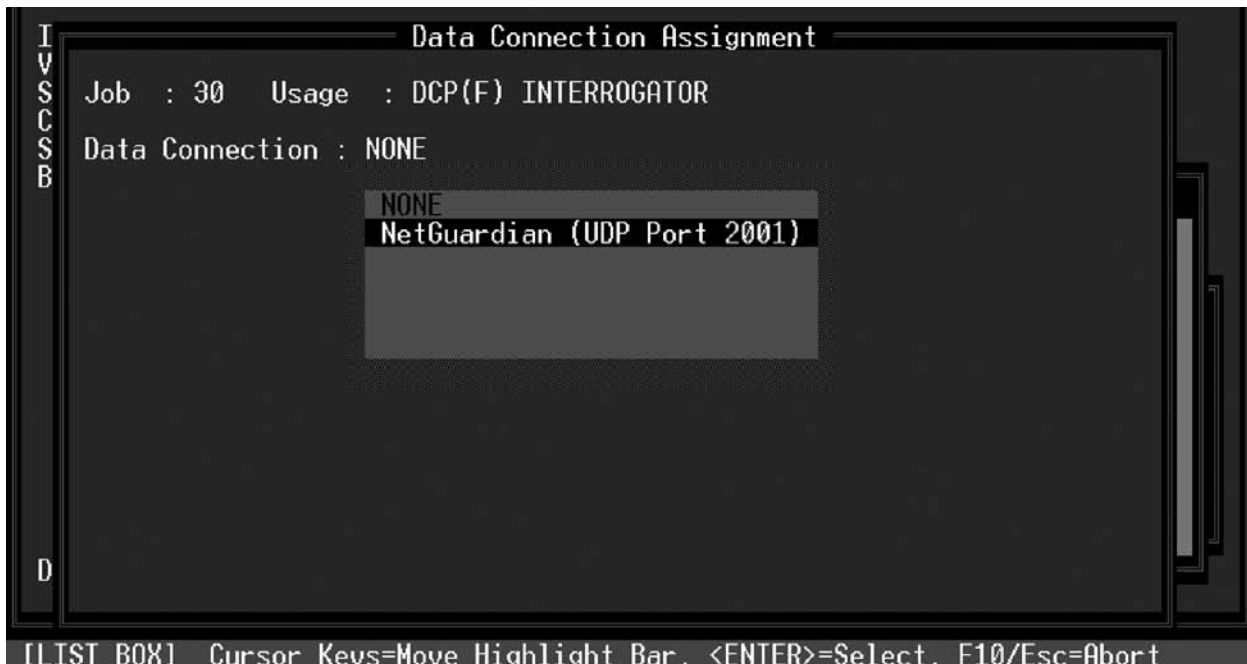


Fig. M1.20 - Select the UDP port in the Data Connection Assignment screen

## Step Four

### Define the NetGuardian

To Provision a NetGuardian in T/Mon, go to Master Menu > Files > LAN-based Remotes > Net Guardian. Then define the NetGuardian on the following screen — see Figure M1.22.

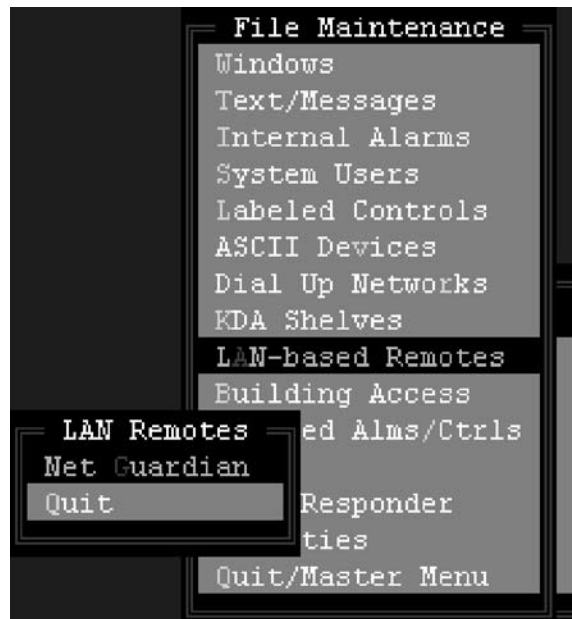


Fig. M1.21 - Select LAN-based Remotes to configure the NetGuardian

```

Net Guardian Definition

Site Number      : 5
Description      : Net Guardian 440 SCHEDULE Y N 1 559 454
Site Name       : FRESNO
Password        :
Device Type     : FULL
Base Proxy Port : 3000
Expansion Units : 1
Expansion Modules : BAC

IP Address / Port : 126.10.220.47 / 2001

Dedicated Port   : 31   Base Addr: 5   Exp Addr #1: 1   Exp Addr #2: N/A

Dialout Port     : 0   Phone:
Polling Type     :
Polling Interval :      Test:
Scheduled Days ---> SUN:   MON:   TUE:   WED:   THU:   FRI:   SAT:
Scheduled Hours  :
Scheduled Minute :

F)ind, E)dit, D)elite, N)ext, P)revious, Q)uit :

F1=Device, F2=Global Options, F3=Int Alarms, F4=Load Firmware, F10/Esc=Exit
  
```

Fig. M1.22 - NetGuardian definition screen

**Table M1.T - Fields in the NetGuardian Definition screen.**

Field	Description
Site Number	3-digit site number. This number is unique over the entire alarm network. This number is the “address” field for responders, derived alarms, and labeled controls.
Description	41 character description of site
Site Name	15 character site name
Password	20-character password. Only needed if T/Mon will be managing the proxy ports.
Device Type	Indicates if the NetGuardian is the standard version or the NetGuardian C version.
Base Proxy Port	Base TCP port for direct data port proxy.
Expansion Units	Number of NetGuardian expansion units connected to base unit.
Expansion Modules	Valid entries: None NMD 4 TBOS/TABS (NetMediator 4-Port TBOS/TABS module) BAC (Building Access Controller module)
IP Address	IP Address and TCP port of NetGuardian
Dedicated Port	If the NetGuardian reports on a dedicated line (DCPF), enter the T/MonXM port number. (Port must have been previously defined.) If the NetGuardian reports only on a dial line, enter ‘0’ (skips to Dial Port field).
Addr:	Enter the DCP(F) address for the unit. This is the address that T/Mon will use to poll the NetGuardian.
Dialout Port	Enter the port number used for dial out, if dial-out only or alternate path is used. Enter ‘0’ if dedicated line only (skips out of edit mode).
Phone	Enter the phone number to reach the remote. <b>Note:</b> See Section 16 (Monitor Mode > Dial-Up Site Monitor) for more information on Dial-up device management.
Test	Enter the number of minutes (0 to 9999) between dial-up integrity tests. This causes T/Mon to check the status of the dial-up link while the primary link is still functional. If T/Mon calls the unit and there is no response from the modem, an alarm condition will occur. The alarm will appear as an internal alarm.
Polling Type	Select Periodic or Schedule from the default box. Periodic polling polls at the interval specified in minutes in the polling interval field. Schedule sets a defined day and time in the week to poll the unit. If periodic is selected, the cursor will skip to the Polling Interval field. If schedule is selected, the cursor will skip to the scheduled days field.
Polling Interval	Periodic polling only. 0 to 9999 minutes. 0 = never. The cursor will skip out of edit mode after entering a value.
Scheduled Days	Enter the whole number of each hour (24 hour clock) to place a polling call (0-23, where 0 = midnight). <b>Example:</b> 0, 8-16 polls at midnight and every hour from 8 AM to 4 PM.
Scheduled Minutes	Enter the whole number of the offset from the hour each call is to be made. (0-59, where 0 = on the hour). <b>Example:</b> 30 polls at half past the hour.

## Step Five

## NetGuardian Device Definition

1. From the Net Guardian Definition screen, press F1 to open the NetGuardian Address Definition screen.
2. Fill in the fields as shown in Fig. M1.23. Be sure to enter the correct firmware version for the NetGuardian you will be using.

```

Remote Device Definition

Port / Job : 30      DCP(F) INTERROGATOR
Device ID  : 1      192.168.63.14 / 1

Description : NetGuardian
Site Name   : DPS Test Lab
Device Type : Standard
Displays    : 1-11
Poll Type   : U
Refresh Rate : 101
Firmware Ver : 3.0J
Log Undefined: N

----- Address Defaults -----
Polarity    : B      Windows      :
Logging     : L      Message      : 0
History     : H
Level       : A
Status      : A
Reverse     : N
Description : <Undefined>

F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit : _

F1=Pnts,F3=Int Alarms,AF1=TL1,AF3=UDP,AF5=Move,AF6=Templates,F10/Esc=Exit

```

Fig. M1.23 - Remote Device Definition screen

Table M1.U - Fields in the Remote Device Definition/Address Definition screen

Field	Description
Port	Non-Editable field showing a virtual port assignment.
Address	Non-Editable field showing assigned address.
Displays	Non-Editable field showing assigned displays. List is automatically created based on the NetGuardian's capacity.
Firmware Ver	Enter the NetGuardian firmware version number. The firmware version is displayed on the LCD menu or immediately after logon via a telnet session. <b>Note:</b> Newer NetGuardian features will not function correctly if this field is left blank. If you do not know the firmware version of your NetGuardian unit, consult DPS Telecom.
Poll Type	Group, Upset or Full Update. Determines how much information to poll for. Group poll will poll for 4 displays at a time, cycling to the next 4 displays at the next poll. Upset will poll only for changes since the last poll. Full Update polls for all displays and information at each poll.
Refresh Rate	Number of polls before a refresh poll cycle occurs (full update). Only active when Poll Type is set to Upset.
Poll TS	Yes (Y) or No (N). Polls for Time Stamped events regardless of NetGuardian firmware version.
Log Undefined	Yes (Y) or No (N). Creates a log of any undefined data received from a poll.

**Note:** Table M1.U continues on the following page.



**Table M1.U - Fields in the Remote Device Definition Definition screen (continued)**

Field	Description
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A (CR), B (MJ), C(MN) or D(ST) [A]
Status	Alarm(A), Status(S) [A] Defines if T/Mon internal relay will change state.
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which undefined alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

## Step Six

### Define Points

1. Press F1 to open the Point Definition screen. By default, the screen will open to Display 3, which shows the first analog channel of the Net Guardian—see Figure M1.24.
2. Press F to use the F)ind command, and type 1. This command will add Display 1 to the NetGuardian definition.
3. Enter alarm information. (See Figure M1.25 for an example.) For complete instructions on defining points, see Section 10 and refer to Section 11 for display mapping.

```

Point Definition
Port : NG Addr: Disp: 3 Display Desc :
P L H L S R
o o s e t v
Pt l g t v s s Description Fail Clear
1 B L H C A N Analog - Channel 1 Minor Under
2 B L H C A N Analog - Channel 1 Minor Over
3 B L H B A N Analog - Channel 1 Major Under
4 B L H B A N Analog - Channel 1 Major Over
5 B N N D A N Analog Data - Channel 1
6 B N N D A N Analog Data - Channel 1
7 B N N D A N Analog Data - Channel 1
8 B N N D A N Analog Data - Channel 1

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

Message

F10/Esc=Exit

```

**Fig. M1.24 - NetGuardian Point Definition screen**

**Point Definition**

Job : NG Site: 1 Disp: 1 Display Desc :

Pt	1	2	3	4	5	6	7	8	Description	Fail	Clear
1	B	L	H	A	A	N			Illegal Entry	Alarm	Normal
2											
3											
4											
5											
6											
7											
8											

Enter polarity. B = bipolar, U = unipolar

---

**Message**

This door has been opened after business hours.  
 Call the Fresno Police Dept. at 454-1681.  
 Location address 4955 E. Yale  
 Cross streets Yale and Fine

F1=GOTO, F2=Desc, F3=Blank, F4=Sect, F5=Range, F6=Read, F8=Save, F9=Help, F10/Esc=Exit

Fig. M1.25 - Point Definition, Display 1

## Step Seven

### Define Analog Points (Optional)

1. From the Remote Device Definition screen, press F5 to open the Analog Provisioning screen, shown in Figure M1.26. Table M1.U explains the fields in this screen.
2. Fill in the Description, Sig, and Unt fields.

**Note:** Provisioning of the NetGuardian through T/MonXM is not supported by recent NetGuardian firmware. This section is included for users of older NetGuardian firmware only.

**Analog Provisioning**

Port: NG Address: 1

Declare Threshold Alarms Locally : NO

(Native Unit Thresholds)

Alg	Description	Sig	Unt	MjOvr	MnOvr	MnUdr	MjUdr
1	Battery A.....	2	VDC	54.00	52.00	44.00	42.00
2	Battery B	2	VDC	54.00	52.00	44.00	42.00
3	Tower Lt curr	3	mA	18.00	15.00	8.000	6.000
4	Outside Temp	2	F	99.37	87.00	16.87	12.75
5	Inside Temp	2	F	78.75	74.62	41.62	33.37
6	Cable Press	2	PAL	18.00	16.00	10.00	8.000
7	Loop Current	3	mA	18.00	15.00	8.000	6.000
8							

Enter description

Description : (Undefined)

E)dit, N)ext, P)rev, Q)uit :

F1=Define Scale, F2=Toggle Threshold Mode, F8=Save, F9=Help, F10/Esc=Exit

Fig. M1.26 - NetGuardian Analog Provisioning screen

**Table M1.V - Fields in the NetGuardian Analog Provisioning screen**

Field	Description
Alg	Point number (fixed field)
Description	Enter the point description. Can be up to 14 characters.
Sig	Significant digits. Enter the number of digits to display after the decimal.
Unt	Enter the Units label, e.g., VDC, VAC F, C, psi, mA, etc.
F1 - Define scale	Calculates offset and scale values for each analog point. This should be done before entering Threshold values. See description below. Press F6 to set scale and offset value to unity.
MjOvr	Major over threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
MnOvr	Minor over threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
MnUdr	Minor under threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
MjUdr	Major under threshold. Enter the threshold value in native units. <b>Note:</b> The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).

## Analog Display Worksheet

**Note:** This operation is optional for NetGuardian users who want to change the analog reference scale so that the displayed analog values correspond to real world values.

To define your analog reference scale, press F1 from the Analog Provision screen. The Analog Display Worksheet screen is used to convert the analog voltage and current readings into meaningful measurements and units. The analog inputs actually only measure either voltage or current. The values must be converted to their actual units by determining the scale and offset for each input. By entering in a few simple values, T/Mon will make the conversion calculations automatically. Each field and its function are described below.

### Analog input type - Volts or Current (V/C)

This field is where the type of electrical input to the analog channel is selected. This is either V or C for voltage or current. Determine this by the type of sensor or input device used for each input.

### Voltage/Current value 1

This is the lowest/minimum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

### Unit value 1

This is the lowest/minimum measurement in the native units of the analog input (degrees, % relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the minimum range here.

### Voltage/Current value 2

This is the highest/maximum voltage or current measurement in the

```

Analog Provisioning
Port: NG   Address: 1
De
Alg
1 Analog input type - Volts or Current (V/C) : C
2
3 Current value 1: 4.00000   Unit value 1 : -45.000 F
4 Current value 2: 20.0000   Unit value 2 : 120.000 F
5
6 Calc Scale :      10.3125   Calc Offset:  -86.250
7
8
En Enter analog input type: V for Volts, C for Current
Description : (Undefined)
E)dit, N)ext, P)rev, Q)uit :
Up Arrow=Previous Field, F6=WDC, F8=Save, F10/Esc=First Field [DPS]

```

Fig. M1.27 - NetGuardian Analog Display Worksheet screen

range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

#### Unit value 2

This is the highest/maximum measurement in the native units of the analog input (degrees, % relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the maximum range here.

After entering the minimum and maximum ranges in both actual voltage or current values and native units, the calc scale and calc offset will automatically be calculated. After exiting the worksheet, key through the remaining entries for that input to make the changes effective.

## Step Eight

### Define Internal Alarms

Entering F3 (Int Alarms) from the Remote Device Definition screen for defined DCP(F) Interrogators will bring you to the Device Internal Alarm Assignment screen. Please refer to Section 14 for more information on Internal Alarms.

## Step Nine

### Define Control Relays (Optional)

You may define labeled, site, and derived control relays for the NetGuardian. See Section 12 (Configuring Controls) for more information.

# Global Options

This option displays the number of connection types in the NetGuardian. The default setting is 1. To go to the Global Options screen press F2 from the NetGuardian Definition screen.

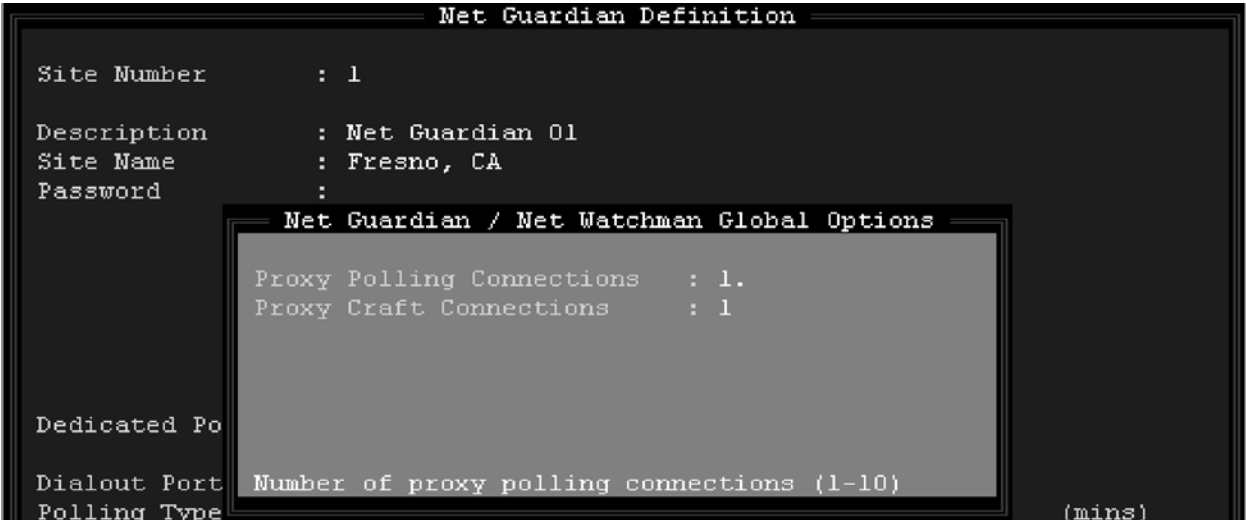


Fig.M1.28 - NetGuardian Global Options screen.

Table M1.W - Fields in the NetGuardian Global Options screen

Field	Description
Proxy Polling Connections	Divides the polling of NetGuardians into as many as 10 proxy polling connections to improve speed. Setting it to '1' causes each NetGuardian to be polled in series.(1-10)
Proxy Craft Connections	Sets the number of T/Mon users that are allowed simultaneous connections to devices connected to NetGuardian craft ports. (1-10)

## Expansion Module — NetMediator 4-Port TBOS/

BAC option is only available if the Building Access Manager Software module is installed. See Software Module 23 for details.

The NetMediator 4-port TBOS/TABS expansion module is an optional module defined in the NetGuardian Definition screen.

To configure T/MonXM to poll the NetMediator expansion module, the Expansion Modules field must be set to “NMD 4 TBOS/TABS” (see Figure M1.29 below) and the Exp Addr #1 field must be set to an available address.

This will create an address entry for the expansion module (see Figure M1.30 below). Displays 1-32 are for the TBOS/TABS alarm points and display 65 is housekeeping points. The next step is to define alarm points for the expansion unit, refer to Section 10 for detailed information on defining points.



Fig. M1.29 - Select NMD 4 TBOS/TABS in NetGuardian Definition screen.

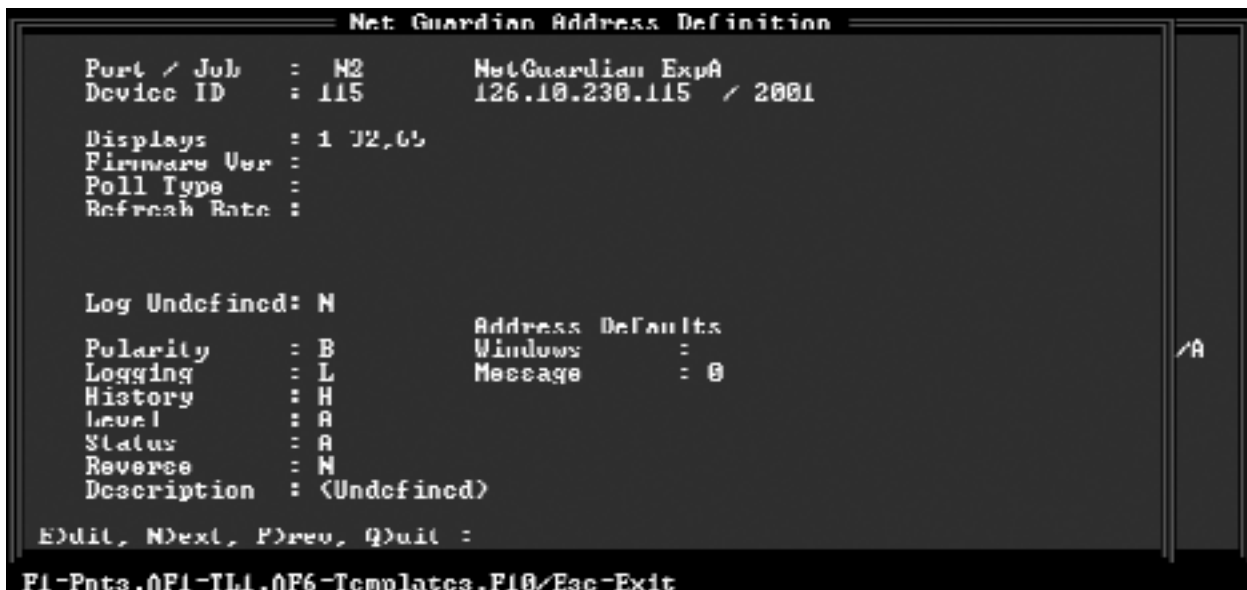


Fig. M1.30 - Address Entry for NetMediator Expansion Module.

---

## Define DCP1 Remotes — Harris™ DS5000

The DCP(F) Interrogator software module can be able to define either a dedicated or virtual (ip) job port to poll your DCP1 Remotes. More specifically, you can select and define your job port for Harris DS5000 Remotes.

There are nine steps to create and define your DCP(F) interrogator module to monitor your Harris DS5000 Remotes:

**Note:** the following pages will explain each step in detail.

1. Install or upgrade your DCP(F) Interrogator module software.
2. Define a remote port for the DCP(F) Interrogator.(Dedicated serial port or virtual port)
3. Create a data connection for polling your DCP over the network. (virtual ports only)
4. Define your Harris DS5000 or any other DCP1 remote device.
5. Define alarm points.
6. Define your analog points and thresholds. (optional).
7. Define internal alarms. (optional)
8. Provision the accumulator.
9. Define control relays. (optional).

---

### Step One

#### **Install or upgrade the software.**

Under normal circumstances installation will only need to be done for software updates or newly ordered modules. The original disks have been supplied with the T/Mon for archival or emergency recovery procedures. See Section 2 for further instructions on upgrading or installing software.

---

### Step Two

#### **Define a Remote Port for the DCP(F) Interrogator**

To define a remote port for communication to DCP(F) equipment, go to Parameters menu > Remote Ports, and then use the Tab key to select DCP(F) Interrogator at the Port Usage field.

**Note:** Do not leave your Caps Locked, or you will have to press Ctrl-D to select your interrogator/responder type.

Enter the appropriate information in each field on the screen, see Figure M1.1.

You must enter “1” in the Protocol (DCPF mode field). For detailed information on each field refer to section M1-1.

---

### Step Three

#### **Create a Data Connection**

For detailed information on creating data connections see section 3-4.

1. In the Remote Parameters screen press F1 for the Device Definition screen. Then press F6 to open the Data Connection screen.
2. Press F1 to open the Ethernet TCP Ports Definition screen.
3. Use the arrow keys to select a new connection.

4. Press Tab to select a port type.

**Note:** Depending on your DCP remote, you may select UDP, TCP, etc.

5. Enter your IP port number and a description. See Section 3, Figure 3.5.

6. Press F8 to save your changes and return to the Data Connection Assignment screen.

7. From the Data Connection Assignment screen, press Tab to select the List Box. Select the IP port you just defined for the data connection. (See Section 3, Figure 3.7). Then return to the Remote Parameters screen.

## Step Four

### Define your DCP1 devices

**Note:** See section M1-5 for detailed information on defining devices and addresses.

1. In the Remote Parameters screen press F1. The Remote Device Definition screen will appear, see Figure M1.31.

2. Enter the port number of your device

3. Enter an address for your device.

4. Enter an optional description and name of the site where your device is located.

5. In the Device Type field use the Tab key to select the type of device. The example below is defined for the Harris DS5000.

6. Complete all the fields on the screen and press F8 to save your definitions.

**Note:** The above definition example will monitor alarm information from a remote addressed as #1 and will report any alarm information that is stored in alarm displays 1 through 140. The polling type is by groups, see Table M1.D for more information.

```

Remote Device Definition

Port      : 3          DCP(F) INTERROGATOR
Address   : 1

Description : Harris DS5000
Site Name  : REMOTE SITE
Device Type : DS5000
Displays   : 1-140
Poll Type  : G
Refresh Rate : 193
Firmware Ver :
Log Undefined: N

----- Address Defaults -----
Polarity    : B      Windows :
Logging     : L      Message  : 0
History     : H
Level       : A
Status      : A
Reverse     : N
Description  : <Undefined>

G=Group, U=Upset, F=Full Update

Up Arrow=Previous Field, F8=Save, F10/Esc=First Field

```

Fig. M1.31 - Example of defined Remote Device Definition screen for DCP(F) Interrogator.



---

## Step Five

### Define Alarm Points

This option allows the you to assign attributes and English descriptions to individual alarm points within the selected displays of the DCP(F). Note that you must have defined the displays previously in the Address Definition section.

1. From the Remote Device Definition screen press F1 (Points). The Point Definition screen will appear, see Figure M1.4
2. If no display was previously entered, the cursor will be at the display number from which the DCP(F) stores the alarm point information.
3. After <Enter> has been pressed at the Display field, the database management system checks to see if any points in that display have been defined previously. If none are found, then the cursor immediately moves into the point editing area.
4. If points in the display have been defined before, then the Standard Key Entry prompt, (See Section 4), appears at the bottom of the window. To edit the points, press 'E' to select the Edit option.
5. When the cursor is in the point editing area, the Message window displays the message associated with the point that is currently being edited.
6. The Up Arrow, Down Arrow, PgUp, PgDn, Home and End keys are used to select a point for editing. Note that these keys are only active when the cursor is at the Pol (polarity) field.

**Note:** For Point Definition Field descriptions refer to Section 10.

---

## Step Six

### Define Analog Points (Optional)

**Note:** refer to section M1-8 for examples.

1. From the Remote Device Definition screen, press F5 to open the Analog Provision screen, shown in Figure M1.5. Table M1.E explains the fields in this screen.
2. Fill in the Description, Sig, and Unt fields.
3. Once you have completely filled each field with the correct information you have the option to change your analog reference scale. Press F1 to go to the Analog Scaling Worksheet screen. For detailed information see section M1-9.

---

## Step Seven

### Define Internal alarm (Optional)

Entering F3 (Int Alarms) from the Remote Device Definition screen for defined DCP(F) Interrogators will bring you to the Device Internal Alarm Assignment screen. Please refer to Section 14 for more information on Internal Alarms.

---

## Step Eight

### Provision the Accumulator Timer

Provisioning the Accumulator Timer will set the number of minutes before the accumulator will clear.

1. Press Alt-F7
2. Enter Accumulator Timeout in minutes (0-1440).

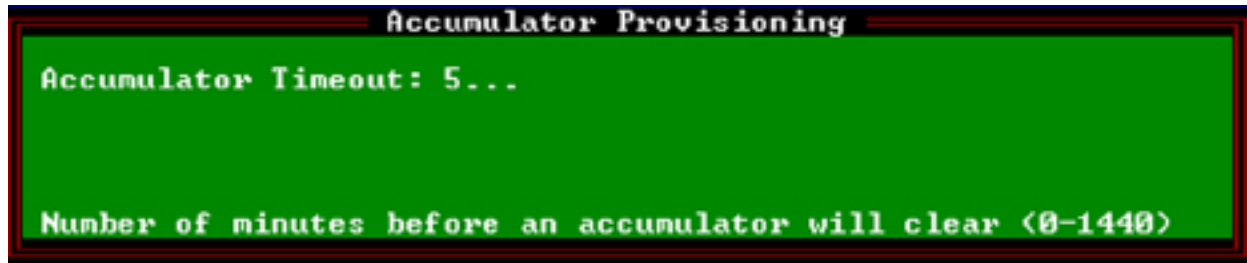


Fig. M1.32 - Accumulator Provision screen.

---

## Step Nine

### Define Control Relays (Optional)

You may define control relays for the DCP device by going to Master Menu > Files Maintenance Menu > Labeled Controls screen. See section 12-6 . See also section 12-10 for more information on derived controls.

## Ring Polling Application

**Note:** The NetGuardian can be configured to use alternate path routing, but NetGuardians must be defined using the LAN-based Remotes command on the File Maintenance menu.

The ring polling application monitors network links between RTUs that are daisy-chained in ring configuration. T/MonXM to monitor the daisy chain from both ends, allowing for precise location of network breaks and continued full visibility, even during a break.

To use ring polling you must have a series of RTUs daisy-chained in ring configuration. Each RTU must be defined in the T/MonXM database, and internal alarms must be defined for the fail and offline conditions of each RTU.

One RTU is defined as the base interrogator, and the remote port of the base interrogator is defined as the Path A port. The final RTU in the daisy chain is connected to a second remote port, which is defined as the Path B port — see Figure M1.33.

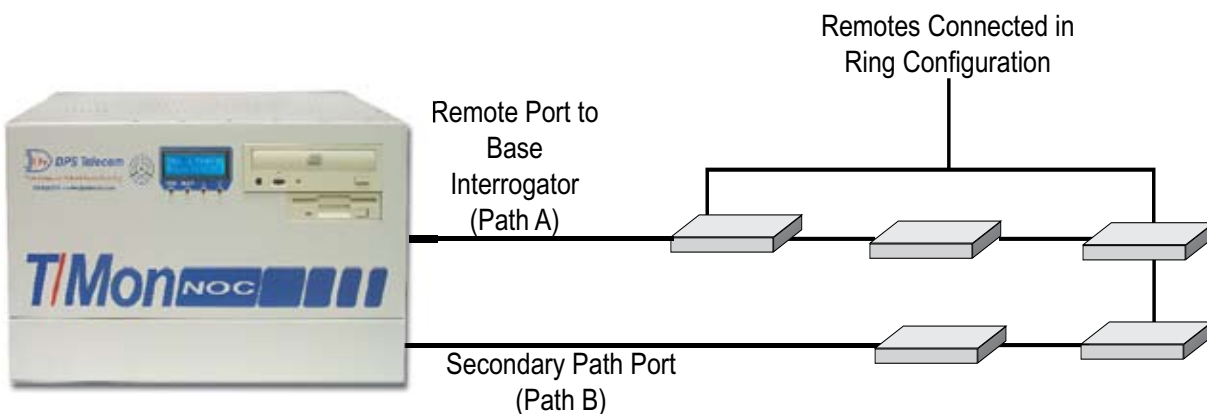


Fig. M1.33 - RTU configuration for ring polling



Fig. M1.34 - Enter a remote port number for Path B in the DCP(F) Interrogator Definition Screen

**Note:** Path B must be a halted port.

To enable ring polling, enter the ID number of the Path B remote port in the Path B field of the remote parameters screen for the base interrogator. T/MonXM will automatically configure the Path B port for ring polling. Press F1 to open the Remote Device Definition screen for the base interrogator. Press F3 to open the Device Internal Alarms Assignment screen.

In the Device Internal Alarms screen, you will see that two internal alarms have been automatically defined. (See Figure M1.35). One internal alarm, “<Port Number>\_A,” represents polls from the Path A port; the second, “<Port Number>\_B,” represents polls from the Path B port. Devices have unique device fail and offline alarms for each path. You must assign internal alarm points to the fail and offline conditions for both internal alarms.

Next create a derived alarm that represents a failure on Path A AND Path B. (For instructions on creating derived alarms, see section 12-10).

You now have a way of determining if there are breaks in your ring network and where they are. Suppose that you have six RTUs configured in a ring. If Path A reports that devices 5 and 6 have failed, while Path B reports that devices 1-4 have failed, there is a break in the network connection between devices 4 and 5. If there is an actual RTU failure, this will trigger the derived alarm representing a failure of both paths.

Device Internal Alarm Assignment				
Port : 1				
Address	Dev	Description	Fail	Offline
1_A	DCPf		13.1.1..	12.1.1
1_B	DCPf		13.1.2	12.1.2
Enter internal point (addr.disp.pnt) (blank=none) (address range: 11-13)				

Fig. M1.35 - The two internal alarms represent polls from different ends of the ring.

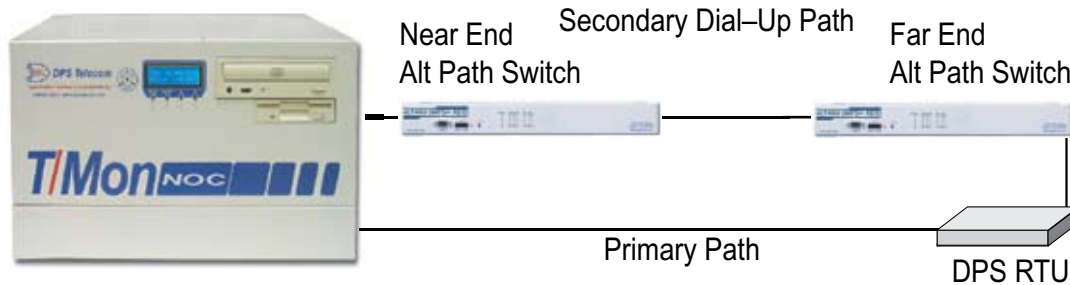


Fig. M1.36 - Typical Alt Path Switch application.

## Alt Path Switch

Multiple near-end Alt Path Switches can be controlled through a single Command channel. For instructions on physically connecting multiple near-end Alt Path switches, see Section 5.6, “Connecting a Command Channel Daisy Chain” in the Alt Path Switch user manual. Software configuration is identical for single and daisy-chained Alt Path Switches.

There are two parts to configuring the Command channel:

1. Define a remote port, device, and alarm points associated with the Alt Path Switch.
2. Download to the near-end Alt Path Switch in Monitor Mode.

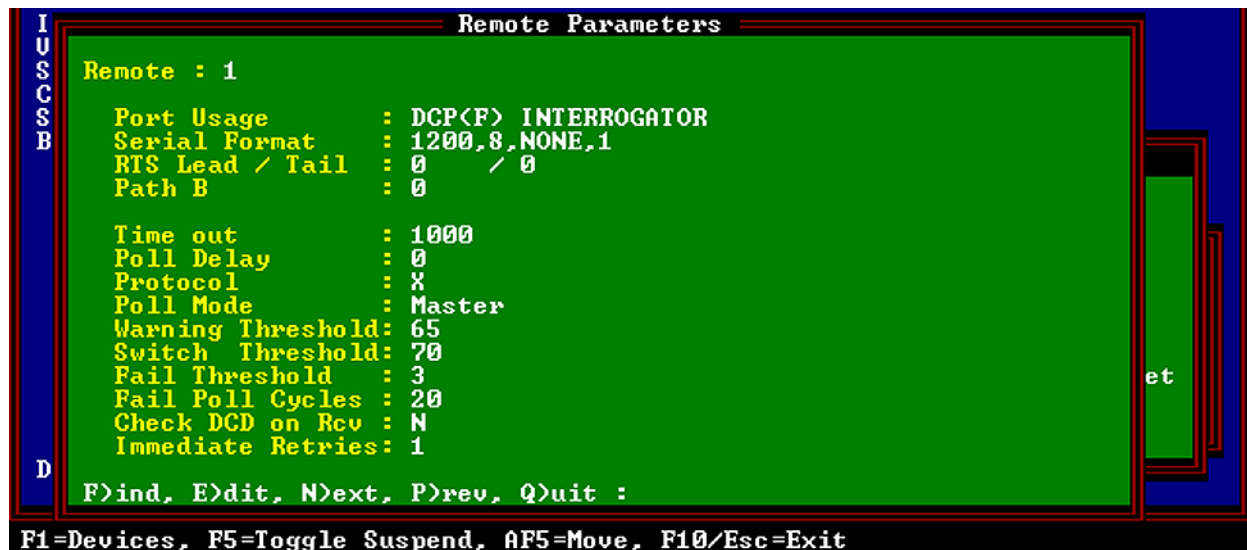


Fig. M1.37 - T/MonXM Remote Parameters screen, defined for Alt Path Switch Command channel.

## Step One

### Define the Remote Port

1. Go to Master > Parameters > Remote Parameters.
2. Choose F)ind and enter the port number of the RS-485 port connected to the Command connector of the near-end Alt Path Switch.
3. Choose E)dit.
4. In the Port Usage field, press Tab to select the List Box and choose DCP(F) Interrogator — see Figure M1.37.

5. Make sure that the Serial Format field is set to 1200, 8, None, 1.
6. Make sure that the Protocol field is set to X for DCP(X) polling.
7. All other fields will be automatically filled with the correct values.

## Step Two

### Define the Remote Device Definition

1. From the Remote Parameters screen, press F1 to access the Remote Device Definition screen .
2. Enter Address 1 in the Address field.
3. Enter an optional description and site name.
4. In the Device Type field, press Tab to select the List Box and choose Alt Path Switch.
5. All other fields will be automatically filled with the correct values.

The screenshot shows a terminal window titled "Remote Device Definition". The background is blue with white text. The configuration is as follows:

```

Port      : 1          DCP<F> INTERROGATOR
Address   : 1

Description : APS
Site Name  : APS 1
Device Type : Alt Path Switch
Displays   : 1-2
Poll Type  : U
Refresh Rate : 261
Firmware Ver :
Log Undefined: N

----- Address Defaults -----
Polarity   : B          Windows :
Logging    : L          Message  : 0
History    : H
Level      : A
Status     : A
Reverse    : N
Description : <Undefined>

F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit :

```

At the bottom of the screen, a legend for function keys is displayed:

```

F1=Pnts, F3=Int Alarms, F5=Prov, AF1=TL1, AF2=Alg, AF5=Move, F10/Esc=Exit

```

Fig. M1.38 - Remote Device Definition screen, defined for the Alt Path Switch.

## Step Three

### Provision the Unit

1. From the Device Definition screen, press F5 to access to APS Unit Provision screen — see Figure M1.39.
2. Enter your choice for each option in the appropriate field. See Table M1.X for an explanation of each option.



Fig. M1.39 - APS Unit Provision screen.

Table M1.X - APS unit provision options

Field	Description
Mode	Operation mode of the Alt Path Switch. Valid choices are: <b>Auto:</b> Switches between channels automatically when the active channel fails. If both channels are operational then the primary channel will be used. <b>Manual:</b> Switches between channels only when a control is issued. <b>Standby:</b> Both channels are idle. Will use the secondary channel only when a control is issued.
Phone Number to Far-End	Phone number of the far-end Alt Path Switch.
Modem Init String	Modem initialization message.
Channel Fail Count	Number of consecutive polls between the near-end and far-end APS without response before the channel is considered failed.
Channel Poll Count	Number of consecutive polls between the near-end and far-end APS when a scheduled test occurs.
Restoration Test Time	The interval in minutes between tests of the primary or failed channel.
Viability Test Time	The interval in minutes between tests of the inactive non-failed secondary channel.
Xmt Packeting Time (100 milliseconds)	The number of milliseconds which must pass without traffic before the accumulated traffic will be transmitted out of the main port. This is typically set to 0 unless going through a terminal server.

## Step Four

### Configure Alarm Points.

1. Press F10 to return to the Remote Device Definition screen.
2. Press F1 to access the Point Definition screen, see Figure M1.40.
3. Two displays of alarms are predefined for the Alt Path Switch. Display 2 alarms are for diagnostic purposes; these must be activated by Control 8 to be viewed (For more information see “Step Five: Configure Controls.”). For a description of the predefined alarms, see Table M1.Y.
4. To view Alt Path Switch alarms in monitor mode, assign the alarms to an alarm window. For full instructions on assigning alarms to alarm windows, see Section 10.

Point Definition									
Port	:	1	Addr:	2	Disp:	1	Display Desc :		
P	L	H	L	S	R	DCP<F> INTERROGATOR			
o	s	e	t	s					
Pt	l	g	t	v	s	Description	Fail	Clear	
1	B	L	H	B	A	Primary Channel Failed			
2	B	L	H	B	A	Secondary Channel Failed			
3	B	L	H	B	A	Secondary Channel Active			
4	B	L	H	B	A	Secondary Channel Manually Selected			
5	B	L	H	B	A	Secondary Channel Manual Test Active			
6									
7									
8									
F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit :									
Message									

Fig M1.40 - The first five predefined alarms for the Alt Path Switch.

Table M1.Y - Alt Path Switch predefined alarms

Display 1 Alarms	
Alarm	Description
1	Primary Channel Failed
2	Secondary Channel Failed
3	Secondary Channel Active
4	Secondary Channel Manually Selected
5	Secondary Channel Manual Test Active
49	Modem Failed
50	No Dial Tone
51	No Carrier
52	Command Error
53	Busy
54	No Answer
55	Erroneous Command Received

**Note:** Table M1.Y continues on the following page.



**Table M1.Y - Alt Path Switch predefined alarms (continued)**

<b>Display 2 Diagnostic Alarms</b>	
<b>Alarm</b>	<b>Description</b>
1	Modem Initializing
2	Modem Initialized and Idle
3	Modem Line Ringing
4	Modem Answering Incoming Call
5	Modem Dialing
6	Modem Channel Established
17-24	Last Received 8-Bit Modem Connect Code

## Step Five

### Configure Controls

There are three controls available for the Alt Path Switch. Site Controls allow the user to operate the controls for a whole window, usually defined by site, thus the name Site Controls. Site Controls can also be defined by status, by device or by any other category assigned to a window. For a description of the controls, see Table M1.Y.

**Note:** Other controls are reserved for internal use. Do not attempt to send any controls other than those listed in this table.

There are two parts to configuring controls for the Alt Path Switch:

1. Define site control categories.
2. Issue site controls.

### Part One Define Site Control Categories

1. Go to the Files > Windows Definition screen, then press F4 to go to the Site Controls Category Definition screen. See Figure M1.41.
2. Enter a category title and description for the site control category. Press Enter and go to the Control Points screen. See Figure M1.42.

**Table M1.Z - Alt Path Switch Controls**

<b>Control</b>	<b>Operation</b>	<b>Result</b>
4	Operate	Manually lock into alternate path mode. Initiate dial out if secondary path not already active.
	Release	Manually unlock alternate path mode. Deactivates secondary channel. Resets modem. Activates primary channel if not failed.
5	Momentary	Manually test alternate path mode.
	Release	Cancel secondary dial out attempt.
8	Operate	Turn on diagnostic display 2 – info will be posted to Display 2
	Release	Turn off diagnostic display 2.

Site Controls Category Definition		
Window Name :		
Group	Category	Description
1	ALTPTH	ALT PATH SWITCH CONTROLS
2	.....	
3		
4		
5		
6		
7		
8		
9		
10		
Enter category id		

Fig. M1.41 - The site controls category definition screen.

**Note:** System Security provides security lockouts on Site Controls by Windows, not by category group or control point entries. Keep this in mind when setting up your control categories and the control point entries under them. See Table M1.AA.

Table M1.AA - Fields in the Site Controls Category Definition screen

Field Name	Description
Category	A six-character title for the category.
Description	The description for the category.

Table M1.AB - Key commands available in the Site Controls Category Definition screen

Function Key	Description
F2	Move to the Control Point Definition screen.
F3	Blank - Deletes current category entry and control point definitions for the category. Leaves an open line. Control Point <b>Note:</b> Definitions deleted in this way cannot be recovered by using F10 or Esc.
Alt F3	Delete - Deletes entry N and its points. Moves all other lines up.
Alt F4	Insert - Moves current line down one group and inserts a blank line for the current group.
F8	Save the category database.
F9	Online help.
F10/Esc	Exit.

Site Control Points						
Window Name :						
Category : ALTPTH ALT PATH SWITCH CONTROLS						
Ent	Description	CMD	Ch	T	ID	Unt Point(s)
1	MANUALLY LOCK INTO ALT-PATH MODE.....	OPR	1		1	1 4
2	MANUALLY UNLOCK ALT-PATH MODE	RLS	1		1	1 4
3	MANUALLY TEST ALT-PATH MODE	MON	1		1	1 5
4	CANCEL SECONDARY DIAL-OUT ATTEMPT	RLS	1		1	1 5
5	TURN ON MODEM DIAGNOSTIC DISPLAY 2	OPR	1		1	1 8
6	TURN OFF MODEM DIAGNOSTIC DISPLAY 2	RLS	1		1	1 8
7						
8						
9						
10						
Enter description						

Fig. M1.42 - Site control points for the Alt Path Switch.

- Enter the control descriptions — refer to Table M1.Z
- Enter your port number (1–24).
- Enter 1 for ID.
- Enter 1 for Unit (display).
- Enter the control point — refer to Table. M1.Z.
- Press F8 to save.

Table M1.AC - Fields in the Control Point Definition screen

Field	Description
Ent	The entry number within the group selected (200 entries per group).
Description	The description of the control points. Up to 40 characters
CMD	The command to be sent to the control point. OPR = OPERATE RELAY RLS = RELEASE RELAY MON = MOMENTARY ON MOF = MOMENTARY OFF SOP = SBO Operate* SRL = SBO Release* SMO = SBO Momentary On* EXE = SBO Execute* CLR = SCO Clear All*
<p>*SBO = Select before operate. This method of control point operation offers extra security by requiring two operator steps before the point actually operates. The desired operation (SOP, SRL, SMO or CLR) is specified and a response from the remote is displayed, indicating that the point is “selected.” Then the EXE command is sent to perform the specified operation. Another use of SBO is to operate several control points simultaneously. The desired control points are “selected” at the remote and one execute command operates all at the same time. This is useful in controlling functions that must occur together, such as channel switching.</p>	

**Note:** Table M1.AC continues on next page.

**Table M1.AC - Fields in the Control Point Definition screen (continued)**

Field	Description
Ch	Channel Number. K1 = VIRTUAL PORT (base and satellite KDA*s with relay exp. card) K2 = VIRTUAL PORT (relay and other expansion cards in base KDAs) RP = REMOTE PORT (Modem port) RC = RELAY CARD (102 card - local controls only) AV = AUDIO/VISUAL CARD (108 Card -Only relays 9-12 can be used.) 1-24 = Port Number. IAM Users - Relays 9-12 are not available on IAM.
T	Device Type. This field is selected only when the selected port is defined for DCM protocol. Selections are: C = CPM S = SBP (Smart Bypass Card -Used only with the Building Access Unit. Three controls may be user-defined for a BAU. See the BAU Operation Guide for details.)
ID	The device address. Valid range is 1-999. This field is skipped when the selected port has been defined for TBOS protocol.
Unt	Unit. The Display (1-64) in which the control points reside. This field is skipped when the selected port has been defined for DCM protocol.
Points	A control point or range of control points that you wish to operate. Ranges may be entered using dashes and/or commas (no spaces). Valid control point ranges may be from 1-64.

**Table M1.AD - Key commands available in the (Site) Control Point Definition screen**

Function Key	Description
F1	Moves the cursor to a selected entry point.
F3	Blank - Deletes current point entry. Leaves an open line. Control Points deleted in this way cannot be recovered by using F10 or Esc.
Alt F3	Delete - Deletes entry and moves all other lines up.
Alt F4	Insert - Moves current line down one group and inserts a blank line.
F6	Read - Read points from window____, Group____. Enter window number to read from (1-720, or 0 for labeled controls)
F8	Saves the control point entries and returns to the Site Controls Category Definition screen.
F9	Displays help for this screen.
F10/Esc	Exit or return to start of line

## Part Two Issue Site Controls

Once you have set up your controls you will be able to issue them in the Monitor mode. For detailed instructions on how to issue your site controls see Section 12.

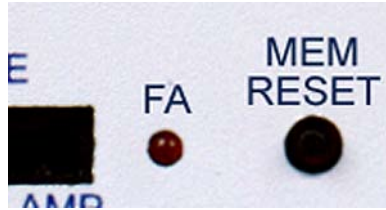


Fig. M1.43 - Pressing the Mem (Memory) Reset button will clear the APS memory.

## Step Six

### Download Configuration to the Alt Path Switch

Once you have completed configuration in T/MonXM, the configuration must be downloaded to the **near-end** Alt Path Switch. To download the configuration, follow these steps.

1. In T/MonXM, enter the Master menu > Monitor mode.
2. From the Alarm Summary screen, press Shift-F6 to access the Site Statistics screen.
3. Select the Port and Address for the Command channel for the Alt Path Switch.
4. Select all other near-end Alt Path Switches and press F5 to put them offline. Note: Each switch has to be taken offline individually.
5. At the point you can clear the Alt Path Switch Memory.  
**Note:** Clearing the memory of the Alt Path Switch puts the unit in auto-addressing mode. When the unit is in auto-addressing mode, it will accept any configuration data on the command channel. Therefore, only one Alt Path Switch can be provisioned at a time. All other near-end Alt Path Switches must be taken offline during provision.
7. Press and hold the Mem Reset button on the front panel of the Alt Path Switch. See Figure M1.43.
8. The front panel LEDs will flash ALL GREEN, then ALL RED, as during rebooting, and then repeat the sequence faster. Then the Modem Status LEDs will trace a left-to-right, right-to-left “Cylon” walk. This indicates the unit is in auto-addressing mode. You may now release the Mem Reset button.
9. Press F3. The configuration will be downloaded to the near-end Alt Path Switch. (See Figure M1.44.)
10. When the configuration is accepted by the Alt Path Switch, the Cylon walk of the modem LEDs will stop. Take device offline, and proceed with the next near-end Alt Pat Switch until you have provisioned all the units.
11. Then place all the near-end Alt Path Switches back online by selecting them and pressing F4.

**Note:** Since no configuration is necessary for far-end Alt Path

Switches, units installed on the far end do not need their memory cleared. However, if you ever transfer an Alt Path Switch from the near end to the far end, its memory should be cleared before re-installation.

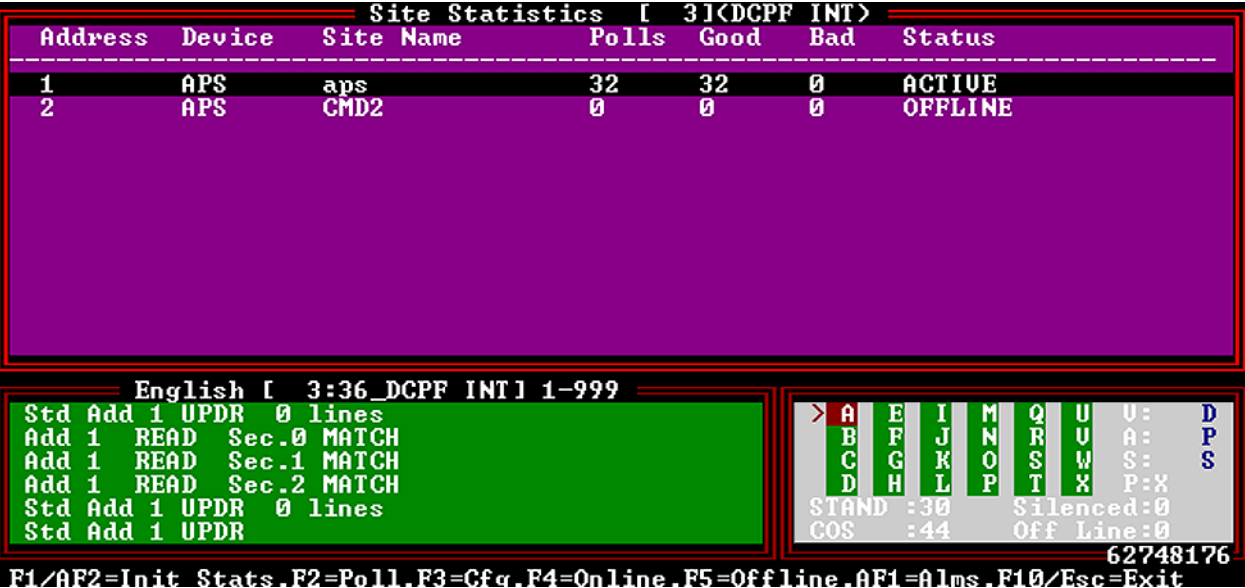


Fig. M1.44 - Downloading the configuration to the Alt Path Switch.



Fig. M1.45 - Set data rate to 9600 baud and DCD on for protection switch port.

## Protection Switch

Implement protection switch in the T/MonXM software as follows:

- Verify the network port is physically RS 445-B. Enter the Parameters > Card Definition sub-menu and verify the card definition is correct.
- Enter the Parameters > TMonNET sub-menu.
- Select TMonNET > Other from the Network sub-menu. A window with two questions will appear.
- Answer the Protection Switch question with an “A” if the system is primary. Answer “B” if it is secondary (backup) — See Figure M1.46.

**WARNING:** These parameters must be set to match the corresponding cabling for proper operations.

- Enter Parameters > Remote Ports menu. Set the port selected for control to DCP(F), 9600 Baud. Make sure DCP(F) Mode is set to “F” and Check DCD on Rcv are both set to “Y”.



Fig. M1.46 - Set your primary or secondary Protection Switch in TMonNET > Other Parameters.



Fig. M1.47 - Select protection switch as device type.

- F) Create a DCP(F) device for each protection switch. (Press F1.)  
Note the protection switch address range of 241 to 246 — see Table 1.AE. Be sure to select “Protection Switch” for the device type field to tell T/Mon that the device is a protection switch.
- G) Define two alarm points for each protection switch (press F1 while in the device definition screen for the switch address).
- H) (Optional) Define Internal alarm by pressing F3 while in the device definition screen for the switch address. Enter the information for internal alarm points for device fail and device off-line.

Table 1.AE - Protection switch address range is 241-246

Protection Switch Number	Ports	T/MonXM Address
1	1-4	241
2	5-8	242
3	9-12	243
4	13-16	244
5	17-20 (IAM only)	245
6	21-24 (IAM only)	246

Table 1.AF - Define two alarm points for each protection switch

Alarm Point	Description	Fail	Clear
1	Primary system on line	RUN	STBY
2	Secondary system on line	RUN	STBY



## MAT (400) and Dial-Up MAT (400)

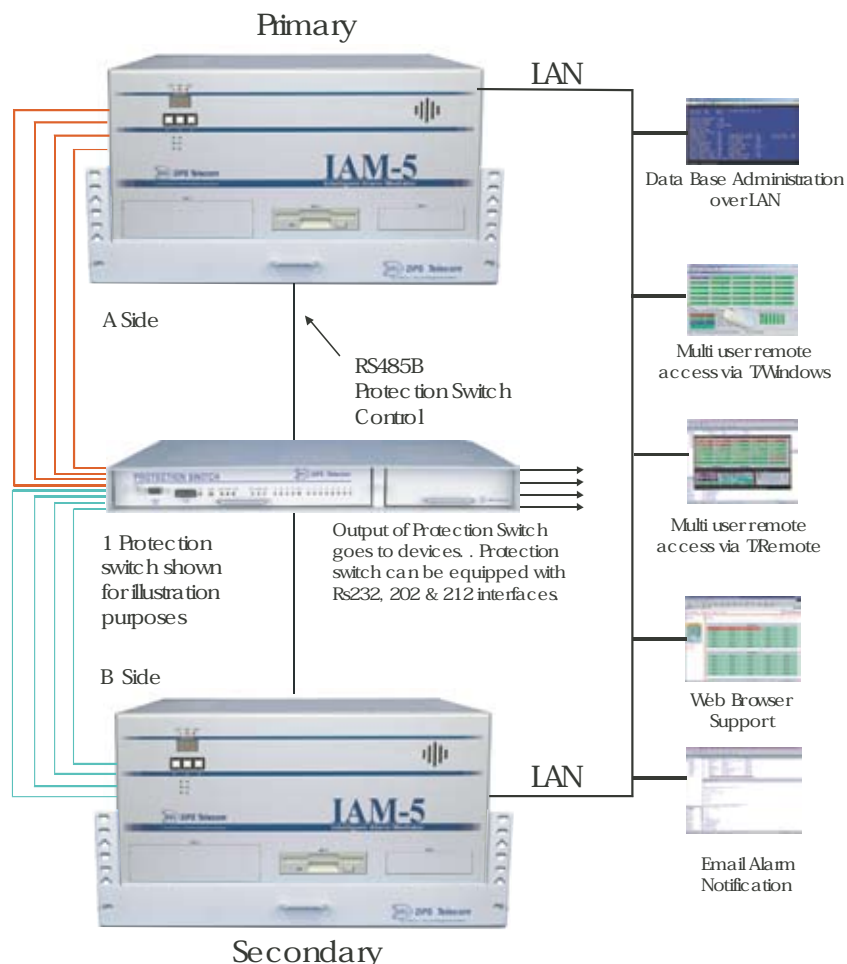


**Fig. M1.48 - Specify levels to initiate dial report if alternate path routing is used.**

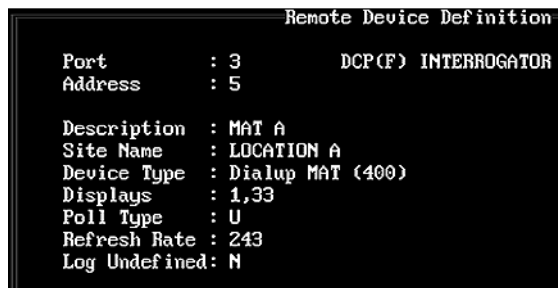
**Note:** See section M1-53 for Dial-up MAT instructions.

Dedicated Line Port To provision a MAT on a dedicated line port (RS232, RS422/485 or 202 modem), proceed as follows:

1. Define a DCP(F) port for the dedicated channel.
2. Press F1. Define the device type as "MAT (400)."
3. Press F5. Enter only the Dial Threshold. Select an alarm level for dial threshold. Exit to the Device Definition screen.
4. Press F1. Define alarm points. If Alternate Path Routing is used, be sure to specify the alarm level for dial threshold on all points that are to initiate dialing for that level.
5. Exit to Master Menu, Initialize and enter Monitor Mode.
10. Press Shift-F6. Use the + and - keys to find the dedicated port. Highlight the MAT to be provisioned and press F3.
11. Exit to monitor screen and test by generating an alarm.



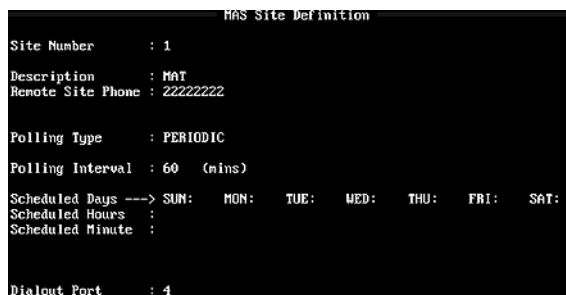
**Fig. M1.49 - Block Diagram of Protection Switch application. For more information about the protection switch, see DPS Telecom Operation Guide OG109086, "Protection Switch Router."**



**Fig. M1.50 - Define device type as “Dial-Up MAT.”**



**Fig. M1.51 - The dial-up MAT provisioning screen.**



**Fig. M1.52 - Enter MAS site information.**



**Fig. M1.53 - Entry #1 must be the MAT with the modem.**

Dial-Up (Alternate Path) A MAT with dial-up modem is provisioned from the master for dialing information. Proceed as follows:

1. Define a DCP(F) port for the dedicated channel.
  2. Press F1. Define the device type as “Dial-Up Mat.”
  3. Press F5. Enter Site Number, Master Phone Number, Modem Init. string (use default) and Dial Threshold. Select an alarm level for dial threshold. Exit to the Device Definition screen.
  4. Press F1. Define alarm points. Be sure to specify the alarm level for dial threshold on all points that are to initiate dialing for that level.
  5. Define a port as DCP(F) Dial-Up (port must be equipped with a modem). Exit to the Master Menu.
  6. Select Files / Dial Up Networks / MAS Sites. Enter information in the fields.
  7. Press F2 (Shelf Provisioning)
  8. Enter the Port and Address #. The site name field will be automatically entered.
- Note:** Entry #1 must be the MAT with the 212 Modem subassembly.
9. Exit to Master Menu, Initialize and enter Monitor Mode.
  10. Press Shift-F6. Use the + and - keys to find the dial port (as defined in step 1). Highlight the MAT to be provisioned and press F3.
  11. Exit to monitor screen and test by generating an alarm.

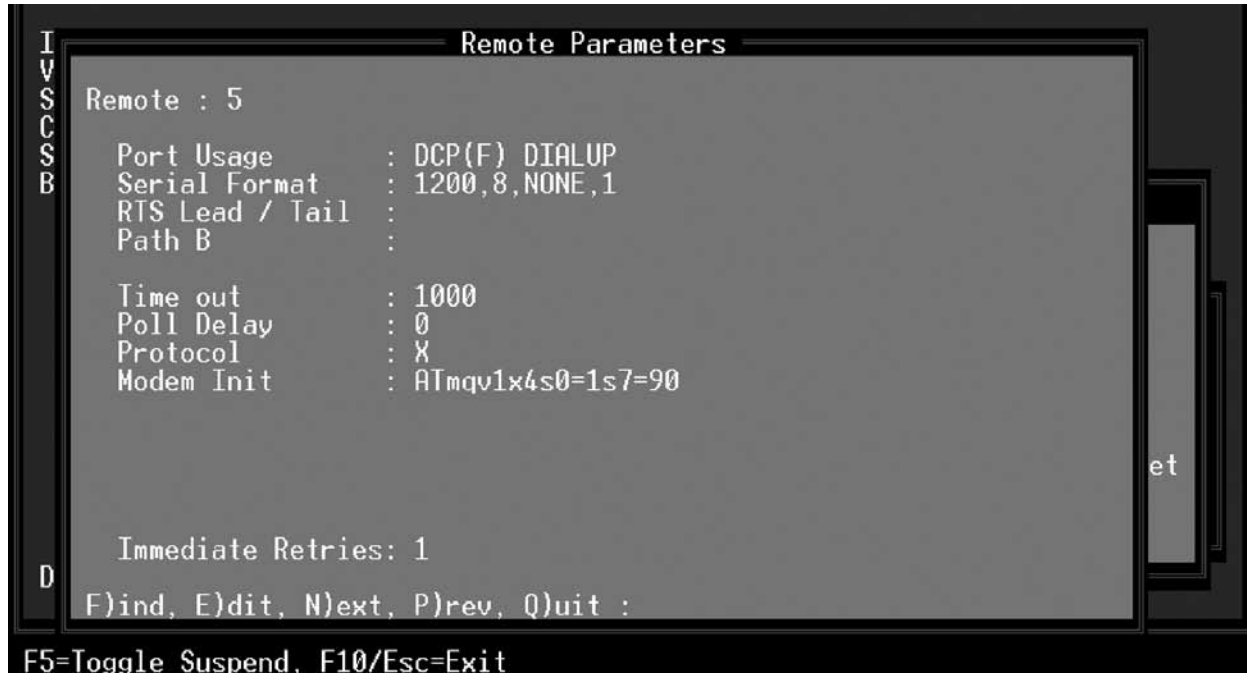


Fig. M1.54 - Remote parameters screen, DCP(F) dial-up usage.

## DCP(F) Dial-Up

Using the DCP(F) Dial-Up port usage, T/MonXM can access dial-up Remotes using DCP(F) protocol. DCP(F) dial-up offers several advantages over TRIP dial-up protocol, including multiple addressing, simplified setup and download provisioning. It can be used with KDAs and MAT 400 modules.

Refer to Table M1.AG for field descriptions and Table M1.AH for function key descriptions available on the Remote Parameters screen.

Table M1.AG - Fields in the Remote Parameters screen, DCP(F) Dial-Up usage

Field	Description
Port Usage	DCP(F) Dialup <b>Note:</b> This usage should only be defined on a physical port that contains a modem.
Serial Format	Baud rate, parity, word length, and stop bits settings that T/MonXM will use to communicate with the equipment.
Time Out	Timeout in milliseconds (200 to 9999) [1000 = 1 sec.] *
Poll Delay	Time between polls in milliseconds (0 to 9999) [0]
DCPF Mode	Enter X = DCP(X), F = DCP(F), N = DCP. [F]
Immediate Retries	Number of times to re-dial before moving on to the next address. [1]
Modem Init String	30 character configuration string. This field defaults to the correct string for standard DPS devices. If you are using a non-standard modem, Refer to Appendix K or consult the modem manufacturer's instructions for details. Default: AT V1 M0 S0=1 Q0 S7=90 X4

**Table M1.AH - Key commands available in the Remote Parameters Screen, DCP(F) Dial-Up usage**

Function Key	Description
F5	Allows you to suspend use of this port without loss of configuration data. Toggles the suspension state. Available only when cursor is on the prompt line at the bottom of the window.
Up Arrow	Move to the previous field.
F8	Save
F9	Help
F10/Esc	Move to the first field or exit without saving (depending on which field the cursor is in).
Tab	List port usage (while cursor is in the Port Usage field.)

**Note:** This port definition only reserves the port for DCP(F) Dial-Up mode. The dial-up Remotes themselves are physically defined in another section of the software. Refer to Module 3 - Standard Dial-Up Remotes for additional information.

# Software Module 2

## TRIP Dial-Up



**Fig. M2.1 - Remote parameters screen, trip dial up usage.**

Using the TRIP Dial-Up port usage, T/MonXM can access dial up remotes using TRIP protocol. Remotes include DPMs, DCMs, KDAs, NetGuardians, and AlphaMax 82A. TRIP ports are also used for certain alternate path alarm reporting devices. Port parameters are specified for TRIP Dial Up as described in the Table M2.A.

**Table M2.A - Fields in the Remote Parameters screen, TRIP Dial-Up usage**

Field	Description
Port Usage	TRIP Dial-Up
Serial Format	Baud rate, parity word length, and stop bits settings that T/MonXM will use to communicate with the equipment.
Modem Setup String	30-character configuration string. This field defaults to the correct string for standard DPS devices. If you are using a non-standard modem, consult Appendix I (Quick Reference Tables) or the modem manufacturer's instructions for details.

Table M2.B lists the key commands you can use while in the Remote Parameters Screen, TRIP Dial Up Usage.

**Table M2.B - Key commands available in the Remote Parameters Screen, TRIP Dial-Up usage**

Function Key	Description
F5	Toggle suspension. Allows temporary suspension of defined port. Available only when cursor is on prompt line at bottom of window.
Up Arrow	Move to the previous field.
F8	Save
F9	Opens online help files.
F10/Esc	Move to first field or exit without saving (depending on cursor location).
Tab	List port usages (while cursor is in the Port Usage field).

**Note:** The dial up remotes themselves are physically defined in another section of the software. Refer to Software Module 3 (Standard Dial-Up Remotes) for additional information or other corresponding remote device sections.

\* **Note:** The port selected for TRIP must be equipped with a modem. Select either an internal 1200 Baud/ 33.6 Baud modem on an intelligent controller card or an external modem on an RS232 port. Refer to your T/ Mon or IAM hardware user manual for external modem connector pinouts.

# Software Module 3

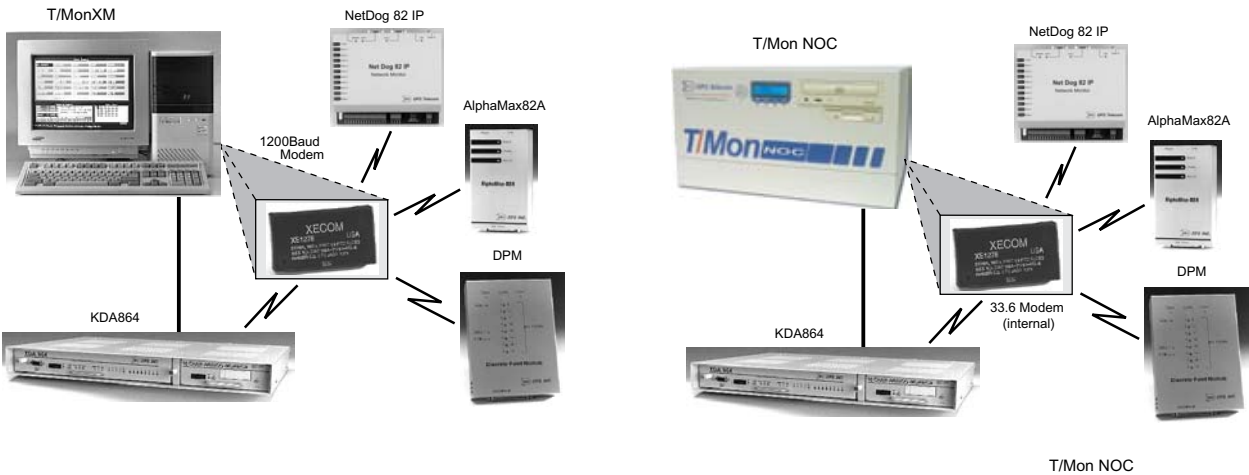
## Standard Dial-Up Remotes

### Dial-Up Networks

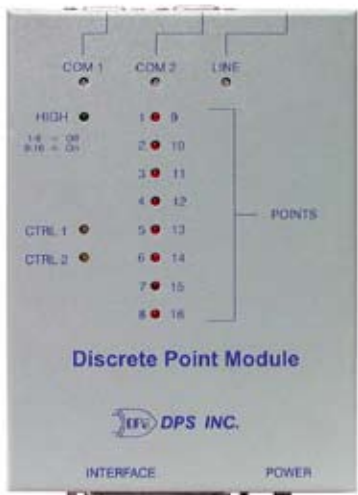
Dial-up networks are used when T/MonXM uses phone lines to dial up remote sites to gather alarm information or when remote sites send alarm data back to T/MonXM. The base T/MonXM system includes the following dial-up remotes: DPM, AlphaMax 82A, Net Dog 82 IP, KDA 864, Time-Stamp KDA, KDA 832-T8 and Modular Alarm System (MAS). Other dial-up software modules, including Datalok 10D and ASCII may be purchased separately.



Fig. M3.1 - The dial-up network menu



**Fig. M3.2 - A T/MonXM and T/Mon NOC dial-up network including the NetDog, AlphaMax 82A, DPM and KDA**



**Fig. M3.3 - The Discrete Point Module (DPM)**

The DPM and AlphaMax 82A are both designed for smaller applications. The KDA is a rack-mounted unit that offers additional features. It has 32 or 64 inputs, compared to 8 on the AlphaMax and 16 on the DPM. The AlphaMax is a dial-up unit. The DPM can be purchased as either a dial-up or direct connect unit. The KDA can use both dial-up and direct connect at the same time, treating the direct connection as a primary data path and the dial-up connection as a secondary back-up data path. (This is commonly referred to as “Alternate Path Routing”.) The MAS is a system of plug-in modules that can make remotes of various sizes with a number of different features, including dial-up reporting. All of these devices use TRIP (T/Mon Remote Interface Protocol) protocol to communicate with the T/MonXM over dial circuits.

**DPM Sites**

DPM units (see Figure M3.3) have 16 alarm input points and 2 control output points with internal relays. DPMs typically are dial-up only, but dedicated versions are available (See Table M3.A).

For more information on this menu option, please refer to section M3-30.

The DPM part numbers and options are listed below. The DPM options are constantly being expanded. As a result, more options may be available than are listed below. Contact DPS inside sales for currently available options.

**Table M3.A - Dial-up DPM options and model numbers**

Model Number	Description
D-PC-221-11A-0V	DPM: Dial-up, 16 Alarms, 2 Controls.
D-PC-221-11A-1V	DPM: Dial-up, 16 Alarms, 2 Controls with ASCII Craft Port access.
D-PC-229-10A-22-0V	DPM 416-S2: Dial-up, 16 Alarms, 4 Controls with 2 ASCII Craft Ports and 2400 Baud modem.



### AlphaMax 82A and 82S Sites

The AlphaMax 82A (see Figure M3.4) is similar to the DPM but has 8 alarm input points and 2 control output points with internal relays. AlphaMax 82As are dial-up only. The AlphaMax 82S has an additional craft port interface. For more information on this option, please refer to section M3-30.

The AlphaMax part numbers and options are listed below. The AlphaMax options are constantly expanded. As a result, more options may be available than are listed below. Contact DPS Telecom at (800) 622-3314 for currently available options.

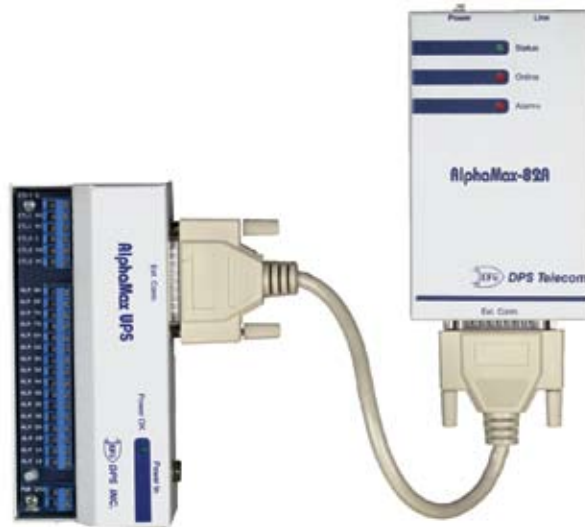


Fig. M3.4 - The AlphaMax 82A with optional UPS

Table M3.B - AlphaMax options and model numbers

Model Number	Description
D-PC-245-20D-R0	AlphaMax-82A - 8 single-ended (ground Activated) inputs and 2 controls, internal 1200 baud modem, DTMF receiver. R: 0 = Normal temp. range (0 to +60 Degrees C.) 2 = Extended temp. range (-30 to +70 Degrees C.)
D-PC-246-10A-R0	AlphaMax-82A - 8 bipolar (ground or battery activated) inputs and 2 controls, internal 1200 baud modem, DTMF receiver. R: 0 = Normal temp. range (0 to +60 Degrees C.) 2 = Extended temp. range (-30 to +70 Degrees C.)
D-PC-247-10A-0X	AlphaMax-82S - 8 single-ended (ground Activated) inputs and 2 controls, ASCII Craft Port (virtual channel), internal 1200 baud modem, DTMF receiver. X: 0 = 1200 Baud modem 1 = 33.6K Baud modem 2 = 2400 Baud modem.
D-PC-254-10A-TB	AlphaMax "UPS" connector Block with Battery Backup T: 0 = Wire Wrap terminals 1 = Screw Lug terminals B: 0 = no UPS 1 = 1 Battery 2 = 2 Batteries.



**Fig. M3.5 - KDA 864 remote telemetry unit provides space for expansion card module.  
(Shown with 8 Analog/4 TBOS Card)**

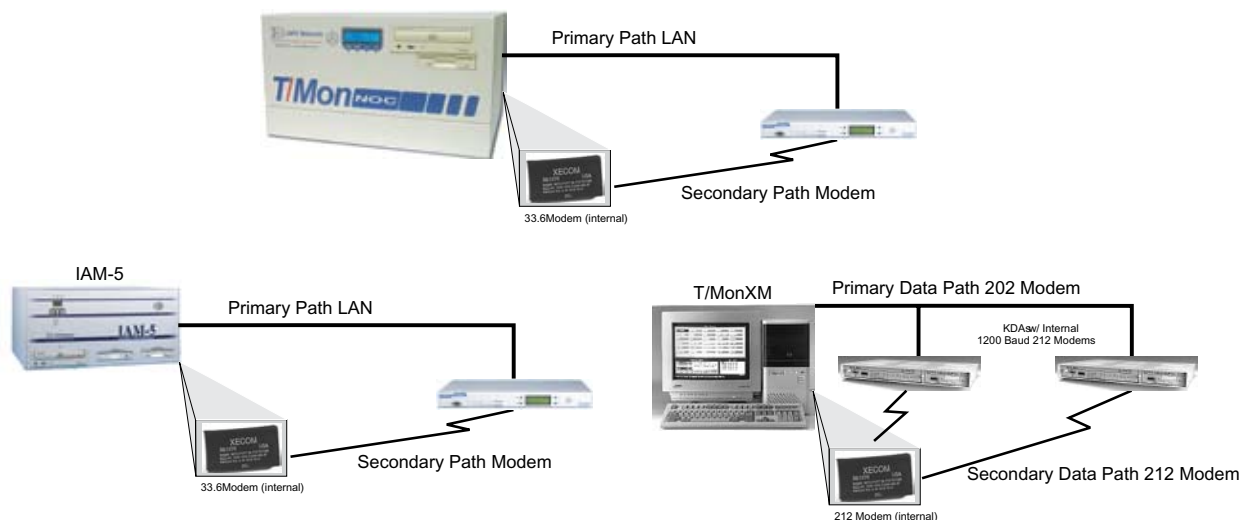
**Note:** DPS recommends that you setup all KDAs, even dial-only in the Files Maintenance menu > KDA Shelves option.

#### KDA 864 and KDA 832-T8 Sites

The KDA 864 and KDA 832-T8 are versatile units equipped with 64 or 32 alarm input points and 8 control output points with internal relays. The KDA 832-T8 has an additional 8 TBOS ports on the base unit. They can be equipped with direct connect and/or dial-up capabilities. The KDA and T/MonXM were designed to compliment each other.

The dial-up ability of the KDA 864 can be used as a secondary data path in case the primary path is lost. If one of the communication links from the KDA (see Figure M3.6) were to be compromised, the unit would report an alarm to the same window in T/MonXM, regardless of how it sends the data. T/MonXM does this by linking the primary device specification to the dial-up data base definition. This makes the system much more user friendly since the user doesn't have to worry about how the alarm arrived.

In dial-up applications the KDAs can be equipped with an LR-24 expansion relay card or any of the analog expansion cards. The TBOS and TBOS/Analog expansion cards are supported only in dedicated line applications.



**Fig. M3.6 - Two alternate path applications**

For more information on this menu option (refer to section M3-24) which is part of the base T/MonXM software.

**Options and Model Numbers**

Refer to the KDA 864 Manual or to the DPS Price Guide for complete Option and Model Number information

**KDA-TS Sites**

The KDA-TS is identical to the KDA 864, with the addition of time-stamping features. Follow KDA 864 data-basing procedures.

An additional display (display 33) and points are predefined in T/MonXM for housekeeping information.

In dial-up applications the KDA-TS can be equipped with an LR-24 expansion relay card or any of the analog expansion cards. The TBOS and TBOS/ASCII expansion cards are supported only in dedicated line applications.

**KDA 832-T8 Sites**

The KDA 832-T8 is like the KDA 864, but with half the alarm points and 8 TBOS ports on the base unit.

A single address is assigned for the KDA 832-T8, which includes displays for the discrete points, the control points and the TBOS ports. The base address also provides displays for satellite discrete alarms and controls and LR-24 expansion cards — refer to Section 11 (Display Mapping).

In dial-up applications the KDA 832-T8 can be equipped with any of the analog expansion cards. The TBOS and TBOS/ASCII expansion cards are supported only in dedicated line applications.

**Datalok 10D Sites**

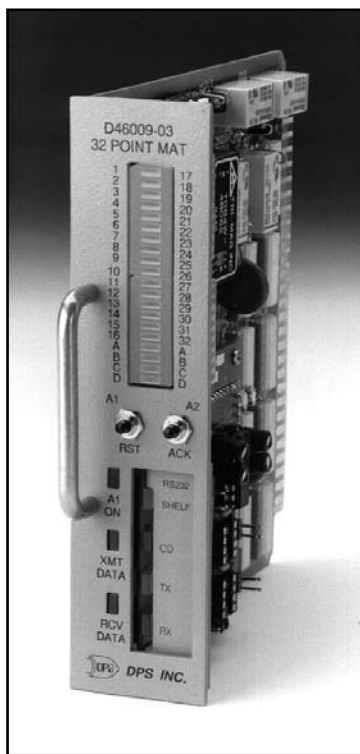
This menu option is only available if the Pulsecom Datalok Software Module is installed. For more information, please refer to Software Module 16.

### ASCII Sites

This section is used to define dial-up ASCII sites. It is available only if one of the ASCII Processor Modules is installed. For more information refer to Software Module 6 - ASCII Interrogator.

**Table M3.C - Software module part numbers**

Model Number	Description
D-SK-163-10A-00	ASCII Dial-Up Multi Port Software Module
D-SK-164-10A-00	ASCII Dial-Up Single Port Software Module
D-SK-160-10A-00	Auto ASCII Dial-Up Multi Port Software Module



**Fig. M3.7 - MAT Module can host dial modem**

### MAS Sites

A DPS Modular Alarm Transmitter (MAT) may be equipped with a 212 modem for dial-line facility reporting. The host MAT may communicate with other alarm modules in the same shelf via the DPS MicroLAN channel, providing dial-up reporting for all. In addition, another MAT in the shelf can be equipped with a dedicated-facility type module (RS232, RS422/485 or 202 modem) for alternate path routing applications — refer to section M1-53.

## KDA Shelves

### Centrally Administered Configuration

Remote provisioning from T/MonXM is an alternative to provisioning from a PC using T/KDA software. This way of provisioning offers many advantages over using T/Config software, including a centrally managed single database and a single program.

**Note:** Before a KDA site can be downloaded from T/MonXM, the protocol, address, data rate (Baud) and base/satellite # must be locally configured using T/KDA software. Time is updated with each download

Provisioning prepares a database file to be downloaded to a KDA-TS to define all software parameters. If a site is to be provisioned from T/MonXM, the port must be pre-defined under the Parameters/Remote Ports menu. If the site reports on a dedicated line, the port must be defined for DCP(F) or DCP(X) Protocol. If the site reports on dial line, or if alternate path routing is used, a port must be defined for Dial-Up TRIP protocol — see Software Module 2.

**Note:** Device address and point definitions are all entered during the provisioning process, described here; they should not be done under the Parameters > Remote Ports menu.



Fig. M3.8 - To provision a remote KDA, select KDA Shelves in the File Maintenance menu

```

      KDA Shelf Definition

Site Number      : 5
Description      : KDA
Site Name       : FRESNO

      | Host                Expansion
      -----
Base | KDA 864             LR-24
Sat 1| KDA 864             8 CHAN ANALOG (B)
Sat 2| NONE               NONE
Sat 3| NONE               NONE

Dedicated Port   : 31   Base Addr: 5   Exp Addr #1: 1   Exp Addr #2: N/A
Dialout Port     : 7     Phone:1 559 454 1600           Test: 440
Polling Type     : SCHEDULE                               Polling Interval : (mins)
Scheduled Days ---> SUN: N MON: Y TUE: Y WED: Y THU: Y FRI: Y SAT: N
Scheduled Hours  :          3-18   3-18   3-18   3-18   3-18
Scheduled Minute :          30     30     30     30     30

Site name (max.30 characters)

Up arrow=Previous Field, F8=Save, F9=Help, F10/Esc=First Field

```

Fig. M3.9 - Define each KDA site for port assignment and polling schedule

Use the following steps to define the KDA shelf:

1. At the Main menu select Files.
2. At the File Maintenance menu select KDA Shelves.
3. The KDA Shelf Definition screen will appear. (See Figure M3.9) Fill in the fields as described in Table M3.D.

**Note:** Table M3.D continues on following page.

Table M3.D - Fields in the KDA Shelf Definition screen

Field	Description
Site Number	3-Digit site number. This number must be unique over the entire alarm network. It is used to describe this KDA remote, including satellites and expansion cards. This number is the address field for responders, derived alarms and labeled controls. (1-999). <b>Note:</b> must match KDA.
Description	41-Character description of site.
Site Name	15-Character site name.
Base Sat 1 Sat 2 Sat 3	Indicates KDA shelf layout with base, satellite, and expansion cards.
Host	Type of KDA unit. Select KDA-TS, KDA-864, or KDA-832 from default box.

**Table M3.E - Fields in the KDA Shelf Definition screen (continued)**

Field	Description
Expansion	Type of expansion card in host. For Base unit, select the expansion card populated in the slot from default box. For satellite unit select NONE or LR-24 from list box.
Dedicated Port	If the KDA reports on dedicated line (DCP <sub>f</sub> or DCP <sub>x</sub> ) enter the T/MonXM port number. (Port must have been previously defined.) If KDA reports only on a dial line enter 0 (skips to Dial Port field).
Base Addr	Enter DCPF address for base unit (1-255). (This is the address that T/Mon will use to poll the KDA.)
Exp Addr #1	Expansion card address #1 (for 16 Chan Analog, or other expansion card in the base unit.)
Exp Addr #2	Expansion card address #2 (for expansion cards that need 2 address exp. cards)
Dial Out Port	Enter port number used for dial, if dial only or alternate path routing is used. Enter "0" if dedicated line only (skips out of edit mode).
Remote Site Phone	Enter Phone Number to reach remote.
Polling Type	Select Periodic or Schedule from the default box. If periodic is selected, the cursor will skip to the Polling Interval field. If Schedule is selected, the cursor will skip to the Scheduled Days field.
Polling Interval	Periodic polling only. 0 to 9999 minutes. (0 = never) (Skips out of edit mode after entering value.)
Test	Enter the number of minutes (0 to 9999) between dial-up integrity tests. This causes T/Mon to check the status of the dial-up link while the primary link is still functional. If T/Mon calls the unit and there is no response from the modem, an alarm condition will occur. The alarm will appear as an internal alarm.
Scheduled Days	Schedule Polling only. For each day of the week enter "Y" to activate polling, enter "N" to deactivate.
Scheduled Hours	Enter the whole number of each hour (24 hour clock) to place a polling call (0 to 23, where 0 = midnight). Example: 0,8-16 polls at midnight and every hour from 8 AM to 4 PM.
Scheduled Minutes	Enter the whole number of the offset from the hour each call is to be made (0-59 where 0 = on the hour). Example: 30 polls at half past the hour.

**Table M3.F - Key commands available in the KDA Shelf Definition screen**

Function Key	Description
F1	Device - Takes you to the Base KDA Shelf Address Definition screen.
F2	Provisioning - Takes you to the Provisioning Target Menu.
F3	Internal Alarms - Brings up a screen for assigning device fail and off-line internal alarms. Follow prompts to specify address, display and point for each device. (Address must be 11 or 12.)
F10/Esc	Exit.

```

Base Kda Shelf Address Definition

Port      : K1      KDA SHELF HOST
Address   : 1

Displays  : 1,2,33,34
Firmware Ver : 1.4D
Poll Type : U
Refresh Rate : 101

Log Undefined: N

----- Address Defaults -----
Polarity   : B      Windows      :
Logging    : L      Message     : 0
History    : H
Level      : A
Status     : A
Reverse    : N
Description : (Undefined)

Edit, N)ext, P)rev, Q)uit :

F1=Pnts, AF1=TL1, F10=Esc=Exit

```

**Fig. M3.10 - Base KDA shelf address definition screen shows port, address and display**

4. Once the KDA Shelf Definition screen fields are filled in, press F1 to enter the Base KDA Shelf Address Definition screen. See Figure M3.10 and the Table M3.G.
5. After completing the Base KDA Shelf Address Definition screen fields, press F1 to enter the Point Definition Screen. See Section 11 (Display Mapping) for more information. Follow the procedures outlined in Section 10 to complete this screen. When finished press F10 to return to the Base KDA Shelf Address Definition screen.

**Table M3.G - Fields in the Base KDA Shelf Address Definition screen**

Field	Description
Port	Non-Editable field showing a virtual port assignment, preceded by K. K1 represents the base and satellite KDAs, with LR-24 Relay cards. K2 represents expansion cards (LR-24 or 16 Channel Analog) in the base KDA, if there are any. Press "N" to advance to the K2 screen, if an expansion card has been defined for the "base" KDA. See additional note on pp. 6-58.
Address	Non-Editable field showing assigned address.
Displays	Non-Editable field showing assigned displays. List is automatically created based on the quantity of KDAs and expansion cards — refer to Section 11 (Display Mapping)
Firmware Ver.	Enter KDA firmware version number for the Base KDA. The firmware version is found on a label on top of the processor chip on the KDA P.C. board or on the KDA front panel. If unknown, leave blank. (Must be between 1.4d and 1.4z to poll satellites for time stamp information.)
Log Undefined through Message	Standard fields found in regular DCP(F) remote device definition screen.



```

KDA Shelf Definition

Site Number      : 1
Description      : Fresno
Site Name       : Airport

| Host      | Expansion
-----|-----
Provisioning
Base | KDA-TS | 16 CHAN ANALOG
Sat 1| KDA-TS | LR-24
Sat 2| NONE   | NONE
Sat 3| NONE   | NONE
      | Quit   |

Dedicated Port      :
Exp Addr #2:

Dialout Port      : 4   Phone      : 555-5555
Polling Type      : SCHEDULE      Polling Interval :      (mins)
Scheduled Days ---> SUN: N MON: Y TUE: Y WED: Y THU: Y FRI: Y SAT: N
Scheduled Hours   : 0,8-16
Scheduled Minute  : 0

<Enter>=Edit Provisioning, F10/Esc=Exit
[DPS]

```

Fig. M3.11 - Provisioning target menu

6. Press "Q" to return to the KDA Shelf Definition screen. Then press F2 to reach the provisioning target menu. (Figure M3.11)
7. Highlight the item and press Enter to select a device to provision. The Provisioning menu will appear. (Figure M3.12) While

```

KDA Shelf Definition

Site Number      : 1
Description      : Fresno
Site Name       : Airport

| Host      | Expansion
-----|-----
Base Shelf
Phone Numbers
Alarm Points
Control Periods
Responder
Advanced
Quit
Base | KDA-TS | 16 CHAN ANALOG
Sat 1| KDA-TS | LR-24
Sat 2| NONE   | NONE
Sat 3| NONE   | NONE

Dedicated Port      : 5   Bas     dr #1: 3   Exp Addr #2:

Dialout Port      : 4   Phone      : 555-5555
Polling Type      : SCHEDULE      Polling Interval :      (mins)
Scheduled Days ---> SUN: N MON: Y TUE: Y WED: Y THU: Y FRI: Y SAT: N
Scheduled Hours   : 0,8-16
Scheduled Minute  : 0

F10/Esc=Exit
[DPS]

```

Fig. M3.12 - Provisioning menu

See the procedure beginning on page M3-21 for Analog Card provisioning. See the procedure beginning on page M3-24 for LR-24 Relay Card provisioning.

in the provisioning menu you will enter the information to be downloaded to the KDA.

The Provisioning menu will list the following six choices:

- Phone numbers
- Alarm points
- Control Periods
- Responder
- Advanced
- Quit

8. Highlight Phone Numbers and press Enter. Field entries are described in Table M3.H.

```

===== KDA Shelf Definition =====
Site Number      : 1
===== KDA Phone Numbers - Base Shelf =====
Primary Report Number : 222-8888.....
Secondary Report Number : 222-8889

Enter the first phone number the KDA will use to report alarms.

F8=Save, F10/Esc=Exit [DPS]
  
```

Fig. M3.13 - General KDA provisioning screen.

Table M3.I - Fields in the KDA Phone Numbers Provisioning screen

Field	Description
Primary Report Number	The first number the KDA will attempt to call in order to report an alarm condition.
Secondary Report Number	The number the KDA will attempt to call should the primary be busy or out of service.

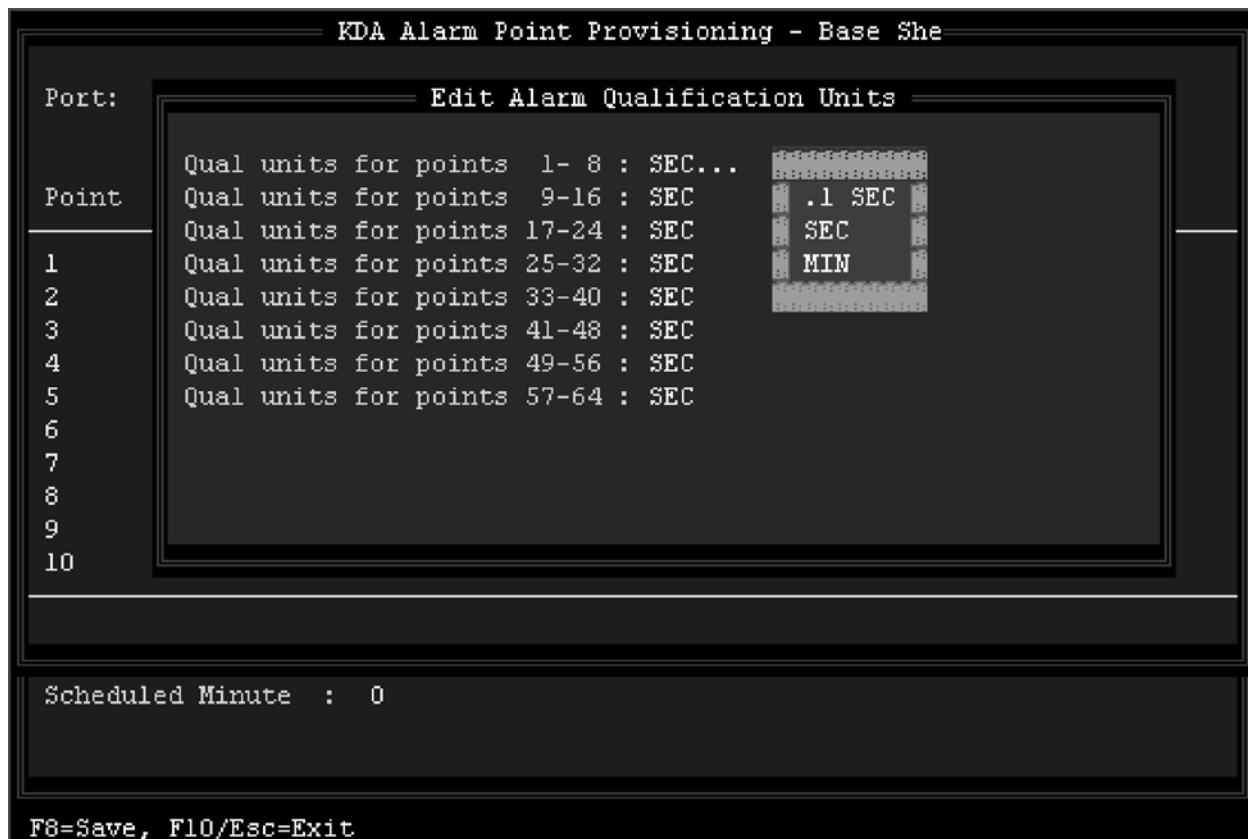
KDA Alarm Point Provisioning				
Port: K1      Address: 1				
Point	Polarity	Dial Type	Alm Qual	Qual Units
1	NORMAL	POLL	0	SEC
2	NORMAL	POLL	0	SEC
3	NORMAL	POLL	0	SEC
4	NORMAL	POLL	0	SEC
5	NORMAL	POLL	0	SEC
6	NORMAL	POLL	0	SEC
7	NORMAL	POLL	0	SEC
8	NORMAL	POLL	0	SEC
9	NORMAL	POLL	0	SEC
10	NORMAL	POLL	0	SEC
Scheduled Minute :				
Tab=Defaults, F1=Edit Qual Units, F8=Save, F10/Esc=Exit				

Fig. M3.14 - KDA Alarm point provisioning screen.

9. Highlight Alarm Points and press Enter. Fields are described in the table below.

Table M3.J - Fields in the KDA Alarm Point Provisioning screen

Field	Description
Point	The number for the alarm point. Not an editable field.
Polarity	Input condition for an alarm. "Normal" is open (no current flow) for a non-alarm condition and closed (current flowing) for an alarm. "Reversed" is closed for a non-alarm condition and open for an alarm. Enter NRM or RVS. Press Tab for a selection menu.
Dial Type	Specifies whether an alarm will be immediately reported or held until the master polls. Applies to dial up or alternate path KDA's when the primary link is down. Valid entries are: DIAL - Dials upon alarm occurrence. Use for high priority alarms. POLL - Alarm is held until polled. Use for low priority alarms. Press Tab for a selection menu.
Alm Qual	The time an alarm must be present before it is considered valid. Alm Qual is multiplied by the Alarm Qualification Units (tenths of a second, seconds or minutes) assigned for the 8 point group containing this point. (See step 10).
Qual Units	Non-editable field showing the Alarm Qualification Time units in either seconds or minutes. (Refer to step 10 for units assignment procedure.)



**Fig. M3.15 - Edit alarm qualification units window**

10. Press F1 to edit the Alarm Qualification Units. Select .1 sec, sec or minutes from the default box for each set of 8 points. (Points that are not used can be left at the default of SEC.) When complete press F8 to save. If you do not wish to save, press F10 to exit. The KDA Alarm point Provisioning Screen will again be displayed. If no further editing is required, press F8 to save and return to the Provisioning menu.

**KDA Shelf Definition**

Site Number

Description

Site Name

-----

Base

Sat

Sat

Sat

Dedicated Port

Dialout Port

Remote Site Phone

Polling Type

Scheduled Days --

Scheduled Hours

Scheduled Minute

**Edit Momentary Relay Periods**

The settings on this screen apply to the 8 relays on the host unit.

Relay	Period	Seconds
1	15.	1.5
2	15	1.5
3	15	1.5
4	15	1.5
5	15	1.5
6	15	1.5
7	15	1.5
8	15	1.5

Range is 1-255 tenths of a second.

Exp Addr #2: N/A

: (mins)

FRI: Y SAT: N

**F8=Save, F10/Esc=Exit**

**Fig. M3.16 - Select 1 to 255 tenths of a second for each relay's momentary control period**

11. Highlight Control Periods and press Enter. A selection menu will appear for setting the momentary operation period for each control point. Enter 1 to 255 tenths of a second for the period. The right hand column shows the actual time in seconds. See Figure M3.16. When complete press F8 to save. If you do not wish to save, press F10 to exit. The KDA Alarm point Provisioning Screen will again be displayed. If no further editing is required, press F8 to save and return to the Provisioning menu.
12. Highlight Responder and press Enter. The KDA Primary Responder Provisioning Screen will appear — see Figure M3.17. Several of the fields are automatically entered with data derived from previously defined fields. Table M3.K describes the fields when DCP, DCPx or DCPf protocol is used. (DSAT is the protocol used for the satellite KDAs. Go to step 13 on page M3-17 for DSAT.) When complete, press F8 to save and return to the provisioning menu. If you do not wish to save, press F10 to exit.

```

KDA Shelf Definition
-----
Site Number      : 5
KDA Primary Responder Provisioning  Base Shelf

Protocol         : DCP
Docking Module   : RS232
Responder Baud   : 1200
Responder Parity : NONE

DCP(F) Address   : 5
DCP(F) Exp Add #1 : 4
DCP(F) Exp Add #2 : N
Periodic Full Updates:
Satellite Count  : 1
Report Satellite Failures : N

Primary communication protocol
18-Save, 110/Exit
DPS

```

Fig. M3.17 - KDA primary responder provisioning screen for DCP, DCPX or DCPF

Table M3.K - KDA Provisioning, DCP, DCP(X) and DCP(F) Protocol

Field	Description
Docking Module	Physical interface module that is plugged into the docking bay. Possible interfaces are :A) RS232, B) 212 modem, C) 202 Modem, D) RS485, E) RS422, F) T202F. Press Tab for a selection menu.
Responder Baud	Baud rate the primary port will use. Possible values are: OFF, A) 300 baud, B)600 Baud, C) 1200 baud, D) 2400 Baud, E) 4800 Baud, F) 9600 Baud. Press Tab for a selection menu. <b>Note:</b> Must match interrogator port setting on the T/MonXM or IAM.
Responder Parity	Primary port parity. Valid values are Even, Odd and None. None is the default for the DCP(F) family. Press Tab for a selection menu.
DCP(F) Address	Address the KDA will respond to when polled. (1-255). <b>Note:</b> Unless the address is being changed, this must match the base address in the shelf definition screen. (Figure 6.31)
DCP(F) Exp Add #1	Enter the address for the first expansion card (1-255, 0=none). Expansion card address is independent of the host address.
DCP(F) Exp Add #2	Enter the address for the second expansion card (1-255, 0=none). Expansion card address is independent of the host address.
Periodic Full Updates	Yes or No. Yes causes remotes to generate a full alarms status report every 250 polls, as opposed to the normal report that gives only changes since the last report. No provides full status reports only when requested by the polling master.
Report Satellite Failures	Yes or No to report a satellite failure.

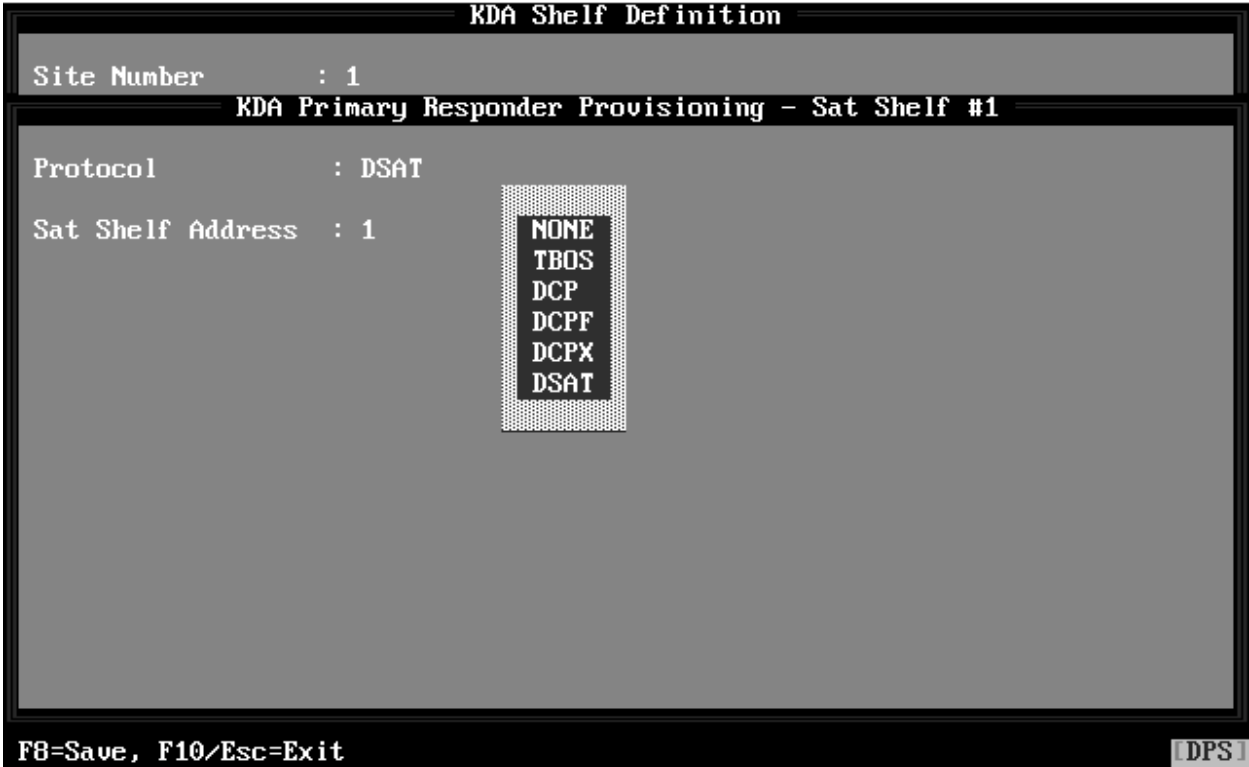


Fig. M3.18 - KDA primary responder provisioning screen for DSAT

13. Field entries for DSAT (used for satellite KDAs only) are described in the following table.

Table M3.L - Fields in the KDA Responder Provisioning screen, DSAT Protocol

Field	Description
Protocol	DSAT (no other protocol should be used here)
Sat Shelf Address	Satellite shelf position number (1, 2, or 3) Note: The satellite address is automatically entered. It should not be changed.

```

KDA Shelf Definition
Site Number      : 1
KDA Primary Responder Provisioning - Base Shelf
Protocol         : UDP
Unit ID          : 1..
IP Address       : 126.10.200.8
Subnet Mask      : 255.255.255.0

Enter unit id (DCPX address)

Up Arrow=Previous Field, F10/Esc=Exit [DPS]

```

**Fig. M3.19 - KDA primary responder provisioning screen for UDP (Ethernet) protocol**

14. Field entries for UDP (used for KDAs equipped with NIA cards, reporting via Ethernet) are described in the following table.

**Note:** Obtain addressing information from network manager. An incorrect address can cause serious system problems.

**Table M3.M - Fields in the KDA responder provisioning screen, UDP protocol**

Field	Description
Protocol	UDP
Unit ID	Assign an ID for this unit if there are other units on the net. Range is 1 to 255.
IP Address	IP address of this KDA. Range is 000.000.000.000 to 255.255.255.255.
Subnet Mask	Subnet IP mask for this KDA. Range is 000.000.000.000 to 255.255.255.255.



```

===== KDA Shelf Definition =====
Site Number      : 1
===== Advanced KDA Provisioning - Base Shelf =====

Check-In Time      : 0.....
Call Delay         : 5      =      minute(s)
Number of Rings    : 2
                   : 0.83
Use RLY 1 as COS Indication : N
Use PNT 1 for Local Ack   : N
Call Control       : NORMAL

0=Disabled, 00:10 - 42:30 (HH:MM)

F8=Save, F10/Esc=Exit
[DPS]

```

Fig. M3.20 - KDA advanced provisioning screen

15. Highlight Advanced and press Enter. The Advanced KDA Provisioning screen will appear. Field entries are described in the following Table M3.N.
16. Highlight Quit and press Enter. You will return to the KDA Shelf Definition screen.

**Fig.M3.N - Fields in the KDA Advanced provisioning screen**

Field	Description
Check-In Time	The time interval the KDA will wait between automatic status report calls. The time period is entered in HH:MM format, to the nearest 10 minutes. The minimum time allowed is 10 minutes (00:10), and the maximum is 42 hours 30 mins (42:30). Entering "0" disables the auto check-in feature. In alternate path mode this is the amount of time the KDA will wait for new alarms to report via the primary port. If a new alarm is not acknowledged within the check-in time it will report via the dial line.
Call Delay	This parameter has two uses depending on the state of the "CALL CONTROL" field. If the KDA is set to normal auto-calling mode, this parameter controls the minimum amount of time in tens of seconds between each call. In backup dial-up mode, this parameter specifies the time the KDA will wait to be polled from the master before it calls to report a COS. T/MonXM will convert the number you entered into minutes and display it to the right of the field. Range: 3-30 (3=30 sec, 4=40 sec, etc.)
Number of Rings*	The number of rings the KDA will wait before it answers the call. Valid values are 2-15.
Use Rly 1 for COS*	Answering "YES" will assign relay 1 of the KDA to be designated as a COS alarm relay. This means that the relay will be closed when an alarm Change Of State occurs. Additional COS's will pulse the relay OFF for 100ms. The relay will release once all COS's have been acknowledged.
Use Pnt 1 for local ACK	Answering "YES" will assign Point 1 (first input point of the KDA) to be a local alarm acknowledgment input. When Point 1 is in Alarm, all COS alarms will immediately be ACK-ed.
Call Control	This field determines the KDA outgoing call behavior. If set to "NORMAL" the KDA will place calls to the master whenever an alarm occurs that was flagged as a "Dial" alarm. If set to "BACKUP" the KDA will only call the master if the primary communication link fails. "BACKUP" should only be used when the KDA is being used in its ALTERNATE PATH configuration. For this configuration to work properly, the KDA must be equipped with both docking pads, one of which must be a dial-up modem. In addition, the master monitoring station must be capable of supporting this mode.

\* These features are useful for local visibility and acknowledgement of alarms.

## Provisioning Expansion Cards - 16 Channel Analog

Use the following to provision a 16 Channel Analog Card. Select the KDA Shelf Definition screen for the card to be provisioned. At the KDA Shelf Definition screen press F2. Select 16 CHAN ANALOG.

The KDA Analog Provisioning Screen will appear. The cursor will be located in the description field for channel 1. The cursor will move across the screen as each field value is entered — see Table M3.O. Threshold values are the actual value of the voltage, including polarity.

The cursor moves to the description field for channel 1. Type in the point description and press Enter. The cursor will move across the screen as each field value is entered. (Refer to the following table.) Note that threshold values are in native units (including polarity).

The Analog Card measures voltages. A given voltage may represent a value in some other units, such as degrees Celsius, current in milli-amps or pressure in p.s.i. These are referred to as “native units.” For each analog point press F1 to call up the Analog Display Worksheet window. — see Figure M3.21 By entering two point values of the measured voltage or current and the corresponding values in reported (local or native) units (for example, degrees), represented by each end point voltage, the scale and offset for the analog point can be obtained via an automatic calculation. Scale and offset will be shown at the bottom of the worksheet.

The screenshot shows the 'KDA Shelf Definition' screen. It contains several fields for site information and a provisioning menu. The provisioning menu is open, showing options for 'Host' and 'Expansion'. The 'Expansion' menu is highlighted, showing '16 CHAN ANALOG' as the selected option. Other options in the 'Expansion' menu include 'LR-24', 'NONE', and 'NONE'. The 'Host' menu shows 'KDA-TS', 'KDA-TS', 'NONE', 'NONE', and 'Quit'. The 'Base' field is set to 'KDA-TS'. The 'Sat 1' field is set to 'KDA-TS'. The 'Sat 2' field is set to 'NONE'. The 'Sat 3' field is set to 'NONE'. The 'Dedicated Port' field is set to '0'. The 'Dialout Port' field is set to '0'. The 'Remote Site Phone' field is empty. The 'Polling Type' field is empty. The 'Polling Interval' field is set to '(mins)'. The 'Scheduled Days' field is set to 'SUN: MON: TUE: WED: THU: FRI: SAT:'. The 'Scheduled Hours' field is empty. The 'Scheduled Minute' field is empty. The 'Exp Addr #2' field is set to 'N/A'. The bottom of the screen shows the instruction '<Enter>=Edit Provisioning, F10/Esc=Exit' and the label '[DP5]'.

```

KDA Shelf Definition

Site Number      : 4
Description      : site 4
Site Name       : four

: Host           Expansion
-----
Base            KDA-TS   16 CHAN ANALOG
Sat 1           KDA-TS   LR-24
Sat 2           NONE     NONE
Sat 3           NONE     NONE
Quit            Quit

Dedicated Port   : 0
Dialout Port     : 0
Remote Site Phone :
Polling Type     :
Polling Interval :      (mins)
Scheduled Days   ---> SUN: MON: TUE: WED: THU: FRI: SAT:
Scheduled Hours  :
Scheduled Minute :

Exp Addr #2: N/A

<Enter>=Edit Provisioning, F10/Esc=Exit [DP5]

```

Fig. M3.21 - Select 16 CHAN ANALOG in the KDA Shelf Definition screen

**KDA Analog Provisioning**

Port: K2    Address: 1

**Analog Display Worksheet**

Enter a pair of analog values and corresponding display units.  
The Display Scale and Display Offset used to convert voltage  
(or current) into display units is calculated automatically.

Alg

1 Analog input type - Volts or Current (V/C) : C

2

3 Current value 1: 4.00000    Unit value 1 : -45.000 F

4 Current value 2: 20.0000    Unit value 2 : 120.000 F

5

6 Calc Scale :        10.3125    Calc Offset:    -86.250

7

8

En Enter analog input type: V for Volts, C for Current

Scheduled Minute : 0

Up Arrow=Previous Field, F6=UDC, F8=Save, F10/Esc=First Field [DPS]

Fig. M3.22 - KDA analog display worksheet

The line at the bottom of the Edit Expansion Ports screen shows the full range capability of the analog card for the native units, scale and offset for the analog point being entered. The value in brackets is the actual measured voltage or current (in mA) for the entered native unit values.

Table M3.O - Fields in the Edit Analog Expansion Port screen

Field	Description
Alg	Point number (fixed field)
Description	Enter the point description. Can be up to 14 Characters.
Sig	Enter the number of digits to display after the decimal.
Unt	Enter the units label (e.g., VDC, VAC, F, C, PSI, etc.). This identifies the native unit.
F1 - Analog Display Worksheet	To calculate Offset and Scale values for this analog point. Should be done before entering Threshold values. See Analog Scaling and Offset section for explanation. Press F6 to set unity value for scale and offset.
MjOvr	Major over threshold. Enter the threshold value in native units. <b>Note:</b> Bottom line in window will show the available range in native units and the value of the input voltage or current (in mA).
MnOvr	Minor over threshold. Enter the threshold value in native units. <b>Note:</b> Bottom line in window will show the available range in native units and the value of the input voltage or current (in mA).

**Note:** Table M3.O continues on following page.

**KDA Analog Provisioning**

Port: K2      Address: 1

Alg	Description	Sig	Unit	(Native Unit Thresholds)				Dial	Dial	Qual	Qual
				MjOvr	MnOvr	MnUdr	MjUdr	ctrl	clr	per	res
1	BATTERY A	2	UDC	54.00	52.00	44.00	42.00	NONE	N	5	SEC
2	BATTERY B	2	UDC	54.00	52.00	44.00	42.00	NONE	N	5	SEC
3	TOWER LT CURR	3	MA	18.00	15.00	8.000	6.000	NONE	N	5	SEC
4	OUTSIDE TEMP	2	F	99.37	87.00	16.87	12.75	NONE	N	5	SEC
5	INSIDE TEMP	2	F	79.90	75.00	40.00	35.00	NONE	N	5	SEC
6	CABLE PRESS	2	PAL	10.00	16.00	10.00	0.000	NONE	N	5	SEC
7	LOOP CURR	3	MA	18.00	15.00	8.000	6.000	NONE	N	5	SEC
8	.....										

Enter description

Scheduled Minute : 0

F1-Define Scale, F8-Save, F9-Help, F10/Esc-Exit [DP3]

Fig. M3.23 - Enter threshold values in the KDA Analog Provisioning screen

Table M3.O - Fields in the Edit Analog Expansion Port screen (continued)

Field	Description
MnUdr	Minor under threshold. Enter the threshold value in native units. <b>Note:</b> Bottom line in window will show the available range in native units and the value of the input voltage or current (in mA).
MjUdr	Major under threshold. Enter the threshold value in native units. <b>Note:</b> Bottom line in window will show the available range in native units and the value of the input voltage or current (in mA).
Dial Ctrl	If the KDA is modem equipped, specify which threshold should cause it to dial the master. Choose from NONE, MJ (Major) or MJ/MN (Major and Minor). Use Tab to highlight choice, Press <Enter> to select.
Dial on Clear	Dial master when voltage retreats past a threshold (equivalent to a cleared alarm) Y = Yes, N = No.
Qualify Period	Qualification time period. Value is times the Qualify Resolution value (see next field). Prompt line gives ranges. <b>Hint:</b> For greatest qualification accuracy choose a resolution that will avoid low numbers; e.g., 120 seconds give better accuracy than 2 minutes.
Qualify Resolution	Units and multiplier for qualification time period. Use tab to choose 0.1 sec, sec or minutes.

## Provisioning Expansion Cards - LR-24 Relay Card

Use the following to provision an LR-24 Relay Card. Select the KDA Shelf Definition screen for the card to be provisioned. At the KDA Shelf Definition screen press F2. Select LR-24.

The KDA LR-24 Momentary Periods window will appear. The momentary operation time periods for groups of six relays are set in this window. The cursor will be located in the field for points 1 through 6. The cursor will move down to the next field as each value is entered. Press Enter after the last field is filled in to exit. Press F10 to return to the Provisioning menu. Select Quit to exit. When all channels have been defined exit the KDA Shelf Definition screen by pressing F10.

The screenshot shows the 'KDA Shelf Definition' screen. It contains the following fields and options:

- Site Number : 1
- Description : FRESNO
- Site Name : AIRPORT
- Host : Provisioning
- Expansion : 16 CHAN ANALOG
- Base : KDA-TS
- Sat 1 : KDA-TS
- Sat 2 : NONE
- Sat 3 : NONE
- Quit
- Dedicated Port
- Dialout Port : 5
- Remote Site Phone : 333-3333
- Polling Type : SCHEDULE
- Polling Interval : (mins)
- Scheduled Days ---> SUN: N MON: Y TUE: Y WED: Y THU: Y FRI: Y SAT: N
- Scheduled Hours : 0,8-16
- Scheduled Minute : 0
- Exp Addr #2: N/A

At the bottom left, it says 'F10/Esc=Exit'. At the bottom right, it says '[DPS]'.

Fig. M3.24 - Select LR-24 in the KDA Shelf Definition screen

## 8 Analog and 4 TBOS Expansion Card

To provision an 8-analog or 4-TBOS card, select the KDA shelf definition screen for the card to be provisioned. At the KDA shelf definition screen, press F2, then select 8 ALG / 4 TBOS.

The Provisioning menu will appear. To provision the 8 analog inputs, select Analog provisioning from the menu. Instructions for analog provisioning are the same as for the 16 channel Analog card.

To provision the 4 TBOS ports, select TBOS Provisioning from the provisioning menu. Refer to the screen and table on the following page for field descriptions for the TBOS provisioning window.

The screenshot displays the 'KDA Shelf Definition' menu. It includes fields for Site Number (1), Description (Fresno), and Site Name (Airport). A table lists expansion cards for Base, Sat 1, Sat 2, and Sat 3. The 'Provisioning' menu is open, showing options for 8 ALG / 4 TBOS, LR-24, NONE, and Quit. The 'Expansion' menu is also open, showing options for 8 ALG / 4 TBOS, LR-24, NONE, and NONE. Below the table, there are fields for Dedicated Port, Dialout Port (4), Phone (555-5555), Polling Type (SCHEDULE), Polling Interval, Scheduled Days (SUN: N, MON: Y, TUE: Y, WED: Y, THU: Y, FRI: Y, SAT: N), Scheduled Hours (0,8-16), and Scheduled Minute (0). The bottom of the screen shows navigation instructions: '<Enter>=Edit Provisioning, F10/Esc=Exit' and a '[DPS]' label.

	Host	Expansion
Base	KDA-TS	8 ALG / 4 TBOS
Sat 1	KDA-TS	LR-24
Sat 2	NONE	NONE
Sat 3	NONE	NONE

Provisioning menu options: 8 ALG / 4 TBOS, LR-24, NONE, Quit

Expansion menu options: 8 ALG / 4 TBOS, LR-24, NONE, NONE

Site Number : 1  
Description : Fresno  
Site Name : Airport

Dedicated Port :  
Dialout Port : 4 Phone : 555-5555  
Polling Type : SCHEDULE Polling Interval : (mins)  
Scheduled Days ---> SUN: N MON: Y TUE: Y WED: Y THU: Y FRI: Y SAT: N  
Scheduled Hours : 0,8-16  
Scheduled Minute : 0

<Enter>=Edit Provisioning, F10/Esc=Exit [DPS]

Fig. M3.25 - 8 Analog and 4 TBOS screen menu

```

===== TBOS Provisioning =====

Port:  K2      Address: 1

Port  Enabled  Baud  Poll List
-----
1      Y        2400   1
2      Y        2400   2,3
3      N
4      N

Y=Enabled, N=Not Enabled

Scheduled Days ---> SUN: N  MON: Y  TUE: Y  WED: Y  THU: Y  FRI: Y  SAT: N
Scheduled Hours   : 0,8-16
Scheduled Minute  : 0

F8=Save, F10/Esc=Exit

```

Fig. M3.26 - KDA expansion card provisioning screen

Table M3.P - Fields in the TBOS Provisioning screen.

Field	Description
Port	TBOS port 1-4
Enabled	Y (Yes) or N (No)
Baud	1200 or 2400
Poll List	Enter TBOS displays to poll (1-8). Use comma to separate list (Ex. 1, 2, 7)



## Downloading the Provisioning File

**Note:** Before a KDA site can be downloaded from T/MonXM, the protocol, address, data rate (Baud) and base/satellite # must be locally configured using T/KDAW software. If this has not been done, the download will not work.

For detailed information refer to the Site Statistics sub-section (Section 16-58). Press Shift-F6 in the Monitor Mode to get the Site Statistics screen. Move the highlight bar with the cursor keys to highlight the base KDA site to be downloaded. Press F3 to start the download. An asterisk appears at the left end of the display line to denote downloading is under way. The status field will indicate the progress. If the download reports FAILED, re-check all physical connections and database addresses.

When the base KDA is downloaded, it will automatically download all associated satellites and expansion cards.

T/MonXM will automatically download a KDA after it has failed and come back on line.

### Virtual Port Type Assignment

This designator makes it possible for T/MonXM to properly route control commands in the case of Alternate Path Routing. The data base looks up the K# definition to determine the path to use in case the dedicated port is not available.

The K# designator will appear in the description field in an alarm report line in the Monitor Mode.

The K# is important in the definition of Site Controls, Labeled Controls, Derived Alarms and Responder Ports.

It is used for Channel Number in the Site Controls and Labeled Controls Point Definition Screens.

It is entered in the Port field in the Derived Definition screen. When writing a formula to derive an alarm or control from an alarm at one of these KDAs the K1 or K2 term is placed at the front of the formula statement in the place of the port number. (i.e.: L K1.27.1.1-3 refers to alarm point 1-3 at the KDA at site number 27, display 1.)

Responder ports (such as TL1) will use the K# designation in addition to 1-500, IA, LC and RP.

## Dial-Up Remotes



**Fig. M3.27 - Select Device Type in the Dial-Up submenu**

This procedure refers to Sections M3-7, which support Versions 1.4D - 1.4M of the KDA-TS. For legacy KDA definition and provision refer to section M3-42

**Note:** KDA Shelves is an improved method of configuring dial-up and alternate path KDAs. See the following pages for more information.

\*The term DCP(F) denotes both DCP and DCP(F) protocols.

Standard Dial-Up Remotes are those that do not require any additional optional software modules in T/MonXM. These include the KDA 864, the Time-Stamp KDA, the KDA 832-T8, the Discrete Point Module (DPM), the AlphaMax 82A, the MAS 46009 Modular Alarm Transmitter (MAT) and the MAS 46030 16 Channel Analog Card (ADC).

Dial-up requires a 212 Modem docking module on the port.

**Note:** Even though this material is treated as a module in this manual, dial-up requires no optional software modules (although dial-up does require that the proper docking module be present on the port being used). It appears here rather than in the standard manual section because of the specialized nature of a dial-up application.

### DPM Sites

This module section supports the following functions for DPM network elements:

- A. Dial Up Device and point definition.
- B. Remote Device Provisioning.
- C. Downloading the Provisioning file to remote devices.

### AlphaMax 82A Sites

This module section supports the following functions for AlphaMax 82A network elements:

- A. Dial Up Device and point definition.
- B. Remote Device Provisioning
- C. Downloading the Provisioning file to remote devices.

### DPM 216 Sites

The Discrete Point Module, DPM 216 is a dedicated line device. It is not supported in this module section. It is treated as a normal DCP(F) device, refer to Software Module 1 for more details.

### KDA 864, KDA-TS, KDA 832-T8 Sites

This module section supports the following functions for KDA 864, Time-Stamp KDA and KDA 832-T8 network elements:

- A. Device and point definition. A KDA can be defined in the T/MonXM data base as:
  1. Dedicated line remote (primary port) using DCP(F)\* protocol;
  2. Alternate Path: Dedicated line primary port with dial-up secondary port;
  3. Dial-up remote (primary port), TRIP protocol;
- B. Remote Device Provisioning (See following pages for dial-up and for KDA-TS on a dedicated line port.)
- C. Provisioning Expansion Cards - 8 Channel Analog (ver. A), Dial-up.

D. Provisioning Expansion Cards - 8 (ver. B) and 16 Channel Analog, Dial-up.

E. Downloading the Provisioning file to remote devices (See the following pages for dial-up and KDA-TS on a dedicated line port.).

#### **Datalok 10D Sites**

Optional module. Refer to Software Module 17 (Pulsecom Datalok Software).

#### **ASCII Sites**

Optional module. Refer to Software Module 7 (ASCII Processor).

#### **MAS Sites**

This module section supports the following functions for 46009 MAT and 46030 ADC network elements:

A. Device and point definition. A MAS device can be defined in the T/MonXM data base as:

1. Dedicated line remote (primary port) using DCP(F) protocol;
2. Alternate Path: Dedicated line primary port with dial-up secondary port;
3. Dial-up remote (primary port).

B. Remote Device Provisioning.

C. Downloading the Provisioning file to remote devices.

## Defining a Remote DPM, AlphaMax, or Net Dog

T/MonXM supports centrally administered provisioning of DPM, AlphaMax, or Net Dog remotes.

The following procedures and tables describe how to define and provision (download) a remote DPM, AlphaMax, or Net Dog device in the T/MonXM database. The DPM, AlphaMax, or Net Dog devices report only via dial-up ports and both are downloadable via a dial-up port from T/MonXM.

Because of the basic similarities between the DPM, AlphaMax, and Net Dog, they are treated together here. Only the alarm point capacities differ.

At the Main Menu select File Maintenance. At the File Maintenance menu select Dial-Up Networks. The Dial-Up submenu will appear.

To begin defining, select the either DPM Sites, AlphaMax 82A Sites, or Net Dog Sites from the Dial-Up submenu.

The DPM, AlphaMax, or Net Dog Site Definition screen will appear. (Figure M3.28)

```

ALP Site Definition

Site Number      : 1
Description      : AlphaMax Site Number One
Remote Site Phone : 555-1472

Polling Type     : PERIODIC
Polling Interval : 60 (mins)

Scheduled Days ---> SUN:   MON:   TUE:   WED:   THU:   FRI:   SAT:
Scheduled Hours  :
Scheduled Minute :
Contact Timeout  : 3 days 0 hours 0 mins

Fail Threshold   : 3
Retry Interval   : 1
Dialout Port     : 4

F)ind, E)dit, D)elete, N)ext, P)revious, Q)uit :

F1=Device, F10/Esc=Exit

```

Fig. M3.28 - DPM, AlphaMax, or Net Dog definition begins at the Site Definition screen

**Site Definition**

Enter information in the Site Definition screen per Table M3.Q.  
Table M3.R lists the key commands you can use while in the DPM, AlphaMax, or Net Dog Site Definition screen.

**Table M3.Q - Fields in the DPM, AlphaMax, or Net Dog Site Definition screen**

Field	Description
Site Number	Must correspond to the site number that is downloaded to the DPM, AlphaMax, or Netdog remote.
Description	Up to 40 characters (Optional)
Remote Site Phone	Phone number to reach the remote. Parenthesis and hyphens optional. <b>Hint:</b> Don't forget the 8 or 9 if using a PABX.
Polling Type	Periodic or Schedule. Press Tab for a selection window. Press Tab again to toggle the selection highlight. Press Enter to choose. Periodic will call remote every 60 minutes, or specified time period, all day, every day. Selecting Periodic causes the cursor to move to the Polling Interval field. Schedule will call the remote only at the times and on the days specified in the Scheduled Days, Scheduled Hours and Scheduled Minute fields that follow. Selecting Schedule causes the cursor to jump to the Scheduled Days field.
Polling Interval	Enter the time between calls to the remote. (If polling type is Period.)
Scheduled Days	Select Y (do call) or N (don't call) for each day of the week. (If polling type is Schedule.)
Scheduled Hours	Select range of hours on the scheduled days to call the remote. (If polling type is Schedule.) Use 0 to 23. Enter a set (such as 5-8) or individual hours (such as 7, 9, 13, 18, 21) in terms of a 24 hour clock.
Scheduled Minute	Enter the time offset from the hour. (If polling type is Schedule.)
Dialout Port	Remote port used for outgoing calls.
Contact Timeout (AlphaMax only)	Determines the period of no contact before a device failure is declared. The ranges are: days = 0-30 hours = 0-23 mins = 0-59. For very best operation however, AlphaMax must be set to periodically call in more frequently than this setting. This feature lets you know if any of your AlphaMax devices fail to check in. <b>Note:</b> This port must have already been defined as a TRIP Dial Up Port. If this remote is not to be polled until a later time, (perhaps because the unit is not yet installed or is out of service) enter "0" here and redefine it for the proper port when appropriate.
Fail Threshold (DPM and AlphaMax only)	A device failure will be declared after the specified number (1-99) of unsuccessful calls.
Retry Interval (DPM and AlphaMax only)	Time interval (1-99 minutes) that a device is retried before it is declared failed.

**Table M3.R - Key commands available in the DPM, AlphaMax, or Net Dog Site Definition screen**

Function Key	Description
F1	Device. Note: Available only after the site has been defined and when the cursor is on the prompt line.
Up Arrow	Move to previous field.
F8	Save
F10/Esc	Exit.

DPM Device Definition	
DPM Site Num : 1	
Description : DPM Environmentals	
Site Name : FRESNO MAIN	
Virtual addr : 2	
Ack Mask : 1-16	
Ack On Rcv : N	
Log Undefined: N	
----- Address Defaults -----	
Polarity : B	Windows :
Logging : L	Message : 0
History : H	
Level : A	
Status : A	
Reverse : N	
Description : (Undefined)	
F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :	
F1=Pnts,F3=Int Alarms,F5=Prov,AF1=TL1,F10/Esc=Exit	

**Fig. M3.29 - Define the DPM, AlphaMax, or Net Dog device****Device Definition**

Table M3.S, below, lists the key commands you can use while in the DPM, AlphaMax, or Net Dog Device Definition screen.

**Table M3.S - Key commands available in the DPM, AlphaMax, or Net Dog Device Definition screen**

Function Key	Description
F1	Points. Takes you to the Point Definition Screen.
F3	Internal Alarms. This brings up a screen for assigning the device fail and device off-line internal alarm points. Follow screen prompts to specify address, display, and point for each device that has been defined. (Address must be either 11 or 12.)
F5	Provisioning. Brings up the device provisioning menu. See details later in this module section.
Alt-F1	TL1. Refer to the TL1 Responder section, Software Module 14, for more information.
F10/Esc	Exit

When site definition is complete press F1 to enter the Device Definition screen (Figure M3.29). Enter information in fields according to Table M3.T.

**Table M3.T - Fields in the DPM, AlphaMax, or Net Dog Device Definition screen**

Field	Description
DPM, AlphaMax, or Netdog Site Number	Same as Site Definition Screen. (Can change only to an existing site number.)
Description	Up 40 characters (optional).
Site Name	Up 15 characters (optional).
Virtual Address	Unique identifying number (0 to 999) for this dial up device. Each dial up device must have a virtual address that is not assigned to any other dial up device. This number could be the port number plus the remote address, the last three digits of the phone number or any other scheme that is practical. Be sure all virtual addresses are unique.
ACK Mask	Enter numbers of points that can be acknowledged by T/MonXM.
ACK on Rcv	Acknowledge alarms on incoming calls? Select Yes or No from the default box.
Log Undefined	Yes(Y) or No(N). This determines whether alarms that have not been defined in the data base will be reported. Can be useful in preventing nuisance alarms from equipment that may be connected to the remote but is not yet on line.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

**Point Definition**

Press F1 while in the Device Definition screen. The Point Definition screen will appear — see Figure M3.30. The information entered in this screen forms the alarm presentation in the T/MonXM monitor screen. Refer to Section 10 for more information on point definition.

Point Definition									
DPM	1	Display Desc :							
P	L	H	L	S	R				
Pt	l	g	t	v	s	Description	Fail	Clear	
1	B	L	H	A	A	N	Open Door.....	Open	Closed
2	B	L	H	A	A	N	Tower Light	Out	Normal
3	B	L	H	A	A	N	AC Power	Off	On
4	B	L	H	A	A	N	Standby Generator	Out	Ready
5	B	L	H	A	A	N	East Transmitter No. 1	A	C
6	B	L	H	A	A	N	East Transmitter No. 1	A	C
7	B	L	H	A	A	N	West Transmitter No. 1	A	C
8	B	L	H	A	A	N	West Transmitter No. 2	A	C

Enter polarity. B = bipolar, U = unipolar

Message	
Call FAA at 555-4325	
Tower height 240 ft.	134.01 lat, 152.03 lgt

F1=GOTO,F2=Desc,F3=Blank,F4=Sect,F5=Range,F6=Read,F8=Save,F9=Help,F10/Esc=Exit

Fig. M3.30 - Define 16 alarm points for the DPM or 8 alarm points for the AlphaMax, or 8 for the Net Dog



## DPM and AlphaMax Provisioning

Press F5 while in the Device Definition screen. The DPM or AlphaMax Provisioning Menu will appear. (Figure M3.31)

The screens and data fields for DPM or AlphaMax provisioning are similar to those described under the T/Config instructions in the manuals for the devices. Those familiar with those screens may wish to proceed without reading the following information.

T/MonXM can provision alarm remotes. This is an optional step as you may opt to configure your remotes with the alternative configuration. Using T/MonXM to do this has the advantage of having a centralized database and uses a single application.

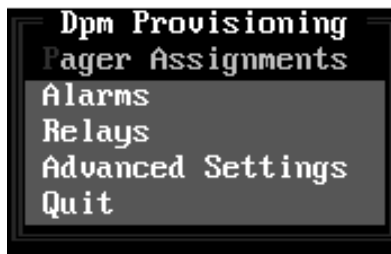


Fig. M3.31 - DPM or AlphaMax Provisioning Starts at the Provisioning screen. AlphaMax, up to ver. 2.2(x) and DPM, ver. 2.1B are supported.

Dpm Pager Provisioning						
Device Number	Device Type	Dial String	Alpha Pager PIN	Pass-word	Report Power On	Report Periodic Status
1	ALPHA..	339-2244	1234	5678	NO	NO
2	NUMERIC	400-9999,,	-	4455	NO	NO
3	ASCII	666-543400443	-	333	NO	NO
4	T/MON	3995555	-	765	NO	NO

ALPHA  
 NUMERIC  
 T/MON  
 ASCII

Enter the device type. Press Tab to select from a list of default values.

↑↓=Up/Dn, Tab=Defaults, F3=Clear Entry, F8=Save, F10/Esc=Abort [DPST]

Fig. M3.32 - Specify Reporting Devices in the Edit Pager Assignments screen

### Pager Assignments

Select Pager Assignments from the provisioning menu. The Pager Assignments screen will appear. (Figure M3.32)

Enter information in fields according to the instructions in Table M3.U.

Table M3.V lists the key commands you can use while in the DPM or AlphaMax Pager Assignments screen.

**Table M3.U - Fields in the DPM or AlphaMax Pager Provisioning screen**

Field	Description
Device Number	This field appears on the screen as a line number before the Type field.
Device Type	Type of device (Alpha, Numeric, T/Mon or ASCII) to be used. T/Mon pager must be defined for reporting to T/Mon or IAM.
Dial String	Phone number that the DPM or AlphaMax will use to dial device. "@" and "," can be used as pauses. Add 2 commas after Numeric pager phone numbers.
Alpha Pager PIN	Pager Identification Number for an alpha pager (provided by the pager company). Up to 7 digits. This field is skipped when defining a numeric pager.
Password	Password for the device. This number is used when calling in from a DTMF (tone dialing) phone. Use up to 5 numbers.
Report Power On	Sends a report to the pager when power is restored after an outage.
Report Periodic Status	Sends a periodic status report according to the Status Report Interval setting.

**Table M3.V - Key commands available in the DPM or AlphaMax Pager Assignments screen**

Function Key	Description
F3	Clear Entry. Deletes contents of all fields in the line.
F8	Save. Save and exit to the provisioning menu.
F10/Esc	Exit. Moves cursor to the top line or exits to the provisioning menu without saving.

Dpm Alarm Provisioning				
Description	Primary Report Device	Delay (min)	Secondary Report Device	Times To Repeat
1 Open Door	1	4	3	2
2 Tower Light	3	0	4	6
3 AC Power	1	1	3	4
4 Standby Generator	1	1	3	4
5 East Transmitter No. 1	1	1	2	4
6 East Transmitter No. 2	1	1	2	4
7 West Transmitter No. 1	1	1	2	4
8 West Transmitter No. 2.....	1	1	2	4

Enter the description for this alarm.

↑↓=Up/Dn, F2=Advanced, F3=Clear Point, F8=Save, F10/Esc=Abort [DPS]

Fig. M3.33 - Define Alarm Points in the DPM, AlphaMax, or Net Dog Alarm Provisioning screen

### Alarm Provisioning

Select Alarms from the provisioning menu. The Alarm Provisioning screen will appear. (Figure M3.33)

Enter information in fields according to the instructions in Table M3.W.

Table M3.W - Fields in the DPM, AlphaMax, or Net Dog Alarm Provisioning screen

Field	Description
Point Number	This field appears on the screen as a line number before the Description field. <b>Note:</b> The DPM accepts 16 point entries, the AlphaMax accepts only 8 point entries; the Netdog accepts 8 as well.
Description	30 character description of the alarm point which is sent to an Alpha pager.
Primary Report Device	Primary device to call when this point is in alarm. (1-4) Enter dash for none.
Delay (min.)	Delay time period (0-269 minutes) that AlphaMax will wait before dialing the secondary device. Default = 0.
Secondary Report Device	Secondary device to call when this point is in alarm. (1-4) Enter dash for none.
Times to Repeat	Number of times to repeat dial loop if alarm is not acknowledged or cleared. (0-15)

Dpm Alarm Provisioning				
ADVANCED PARAMETERS:		Qualifying	Call	
Description		Period	When	Normal
		hh:mm:ss.t	Clear	State
1	Open Door.....	2:00.0	NO	CLOSED
2	Tower Light	0.0	YES	CLOSED
3	AC Power	1:00.0	YES	CLOSED
4	Standby Generator	0.0	YES	OPEN
5	East Transmitter No. 1	0.0	YES	OPEN
6	East Transmitter No. 2	0.0	YES	OPEN
7	West Transmitter No. 1	0.0	YES	OPEN
8	West Transmitter No. 2	0.0	YES	OPEN
Qualifying Period Base Time:		1:00.0		
Alarm Point Description. RANGE: ASCII				
↑↓=Up/Dn, F4=Edit Base Period, F8=First Page, F10/Esc=First Page				[DPSP]

Fig. M3.34 - Press F2 to display the Advanced Parameters screen

Press F2 to see the Advanced Parameters portion of the Alarm Provisioning screen (Figure M3.34 and Table M3.X). Table M3.Y describes the key commands in the Alarm Provisioning Window.

Table M3.X - Fields in the DPM, AlphaMax, or Net Dog Advanced Parameters screen (F2)

Field	Description
Qual. Period Base Time(F4)	Base time is the multiplier factor that is applied to the Qualifying Period for each point. (0.1 sec to 1 hr) Hours/Minutes/Seconds /Tenths
Qual. Period	Time the alarm condition must exist to activate an alarm. A default box lists the available point times, determined by the Base Time.
Call on Clear	If "YES" the DPM, AlphaMax, or Netdog will call to report a COS when the point clears.
Normal State	Determines normal (non-alarmed) current flow condition in the input optical coupler. OPEN is no current when not alarmed (NORMALLY OPEN), CLOSED is current flow when not alarmed (NORMALLY CLOSED).

Table M3.Y - Key commands available in the Alarm Provisioning screen

Function Key	Description
F2	Displays Advanced Parameters window.
F3	Clear Point. Deletes contents of all fields in the line.
F8	Save. Save and exit to the Provisioning menu.
F10/Esc	Moves cursor to top line or exits to Provisioning menu without saving.

**Relay Provisioning**

Select Relays from the provisioning menu. The Relay Provisioning screen will appear. (Figure M3.35)

Enter information in fields according to the instructions in Table M3.Z.



**Fig. M3.35 - Define two Control Points in the Relay Provisioning screen**

**Table M3.Z - Fields in the DPM, AlphaMax, or Net Dog Relay Provisioning screen**

Field	Description
Relay 1 Description	Description for control relay 1. Use up to 30 characters
Relay 2 Description	Description for control relay 2. Use up to 30 characters
Momentary Activation Period	Activation time period for momentary controls. (0.1-25.5 sec)

```

Dpm Advanced Provisioning

Paging Parameters
  Callout Delay           : 0:50 m:ss
  Redial Attempts         : 2
  TAP Baud                : 300

Alarm Parameters
  Alarm Message           : ALARM
  Clear Message           : CLEAR
  Use Alarm 1 for Local Ack : NO
  Activate Relay 1 on COS : NO
  Auto-Ack for ASCII Pager : NO

Periodic Status Reporting
  Status Report Interval  : 1:00   hhh:mm
  Alarm Character         : A
  Clear Character         : C

Remote Unit Parameters
  Remote Modem Initialization : ATHEQUX4F1TS0=OS8=5
  Number of Rings          : 2

Minimum delay between calls to pagers. RANGE: 0-5:00 min to nearest 10 sec

```

Fig. M3.36 - Enter values in the Advanced screen only if defaults are not used

**Advanced Provisioning**

The fields in the Advanced Provisioning screen are pre-set to commonly used default values. If default values are not acceptable, select Advanced Settings from the provisioning menu. The DPM, AlphaMax, or Net Dog Advanced Provisioning screen will appear. (Figure M3.36)

Enter information in fields according to Table M3.AA.

```

Dpm Advanced Provisioning

DERIVED CONTROLS:

Conditions That Will Activate Relay 1
-----
Condition #1 ---> IF Set : 1-3          AND Clear : 2,5
OR
Condition #2 ---> IF Set : 1-3          AND Clear :

Conditions That Will Activate Relay 2
-----
Condition #1 ---> IF Set : .....      AND Clear :
OR
Condition #2 ---> IF Set :              AND Clear :

Alarm points RANGE: 9-16. Use commas and/or dashes to specify a range.

```

Fig. M3.37 - Derived Controls automatically operate when a combinations of alarms occur

**Table M3.AA - Fields in the DPM, AlphaMax, or Net Dog Advanced Provisioning screen**

Field	Description
Paging Parameters	
Call-Out Delay	Minimum delay between alarm reports. (0 to 5 min. to nearest 10 sec.) Overrides "Delay to Calling Secondary Device," if greater.
Re-dial Attempts	Number of times to repeat dial loop if the remote is not reached. (0-15)
Tap Baud	Select 300 or 1200 Baud for TAP Protocol.
Alarm Parameters	
Alarm Message	State description. Seven character message indicating alarm status in a COS report to an alpha pager or to the monitor screen. Use up to 7 characters.
Clear Message	State description. Seven character message indicating cleared status in a COS report to an alpha pager or to the monitor screen. Use up to 7 characters.
Pnt 1 for Local Ack	Assigns alarm input 1 to be used as local acknowledgment input.
Use Relay1 For COS	Assigns control relay 1 for alarm change of state (COS) latch.
Auto ACK for ASCII	Determines if an alarm is automatically acknowledged for points reporting with ASCII pager.
Periodic Status Reporting	
Status Report Interval	Time between status reports to pager. Enter "0" to disable. (15 min. to 255 hours:59 min)
Alarm Character	Character that represents an alarm in the status report to alpha pagers.
Clear Character	Character representing a cleared point in the alpha pager status report.
Remote Unit Parameters	
Remote Modem Initialization	The initialization download for a remote modem. Press "F" <ENTER> to reset to factory defaults.
Number of Rings	Number of rings that the remote will wait before answering call. (1-15)

**Derived Controls**

Press F4 while in the Advanced Provisioning to set derived controls. Two equations may be specified for each two control point. There are two IF SET fields and two IF CLEAR fields for each control point.— see Table M3.AB.

**Table M3.AB - Fields in the Derived Controls screen**

Field	Description
IF SET	List alarm points that must be in alarm for the control point to activate. Use commas or dashes, no spaces. <b>Note:</b> DPM uses points 1-8 for relay 1, points 9-16 for relay 2.
IF CLEAR	List alarm points that must be cleared for control point to activate. <b>Note:</b> Field can be blank. DPM uses points 1-8 for relay 1, points 9-16 for relay 2.

**This page intentionally left blank.**



# Software Module 4

## Badger Interrogator

Through the Badger Interrogator port usage T/MonXM can poll Badger remote telemetry units, models 433, 475, 481, and the Badger/CentraLine 475. The Badger Interrogator fully supports analogs, discrete alarms and controls.

**Note:** “Badger” is a trademark of its respective owners.

### Install or Upgrade the Software

Under normal circumstances installation will only need to be done for software updates or newly ordered modules. The original disks have been supplied with the T/Mon for archival or emergency recovery procedures. See Section 2 (Starting T/MonXM Software) further instructions on upgrading or installing software. preset databasing of internal alarms and analog points for all legacy remotes

### Configure the Badger Interrogator

The Badger Interrogator is configured in six steps:

1. Define a remote port for the Badger Interrogator.
2. Define Badger remote device.
3. Define your alarm points
4. Define your analog points and threshold.
5. Define internal alarms
6. Define control relays, if any.

## Step One

### Define the Remote Port

1. From the Master menu, select Parameters > Remote Ports.
2. Using the F)ind, P)revious, or N)ext commands, navigate to the remote port number for the port that is connected to the Badger remotes.
3. Choose E)dit.
4. Press Tab to select the list box and choose “Badger Interrogator” from the list of available port usages.
5. Enter appropriate values in the other fields in the Remote Parameters screen. See Figure M4.1 for a screen capture of the Remote Parameters screen and Table M4.A for an explanation of the fields.



Fig. M4.1 - Remote Port defined for Badger Interrogator

Table M4.A - Fields in the Badger Interrogator Remote Parameters screen

Field	Description
Port Usage	Badger Interrogator
Serial Format	Baud rate, parity word length, and stop bits settings that T/MonXM will use to communicate with the equipment.
Time out	Time interrogator will wait for a response before failing the poll (200-9999 milliseconds).
Poll Delay	Enter the time between polls in milliseconds. (0-9999)
Check DCD on Rcv	Y=enable Dcd checking to validate Rcv, N=disable.
RTS Lead	Time lead (0-2500 milliseconds in 10 millisecond increments)
RTS Tail	Time RTS off time (0-2500 milliseconds in 10 millisecond increments) Fail.
Fail Threshold	Number of polls before device failure is declared (3-20).
Fail Poll Cycles	None. Number of polling cycles before failed device are polled (0-255).

## Step Two

### Define Badger Remote Devices

1. From the Remote Ports screen press F1 to open the Remote Device Definition screen — see Figure M4.2.
2. Enter appropriate information in the fields. See Table M4.B for an explanation of the fields.
3. Define a different address for each Badger site.

```

Remote Device Definition

Port      : 10      Badger Interrogator
Address   : 1

Description : BADGER SITE
Site Name  : REMOTE BADGER SITE

Displays  : 1-17
Refresh Rate : 548

Log Undefined: N
-----
Polarity   : B      Address Defaults -----
Logging    : L      Windows      :
History    : H      Message     : 0
Level      : A
Status     : A
Reverse    : N
Description : <Undefined>

F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit : _
F1=Pnts, F3=Int. Alarms, F5=ALG, AF1=TL1, AF6=Templates, F10/Esc=Exit

```

Fig. M4.2 - Remote Device Definition screen for Badger Interrogator

Table M4.B - Fields in the Badger Interrogator Remote Device Definition screen

Field	Description
Port	This port number.
Address	Address of this Badger site. (Matches the RTU.)
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Displays	Number of displays to be reserved for collection. The default setting is 1–17, which should never be changed.
Refresh Rate	Number of poll cycles before a refresh cycle occurs.
Expander Cnt	Number of expander units connected to base unit. Available range is 0–1.
Log Undefined	Select Yes or No to log undefined alarms.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/ MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L]. <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H]. <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.



Fig. M4.3 - Point Definition screen

## Step Three

### Define Alarm Points

1. Press F1 in the Remote Parameters screen to go to the Point Definition screen — refer to Figure M4.3 and Table M4.D.
2. Press E (Edit) and enter your point descriptions. See Table M4.C for more Point Edit help. For more information on alarm point definition see Section 10 (Point Definition Tutorial).

Table M4.C - Key commands in the Point Definition screen

Key	Command	Description
F1	GOTO	Go directly to a point.
F3	Blank	Blanks out a point definition.
F4	Attribute Section	Displays next section of attributes.
F5	Range Functions	Access commands that operate a range of points (e.g. translations, copies).
F6	Read	Reads point definitions from another display or address.
F8	Save	Save point definitions and return to polling list.
F10/Esc	Exit	Leaves the database screen without saving any changes that have been made.
Alt-F3	Delete Point	Deletes point under cursor and all below to move down one positions. And undefined point is then inserted at the cursor.
Alt-F4	Insert Point	Inserts an undefined point above cursor.
Alt-F5	Block Move	Moves a block of points within a display.
Alt-F6	Block Copy	Copies a black of points within a display.
Ctrl-F6	Extended Read	Reads in a portion of another display to a starting point in the current display.

**Note:** Vertical editing is available in the point editing section via the CTRL-PGUP and CTRL-PGDN keys. Press Ctrl-H for help online.

**Table M4.D - Fields in the Point Definition screen**

<b>Field</b>	<b>Description</b>
Polarity	Enter "B" for Bipolar, "U" for Unipolar
Logging	Enter "L" for Log, "N" for No log.
History	Enter "H" for History, "N" for No history.
Level	Enter the default alarm level. Valid entries A, B, C, D.
Status	Enter "A" for Alarm, "S" for Status.
Reverse	Enter "R" for Reverse, "N" for No Reverse.
Description	Enter the default point description. This field is initially "Undefined."
Windows	Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.
Qualification	Enter the duration alarm qualification time setting followed by a letter indicating the time units being used. The maximum numeric value is 99. Valid units are M for minutes, H for hours, and Q for quarter hours. Example: "10M" means 10 minutes.
Counter Qualification	Enter counter alarm qualification setting. In counter qualification, the alarm qualifies when a specified number of occurrences of the alarm occur in specified amount of time.  For no counter qualification enter a 0. Otherwise enter the qualification time followed by a letter indicating the time units being used. Follow this with a slash and the number of occurrences that will cause the alarm to qualify.  The maximum value for the period length is 99. Valid time units are M = minutes, H = hours, and Q = quarter hours. The maximum value for occurrences is 250.  Example: 30M/10 MEANS 10 occurrences in 30 minutes.
Pager	Pager Profile Number (1-99)    0 = none

## Step Four

## Define Analog Points

1. From the Remote Device Definition screen, press F5 to open the Analog Provision screen — see Figure M4.4. Table M4.E explains the fields in this screen.
2. Fill in the Description, Sig, and Unt fields.
3. You may also define analog threshold values, to display actual or appropriate values. Complete the Analog Display Worksheet, by pressing F1 in the Analog Provision screen — see Figure M4.5.

Alg	Description	Sig	Unt	MjOvr	MnOvr	MnUdr	MjUdr
1	BATTERY A	2	UDC	54.00	52.00	44.00	42.00
2	BATTERY B	2	UDC	54.00	52.00	44.00	42.00
3	TOWER LT CURR	3	mA	18.00	15.00	8.000	6.000
4	OUTSIDE TEMP	2	F	99.37	87.00	16.87	12.75
5	INSIDE TEMP	2	F	78.75	74.62	41.62	33.37
6	CABLE PRESS	2	PaL	18.00	16.00	10.00	8.000
7	LOOP CURRENT	3	mA	18.00	15.00	8.000	6.000
8	.....						
9							
10							
11							
12							
13							
14							
15							
16							

Enter description <begin with ":" to include threshold crossed in SNMP Trap>

F1=Define Scale, F8=Save, F9=Help, F10/Esc=Exit

Fig. M4.4 - Analog Provisioning screen

Table M4.E - Fields in the Analog Provisioning screen

Field	Description
Port, Address, Site Name	Non-editable fields identifying this Badger device.
Point	ID of alarm point (1–16).
Description	Optional description of this alarm point. Note: If analog alarms from this remote will be forwarded as SNMP traps, typing a colon (:) at the beginning of the description will include the analog threshold crossed in the trap.
Sig	Number of digits to display after the decimal point.
Unt	Type of analog unit (i.e. VDC or %RH).
<b>Note:</b> You must complete the Analog Display Worksheet before completing the next four fields. Press F1 to open the Analog Display Worksheet, and follow the instructions given below under “Analog Display Worksheet.” See the following pages for more information.	
MjOvr	Major Over threshold. Enter the threshold value in native units.
MnOvr	Minor Over threshold. Enter the threshold value in native units.
MnUdr	Minor Under threshold. Enter the threshold value in native units.
MjUdr	Major Under threshold. Enter the threshold value in native units.
<b>Note:</b> When these fields are selected, the available range and the value of the input voltage or current will be shown at the bottom of the screen.	

```

Analog Provisioning
Port: 10  Address: 1
<Native Unit Thresholds>
Analog Display Worksheet

1  Enter a pair of analog values and corresponding display units.
2  The Display Scale and Display Offset used to convert voltage
3  <or current> into display units is calculated automatically.
4
5  Analog input type - Volts or Current (V/C) : V
6
7  Voltage value 1: 0.00000  Unit value 1 : 0.00000
8  Voltage value 2: 79.9000  Unit value 2 : 79.9000
9
10 Calc Scale : 1.00000  Calc Offset: 0.00000
11
12
13
14 Enter analog input type: V for Volts, C for Current
15
16

Enter description <begin with ":" to include threshold crossed in SNMP Trap>

Up Arrow=Previous Field, F6=VDC, F8=Save, F10/Esc=First Field  DPS

```

Fig. M4.5 - Analog Display Worksheet

**Note:** This operation is optional for users who want to change the analog reference scale so that the displayed analog values correspond to real world values.

## Analog Display Worksheet

The analog alarms are set to measure voltage by default and the thresholds are reported as native units. For example, Channel 3 below is measuring outside temperature. If you were using a sensor with a measurable temperature range between -4 degrees to +167 degrees Fahrenheit (-20 degrees to +75 degrees Celsius). The voltage for that channel varies between 1 and 5 VDC for that sensor, which is to be reported as degrees Fahrenheit (native units) where 1 volt represents -4 degrees Fahrenheit and 5 volts represents +167 degrees Fahrenheit.

To define your analog reference scale, press F1 from the Analog Provision screen. The Analog Display Worksheet screen is used to convert the analog voltage and current readings into meaningful measurements and units. The analog inputs actually only measure either voltage or current. The values must be converted to their actual units by determining the scale and offset for each input. By entering in a few simple values, T/Mon will make the conversion calculations automatically. Each field and its function are described below.

### Analog input type - Volts or Current (V/C)

This field is where the type of electrical input to the analog channel is selected. This is either V or C for voltage or current. Determine this by the type of sensor or input device used for each input.

### Voltage/Current value 1

This is the lowest/minimum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

**Unit value 1**

This is the lowest/minimum measurement in the native units of the analog input (degrees, percent relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the minimum range here.

**Voltage/Current value 2**

This is the highest/maximum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

**Unit value 1**

This is the highest/maximum measurement in the native units of the analog input (degrees, percent relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the maximum range here.

After entering the minimum and maximum ranges in both actual voltage or current values and native units, the calc scale and calc offset will automatically be calculated. After exiting the worksheet, key through the remaining entries for that input to make the changes effective.

---

**Step Five**
**Define Internal Alarms**

Entering F3 (Int Alarms) from the Remote Device Definition screen will bring you to the Device Internal Alarm Assignment screen.

User defined internal alarms originate from remote port device failures or derived alarms — refer to Section 14 (Defining Internal Alarms) for detailed information.

```

Device Internal Alarm Assignment

Port : 10

Address Dev   Description                               Fail   Offline
-----
1    BGR    BADGER SITE                               .....

Enter internal point <addr.disp.pnt> <blank=none> <address range: 0-13>

F8=Save. F10/Esc=Exit
  
```

Fig. M4.6 - Device Internal Alarm Assignment screen



---

## Step Seven

### Define Control Relays

You may define control relays for the Badger by going to Master Menu > Files Maintenance Menu > Labeled Controls screen—see section 12-6. Also refer to section 12-10 for more information on derived controls.

**This page intentionally left blank.**

# Software Module 5

## Larse Interrogator

The Larse Interrogator software module enables T/MonXM to poll Larse and Badger remote telemetry units, model numbers 1200, 1240, 1241, 1242, 1400, 1440, 1441, and 1442.

The Larse Interrogator software module fully supports all features of these remotes, including discrete alarms, analog alarms, control relays, and provisioning downloads to Larse/Badger remotes.

**Note:** An FSK Converter unit must be used as a physical interface between your T/MonXM system and Larse/Badger remotes. Refer to the FSK Converter User Manual, DPS Telecom document number D-OC-UM037.15100, for information on hardware installation and communication diagnostics.

---

### Software Installation

---

If you ordered the Larse Interrogator with a new T/MonXM system, it will be factory-installed and preconfigured. The configuration instructions in this section are only for users who have not ordered preconfigured systems. To install the Larse Interrogator on an existing system, follow the instructions for installing new modules in Section 2, Software Installation.

---

### Configuration

---

**Note:** “Larse” and “LarScan” are trademarks of Larscom, Incorporated.

“Badger” is a trademark of Applied Innovation, Inc.

The Larse Interrogator is configured in seven steps:

1. Define a remote port for the Larse Interrogator.
2. Define Larse/Badger remote device.
3. Provision Larse/Badger device.
4. Define alarm points.
5. Define T/MonXM analog alarm thresholds for any analog alarm inputs.
6. Define internal alarms.
7. Define control relays, if any.

### Step One

#### Define the Remote Port

1. From the Master menu, select Parameters > Remote Ports.
2. Using the F)ind, P)revious, or N)ext commands, navigate to the remote port number for the port that is connected to the FSK Converter. For new T/MonXM systems, refer to the Port Allocation Table to find the correct port. This port must be equipped with an RS-232 interface.
3. Choose E)dit.
4. Press Tab to select the list box and choose “Larse Interrogator” from the list of available port usages.
5. Enter appropriate values in the other fields in the Remote Parameters screen. See Figure M5.1 on page M5-2 for a picture of the Remote Parameters screen and Table M5.A for an explanation of the fields.



Fig. M5.1 - Remote Port defined for Larse Interrogator

Table M5.A - Fields in the Larse Interrogator Remote Parameters screen

Field	Description
Port Usage	Larse Interrogator.
Serial Format	Baud rate, word length, parity, and stop bits settings. <b>Note:</b> Be sure these settings match those of the Larse/Badger remotes.
Time out	Time interrogator will wait for a response before failing the poll (200-9999 milliseconds).
Poll Delay	Time between polls in milliseconds (0-9999).
Fail Threshold	Number of polls before device failure is declared (3-20)
Fail Poll Cycles	Polling loop cycles before failed devices are polled (0-255).
Immediate Retries	Number of retries before proceeding with next address.
Download on Edit	Selects automatic download of provisioning information. Choices are: Y = If provisioning information is changed, new data will be downloaded to the Larse/Badger remote when T/MonXM enters Monitor Mode. N = New provisioning information will not be sent automatically. New configuration must be transferred manually by choosing Config (F3) in the Site Statistics screen.
<b>Note:</b> All provisioning information is lost from the Larse/Badger remote's memory if it suffers a power loss. In this case, T/MonXM will automatically re-provision the remote with the current provisioning information when the remote comes back online, no matter which setting is selected for Download on Edit.	

## Step Two

**Note:** DPS recommends that you define Address 0.

## Define Larse/Badger Remote Devices

1. Press F1 to open the Remote Device Definition screen.
2. Enter appropriate information in the fields. See Figure M5.2 for a picture of the Remote Device Definition screen and Table M5.B for an explanation of the fields.
3. Define a different address for each Larse/Badger site.

**Note:** Address 0 is reserved for the FSK Converter. By defining internal alarms for Address 0, you will enable T/MonXM to report device offlines and failures for the FSK Converter.



Fig. M5.2 - Remote Device Definition screen for Larse Interrogator

Table M5.B - Fields in the Larse Interrogator Remote Device Definition screen

Field	Description
Port	This port number.
Address	Address of this Larse/Badger site. (Matches the RTU.)
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Displays	Number of displays to be reserved for collection. The default setting is 1–17, which should <b>never</b> be changed.
Refresh Rate	Number of poll cycles before a refresh cycle occurs.
Expander Cnt	Number of Series 1400 expander units connected to base 1200 unit. Available range is 0–1. <b>Note:</b> This field does nothing for Address 0.
Log Undefined	Select Yes or No to log undefined alarms.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/ MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L]. <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H]. <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter “0” for no message. The maximum messages available are limited by the number of messages in the message file.

### Step Three

Provisioning information is operational characteristics and configuration data sent to the Larse/Badger RTU.

### Provision the Larse/Badger Remote Unit

1. From the Remote Device Definition screen, press F2 to open the Larse Provisioning menu.
2. From the Larse Provisioning menu, choose Base Unit to open the Base Unit Provisioning menu.
3. From the Base Unit Provisioning menu, choose General to open the Base Unit Provisioning – General screen, shown in Figure M5.3. Table M5.C explains the fields in this screen.
4. Press F8 to save your changes and return to the Base Unit Provisioning menu.
5. From the Base Unit Provisioning menu, choose Monitor Points to open the Base Unit Provisioning — Monitor Points screen,



Fig. M5.3 - Base Unit Provisioning — General screen

Table M5.C - Fields in the Base Unit Provisioning — General screen

Field	Description
Annunciator Mode	Selects when the remote unit's annunciator relay is activated. Choices are: <b>A)II COS:</b> Annunciator is activated whenever an alarm point changes state. <b>C)OS-to-A)larm:</b> Annunciator is activated only when an alarm point changes to Alarm.
Min Alarm Time B-level-1	Set Alarm Qualification Time B (0–300 sec).
Set Alarm Qualification Time B (0–300 sec)	Set Alarm Qualification Time C (0–300 sec).
Momentary Control Pulse Duration	Momentary control activation time. (100–3200 msec).
Enable Event Time Reporting	Select Y)es or N)o. Enable Time Stamping. Time stamping is useful because it lets you know when the RTU received the alarm in addition to when the T/Mon received the alarm.

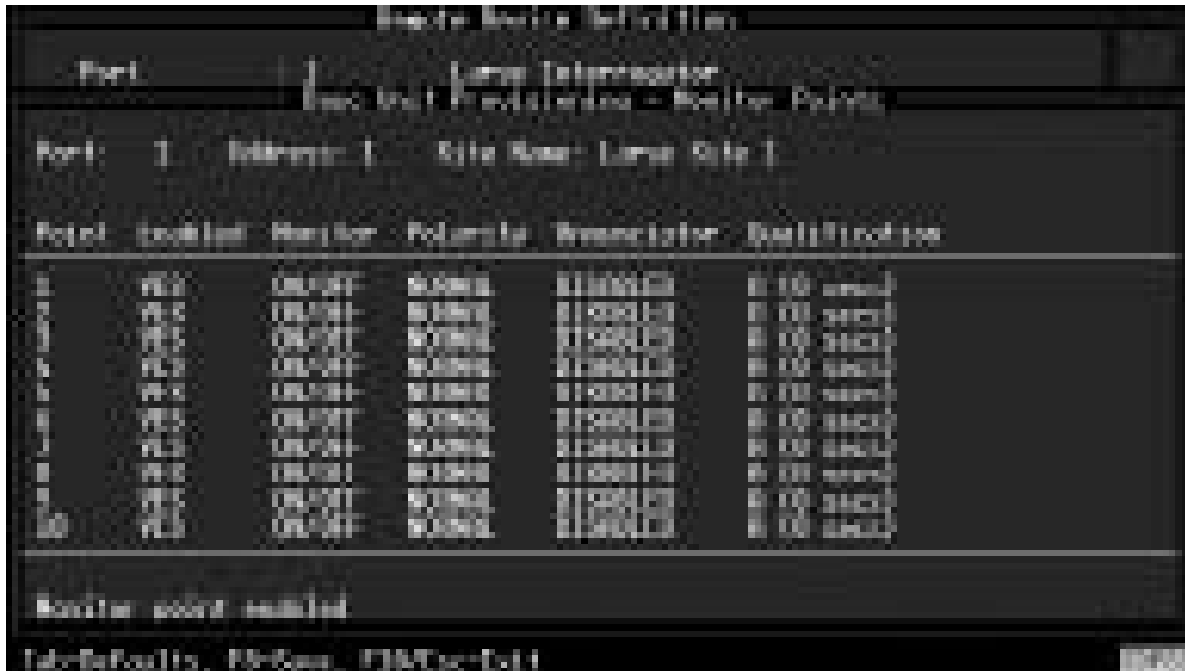


Fig. M5.4 - Base Unit Provisioning — Monitor Points screen

Table M5.D - Fields in the Base Unit Provisioning — Monitor Points screen

Field	Description
Port, Address, Site Name	Non-editable fields identifying this Larse/Badger device.
Point	ID number of alarm point. (1–32).
Enabled	Select YES or NO to enable or disable the alarm point.
Monitor	Select ON/OFF (discrete) or ANALOG operation. <b>Note:</b> Only Points 1–16 can be selected for either analog operation or discrete; Points 17–32 are discrete only.
Polarity	Select NORMAL or REVERSE polarity. Normal: Closed = Alarm Reverse: Open = Alarm
Annunciator	Select ENABLED or DISABLED to choose whether the annunciator relay is activated when this alarm point changes state.
Qualification	Select alarm qualification time for this alarm point. Choices are: A: No alarm qualification B, C: Alarm qualification time defined by user in Base Unit Provisioning — General screen.

shown in Figure M5.4. Table M5.D explains the fields in this screen.

- Press F8 to save your changes and return to the Base Unit Provisioning menu.
- If you selected analog operation for any alarm points, choose Analog Points from the Base Unit Provisioning menu to open the Base Unit Provisioning — Analog Points screen. This screen is shown in Figure M5.5, and Table M5.E explains the fields in this screen.

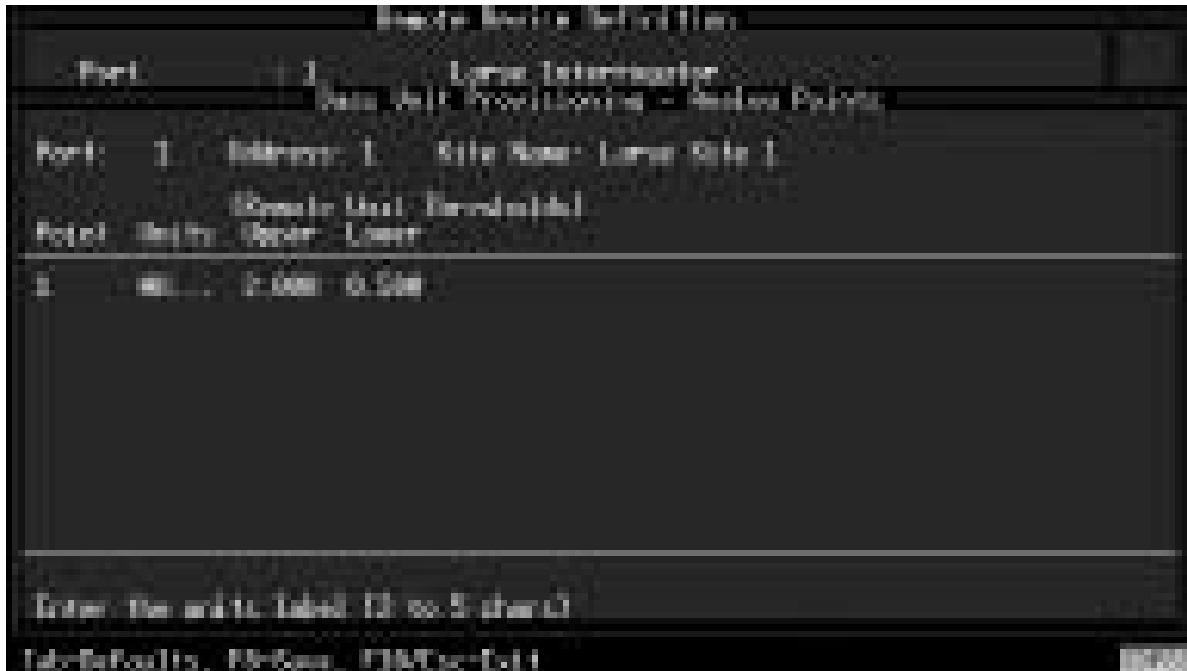


Fig. M5.5 - Base Unit Provisioning — Analog Points screen

Table M5.E - Fields in the Base Unit Provisioning — Analog Points screen

Field	Description
Port, Address, Site Name	Non-editable fields identifying this Larse/Badger device.
Point	ID number of alarm point. (1–16). Note: Only points selected for analog operation in the Base Unit Provisioning — Monitor Points screen appear here.
Units	Type of analog unit. <b>Note:</b> This field is used for description only.
Upper	Upper threshold (0.000–2.000 units).
Lower	Lower threshold (0.000–2.000 units).

It is recommended that you set Threshold Mode to RTU for these because T/Mon will give you four thresholds as opposed to the RTUs two thresholds.

8. Press F8 to save your changes and return to the Base Unit Provisioning menu.
9. If there is a Series 1400 expander unit connected to this Larse/Badger 1200 remote, return to the Larse Provisioning menu and select Expansion Unit. Provision the expander unit (points 33–64) in the same manner as the base unit. Note that points 33–48 can be defined as analog alarm points.
10. If there is no expander unit, return to the Remote Device Definition screen.





Fig. M5.6 - Analog Provisioning screen

## Step Four

### Define T/MonXM Analog Alarm Thresholds

1. From the Remote Device Definition screen, press F5 to open the Analog Provisioning screen, shown in Figure M25.5. Table M25.E explains the fields in this screen.
2. Fill in the Description, Sig, and Unt fields. Before you can define analog threshold values, you **must** complete the Analog Display Worksheet, which is accessed by pressing F1 in the Analog Provisioning screen.

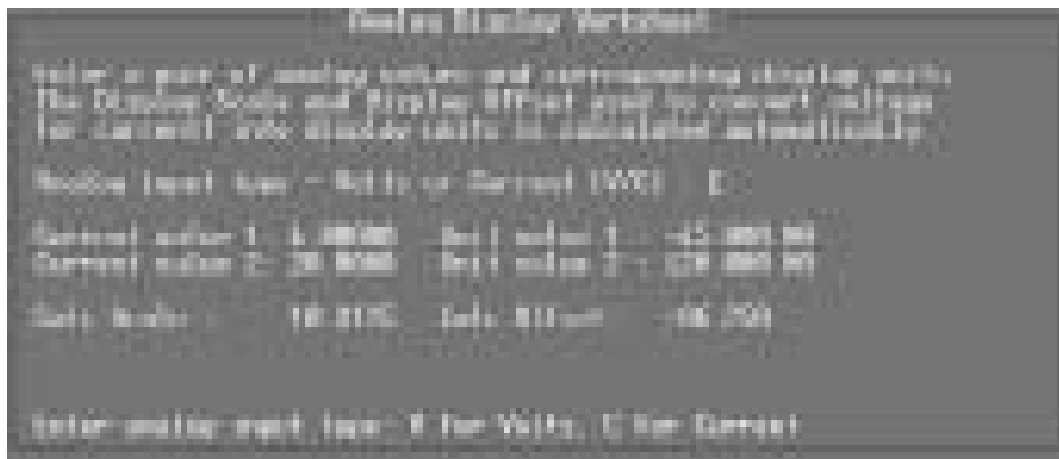
Table M5.F - Fields in the Analog Provisioning screen

Field	Description
Port, Address, Site Name	Non-editable fields identifying this Larse/Badger device.
Threshold Mode	Indicates which thresholds are used. Choices are: TMON = Local thresholds (T/MonXM thresholds defined in this screen) are used. RTU = Native Larse thresholds (defined in Larse Provisioning screen) are used. This setting is toggled by pressing F2.
Point	ID of alarm point (1–16).
Description	Optional description of this alarm point. Note: If analog alarms from this remote will be forwarded as SNMP traps, typing a colon (:) at the beginning of the description will include the analog threshold crossed in the trap.
Sig	Number of digits to display after the decimal point.
Unt	Type of analog unit (i.e. VDC or %RH).
<b>Note:</b> You <b>must</b> complete the Analog Display Worksheet before completing the next four fields. Press F1 to open the Analog Display Worksheet, and follow the instructions given below under “Analog Display Worksheet.” See the following pages for more information.	

**Note:** Table M5.F continues on following page.

**Table M5.F - Fields in the Analog Provisioning screen continued**

Field	Description
MjOvr	Major Over threshold. Enter the threshold value in native units.
MnOvr	Minor Over threshold. Enter the threshold value in native units.
MnUdr	Minor Under threshold. Enter the threshold value in native units.
MjUdr	Major Under threshold. Enter the threshold value in native units.
<b>Note:</b> When these fields are selected, the available range and the value of the input voltage or current will be shown at the bottom of the screen.	

**Fig. M5.7 - Analog Display Worksheet**

**Note:** This operation is optional for users who want to change the analog reference scale so that the displayed analog values correspond to real world values.

### Analog Display Worksheet

The analog alarms are set to measure voltage by default and the thresholds are reported as native units. For example, Channel 3 below is measuring outside temperature. If you were using a sensor with a measurable temperature range between -4 degrees to +167 degrees Fahrenheit (-20 degrees to +75 degrees Celsius). The voltage for that channel varies between 1 and 5 VDC for that sensor, which is to be reported as degrees Fahrenheit (native units) where 1 volt represents -4 degrees Fahrenheit and 5 volts represents +167 degrees Fahrenheit.

To define your analog reference scale, press F1 from the Analog Provision screen. The Analog Display Worksheet screen is used to convert the analog voltage and current readings into meaningful measurements and units. The analog inputs actually only measure either voltage or current. The values must be converted to their actual units by determining the scale and offset for each input. By entering in a few simple values, T/Mon will make the conversion calculations automatically. Each field and its function are described below.

#### Analog input type - Volts or Current (V/C)

This field is where the type of electrical input to the analog channel is selected. This is either V or C for voltage or current. Determine

this by the type of sensor or input device used for each input.

#### **Voltage/Current value 1**

This is the lowest/minimum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

#### **Unit value 1**

This is the lowest/minimum measurement in the native units of the analog input (degrees, percent relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the minimum range here.

#### **Voltage/Current value 2**

This is the highest/maximum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

#### **Unit value 1**

This is the highest/maximum measurement in the native units of the analog input (degrees, percent relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the maximum range here.

After entering the minimum and maximum ranges in both actual voltage or current values and native units, the calc scale and calc offset will automatically be calculated. After exiting the worksheet, key through the remaining entries for that input to make the changes effective.

### **Note on Analog Alarms**

The Larse/Badger Series 1200 remote defines only two thresholds for analog alarm points, an upper threshold and a lower threshold. T/MonXM defines four: Major Over, Minor Over, Minor Under, and Major Under.

The T/MonXM thresholds provide greater accuracy for two reasons. First, because of basic incompatibilities between the Larse and T/MonXM systems, the Larse/Badger Series 1200 remote can only report to T/MonXM the fact that an analog threshold has been crossed; the remote cannot specify whether the upper or lower threshold has been crossed, nor does the Larse/Badger remote report the actual analog value measured by the analog sensor.

Second, because T/MonXM defines more thresholds, it provides more precise definition of threats and better notification of potential trouble. For example, let's suppose that the equipment at a remote site will fail when the temperature reaches 110 degrees Fahrenheit. With T/MonXM, you can set 110 degrees as the Major Over threshold and also define 95 degrees as the Minor Over threshold. That way you'll have an alarm warning you when things are starting to

go wrong at your site, potentially giving you time to take corrective action and avert equipment failure.

Because of the greater accuracy of the T/MonXM thresholds, DPS Telecom **strongly recommends** that you should use local T/MonXM analog thresholds for your analog alarm points to obtain the most accurate visibility.

Define Alarm Points

Step Five

- 1. From the Remote Device Definition screen, press F1 to open the Point Definition screen.
- 2. Define fail and clear conditions and assign a window for each alarm point — see Figure M5.8. For detailed information on alarm point definition see Section 10 (Point Definition Tutorial).



Fig. M5.8 - Point Definition screen

Step Six

Define Internal Alarms

Internal alarms give you visibility of device failures. For instructions on defining internal alarms see Section 14 (Defining Internal Alarms).

**Note:** Define internal alarms for Address 0 to monitor device offlines and failures for the FSK Converter. Address 0 must be defined to have this option.

Device Internal Alarm Assignment				
Port : 1				
Address	Dev	Description	Fail	Offline
1	LRSE	LARSE DEVICE	1.1.13	▲.....
Enter internal point <addr.disp.pnt> <blank=none>				
Up Arrow=Previous Field. F10/Esc=First Field				

Fig. M5.9 - Device Internal Alarm Assignment screen

## Step Seven

### Define Control Relays

You may define control relays for the Larse by going to Master Menu > Files Maintenance Menu > Labeled Controls screen — see section 12-6. Also refer to section 12-10 for more information on derived controls.

**This page intentionally left blank.**

# Software Module 6

## ASCII Interrogator

DPS has an ASCII training DVD. Please contact the sales department at 1-800-622-3314 for additional information.

---

### Introduction

ASCII Processing gives T/MonXM the ability to monitor the English output of your telecom network and declare alarms based on your selection criteria. This output typically comes from the craft, admin and logging ports of devices like switches and private branch exchanges (e.g., Lucent, Nortel and Ericsson). ASCII data can be imported into T/MonXM either through the Intelligent Controller Card serial ports (ports 1-29) or the LAN ports (ports 30 and above).

Unlike other protocols that may be used to report alarm information, ASCII is free-form, non-standard, and may say almost anything. ASCII Processing is one of the most powerful and flexible features supported by T/MonXM. Unfortunately, there is always a balance between program versatility and programming complexity. In T/MonXM, emphasis is placed on providing a software module that can process practically any kind of ASCII input. Consequently there is a greater burden on the database administrator to properly configure the ASCII Processor than there is in other areas of T/MonXM.

However, DPS Telecom offers features to make the job easier. DPS has created predefined rules that may be used as templates for many commonly used switches. Contact DPS Technical support to see if a template is available for your device type.

Additionally, DPS Telecom strongly recommends the Turn-Up Assistance Package for new systems that will use ASCII monitoring.

This chapter is arranged as follows:

- **Terms Explained:** A glossary of terms used in the remainder of the documentation.
- **Basic Concepts:** An overview of ASCII Processing as a whole.
- **Message Processing:** A technical description of databasing for the ASCII message processing phase, focusing on what entries are available, and how to enter them.
- **ASCII Processing Language:** A technical description of each ASCII processing command.
- **ASCII Debugger:** How to use the debug system.
- **Alarm Processing:** A technical description of databasing for the ASCII alarm processing phase, the second half of ASCII processing, which is generally much simpler than the message processing phase.
- **ASCII Tutorial:** Gives practical advice on determining what to enter, with examples, hints, and hands-on practice that may be helpful in setting up your application.

---

## How to Use this Section

We suggest that you:

- Scan through Terms Explained and Basic Concepts to get a general idea of how ASCII processing works, without at this point trying to understand it all.
- Scan through the reference section to get a general idea of how databasing is done.
- Scan through the language section to get a general idea of what the various commands do.
- Scan through the debugger section to get a general idea of what it can do.
- Go through the tutorial in detail, working the exercises and relating them to the preceding reference materials.
- Review the Alarm Processing section.
- Work your real-life programming problem, starting with a capture on disk of actual messages coming from your external equipment. These will be invaluable in setting up your database, and may be used directly with the debugger to test your databasing efforts.

**Note:** Refer also to section A-33 for ASCII databasing map.



---

## ASCII Terms/Glossary

<b>ASCII:</b>	American Standard Code for Information Exchange. This is a practically universal system for expressing ordinary written text — letters of the alphabet, numerals, punctuation marks, and certain control characters — as numeric values that may be manipulated and transmitted by digital systems. (See ASCII Table, Appendix A, page A-15).
<b>ASCII Processing:</b>	The method used by T/Mon to interpret information that is being received from external devices in ASCII — that is, as ordinary human-readable text — and from it, generate standard alarm responses. It consists of two distinct processes: <ul style="list-style-type: none"><li><b>Message Processing:</b> The first half of ASCII Processing, in which incoming messages are qualified and recognized as alarm data.</li><li><b>(Pattern Matching)</b></li><li><b>Alarm Processing:</b> See “Extract.”</li><li><b>(Extraction)</b> Message Processing are used to generate actual alarms.</li></ul>
<b>Extract:</b>	The second half of ASCII processing, in which the T/Mon parses the qualified alarm messages into short segments of text called “keys” that are used to generate actual alarms.
<b>Character:</b>	An individual letter, numeral, punctuation mark, or control character.
<b>Control Character:</b>	An ASCII character indicating something special in the text, such as a tab or new page. These characters are usually invisible when the text is viewed, and are assigned to the first 32 ASCII codes (decimal values 0-31).
<b>String:</b>	A sequence of characters connected together to form words, phrases, lines, etc. A string could also consist of a single character, or could be empty altogether.
<b>Line:</b>	A string ending with a Line Terminator. When viewed, these usually look like ordinary lines of text, like the lines on this page.
<b>Line Terminator:</b>	A character that marks the end of a line. Most ASCII devices put two characters at the end of a line: a Carriage Return (decimal 13, hex 0D, often abbreviated <CR>) followed by a Line Feed (decimal 10, hex 0A, abbreviated <LF>). In this case, <LF> is the line terminator.
<b>Field:</b>	A segment of text that can be distinguished from surrounding text in some way. For instance, it may be enclosed in quotation marks, or be followed by a comma, or have spaces on either side like the individual words on this page.
<b>Field Separator:</b>	A character, such as a quotation mark, comma, or space, that the system can use to recognize the boundary of a field. T/Mon uses two kinds of field separator: Hard Separators and Soft Separators. <ul style="list-style-type: none"><li><b>Hard Separators:</b> Are recognized by all commands involving fields. Consecutive separators mark separate fields, all empty.</li><li><b>Soft Separators:</b> Are ignored if a particular command specifies hard separators only. Consecutive separators are treated as a single separator. A space is typically a soft separator as well as Carriage Return (hex 0D).</li></ul>
<b>Key:</b>	A string derived from an incoming message that expresses the significant parts of the message, usually in highly abbreviated form. Several keys are created for different purposes: <ul style="list-style-type: none"><li><b>Action Key:</b> Used to set or clear alarms. Each possible incoming alarm message from a particular site must generate a unique Action Key so the system can identify the incoming alarm.</li><li><b>Site Key:</b> Identifies a particular site. Each possible incoming alarm message from</li></ul>

## T/MonXM 6.8 User Manual

	a particular site must generate a Site Key that is unique to that site.
<b>Other Key:</b>	Several other keys may be generated if you are using ASCII Auto-Databasing.
<b>Variable Key:</b>	Place holders for data processing that are not necessary in alarm point configuration.
<b>Slots:</b>	A set of computer memory locations, which may be thought of as pigeonholes, for temporarily holding strings the system will process to assemble keys.
<b>Literal:</b>	A string with a predefined value (called a constant in some programming languages).
<b>ASCII Device:</b>	Depending upon context, either a particular type or a particular piece of external equipment that reports alarm information to T/Mon in ASCII.
<b>Rule:</b>	A set of definitions and commands for ASCII message processing. Two kinds of rules are used with each ASCII device type: <ul style="list-style-type: none"> <li><b>Header Rule (Rule 0):</b> This is the first rule defined for a particular device type. It describes certain characteristics that all the other rules will follow, such as characters to use for Field Separators and Line Terminators. <b>NOTE:</b> Rule 0 is required and will result in initialization error if not present.</li> <li><b>Numbered Rule (Rule N, where N is a number 1-999)</b> Each numbered rule consists of a set of ASCII Command Lines that perform the two major functions of Message Processing: Pattern Recognition, which detects incoming alarm messages, and Action Extraction, which builds keys. One or more numbered rules may be defined. The system tries them in their numbered order until it either recognizes a pattern or runs out of rules.</li> </ul>
<b>Command:</b>	A particular instruction written in the T/Mon ASCII Processing Language (see Language Reference, section M6-11).
<b>Command Line:</b>	A sequence of commands written one after another on a single line within an ASCII rule. One command line usually corresponds with a single line of incoming text and will operate on the message text between 2 line termination characters.
<b>Pointer:</b>	<p>The message processor reads incoming text much the same way you do, <b>from left to right and top to bottom</b>—in other words, the processor never goes backwards. The pointer indicates where the ASCII processor is currently looking, and determines which text to use with the next command.</p> <p><b>The pointer is a very important ASCII processing tool, especially in the extraction phase. Moving the pointer through the text to get to a particular type of data is essential to correct data extraction.</b></p>
<b>ASCII Table:</b>	
<b>Standard Table:</b>	A relational table used to translate alarm text to more usable or standard strings; for example: ALM => SET.
<b>Auto Table:</b>	A rational table used in Auto databasing ASCII to automatically database the pending alarm-clear action string based on the alarm set text string values.

---

## Basic Concepts

- ASCII Messages:** Some external devices transmit alarm information in the form of ordinary text-based messages. In computer applications, ordinary human-readable text is called ASCII because it is represented in the standard encoding system by that name. ASCII Messages consist of one or more lines of text, just like the text you are reading now. In telecom network applications, this output typically comes from the craft, admin and logging parts of devices like switches (Nortel, Ericsson, Lucent, etc.).
- ASCII Processing:** In T/MonXM, the purpose of ASCII processing is to receive incoming ASCII text, interpret the message, and generate appropriate alarm responses. To the user, alarms triggered by ASCII input look just like any other alarm. ASCII Processing has two major parts.
- Message Processing:** The first half of ASCII Processing, receives text as it is imported and performs a two-phase operation on it. Both the Pattern Recognition and Extraction phases work through ASCII rules, which are sets of characteristics and commands written by the user. These commands are databased under Files-ASCII Devices using the special-purpose T/MonXM ASCII Processing Language, and define generic device types that later get assigned to specific physical devices.
- Pattern Recognition:** Attempts to recognize the format of alarm-related messages. Any lines that cannot be recognized are thrown away. Once the alarm format is recognized, the extraction phase begins.
- Extraction:** Looks at specific portions of the message to capture relevant text identifying the alarm. Typically, these are phrases like “site ID,” “alarm desc,” “alarm state,” etc. These phrases are used to form keys, which are basically highly abbreviated forms of the original message containing sufficient information to uniquely identify a particular alarm or site. These keys are then passed on for Alarm Processing.
- Alarm Processing:** The second half of ASCII Processing, works with an installed physical device to generate actual alarms. In T/MonXM, ASCII Alarm Points are set up for a particular physical device exactly like any other alarm, using the standard T/Mon point editing screens. In addition, the physical device is associated with a specific ASCII device type, so that the Message Processor knows what set of rules to use with it, and each ASCII alarm point is databased with two action strings, one to set the alarm and another to clear it. When an action key is received from the Message Processor, the Alarm Processor searches for a matching action string and takes appropriate action if it is found. It is this match of action keys to action strings that links an incoming ASCII message to a particular alarm point and generates an actual alarm.

## Message Processing

This phase of ASCII Processing interprets incoming ASCII messages and parses them to form keys. To set up the database for ASCII message processing, select Files - ASCII Devices from the Master Menu.

**ASCII Rules:** ASCII Rules form a set of definitions and commands for ASCII message processing. Two kinds of rules are used with each ASCII device type:

**Header Rule (Rule 0):** This is the first rule defined for a particular device type. It describes certain characteristics that will be followed by all the other rules, such as which characters to use for Field Separators and Line Terminators.

**Numbered Rule:  
(Rule N, where N  
is a number 1-999)** Each numbered rule consists of a set of ASCII Command Lines that perform the two major functions of Message Processing: Pattern Recognition, which detects incoming alarm messages, and Action Extraction, which builds keys. One or more numbered rules may be defined. The system tries them in their numbered order until it either recognizes a pattern or runs out of rules.

To edit ASCII Rules, select Files - ASCII Devices from the Master Menu, then select ASCII Rules. The screen below will appear.

```
ASCII DEVICE : CSU          DEVICE HEADER

Descr :

    Soft Field Separators : <SPC> <CR>
    Hard Field Separators :
    Line Terminator (hex) : 0A    <LF>

Log On :
CMD 1  : <CR><D>DIS-CSU-ALA:1<CR><D>DIS-CSU-ALA:2<CR><D>DIS-CSU-ALA:3<CR>
CMD 2  : DIS-CSU-ALA:4<CR><D>DIS-CSU-ALA:5<CR><D>DIS-CSU-ALA:6<CR>
CMD 3  : DIS-CSU-ALA:7<CR><D>DIS-CSU-ALA:8<CR>
Log Off :

Inactivity Delay (sec):    3
Response Samples          :    0
Filter                    :    NONE

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

F2=Define Connectivity Test, F7=Auto, F10/Esc=Exit
```

Fig. M6.1 - ASCII Device Header screen

**Note:** Refer to Section 18 (Utilities > Import/Export ASCII Rules) for more information on importing and exporting ASCII rules from a saved file.

---

## Navigating the ASCII Device Rules screens

### ASCII Device Rules

ASCII Device Rules are grouped alphabetically by ASCII Device name, and within each device by Rule number. The first rule for each device is always a Device Header, sometimes called Rule 0. The N)ext and P)rev commands page through this sequence of rules.

**Note:** Rule 0 must be defined.

To define a new device, select F)ind, enter the new device name, and enter 0 for Rule number.

To define a new numbered rule, page to an existing rule for this device, select F)ind, and enter the new rule number.

**Table M6.A - Fields for ASCII Device Rules  
Header (Rule 0) screen**

Field	Description
ASCII DEVICE	A name for a device type that reports alarm information in ASCII. All rules for this device type will be grouped under this name. It will later be assigned, during the Alarm Processing databasing phase, to an actual physical device that is installed at some site. Multiple physical devices may share a single device type.
Rule #	A sequence number assigned to rules for this device type. The Header rule is always Rule 0. (Range 0-999)
Descr	Description for this device type.
Soft Field Separators	Up to five characters may be defined as Soft Field Separators (see ASCII Terms/Glossary, section M6-3). These may be entered as a single character or as a two-digit hex ASCII code (see ASCII table, Appendix A). Once entered, a space will be displayed as <SPC>, a Line Feed as <LF>, a Carriage Return as <CR>. All other entries will be displayed as printable characters or hex codes. The most common entries here are spaces (20), tabs (08), and carriage returns (0D).
Hard Field Separators	Up to five characters may be defined as Hard Field Separators (see ASCII Terms/Glossary, M6-3). These may be entered as a single character -- hex control codes are not permitted - and do not necessarily have to be defined. If used, the most common entries here are commas, tabs, and colons.
Line Terminator (hex)	A single character must be defined as the Line Terminator character (see ASCII Terms/Glossary, section M6-3). It is entered as a two-digit hex ASCII code (see ASCII table on section M6-35, Appendix A page A-15). The most common entry here is a Line Feed (0A).
The next five fields define messages that may be sent from T/Mon to the ASCII device. These messages may include the following symbols to represent special characters and commands:	
<CR>	Carriage Return
<LF>	Line Feed
<^?>	Control key plus a letter between A-Z. Example: <^C> sends Ctrl-C (hex 03)
<Dn>	Delay n tenths of seconds, where n is 1-999, before sending any more characters. Example: <D10> delays 1 second.
<D>	Delay until a time out occurs before sending any more characters
<Tn>	Substitute Token n where n is 1-5 (see Alarm Processing section M6-44). Tokens can be defined per address. The ASCII jobs poll interval field sets the time period between subsequent Logon commands
Log On	A message sent to log onto the remote device. The ASCII jobs poll interval field sets the time period between subsequent Log on commands. Sent in order one period of the Inactivity Delay after the Logon command, or Connectivity Test when defined. CMD 2 and 3 sent after one period of the Inactivity Delay after the previous command.
Cmd 1-3	Commands sent to poll the remote device. CMD1 sent in order one period of the Inactivity Delay after the Log On command, or Connectivity Test when defined. CMD2 and 3 sent after one period of the Inactivity Delay after the previous command. Sent one period of the Inactivity Delay after the previous defined CMD
Log Off	A message sent to log off the remote device. Sent one period of the Inactivity Delay after the previous defined CMD.

**Table M6.A - Fields for ASCII Device Rules  
Header (Rule 0) Screen (continued)**

Field	Description
Inactivity Delay (sec)	Time in seconds after the command is sent and the response received, with no activity in between, before the next command is issued. <b>Note:</b> used with <D> command.
Response Samples	This entry is used to compensate for line noise on some systems. It works by sending each command in the CMD 1-3 fields x number of times, where x is any number 2-9. If the response from the remote is the same each time, T/MonXM will continue to the next CMD line. Otherwise, it will declare a device failure and abandon the attempt. This entry is usually 0, which tells T/MonXM to simply send the commands one time and accept whatever responses it gets.
Filter	Tells T/Mon to perform some special processing on incoming ASCII lines. <ul style="list-style-type: none"> <li>• DEFINITY: A special-purpose filter used when monitoring Definity phone system.</li> <li>• NOKIA: some Nokia systems use the character sequence #E# to mark the end of a line, instead of using a conventional line terminator character. The Nokia Filter changes this to #E followed by the line terminator character defined above.</li> </ul>

**Table M6.B - Key commands available in the ASCII Device Rules screen**

Function Key	Description
F2	Define connectivity test. Useful for dial up systems in order to determine if you are in fact connected to the right device and that the device is in the proper mode. The test issues a command and then examines the response to see if it passes the connectivity pattern match. See next page for more information.
F3	Sample Text Window. Brings up the ASCII sample message window. Allows to view or set the sample message.
Alt-F6	Import/Export ASCII Rules
F7	Auto-definitions. Brings up menu for Auto ASCII definitions.
F8	Save. Only available during field editing.
F9	Help. Only available during field editing.
F10/Esc	Exit.

## ASCII Connectivity Test

This screen is reached by selecting Function Key F2 when on the ASCII Device Rules Header (Rule 0) Screen.

The test will send a command to your device. If the expected response does not return, then a device failure has occurred. Refer to Table M6.C to complete the fields on the screen.

This is an optional command for users who want to make sure they have an active connection to the device.

**Note: Connectivity Test happens after "Log on" and before "CMD 1".**





## Numbered Rules

Numbered Rules are the heart of ASCII processing. These rules perform two major functions:

- Pattern Recognition attempts to recognize alarm-related messages, and identify their format. Any lines that cannot be recognized are thrown away. If a message has been recognized, it goes into the next phase:
- Action Extraction looks at specific portions of the message and forms keys, which are basically highly abbreviated forms of the original message containing sufficient information to uniquely identify a particular alarm or site (several other keys may be generated if you are using ASCII Auto-Databasing). These keys are then passed on for Alarm Processing, which generates the actual alarms.

Both phases are defined on the ASCII Device Rules editing screen shown in Figure M6.3, using the T/Mon ASCII Processing Language. To get to this screen, select Files – ASCII Devices from the main menu, then select a specific rule as follows:

- Rules are grouped alphabetically by ASCII Device name, and within each device by Rule number. The first rule for each device is always a Device Header, called Rule 0. The N)ext and P)rev commands page through this sequence of rules.
- To define a new device, select F)ind, enter the new device name, and enter 0 for Rule number. To define a new numbered rule, page to an existing rule for this device, select F)ind, and enter the new rule number. The header rule must be defined before any numbered rules can be entered for a device.

```

ASCII Device Rules

ASCII DEVICE : TEST          Rule #      : 20  Sample Msg Not Assigned
Descr  :                      Log Type  : STANDARD
Comment:                      Special   : NONE
                                   Ignore    : N

      Pattern Recognition
1 \MASCII
2
3
4
5
6

      Action Extraction
1 \F1\K5
2
3
4
5
6

F)ind, E)dit, D)elele, N)ext, P)rev, M)ove, R)ead, Q)uit :

F3=Sample, F4=Debug, F5=Compile, F6=Manage, AF6=Import/Export, F9=Help, F10/Esc=Exit
  
```

Fig. M6.3 - The ASCII Device Rules Editing screen.

**Table M6.E – Fields for the ASCII Device Numbered Rules Screen**

Field	Description
ASCII DEVICE	Same as the name defined in the header rule for this device
Rule #	A sequence number assigned to rules for this device type. These can be any arbitrary value in the range 1-999 and do not have to be consecutive. <b>Rules are executed in the order of their Rule Numbers. Processing for a particular message halts on the first rule that succeeds.</b> If a message does not pass the tests given in a particular rule, the next rule is tried restarting at the beginning of the message. If all rules fail, the first line of text is discarded and the cycle repeats. <b>In general, you need a separate numbered rule for each message format that is received from this device.</b> If all messages have the same format, but vary only in the value of particular fields, a single rule would suffice. In other cases, a single rule could handle all messages except for one or two exceptions. In this case, give the general rule a high number such as 100, and give rules to handle the exceptions lower numbers such as 10 and 20 so those messages will be intercepted before getting to the general rule. It is always a good idea to leave spaces between your rules (e.g. 10 20 30 40 , etc). Sample message indicator will appear next to the rule # if a sample message has not been assigned. It will display when the sample message has been set or updated for the specific rule.
Descr	Description of this rule
Comment	Description of the action extraction key format
Log Type	Controls what is seen when an ASCII alarm is highlighted on the Standing Alarms page in monitor mode and you select function key F7=Asc. <ul style="list-style-type: none"> <li>• If <b>STANDARD</b>, you will see all of the text that was processed during the Pattern Match and Extraction phases that triggered the alarm.</li> <li>• If <b>DETAILED</b>, additional text may be available as defined on the ASCII Logging Options screen (see page M6-33).</li> <li>• If <b>NONE</b>, you won't see anything.</li> </ul> <b>Note:</b> this function does not produce a permanent log. There are three other ways to view or capture incoming ASCII text: <ul style="list-style-type: none"> <li>• Turn on Log Exceptions or Log All Activity on an ASCII port (see pages M6-38, M6-54, and Section 9 (Remote Ports and Virtual/LAN Jobs).</li> <li>• Use the ASCII Processor Analyzer (see section 9-10, Table 9.E).</li> <li>• Use the \!LOG command in an extraction rule (see page M6-30).</li> </ul>
Special	<ul style="list-style-type: none"> <li>• If AUTO CLR, alarms set under this rule will automatically clear after 30 secs.</li> <li>• Overrides standard processing (is usually set to None).</li> <li>• If FORCE COS, a COS will be generated for this alarm, even in the case that it is already standing..</li> <li>• If SINGLE LOG, only the first of multiple messages is logged and creates an alarm.</li> </ul>
Pattern Recognition	A set of up to six lines containing T/MonXM ASCII Processing Language commands for use in the Pattern Recognition phase of message processing. Each line corresponds to a single line of incoming text. See the Language reference, page M6-14 for details.

Field	Description
Action Extraction	A set of up to six lines containing T/MonXM ASCII Processing Language commands for use in the Extraction phase of message processing. In general, each line corresponds to a single line of incoming text starting with the first line accepted during the Pattern Recognition phase and continuing no farther than the last accepted line. If you need more lines for extraction than you processed during Pattern Recognition, add 'Match any line' command lines to Pattern Recognition to make those lines available. An exception is available for cases where incoming messages consist of a fixed number of header lines followed by a variable number of detail lines: you only need to recognize lines down to the first detail line, and can extract the remainder in a loop. See the Language reference, page M6-26 for details.

## ASCII Rule Syntax Checker

The ASCII rule syntax checker is used for checking the syntax of ASCII rules written in T/Mon to make sure they are formatted correctly. The ASCII rules syntax checking functionality is built into the “ASCII Device Rules” (see Figure. M6.3) window of the T/Mon. Syntax checking operates in two modes which are automatic and manual mode:

### Automatic Mode:

The syntax of the ASCII rule currently being edited is checked automatically every time the rule is saved. If an error is found then the user will be prompted to view the error log. If no errors are found then it will be transparent to the user that the syntax checking ever took place.

### Manual Mode:

The syntax of any ASCII rule can be checked manually by pressing F5 (Compile option) in the ASCII Device Rules window. The user will then have the option of compiling only the current ASCII rule or all ASCII rules.



Fig. M6.4 - Press F5 to compile the current rule or all rules

After the user has made a selection the compiler window will pop-up and display the status as the rule(s) are compiled.



Fig. M6.5 - ASCII Compiler Status window

Just like in Automatic Mode the user will be prompted to view the error log if any errors are found. If no errors are found then the user will also be notified, but will not be prompted to view the error log.



Fig. M6.6 - ASCII Compiler Error Log window

The ASCII rule syntax checker can produce the following error messages:

- **'\' expected:** The required '\' which must precede every command was not detected.
- **Quantity expected:** A numeric value was expected in the command but was not detected.
- **Literal expected:** A string value was expected in the command but was not detected.
- **Invalid command:** The command was not formatted correctly or not supported at all.
- **Extraction phase only:** A command that is only supported in the extraction phase was used in the pattern matching phase.
- **Value out of range:** The value that was entered (a literal or a quantity) was not within the allowable size.
- **Invalid hex byte:** A hex byte was used in a command that was not made up of two characters.
- **Problem with '()' format:** The formatting of the parameters within the command was incorrect.
- **Uneven number of Pattern Rec. and Action Ext. rule lines:** There was an uneven number of Pattern Recognition and Action Extraction rule lines. This is with factoring in the throw away line commands (\Tnum) and loop commands (i.e. \W, \WL, etc...).
- **Blank line in between defined rule lines:** A blank rule line was detected in between two non-blank rule lines. Blank rule lines are only allowed at the end of the Pattern Recognition and Action Extraction sections.
- **'!AUTO' in rule used by Non-Auto Databasing job XXX:** The auto-databasing command (!AUTO) was detected in a rule which is in use by ASCII Input job XXX which has it's "Auto Databasing" field set to No (Remote Parameters screen).

---

## ASCII Processing Language

Pattern recognition, action extraction, and several other aspects of message processing make use of the T/MonXM ASCII Processing Language. Commands in this language are arranged in lines. One command line usually corresponds with a single line of incoming text. The message processor reads incoming text much the same way you do, from left to right and top to bottom. The pointer indicates where it is currently looking, and determines which text to use with the next command. All commands begin with a backslash (\) – if you need to use a backslash in a literal, enter two in succession (\\). The processor is not case-sensitive; all incoming text is converted to upper case when it is received. The following pages describe all commands available in this language.

**Table M6.F - Conventions used in the Language Reference**

Symbol	Description
num,pos,qty	Represent numbers, are replaced by one or more digits in an actual command
lit	Represents a literal, is replaced by one or more characters in an actual command
underline	In examples, shows current position of the pointer in input line

## Match commands

The Match commands on the following page have a pass-fail result. If a match passes, processing continues with the next command. If it fails, the entire numbered rule is abandoned, the pointer is reset to the first character of the first line of the incoming message, and processing resumes at the beginning of the next numbered rule. If there are no more numbered rules for this device, the first line of the incoming message is discarded and the cycle repeats. The Match commands are widely used in both the Pattern Recognition and Action Extraction phases.

In the examples,

- ‘Input’                      The text being processed from an incoming message, with the starting position of the pointer indicated by an underline and bold character.
- ‘Objective’                What you are trying to do.
- ‘Command’                What would be contained within a rule
- ‘Result’                    What happens when the rule executes, with the ending position of the pointer indicated by an underline and bold character.

**Table M6.G - Language Reference, Match Commands**

Command	Description	
\Mlit	Purpose	Match literal. Searches for the specified literal to the right of the current pointer. Use to test if a particular literal occurs in the input line, or to position the pointer to the location where the literal occurs.
	Result	Passes if literal is found, moves pointer to first character where found.
	Notes	There is no space between \M and the literal, and spaces are not allowed in the literal itself (even if ASCII Parameters permit it). The \Mlit command will match on the first occurrence of lit that it finds to the right of the pointer—watch out for literals that are embedded in places where you don't expect them. See second example below.
	<b>Examples</b>	
	Input	<u>A</u> LARM SCANNING:CELL 105
	Objective	Determine if word CELL occurs in input line
	Command	\MCELL
	Result	ALARM SCANNING: <u>C</u> ELL 105 Passes
	Input	<u>M</u> ODULATION STATUS: OFF
	Objective	Search for ON to determine if modulation status is ON or OFF
	Command	\MON
	Result	MODULATION <u>O</u> N STATUS: OFF Passes unexpectedly, finds embedded ON in MODULATION
\M~AL	Purpose	Match Any Line. Used to accept lines that have nothing special in them to search for, but contain or are followed by lines that will be used during extraction.
	Result	Always passes line, advances pointer to first character in next line.
	Notes	Should be the only command on the line. Other commands succeeding this will not be processed.
	<b>Example</b>	
	Input	** 342 REPT ALM T1 "0064-27:CR,RED,SA,09-09,09-38-36,NEND,: \RED" \":,ISLTD" END
	Objective	In Pattern Recognition phase, if a line contains REPT ALM, accept the next line for use during Extraction phase.
	Command	\MREPT\MALM\M~AL
	Result	** 342 REPT ALM T1"0064-27:CR,RED,SA,09-09,09-38-36,NEND,: \RED" \":,ISLTD" <u>E</u> ND First two lines pass.

**Table M6.G - Language Reference, Match Commands (continued)**

Command	Description	
\M~BL	Purpose	Match Blank Line. Tests for a blank line.
	Result	Passes line if it is either null or consists entirely of soft separators, advances pointer to first character in next line. Fails if line has anything on it.
	Notes	Must be the only command on the line. Other commands succeeding this will not be processed.
	<b>Example</b>	
	Input	<u>E</u> MG CONTROL DOWN END
	Objective	Accept if input contains EMG CONTROL followed by a blank line
	Command	\MEMG CONTROL \M~BL
	Result	EMG CONTROL DOWN <u>E</u> ND First two lines pass.
\~Mlit	Purpose	Negative Match Literal. Tests for the <b>absence</b> of a literal.
	Result	Passes if literal is not found to right of pointer. Does not move pointer.
	Notes	Spaces are not allowed in lit (even if ASCII Parameters permit it). This rule is useful for eliminating classes of rules containing certain words — sometimes easier to look for what message shouldn't contain.
	<b>Example</b>	
	Input	<u>E</u> MG CONTROL DOWN
	Objective	Fail if input contains UP
	Command	\~MUP
	Result	<u>E</u> MG CONTROL DOWN Passes
\#M	Purpose	Match digit. Searches for the next occurrence of a digit (0-9) to the right of the current pointer. Use to test if a digit occurs in the input line, or to position the pointer to the location where the digit occurs.
	Result	Passes if digit is found, advances pointer to digit.
	<b>Example</b>	
	Input	<u>_</u> 342 REPT ALM
	Objective	Move to start of numeric field
	Command	\#M
	Result	<u>**</u> <u>3</u> 42 REPT ALM (Passes)



**Table M6.G - Language Reference, Match Commands (continued)**

Command	Description	
\M~T(pos,qty,type)	Purpose	Match Type. Starting absolute pos characters from the start of the line, looks for a string of qty consecutive characters all of the same type.
	Types	A: Alphabetic (A-Z)
		D: Digits (0-9)
		#: Digits, decimal point, minus, plus
		B: Spaces (Blanks)
		S: Soft separators
		H: Hex digits (0-9, A-F)
	Result	Passes if appropriate characters are found at the specified position. No affect on pointer.
	Notes	Used primarily when input is arranged in columns.
	<b>Example</b>	
	Input	** 342 REPT ALM
	Objective	Test that a 3-digit number resides in columns 4-6.
	Command	\M~T(4,3,D)
	Result	** 342 REPT ALM(Passes)
\M~L(pos,lit)	Purpose	Match literal at absolute position. Starting pos characters from the start of the line, looks for the given literal.
	Result	Passes if the literal is there. No effect on pointer.
	Notes	Used primarily when input is arranged in columns. Spaces are not allowed in lit (even if ASCII Parameters permit it).
	<b>Example</b>	
	Input	** 342 REPT ALM
	Objective	Test that the word REPT is there starting in column 8.
	Command	\M~L(8,REPT)
	Result	** 342 REPT ALM (Passes)
\M~Hhh	Purpose	Match Hex byte. Searches for a control character with hex ASCII value hh to the right of the pointer (hh should be in range 00-7F).
	Result	Passes if control character is there, moves pointer to that character.
	<b>Example</b>	
	Input	** 342 <u>RE</u> PT ALM<07><0D><0A>
	Objective	Check for "BEL" character (hex 07)
	Command	\M~H07
	Result	** 342 REPT ALM< <u>07</u>

## Positioning Commands

The following positioning commands simply move the pointer. They are widely used in both the Pattern Recognition and Action Extraction phases.

**Table M6.G - Language Reference, Positioning Commands (continued)**

Command	Description	
\Apos	Purpose	Absolute Position
	Result	Sets pointer to column pos
	<b>Example</b>	
	Input	<b>_</b> 342 REPT ALM
	Objective	Position pointer to column 4.
	Command	\A4
	Result	<b>** 3</b> 42 REPT ALM(Passes)
\Snum	Purpose	Skip characters.
	Result	Sets pointer num characters to the right of its current position. The value of the characters is not taken into consideration, so it skips over soft or hard separators just like any other character.
	<b>Example</b>	
	Input	<b>_</b> 342 REPT ALM
	Objective	Position pointer 4 more characters to the right
	Command	\S4
	Result	<b>** 3</b> 42 <u>R</u> EPT ALM
\Fnum	Purpose	Skip num fields delimited by hard or soft separators.
	Result	Sets pointer num fields to the right or left of its current position, stopping on the first character in that field.
	Notes	Pointer passes over num separators in moving to its new position. Consecutive soft separators only count as one, all hard separators are counted individually. Supports positive and negative numbers
	<b>Example</b>	
	Input	<b>** 3</b> 42 REPT ALM,MAJOR,ENVIRONMENTAL
	Objective	Position pointer two hard or soft fields to the right (commas are defined hard separators and spaces are defined as soft)
	Command	\F2
	Result	<b>** 3</b> 42 REPT ALM,MAJOR, <u>E</u> NVIRONMENTAL
\FHnum	Purpose	Skip num fields delimited by hard separators only.
	Result	Sets pointer num fields to the right of its current position, stopping on the first character in that field.
	Notes	Pointer passes over num hard separators in moving to its new position.
	<b>Example</b>	
	Input	<b>** 3</b> 42 REPT ALM,MAJOR,ENVIRONMENTAL
	Objective	Position pointer two hard fields to the right (commas are hard separators)
	Command	\FH2
	Result	<b>** 3</b> 42 REPT ALM,MAJOR, <u>E</u> NVIRONMENTAL

### Table M6.G - Language Reference, Positioning Commands (continued)

Command	Description			
\Tnum	Purpose	Throw away num input lines.		
	Result	Sets pointer num lines below its current position, positioned on the first character in that line.		
	Notes	If used, this should be the first command on a command line, and is usually followed by other commands that act on the line it lands on. It is intended to conserve command lines. The same effect could be achieved by putting a \M~AL (Match Any Line) on each line to be skipped, but this could be prohibitive if many lines are involved since only six command lines are available.		
	Example			
	Input	- ALARM HISTORY - SCU 4 - 06/29/94		
		-----		
		Type	Date	Initial Current Count
		-----		
		LOS,Line	06/01/94	13 31 27 ok ALARM 195
LOS,DTE		06/16/94	02 16 58 ok ALARM 5	
Objective	LOS,SCU	00/00/00	00 00 00 ok ok 0	
	LOF,Line	06/15/94	21 29 53 ok ok ALARM 5	
Command	\MALARM\MHISTORY \T4\MLOS			
Result	- ALARM HISTORY - SCU 4 - 06/29/94			
	-----			
	Type	Date	Initial Current Count	
	-----			
	LOS,Line	06/01/94	13 31 27 ok ALARM 195	
	LOS,DTE	06/16/94	02 16 58 ok ALARM 5	
	LOS,SCU	00/00/00	00 00 00 ok ok 0	
	LOF,Line	06/15/94	21 29 53 ok ok ALARM 5	

Command	Description	
\@	Purpose	Allow user comment lines.
	Result	Line after comment command is not parsed.
	Notes	Useful for leaving comments for other users.
	<b>Example</b>	
	Input	\@ Next line written by Bob in Feb. 2007 to correctly parse...
	Objective	Allow other users to quickly understand Bob's additions.
	Command	\@ [user comment]
	Result	(Line not parsed, does not cause a parse error)

## Slot Commands

The following Slot commands place strings in slots. They may be used only in the Extraction phase.

Slots are numbered pigeonholes for temporarily holding strings. Three sets of slots are available:

- **Key slots:** Numbered 1-14 (1-30 if the Auto-Databasing module is installed). Key Slots 1-9 are reserved for action keys, which identify particular alarms. Slots 10-14 are reserved for site keys, which identify a particular site. When keys are generated, slot contents are connected together in **slot number order** to form their respective keys. Empty slots are ignored. Key generation, and subsequent alarm processing, usually occurs automatically when the extraction phase is complete, but could also be triggered as a result of ASCII Table operations or within a loop (see ASCII Tables, section M6-34, and Loops, page M6-26). See section M6-44 (Alarm Processing) and the ASCII Tutorial (Appendix A) for information on how keys are used to create actual alarms.
- **Pager slots:** Numbered 1-9. When keys are generated, pager slot contents are connected together with spaces between them to form an ASC Extract that can be inserted into pager formats. Multiple spaces are reduced to a single space and empty slots are ignored. See Section 8 (Pager and Email Configuration > Alphanumeric Pager Formats) for use in actual paging.
- **Variable slots:** Numbered 1-9, and are provided for general use in ASCII Table processing. Variable slots can be created when a workspaces is needed that doesn't occupy a Key slot.

Variables can be initially created by ASCII rules with “\V” parameters or by tables. For variables to be effective, they must completely be used in an input or output side of a table. One use is to make a second copy of a Key slot in extraction that can be used to make another key. Refer to Appendix A (ASCII Tutorial) for examples.

**Example:** if after extraction key slot 3 contains OVERTEMP, key slot 5 contains a colon, key slot 8 contains the digit ‘5’, key slot 12 contains ‘TRONA’, pager slot 2 contains TR, and pager slot 5 contain OVRTMP, the following would be automatically generated:

Action Key=OVERTEMP:5                      Site Key=TRONA                      ASC Extract=TR OVRTMP

Most slot commands can be used with Key, Pager, and Variable slots, differentiated by the use of \K, \P, or \V in the command. All three forms are shown on the following pages.

**Note:** Although Key data can only be extracted by scanning the ASCII text from left to right and from top to bottom, you can place that Key data in any order you want. It is therefore possible to have data from latter in the ASCII message used in an earlier part of the key.

**Table M6.H - Language Reference, Slot Commands — Extraction Phase**

Command	Description	
\Cnum	Purpose	Clear action key slot num 1-9. \C0 clears all action slots (key slots1-9).
	Result	Affected action key slots are emptied. No effect on pointer..
	Notes	Action key slots are automatically cleared when the extraction phase begins. This command is necessary only when multiple keys are being generated, such as in a loop..
	<b>Example</b>	
	Input	\C7
	Result	Clears action key slot 7.
\Knum \Pnum \Vnum	Purpose	Place the field at the current pointer in slot number num. Field may be delimited by either hard or soft separators.
	Result	Text starting at the current pointer location and continuing to the first separator encountered to the right of the pointer is placed in the affected slot. No effect on pointer.
	<b>Example</b> (assumes spaces have been defined as soft field separators)	
	Input	** 342 REPT ALM,MAJOR,ENVIRONMENTAL
	Objective	Put the field in this location in key slot 12
	Command	\K12
	Result	** 342 REPT ALM,MAJOR,ENVIRONMENTAL Key slot 12 now contains 342

**Table M6.H - Language Reference, Slot Commands — Extraction Phase only (continued)**

Command	Description	
\Knum(pos,qty) \ Pnum(pos,qty) \ Vnum(pos,qty)	Purpose	Place the field starting at absolute column position pos and continuing for qty characters in slot number num. Field may be delimited by hard or soft separators).
	Result	Text is placed in the affected slot, starting at the specified position and continuing for qty characters, or until encountering a soft separator, hard separator, or line terminator (whichever comes first). No effect on pointer.
	<b>Example</b>	
	Input	LOS, <u>D</u> TE 06/16/94 02:16:58 ok ALARM 5, CRITICAL
	Columns*	0 0 1 1 2 2 3 3 4 4 1 5 0 5 0 5 0 5 0 5
	Objective	Put 3 characters starting at column 30 in key slot 9
	Command	\K9(30,3)
	Result	LOS,DTE 06/16/94 02 16 58 ok <u>A</u> LARM 5, CRITICAL Key slot 9 now contains ALA.
\KAnum \PAnum \VAnum	Purpose	Place all characters from the current pointer up to the line terminator in slot number num.
	Result	Text starting at the current pointer location and continuing to the line terminator is placed in the affected slot. Trailing soft separators are removed. No effect on pointer.
	<b>Example</b> (assumes spaces and <0D> are soft field separators, <0A> is EOL)	
	Input	** 342 REPT ALM, <u>M</u> AJOR, ENVIRONMENTAL <0D><0A>
	Objective	Put everything following the pointer in key slot 12
	Command	\KA12
	Result	** 342 REPT ALM, <u>M</u> AJOR, ENVIRONMENTAL Key slot 12 now contains MAJOR, ENVIRONMENTAL
\KAnum(pos,qty) \ \PAnum(pos,qty) \ \VAnum(pos,qty)	Purpose	Place all characters starting at absolute column position pos and continuing for qty characters in slot number num. Field may be delimited by line terminator only.
	Result	Text is placed in the affected slot, starting at the specified position and continuing for qty characters or encountering the line terminator character (whichever comes first). Trailing soft separators are removed. No effect on pointer.
	<b>Example</b> (assumes spaces are soft separators, <0A> is line terminator)	
	Input	LOS, <u>D</u> TE 06/16/94 02:16:58 ok ALARM 5, CRITICAL
	Columns*	0 0 1 1 2 2 3 3 4 4 1 5 0 5 0 5 0 5 0 5
	Objective	Put up to 20 characters starting at column 30 in key slot 9
	Command	\KA9(30,20)
	Result	LOS,DTE 06/16/94 02 16 58 ok <u>A</u> LARM 5, CRITICAL <0A> Key slot 9 now contains ALARM 5, CRITICAL

\***Note:** column number reads top to bottom — column 25 appears as:

2  
5

**Table M6.H - Language Reference, Slot Commands — Extraction Phase only (continued)**

Command	Description										
\KCnum \PCnum \VCnum	Purpose	Place the current pointer column position in slot number num.									
	Result	The current pointer location, expressed as a 3-digit number with leading zeros, is placed in slot number num. No effect on pointer.									
	Example										
	Input	LOS, <u>D</u> TE 06/16/94 02:16:58 ok ALARM 5, CRITICAL									
	Columns*	0	0	1	1	2	2	3	3	4	4
		1	5	0	5	0	5	0	5	0	5
	+ column display										
	Objective	Put current pointer location in key slot 8									
Command	\KC8										
Result	LOS, <u>D</u> TE 06/16/94 02 16 58 ok ALARM 5, CRITICAL. <b>Note:</b> Key slots now contains 005.										
\KGnum(qty) \PGnum(qty) \VGnum(qty)	Purpose	Grab the next qty characters and place in slot number num.									
	Result	Text is placed in the affected slot, starting at the current pointer position and continuing for qty characters. The value of the characters is not taken into consideration, so soft or hard separators or the line terminator are grabbed just like any other characters. No effect on pointer.									
	Example										
	Input	LOS,DTE 06/16/94 02:16:58 ALARM 5, CRITICAL									
	Columns*	0	0	1	1	2	2	3	3	4	
		1	5	0	5	0	5	0	5	0	
	Objective	Put 10 characters starting at column 1 in key slot 9									
	Command	\KG9(10)									
Result	<u>L</u> OS,DTE 06/16/94 02:16:58 ok ALARM 5, CRITICAL. <b>Note:</b> Key slot 9 now contains LOS, DTE 06										
\KHnum \PHnum \VHnum	Purpose	Place the hard field at the current pointer in slot number num. Field may be delimited by hard separator only.									
	Result	Text starting at the current pointer location and continuing to the first hard separator encountered to the right of the pointer is placed in the affected slot. Trailing soft separators are removed. No effect on pointer.									
	Example (assumes spaces are soft field separators, commas hard)										
	Input	** <u>3</u> 42 REPT ALM, MAJOR, ENVIRONMENTAL									
	Columns	Put the field in this location in key slot 12									
	Objective	Put characters up to first hard separator in key slot 12									
	Command	\KH12									
	Result	** <u>3</u> 42 REPT ALM,MAJOR,ENVIRONMENTAL. <b>Note:</b> Key slot 12 now contains 342 REPT ALM.									

\***Note:** column number reads top to bottom — column 25 appears as:

2  
5

**Table M6.H - Language Reference, Slot Commands — Extraction Phase only (continued)**

Command	Description									
\KHnum(pos,qty) \PHnum(pos,qty) \VHnum(pos,qty)	Purpose	Place the field starting at absolute column position pos and continuing for qty characters in slot number num. Field may be delimited by hard separators only.								
	Result	Text starting at the specified position and continuing for qty characters, or until encountering a hard separator or line terminator (whichever comes first), is placed in the affected slot. Trailing soft delimiters are removed. No effect on pointer.								
	Example (assumes commas are defined as hard separators)									
	Input	LOS,DTE 06/16/94 02:16:58 ALARM 5, CRITICAL								
	Columns*	0	0	1	1	2	2	3	3	4
		1	5	0	5	0	5	0	5	0
	Objective	Put 10 characters starting at column 27 in key slot 9								
	Command	\KH9(27,10)								
Result	LOS,DTE 06/16/94 02:16:58 ok <b>A</b> LARM 5, CRITICAL Key slot 9 now contains ALARM 5 (terminated when comma found)									
\KLnumlit \PLnumlit \VLnumlit)	Purpose	Place literal lit in slot number num.								
	Result	lit is placed in slot number num. No effect on pointer.								
	Notes	Spaces may appear in literal if ASCII Parameters permit it. Multiple \KL commands may place literals in slots in any order, but it is easier to read command lines if they are put in ascending order. A literal such as a colon is often placed between numeric fields in a key to show where one ends and the next begins.								
	Example									
	Objective	Put NOPAGE in key slot 3 and a colon in key slot 7								
	Command	\KL3NOPAGE\KL7:								
	Result	Key slot 3 now contains NOPAGE and slot 7 now contains a colon (:)								
\KPnum \PPnum \VPnum	Purpose	Place the port number in slot number num.								
	Result	The port that the incoming message was received on, expressed as a 3-digit number with leading zeros, is placed in slot number num. No effect on pointer.								
	Example									
	Input	Any message received on port 5								
	Command	\KP3								
	Result	Key slot 3 now contains 005								

\***Note:** column number reads top to bottom — column 25 appears as: 2  
5



**Table M6.H - Language Reference — Extraction Phase only (continued)**

Command	Description	
\KTnum(type) \PTnum(type) \VTnum(type)	Purpose	Place the field starting at the current pointer position, and continuing as long as the characters are of the specified type, in slot number num.
	Types	A Alphabetic (A-Z) D Digits (0-9) # Digits, decimal point, minus, plus H Hex digits (0-9, A-F) ! Printable characters (ASCII codes 32-127) * Alphanumeric (Alphabetic A-Z and digits 0-9)
	Result	Text starting at the specified position and continuing for qty characters, or until encountering a hard separator or line terminator (whichever comes first), is placed in the affected slot. Trailing soft delimiters are removed. No effect on pointer.
	<b>Example</b>	
	Input	** 342 REPT ALM,MAJOR,ENVIRONMENTAL
	Objective	Put the entire number starting at the pointer in key slot 4, regardless of the number of digits.
	Command	\KT4(#)
	Result	** 342 REPT ALM,MAJOR,ENVIRONMENTAL. Key slot 4 now contains 342
\Lnumlit	Purpose	Place literal lit in Key slot number num, where num is 1-9.
	Result	lit is placed in Key slot number num. No effect on pointer.
	Notes	Works same as \KLnumlit, except num is limited to slots 1-9 and spaces may <b>not</b> appear in literal even if ASCII Parameters permit it. This command has been retained primarily for backwards compatibility. \KLnumlit is more flexible and should generally be used instead.
	<b>Example</b>	
	Objective	Put NOPAGE in key slot 3 and a colon in key slot 7
	Command	\L3NOPAGE\L7:
	Result	Key slot 3 now contains NOPAGE and slot 7 now contains a colon (:)
\KDlit	Purpose	Force the incoming ASCII dial-up device to use the site name and the rule set associated with it contained in the lit.
	Result	The ASCII processor will use the device type that has been assigned to that physical device for determining the next rule set to use.
	<b>Example</b>	
	Objective	Use rule set for the site name FRESNO
	Command	\KDFRESNO — see Figure M6.18
	Result	The site name FRESNO will be used for determining the next rule set to be used

## ASCII Block Copy

The following commands allow the user to copy a block of text into a key slot and can be used in the extraction phase only. The mark block command (“\B”) marks the current cursor position. The user can then move the cursor forwards or backwards and call the “\KBnum” command, which will copy the block of text in between the block marker and the cursor into key slot “num”. The \B command and the \KBnum commands must always be used together and the \KBnum command must always follow the \B command. The \KBnum command has the same result whether the block marker is before or after the cursor.

**Table M6.H - Language Reference — Extraction Phase only (continued)**

Command	Description	
\B	Purpose	Marks the current cursor position as the start or the end of the block to copy (sets the block marker).
	Result	The current cursor position is saved.
	Notes	Must be followed by the \KBnum command.
	Example	\B\F3\KB5
\KBnum	Purpose	Copies the block of text between the block marker and the current cursor position into key slot “num”.
	Result	Text block is copied into key slot “num”.
	Notes	Must be preceded by the \B command
	Example	\B\F3\KB5

## Loop Commands

The following Loop commands are used when several different alarms may be reported in a single input message, with each alarm contained in some kind of repeating pattern. The loop permits the same extraction commands to be used over and over again with each repetition of the pattern. The number of repetitions may vary from message to message, ending only when the pattern is no longer detected.

### While Loops

While Loops are used when the repeating pattern consists of one or more entire lines. There is usually one line per alarm, but the processor can handle cases where there are two lines per alarm, three lines per alarm, etc, as long as the number of lines per alarm is the same. A While Loop always contains the following commands, in the order given:

**Table M6.H - Language Reference, While Loops — Extraction Phase Only (continued)**

Command	Description	
\Wcond	Purpose	Start of <b>While</b> loop, evaluates cond and determines if loop should continue. cond can be any set of pattern recognition commands with a pass-fail result.
	Result	If cond passes, processing continues with the Do part of the loop. If it fails, the entire rule terminates.
	Notes	As cond is evaluated, the pointer is advanced through the input message in the normal manner.
\D	Purpose	Do the extraction part of the loop. Marks where cond ends and extraction processing begins. Is followed by any number of extraction commands (possibly on several lines, if the repeating pattern in the input covers several lines).
	Result	When \D is executed, the pointer is reset to the beginning of the input line. Commands following \D are then executed in the usual manner and have the usual effect on the pointer. This includes skipping to the next input line if you skip to the next command line.
	Notes	<b>\W and \D must be on the same command line. Use \Cnum to clear appropriate slots at the beginning of the Do.</b>
\E	Purpose	<b>End</b> the loop. Marks where Do ends.
	Result	Generates a new Action Key, pager Asc Extract, and resultant alarms. Resets the pointer to the beginning of the next line of input, and restarts command execution on the \W at the beginning of the loop.
	<b>Example</b>	
	Input	FRESNO 12/05/00 11:18 POINT 2 FAIL POINT 5 FAIL POINT 4 NORMAL END REPORT
	Objective	Build a key and generate resultant alarm state for each POINT in msg.
	Command	\K1\KL2: \W\MPPOINT\D\C3\C4\F1\K3\F1\K4\E
	Result	Put FRESNO followed by a colon in slot 1. Then, on each line where POINT is found: start at the beginning of the line, clear slots 3 and 4, skip a field, put current field in slot 3, skip another field, put it in slot 4, and generate keys and resultant alarms. Resultant keys are: FRESNO:2FAIL FRESNO:5FAIL FRESNO:4NORMAL

## Repeat Loops

Repeat Loops are similar to While loops, and are used when the repeating pattern consists of one or more entire lines. There is usually one line per alarm, but the processor can handle cases where there are two lines per alarm, three lines per alarm, etc, as long as the number of lines per alarm is the same. The difference between a While Loop and a Repeat Loop is

- A While Loop checks a condition *before* starting into the loop, and terminates if the condition fails. A Repeat Loop checks a condition *after* completing the loop, and terminates if the condition passes.
- Both types of loop check their respective conditions on their current lines. In the case of multi-line loops, a While loop checks the *first* line of a pattern, a Repeat loop checks the *last*.

A Repeat Loop always contains the following commands, in the order given.

**Table M6.H - Language Reference, Repeat Loops — Extraction Phase Only (continue)**

Command	Description	
\R	Purpose	Start of <b>Repeat</b> loop, is followed immediately by any extraction commands that are processed in the loop (possibly on several lines, if the repeating pattern in the input covers several lines).
	Result	All commands within the loop are executed at least once.
	Notes	The pointer is advanced through the input message in the normal manner starting at its position when \R is executed. <b>Use \Cnum to clear appropriate slots at the beginning of the loop.</b>
\Ucond	Purpose	Marks end of loop. Loop repeats Until cond passes. Pointer is reset to start of current line before evaluating cond. cond can be any set of pattern recognition commands with a pass-fail result.
	Result	If cond fails, looping process is not over. Generates a new Action Key, pager ACS Extract, and resultant alarms. Resets the pointer to the beginning of the next line of input, and restarts command execution on the \R at the beginning of the loop. If cond passes, the entire rule terminates.
	<b>Example</b>	
	Input	FRESNO 12/05/00 11:18 POINT 2 FAIL POINT 5 FAIL POINT 4 NORMAL END REPORT
	Objective	Build a key and generate resultant alarm state for each POINT in msg.
	Command	\K1\KL2:\R\C3\C4\F1\K3\F1\K4\U\~MPOINT
	Result	Put FRESNO followed by a colon in slot 1. Then, on each succeeding line: start at the beginning of the line, clear slots 3 and 4, skip a field, put current field in slot 3, skip another field, put it in slot 4. Then reset to beginning of line and search for POINT. If POINT is not found, terminate the loop; otherwise, generate keys and resultant alarms, skip to the next input line, and restart commands at \R. Resultant keys are: FRESNO:2FAIL FRESNO:5FAIL FRESNO:4NORMAL

## While Line Loops

While Line Loops are similar to While loops, but are used when the repeating pattern recurs *within* a single line. Multiple alarms can consequently be generated from a single line of text.

A While Line Loop always contains the following commands, in the order given.

**Table M6.H - Language Reference, While Line Loops — Extraction Phase Only (continued)**

Command	Description	
\WL	Purpose	Start of <b>While Line</b> loop, is followed immediately by any extraction commands that are processed in the loop (must all be on one line).
	Result	Extraction commands are processed normally. If any Match commands fail within the loop, execution jumps to the command following \EL. However, it is not necessary to have an explicit test to terminate the loop, since it will end automatically upon reaching the end of the input line.
	Notes	The pointer is advanced through the input message in the normal manner starting at its position when \WL is executed. <b>Use \Cnum to clear appropriate slots at the beginning of the loop.</b>
\*	Purpose	Generate key from current slot contents.
	Result	An Action Key and pager ASC Extract, and any resultant alarm state, are generated using whatever the current slot contents may be.
\EL	Purpose	Mark the End of the Line Loop.
	Result	If the end of the input line has not been reached, and there have been no fails within the loop itself, execution jumps back to \WL. Otherwise, execution continues with any commands following \WL.
	<b>Example</b> (assumes commas are defined as hard separators)	
	Input	OVERTEMP,SMOKE,FIRE,HALON
	Objective	Create an alarm for each of the listed conditions
	Command	\WL\K1*\F1\EL\C0
	Result	\K1 puts the current field in slot 1, and \* command forces a key and resultant alarm to be generated from it, on each iteration of the \WL loop. The \F1 command makes the loop step through the input line field by field.
	Notes	C0 clears all slots and suppresses the normal generation of a key that would occur upon reaching the end of a rule. Otherwise HALON alarms would be generated twice.

**Table M6.H - Language Reference, Directives — Extraction Phase Only (continued)**

The following Directives are special-purpose commands to the ASCII processor itself.

Command	Description	
\Xlit	Purpose	Execute an ASCII table named lit (see ASCII Table section, pg M6-34)
	Result	Slot contents are modified in accordance with table instructions.
	<b>Example</b>	
	Objective	Use ASCII table MYTBL to modify slot contents.
	Command	\XMYTBL
	Result	MYTBL is executed, operating upon whatever was contained in the slots at the moment it was called.
\%	Purpose	Skip automatic key generation
	Result	An Action Key and pager ASC Extract, and any resultant alarm state, are normally generated automatically when the extraction phase is complete or upon completion of a pass through a While Do or Repeat-Until loop. The \% command suppresses this.
	Notes	In addition to the normal generation process, Action Keys, pager Extracts, and resultant alarms may be generated when executing ASCII Tables or within While-Line loops. Use the \% command if you are doing this and want to suppress normal generation.
	<b>Example</b>	
	Objective	Use table MYTBL to generate action keys, skip normal generation.
	Command	\XMYTBL\%
	Result	Action keys (and corresponding alarms) are generated only by the table. If the \% were not present, an additional alarm would be generated based upon slot contents at the end of extraction.
\!DEFAULT_KEY>lit	Purpose	Assign an action key lit to be used if no other action key is found. <b>Not</b> used with Auto Databasing ASCII.
	Result	If, in the Alarm Processing phase, no alarm action string is found to match any action key generated under this rule, alarm processing is repeated using the default key lit.
	Notes	This directive can appear anywhere in an extraction command line. To have any effect, lit must be assigned as the action string for a corresponding default alarm (see Alarm Processing, section M6-42).
	<b>Example</b>	\!DEFAULT_KEY>UNKNOWN_ALARM
\!FWD>num	Purpose	Forwards logged text to port num.
	Result	Text captured by this numbered rule gets sent out port num.
	Notes	num port usage must be ASCII Interrogator or Craft.
	<b>Example</b>	\!FWD>7

**Table M6.H - Language Reference, Directives — Extraction Phase Only (continued)**

Command	Description	
\!BEGIN_LOG>adr	Purpose	Initializes a refresh for alarms that don't send a clear message, but can tell when cleared by observing that they are no longer present on a list of active alarms. Affects alarms at addresses adr, where adr is one or more numbers 0-999 separated by commas or hyphens (e.g. 1,2,4-7,12).
	Notes	The source device must be able to generate a summary of current alarms. Put the BEGIN_LOG command in the extraction part of a rule that recognizes that such a summary is starting.
	<b>Example</b>	
	Input	The following is the heading on a list of active alarms: ID SEV DESCRIPTION
	Objective	Start a refresh of active alarms
	Command	\MID\MSEV\MDESCRIPTION {in pattern match section} \!BEGIN_LOG>1-999 {in extraction section}
	Result	System begins the refresh process.
\!END_LOG>adr	Purpose	Completes a refresh process started with \!BEGIN_LOG. Must specify same adr as the corresponding BEGIN_LOG.
	Result	Any alarms that were being carried as active at BEGIN_LOG, but are not on the summary list generated by the device, are cleared. Any new alarms are set.
	Notes	Put the \!END_LOG command in the extraction part of a rule that recognizes the end of summarized current alarms.
	<b>Example</b>	
	Input	The following is received at the end of the active alarm list SUMMARY COMPLETE
	Objective	Complete the refresh of alarms at this address
	Command	\MSUMMARY\MCOMPLETE {in pattern match section} \!END_LOG>1-999 {in extraction section}
	Result	Currently active alarms are set (if they're not already), all other alarms at these addresses are cleared.
\!LOG	Purpose	Log the key and text associated with this rule to the exception file regardless of whether an exception occurs (see section M6-38, M6-54).
	Notes	This directive can appear anywhere in an extraction command line.
\!NOLOG	Purpose	Don't log exception information for this rule, even if exception logging has been turned on (see section M6-38).
	Notes	This directive can appear anywhere in an extraction command line.
\!SCRIPT>lit	Purpose	Executes the script named lit.
	Results	The script by this name runs (see ASCII Scripts, section M6-37).
	<b>Example</b>	\!DEFAULT_KEY>UNKNOWN_ALARM



**Table M6.I - Language Quick Reference**

<b>Match commands. Pass-Fail. Can be used in Pattern Recognition and Extraction phases.</b>	
\Mlit	Match literal. Searches for the specified literal.
\M~AL	Match Any Line.
\M~BL	Match Blank Line.
\~Mlit	Negative Match Literal. Tests for the absence of a literal.
\#M	Match Any digit.
\M~T(pos,qty,type)	Match Type. Looks for a string of consecutive characters all of the same type.
\M~L(pos,lit)	Match literal at position.
\M~Hhh	Match Hex byte (control character)
<b>Positioning commands. Can be used in Pattern Recognition and Extraction phases.</b>	
\Apos	Absolute Position. Sets pointer to column pos.
\Snum	Skip characters.
\Fnum	Skip num fields delimited by hard or soft separators.
\FHnum	Skip num fields delimited by hard separators only.
\Tnum	Throw away num input lines.
\@	User comment (will not be parsed)
<b>Slot commands. Extraction phase only. Work with Key, Pager, and Variable slots.</b>	
\Cnum	Clear action key slot num 1-9. \C0 clears all action slots (key slots 1-9).
\Knum \Pnum \Vnum	Place the field at the current pointer in slot number num. Field may be delimited by either hard or soft separators.
\Knum(pos,qty)\Pnum(pos,qty) \Vnum(pos,qty)	Place the field starting at absolute column position pos and continuing for qty characters in slot number num. Field may be delimited by hard or soft separators.
\KANum \PANum \VANum	Place all characters from the current pointer up to the line terminator in slot number num.
\KANum(pos,qty) \ PANum(pos,qty) \ VANum(pos,qty)	Place all characters starting at absolute column position pos and continuing for qty characters in slot number num. Field may be delimited by line terminator only.
\KCnum \PCnum \VCnum	Place the current pointer column position in slot number num.
\KGnum(qty) \PGnum(qty) \ VGnum(qty)	Grab the next qty characters and place in slot number num.
\KHnum \PHnum \VHnum	Place the hard field at the current pointer in slot number num. Field may be delimited by hard separator only.
\KHnum(pos,qty) \ PHnum(pos,qty) \ VHnum(pos,qty)	Place the field starting at absolute column position pos and continuing for qty characters in slot number num. Field may be delimited by hard separators only.
\KLnumlit \PLnumlit \VLnumlit	Place literal lit in slot number num.
\KPnum \PPnum \VPnum	Place the port number in slot number num.
\KTnum(type) \PTnum(type) \ VTnum(type)	Place the field starting at the current pointer position, and continuing as long as the characters are of the specified type, in slot number num.
\Knumlit \Pnumlit \Vnumlit	Place literal lit in slot number num, where num is 1-9.



**Table M6.I - Language Quick Reference (continued)**

<b>Slot commands. Extraction phase only. Work with Key, Pager, and Variable slots. (continued)</b>	
<code>\B</code>	Save current pointer position. NOTE: Must be followed by <code>\KNum</code>
<code>\KNum</code>	Place all the characters between saved pointer position and current pointer position in slot number "num". NOTE: Must be preceded by <code>\B</code>
<b>Loop Commands. Extraction Phase only.</b>	
<code>\Wcond</code>	Start While loop, check if cond is satisfied.
<code>\D</code>	Do the extraction part of a while loop.
<code>\E</code>	End a While loop. Marks where Do ends, generates keys.
<code>\R</code>	Start Repeat-Until loop.
<code>\Ucond</code>	End Repeat-Until loop. Check cond, generate keys and repeat if cond fails.
<code>\WL</code>	Start of While Line loop.
<code>\*</code>	Generate key from current slot contents in While Line loop.
<code>\EL</code>	Mark the End of the While Line Loop.
<b>Directives. Extraction Phase only.</b>	
<code>\Xlit</code>	Execute ASCII table named lit
<code>\\$</code>	Skip automatic key generation.
<code>\!DEFAULT_KEY&gt;lit</code>	Assign an action key lit to be used if no other action key is found.
<code>\!DEFAULT_SITE&gt;lit</code>	Assign a site key lit to be used if no other site key is found.
<code>\!FWD&gt;num</code>	Forwards captured text out another port called in.
<code>!!!SET_DEVICE!!</code>	Dial-up ASCII only (a separate module)
<code>\!BEGIN_LOG&gt;adr</code>	Initializes a refresh for alarms that don't send a clear message.
<code>\!END_LOG&gt;adr</code>	Completes a refresh process started with <code>\!BEGIN_LOG</code> .
<code>\!LOG</code>	Log the key and text associated with this rule to the exception file.
<code>\!NOLOG</code>	Don't log exception information for this rule.
<code>\!SCRIPT&gt;lit</code>	Execute script named lit
<code>\KDlit</code>	(Incoming Call Device Type Identification only) Force the incoming ASCII Dial-up device to use the site name, and the rule set associated with it, contained in the LIT This is an alternative to using <code>!!!SET_DEVICE!!!</code> — see section M6-47 (Incoming Call Device Type Identification).

## Detailed Logging

The logging screen shown in Figure M6.7 will only be available to you if you've selected Detailed option in the Logging field of the ASCII Rules Definition screen (see Fig. M6.3). To reach this screen select Files from the Master Menu, then select ASCII Devices, then select ASCII Rules. Then select function key F1=Logging Match.

When the ASCII processor declares an alarm, it captures a portion of the original text string and attaches it to the alarm point. This permits the operator to see the ASCII that triggered the alarm.

**If the message triggered a rule that was set to standard logging then the lines captured will be from the first line matched to the last line that was accessed by either the pattern recognition or Action Extraction sections.** Sometimes it is desirable to capture more information about the alarm that might go into greater detail regarding the cause of an alarm. Should that be the case, Detailed logging could be used which will capture alarm data until the criteria you specified has been reached.

See Table M6.J for field and function key descriptions for the ASCII Logging Options screen.

Special Error log files to stop excessive captures.

**WARNING: Improper logging could "eat-up" lines from subsequent alarm messages. (The system will log all data until the log match is detected, including valid messages.)**

ASCII Tables

Table Name : DACSET      Entry # : 1

Descr : SET KEY INTO CLEAR

Condition #1

Key: K9    Type: STRING    OP: =    VALUE: :SET

AND Condition #2

Key:    Type:    OP:    :

TRUE Action

Key: K9    New Value: :CLR    Gen Key: N

FALSE Action

Key:    New Value:    Gen Key:

F)ind, E)dit, D)elite, N)ext, P)rev, M)ove, R)ead, Q)uit :

F10/Esc=Exit

Fig. M6.7 - The ASCII logging options screen

**Table M6.J - Field names and descriptions for the ASCII Logging Options screen.**

Field	Description
Logging Pattern Match	A set of up to six line of "Pattern Recognition commands" such as \Mlit, that will continue logging until the logging commands match. In most cases, only a single line of commands is required to achieve the proper results. For Example: \M~BL Would match till a blank line was found. \M*** Would match until 3 asterisks were found on a line.

**Table M6.K - Key commands available in the ASCII Logging Options screen**

Function Key	Description
F1	Insert. Inserts a line at the current position.
F2	Delete. Deletes a line at the current position.
F8	Save. Saves the current editing.
F10/Esc	Exit.

**Note:** The Logging function does not work on alarms that are No Log.

## ASCII Tables

ASCII Tables provide a way to modify slot contents, and consequently keys and alarms, based upon ‘ifs’ – *if* such-and-such a condition is true, then change slot so-and-so to a new value and use that for subsequent processing. For example, a remote device may report the number of times in the last hour that it has had to reject transactions because it was busy. *If* that number is less than 5 you don’t want to know about it, *if* between 5 and 10 you want a minor alarm, and *if* more than 10 you want a major. You can use ASCII Tables to evaluate these *ifs* and create a separate key, and consequently a separate alarm, for each condition.

An ASCII table has a name and one or more numbered entries – the screen above represents a single such entry. It essentially says:

**If** Condition 1 is true **AND** Condition 2 is true  
**then** do the ‘TRUE’ action  
**otherwise** do the ‘FALSE’ action

- Each Condition compares the contents of a slot with some predefined value.
- Each Action puts something in a slot, thereby modifying any keys build from the slot.
- It is not necessary to completely fill out all lines in an entry.
- If there is no Condition 2, TRUE and FALSE is based entirely on Condition 1.
- Either the TRUE or the FALSE action may be omitted if there is nothing special to do.
- There may be multiple numbered entries, all of which are processed in numeric order. Higher-numbered entries may modify data created in lower-numbered entries.
- A table is executed, by name, from an \X command in the extraction phase of a rule.

**For examples of how ASCII tables are used—see Appendix A - ASCII Tutorial.**

ASCII Tables			
Table Name	: SCU	Entry #	: 2
Descr	: SCU MINOR		
Condition #1			
Key: V1	Type: NUMERIC	OP: >	VALUE: 0
AND Condition #2			
Key: V1	Type: NUMERIC	OP: <=	VALUE: 10
TRUE Action			
Key: K5	New Value: MIN	Gen Key: N	
FALSE Action			
Key:	New Value:	Gen Key:	
F)ind, E)dit, D)elite, N)ext, P)rev, M)ove, R)ead, Q)uit :			
F10/Esc=Exit			

Fig. M6.8 - The ASCII Tables screen.

This screen is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Tables.

**Table M6.L - ASCII Tables**

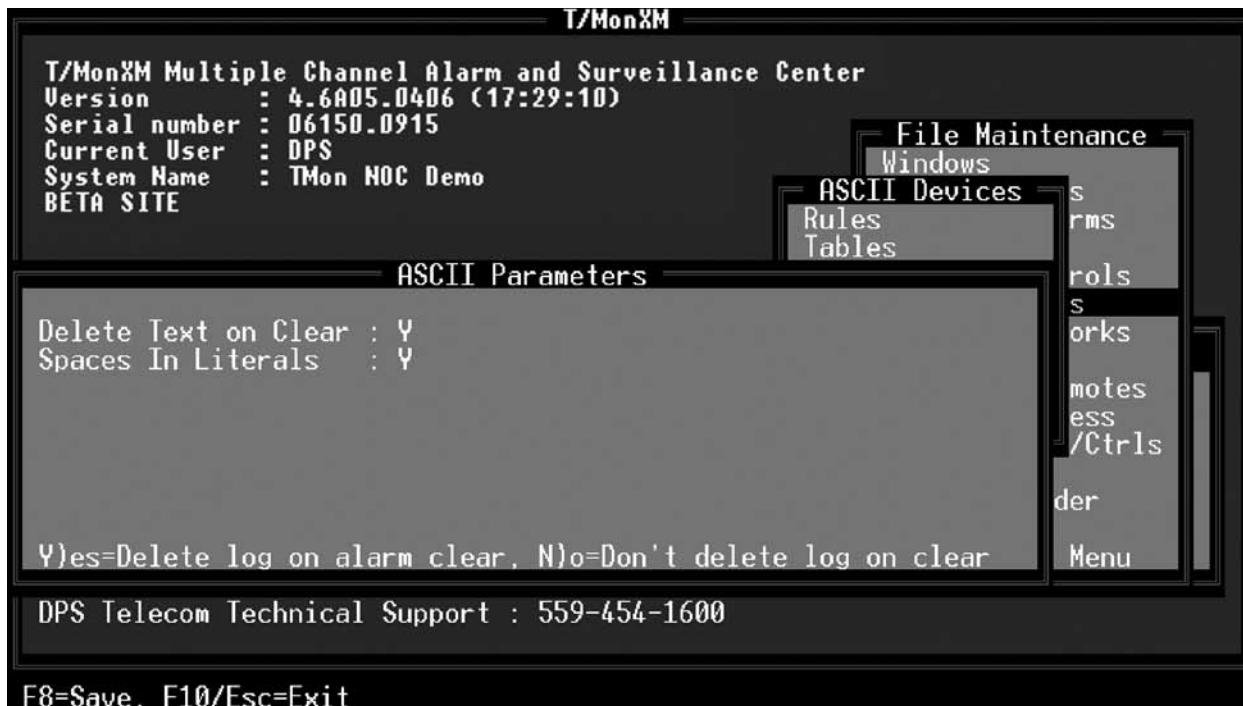
Function Key	Description
<b>Header Section</b>	
Table Name	Name that will be used in the \X command that executes this table. Up to six characters. Example: MYTABL (Trailing spaces will be truncated)
Entry #	Sequence number for this entry. All entries are processed, in numeric order, every time the table is called.
Descr	An informational description of this entry.
<b>Condition Section</b>	
Key	The slot whose contents is being evaluated, can be: • Knum for a Key slot, where num is 1-14 (1-30 if Auto Databasing installed) • Vnum for a Variable slot, where num is 1-9 Example: K8
Type	Numeric or String (alphabetic). Makes a difference if comparing numbers, because numerically 54 is less than 129 but alphabetically 129 is less than 54.
OP	The comparison operation to be carried out between Key and Value. Can be: = (True if Key equals Value) <> (True if Key does not equal Value) < (True if Key is less than Value) <= (True if Key is less than or equal to Value) > (True if Key is greater than Value) >= (True if Key is greater than or equal to Value)
Value	A number or string that Key is to be compared with.
<b>Action Section</b>	
Key	The slot whose contents are to be modified as a result of the comparison, can be: • Knum for a Key slot, where num is 1-14 (1-30 if Auto Databasing installed) • Vnum for a Variable slot, where num is 1-9 <b>Example:</b> K5 (this could be a slot involved in the comparison, or another slot entirely).
New Value	A number or string that is to be placed in the slot as a result of the comparison
Gen Key	Yes = Generates Action Key or pager Asc Extract keys based on current key values This could lead to an alarm being generated. No = Don't generate a key. <b>Note:</b> In the majority of cases this should be set to No, since the key will auto generate one time after normal extraction. • A table could consist of multiple numbered entries, each of which could generate a key and an alarm of its own. A single execution of the table could consequently generate many alarms, if that is what you want it to do. • This entry has no effect on key and alarm generation after table processing is complete. Unless suppressed, normal key and alarm generation will occur based upon whatever happens to be in the slots at the completion of extraction or at the end of a loop. Use \\$ or clear all action slots with \C0 to suppress.

## ASCII Parameters

This screen defines a few miscellaneous settings used by the ASCII Processor.

**Table M6.M - Field names and descriptions for the ASCII Parameters screen.**

Field	Description
Delete Text on Clear	Controls what happens to text logged with an alarm when the alarm clears. This is the text you see on the ASCII Text Log screen, reached by highlighting an ASCII alarm on the Standing Alarms page in monitor mode and selecting function key F7=Asc. <ul style="list-style-type: none"> <li>If this setting is Yes, the text is deleted from the system. This is the recommended setting because it keeps the log file from filling up with obsolete information that is probably of no interest anyway.</li> <li>If No, the text is retained and may be viewed on subsequent occurrences of the same alarm by going to the ASCII Text Log screen and using F1 and F2 to scroll through any messages that may be there. F3=Ack deletes a message; if all messages are deleted, the alarm itself is cleared.</li> </ul>
Spaces In Literals	Determines if embedded spaces are permitted in literals used with the \KLnumlit, \PLnumlit, and \VLnumlit commands. Does not affect literals used elsewhere - all other commands truncate literals at the first space they find.



**Fig. M6.9 - The ASCII Parameters screen. This screen is reached from the Master menu by selecting Files-ASCII Devices - ASCII Parameters.**

## ASCII Scripts

Scripts are a series of commands that may be sent to an ASCII device. For example, you could write a rule to recognize when a remote device has spontaneously logged you off, and automatically send a script to log you back on when such a message is received.

ASCII Scripts define messages that may be sent from T/Mon to the ASCII device. These messages may include the following symbology to represent special characters and commands:

- <CR> Carriage Return
- <LF> Line Feed
- <^?> Control key plus a letter between A-Z.  
Example: <^C> sends Ctrl-C (hex 03)
- <Dn> Delay n tenths of seconds, where n is 1-999, before sending any more characters
- <D> Delay until a time out occurs before sending any more characters
- <Tn> Substitute Token n where n is 1-5 (see Alarm Processing section, page M6-45)

**Table M6.N - Field names and descriptions for the ASCII scripts screen.**

Field	Description
Descr	Description of this script.
Line 1-10	Commands to be sent. These are normal text strings, and in addition may contain the symbols listed above for special characters and commands.

```
ASCII Scripts

Script Name : LOGON
Descr : Auto log in
Line 1 : <CR><D20>nmcal<CR><D>nmcal!<CR><D>
Line 2 : echo begin log dps <CR><D>
Line 3 : nml -a<CR>
Line 4 : <D><CR>allip;<CR>
Line 5 :
Line 6 :
Line 7 :
Line 8 :
Line 9 :
Line 10:

F)ind, E)dit, D)elite, N)ext, P)rev, Q)uit :

F10/Esc=Exit
```

**Fig. M6.10 - ASCII script page.** This screen is reached from the Master menu by selecting Files-ASCII Devices-ASCII scripts.

## ASCII Sample Message

### Sample Messages May Now Be Saved Directly in T/Mon

To make working with ASCII easier, a sample message may now be saved for each set of matching rules. Although this is a fairly simple concept, it provides several powerful benefits:

1. It's impossible to forget which message format your rules were built for because you always have a sample available for reference.
2. If you make a change to one of your rule sets, you can see if it still parses the sample message correctly.
3. Training new technicians is easier because they have instant access to message examples and rule sets.

```
ASCII Device Rules
ASCII DEVICE : TEST          Rule #      : 20  Sample Msg Not Assigned
Descr       :                               Log Type  : STANDARD
Comment     :                               Special   : NONE
                               Ignore    : N
Pattern Recognition
1 \MAScii
2
3
4
5
6

ASCII Sample Message
1 : 02/21/01 09:04:10 #25623
2 :
3 : ** 04 REPT:CELL 14 ALARM SCANNING
4 : SCAN POINT: 27
5 : ALARM: CELL SITE INTRUSION
6 : STATE: ALARM

Down=PageDown

F2=Select New, AF7=Delete, F8=Save, F10/Esc=Exit
```

You can now assign sample ASCII messages with your rule sets.

Now you'll never struggle to remember which message formats correspond to your rule sets. You'll always have single-keystroke access to a sample message stored right with the rule itself, saving a lot of time and frustration.



### To Create A Sample Message

Sample messages can be assigned to each ASCII rule except rule 0. This message can be viewed or set by pressing F3 on the ASCII Device Rules window.

ASCII sample messages can be used to help create the ASCII rules by having a sample to work with.

```
ASCII Device Rules
ASCII DEVICE : TEST      Rule #      : 20  Sample Msg Not Assigned
Descr  :                               Log Type : STANDARD
Comment:                               Special  : NONE
                               Ignore   : N
      Pattern Recognition
1 \ASCII
2
3
4
5
6
      Action Extraction
1 \F1\K5
2
3
4
5
6
F)ind, E)dit, D)elite, N)ext, P)rev, M)ove, R)ead, Q)uit :
F3=Sample, F4=Debug, F5=Compile, F6=Manage, AF6=Import/Export, F9=Help, F10/Esc=Exit
```

The F3 and F4 keys are used to create sample messages and test ASCII rules.

It can also be used to quickly test ASCII rules by pressing F4 (Debug) on the ASCII Device Rules window. A new F key (F4) will appear on the bottom of the debug window if a sample message was set on the last viewed rule. This will allow users to load the sample ascii message into debug and run through all rules to make sure that the rules are processing the way they should be. This eliminates the need to have to search through ASCII log files for an ASCII text block that will trigger a specific ASCII rule.

### ASCII Hotkeys

From the ASCII Key Map Definition screen (used with Auto-Databasing ASCII), select a string type and press F2 to define expected values for that string.

From the ASCII Device Definition screen, press F4 to reach the ASCII Rules screen. You may alternatively press ALT + F4 to bring up the ASCII Devices menu.

Finally, you may now reach the Auto Definitions menu by pressing F7 from any Device Rules screen. Previously, the F7 hotkey would perform this function on a "Rule" screen only.

The most commonly used hotkeys are listed for reference on the bottom line of almost every screen in T/Mon. You also have the option to press F9 (Help) from almost every T/MonXM screen to view a list of all available hotkeys, as well as additional context-sensitive information. See M6-59 for table.

## ASCII Debug

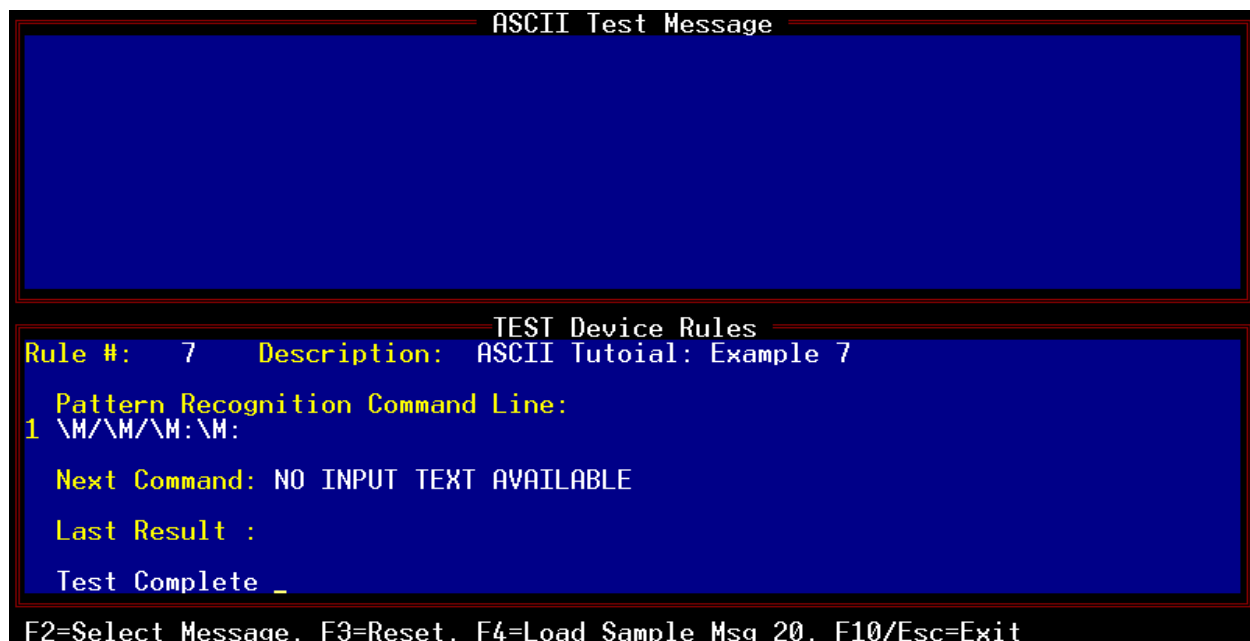
(**Note:** See section M6-65, ASCII Analyzer, for information about real-time analysis. This is invaluable if ASCII rules do not yield the results you think they should.)

ASCII Debug permits ASCII message processing to be visualized, error-checked, and executed without having to receive actual ASCII messages on an input port.

Test Messages: for input, the debugger uses ASCII text that has been saved on disk. There are several ways to obtain such files:

- If text is being received on a dedicated ASCII input port, from the master menu select Parameters - Remote Ports, scroll to that port, and set Log All Activity to Yes. This will save all incoming traffic to a file named ALnnn.REP, where nnn is the port number (three digits with leading zeros).
- If Log Exceptions has been turned on (either through Log Exceptions on the same Remote Port screen or by a \!LOG directive in an ASCII rule) text is saved in a file named AEnnn.REP, where nnn = Port #.
- Text could be captured by an external terminal program or logger.
- You could create simulated input files using a text editor such as DOS Edit, Windows Notepad, or Windows Wordpad (watch out for control characters that often cannot be entered with such editors). Verify this file is saved as A1xxxxx.Rep format.

Files obtained from protocol captures or the monitor-mode ASCII Monitor screen will generally not work because they convert control characters (end-of-line indicators, etc) into a human-readable hex format. The ASCII debugger works with raw hex just as received.



**Fig. M6.11 - ASCII debug page.** This screen is reached from the Master menu by selecting Files ASCII Devices-ASCII Rules, then select function key F4=Debug from any numbered rule page (not available if page is in edit mode).

```

Select Ascii Debug Test Message
=====
EXAMPLE 1: USING SEPARATORS
Separator Demo      ,Commas,,, End Demo
=====
EXAMPLES 2 & 7: A TYPICAL MULTILINE INPUT MESSAGE
  Example of alarm occurring:
02/21/01 09:04:10 #25623
** 04 REPT:CELL 14 ALARM SCANNING
SCAN POINT: 27
ALARM: CELL SITE INTRUSION
STATE: ALARM

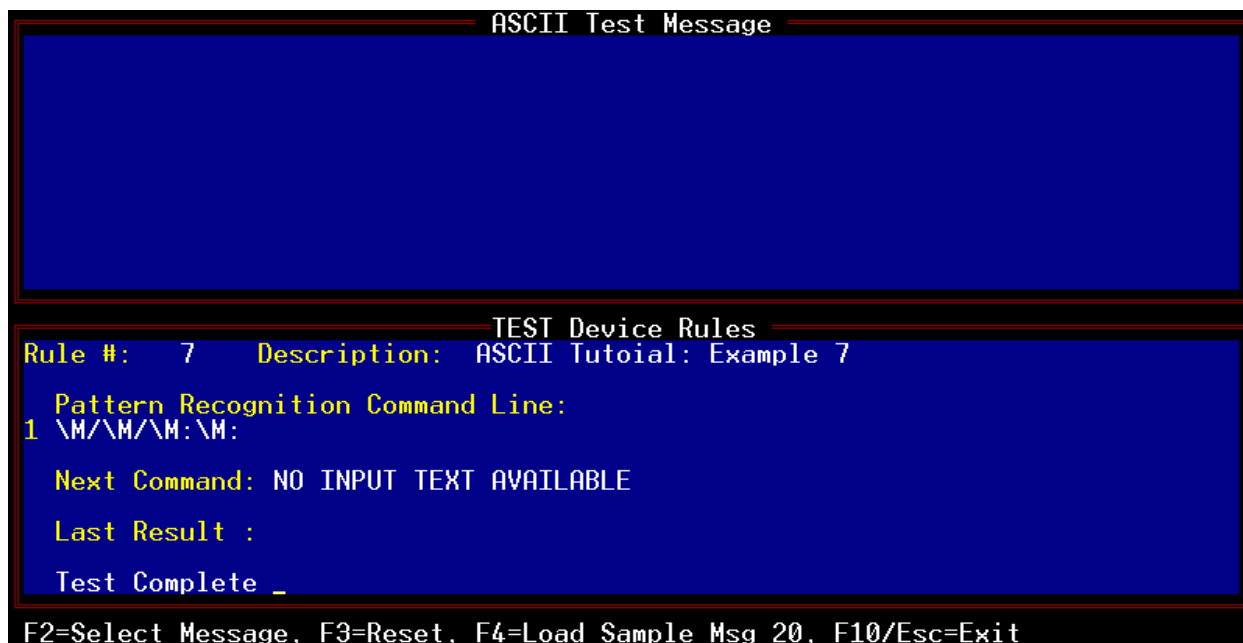
  Example of alarm clearing:
File : ALDEMO.REP      Size: 3172      Date/Time: Jun 26,2000 17:43:08
F2=File F3=Search F4=Select ON/OFF F5=Top Enter=Ok F9=Help F10/Esc=Cancel

```

**Fig. M6.12 - ASCII debug select input message screen.** This screen is reached by selecting F2-Select from the ASCII Debug main screen.

**Table M6.O - Functions available on the ASCII Debug - Select Input Message screen**

Function Key	Description
F2	Selects File. Hit Tab to select from list. Only files named ALxxx.REP are shown, where xxx is up to 6 characters. These will usually be ASCII LogAll files created as outlined on the preceding page. Other file names may be manually entered and used if present.
F3	Search. Type in something to search for and hit Enter. Hit F3-Enter to repeat.
F5	Top. Reset viewer to top of file.
F4	Enable/Disable text selection mode. When text selection mode is enabled, you can mark the text using the up and down arrow keys and then press Enter to accept. The first line marked should correspond with the first pattern recognition command line in the rule being tested. A maximum of 20 lines may be selected.
Enter	Accepts selected text and returns to debug.
F9	Displays help for this screen.
F10/Esc	Abandon text selection, continue using previously selected text.



**Fig. M6.13** - This screen is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, then select function key F4=Debug from any numbered rule page (not available if page is in edit mode). It will always come up on the first numbered rule for this device, regardless of the rule number you were on. Then use F2 to select a test message in accordance with the instructions on the previous page.

The **ASCII Debug** screen contains two panels:

- The **ASCII Test Message** panel shows the ASCII text being operated on by the rules below. Soft Separators are green (these usually include spaces, shown as a green bar or square). Hard Separators are yellow. The Line Terminator character is red. The most informative feature of this display is the **pointer**, which is highlighted in inverse video and is located at the start of the text that will be operated on by the next command.
- The **Device Rules** panel shows the commands being processed. The debugger processes text exactly as a live system would, starting with the first command in the lowest-numbered rule for a particular device, restarting on the next higher-numbered rule if a pattern recognition command fails, and terminating when an entire numbered rule successfully completes. Only one command line at a time is shown, with the **next command** to be executed highlighted in inverse video. Below that is a translation in plain English of what that command is supposed to do, and below that is the result of the command that has just finished executing. Note that state of the entire system is shown as it would be just before the currently highlighted command is executed.

**Table M6.P - Functions available on the main ASCII Debug screen**

Function	Description
Run Test, step by	Execute one or more commands, depending upon the step increment selected:
D)evice	Execute all numbered rules remaining for this device. Halts when a rule successfully completes or when all rules are exhausted, just as the live system would. Also halts and highlights any errors found in a command expression, which the live system generally does not — it just ignores invalid commands.
R)ule	Execute all commands remaining for the current numbered rule. Will pause when a rule successfully completes, or pause and highlight any command that fails before going on to the next rule, or halt if there is an error in a command expression.
L)ine	Execute all commands remaining on the current command line. Will pause after each line, or pause and highlight any command that fails before going on to the next rule, or halt if there is an error in a command expression.
C)ommand	Execute a single command. This is the most common selection, and is executed repeatedly to view the results of each command in turn.
F2	Select Message. Brings up the input message selection screen.
F3	Reset. Restarts the debug processor on the first command in the lowest-numbered rule for this device, and resets the pointer to the first input line.
F4	Loads sample text message from last viewed ASCII rule.
F5 (extraction only)	View Slots. Function is available only in the extraction phase, shows current slot contents (see screen page M6-43).
F7 (auto only)	View Auto Keys. Function is available only if the Auto Databasing module is installed and auto processing has taken place (see screen page M6-44).
F10/Esc	Exit. Returns to the ASCII rule editing screen.

## Debug Slot Contents

There are actually three sets of slots: key slots, pager slots, and variable slots, addressed by \K, \P, and \V commands respectively. These slots are displayed in five groups with empty slots omitted. Slot numbers read down, positioned on the first character in the slot.

- **Action slots:** those addressed by \K commands for slots numbered 1 to 9. When keys are generated, normally at the end of processing but possibly in a loop or table, these slots are connected together to form an action key. This is also the way they are shown in this display, so you are actually viewing the action key as it develops.
- **Site slots:** those addressed by \K commands for slots numbered 10 to 14. The site key is generated by connecting these slots together, so you also see this key as it develops.
- **Other slots:** those addressed by \K commands for slots numbered 15 to 30. They are available only if the Auto Databasing module is installed, are for general-purpose auto processing, and do not directly represent keys. See section M6-68 (Auto Databasing ASCII) for details.
- **Pager slots:** those addressed by \P commands, always for slots numbered 1 to 9. When keys are generated, these slots are connected together with spaces between to form an ASCII Extract that may be included in a pager message. This is also the way they are shown in this display.
- **Variable slots:** those addressed by \V commands, always for slots numbered 1 to 9. They are for general-purpose use, usually with ASCII tables.

```
Slot Contents
Slot numbers read down.  Only occupied slots shown.

Slot 0 00 00
Num: 1 23 45
Action: 14:27:CLR

Slot 1
Num: 0
Site : 14

Slot 1 1 2
Num: 5 8 6
Other : **CELL SITE INTRUSIONEX7

Slot 0 0
Num: 1 8
Pager : 14 CELL SITE INTRUSION

Slot
Num:
Var :

F10/Esc=Exit
```

**Fig. M6.14** - This screen is reached from the main ASCII Debug screen by selecting F5=View Slots. It is available only when processing commands in the Extraction phase (not Pattern Recognition). It shows slot contents as they exist at the current point in ASCII processing.

```

===== Auto-Generated Keys =====
      Keys created directly from slot contents:
SET   : 14:27:SET
CLEAR : 14:27:CLR
SITE  : 14
DESC  : CELL SITE INTRUSION
AUX   :
Keys mapped from slots, then matched with Target Strings to get value:
      Key                                     Value
Status      : CLR                           CLEAR
Level       : **                             B
Log          :
History      :
Qualification:
Counter      :
Text Message : CELL SITE INTRUSION           2
Page Profile : 14**                           2
Cat (Win) 1  : **                             3
              2 : EX7                          27
              3 :
              4 :
              5 :
              6 :

F10/Esc=Exit
```

**Fig. M6.15 - Auto Generated Keys** - This screen is reached from the main ASCII Debug screen by selecting F7=View Auto Keys. It is available only if the Auto Databasing module is installed and auto processing has taken place. It shows keys as they exist at the current point in ASCII auto processing.

---

## Alarm Processing — Overview

Alarm Processing is the ‘second half’ of ASCII processing, in which actual alarms are set or cleared based upon keys generated in the Message Processing phase. Databasing for ASCII alarms is quite similar to databasing for alarms obtained from any other source, and is set up in one of two places depending on how the alarm messages are received.

- **If by dedicated connection, entries are made under Parameters-Remote Ports.** There are three ways to create the alarm database:
  - **Manually:** This is similar to databasing for other alarm-reporting devices: entries are keyed in for each individual alarm under each port, address, and display.
  - **Through templates:** This method works well if several different devices report identical alarm information, differing only in details such as location. For instance, you might have a number of identically-equipped cell sites sending the same alarm messages for particular faults. A template lets you enter alarm information once and share it among sites.
  - **Automatically:** This method is available only if you have purchased the Auto Databasing ASCII module. You do not have to enter alarm information at all; instead, the system derives it from incoming messages. If a particular alarm has not yet been entered in the database it is added automatically. Over time, the database populates itself. This method is not discussed here, but is described in section M6-68 (Auto Databasing ASCII).
- **If by dial-up:** Entries are made under Files-Dial Up Networks-ASCII Sites.
  - **Manual databasing:** The only method available for dial-up devices.



## Properties to be Databased Overview

ASCII device types have to be defined under Message Processing before proceeding with databasing for Alarm Processing, because those generic types are going to be assigned to actual physical devices here. Return to Files-ASCII Devices-ASCII Rules if your device types haven't been set up yet. Then follow the table below:

**Table M6.Q - Alarm Processing References**

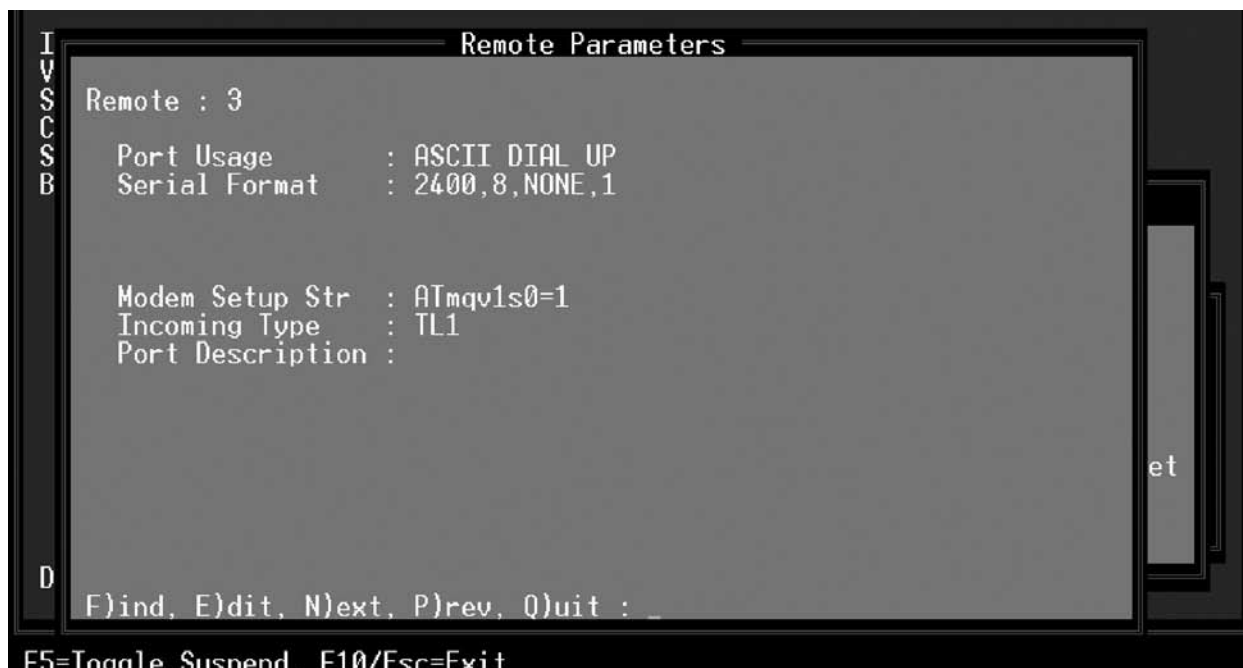
Properties to be databased	T/MonXM Manual Reference
Dialup ASCII Port - Basic Port Definition	page M6-46
Dialup ASCII Sites	
Incoming Call Device Identification	page M6-48
Site Definition	page M6-51
Dialup ASCII Devices	page M6-53
Point definition and ASCII Actions (Manual Entry)	pages M6-59, M6-62
Dedicated ASCII Port - Basic port definition	page M6-55
Remote Device Definition	page M6-57
Point Definition and ASCII Actions, using:	
• Manual entry	page M6-59
• Templates	page M6-64
• Auto Databasing	page M6-69

## Remote Ports, ASCII Dial-Up

The Remote Ports selection allows you to define the parameters for the remote port that you will connect with your ASCII dial-up device.

From the Parameters menu select Remote Ports. Press F and enter the port number. Enter Y to define a new port or E to edit an existing port. Use the tab key to select ASCII dial-up port usage. Use the following tables and subsections to define the port, sites, devices, points and ASCII actions.

Table M6.R lists field definitions for ASCII dial-up devices.



**Fig. M6.16 - The Remote Parameters screen, ASCII dial-up usage.**

**Table M6.R - Fields in the Remote Parameters screen.**

Fields	Description
Port Usage	ASCII DIAL UP
Serial Format	Baud rate, word length, parity, and stop bits settings.
Modem Setup Str	The Modem Setup String is a set of initial commands the modem needs to communicate with. A standard Modem Setup String is automatically entered here and should not be changed unless your modem documentation specifies a different setup. For more information on modem setup strings see Appendix J - Modem Setup Strings. [AT M1 V1 Q0 S0=1]
Incoming Type	Selects the device type that will be calling into this port. If you wish to disable incoming calls then leave this field blank. Press Tab and select from list. Available types are the ASCII devices that have been defined under Files-ASCII Devices-ASCII Rules. Associated rules will be used on all messages coming in on this port. <b>Note:</b> Multiple device types (message formats) can be supported by using device identification. See the following section for more details.
Port Description	Any description you would like to give to the port that might help explain what the purpose of the device or what areas it applies to. Up to 30 characters. This will be seen in the Craft Port selection screen.

**Table M6.S - Key commands available in the Remote Parameters screen, ASCII dial-up.**

Function Key	Description
F5	Toggle/Suspend. Allows you to define but temporarily halt or suspend this function.
F8	Save port page.
F10/Esc	Move to first field or exit without saving (depending on cursor location).

---

## Incoming Call Device Type Identification

There are two ways of determining the site name of an incoming call. Both are listed in the section below.

### Selecting the Device Type Using the **!!!SET\_DEVICE!!!** Command

If messages dialed in from a remote device contain some kind of unique device identification early in the message, it may be possible to accommodate several different device types on a single dial-up port. The ASCII processor has special provisions for determining the site name associated with an incoming call. Once identified, the ASCII processor will use the device type that has been assigned to that site name for determining the next rule set to use. This ability to change device types on the fly may allow different device types to call into the same modem line. Message formats may not always permit this, in which case you will need to have separate phone lines and ASCII ports for the different device types — see Figure M6.20, Option 2. Outgoing calls to ASCII devices do not need this special consideration because the ASCII processor already knows which device it is calling. The same goes for dedicated ASCII Input jobs.

Using this command requires that messages dialed in from a remote device contain some kind of unique device identification early in the message. DPS only recommends using this command when there are several different device types on a single dial-up port. A side effect of this command is that it will discard the line containing the unique device identification, which means that the line cannot be used for further processing.

Use the following steps to configure the **!!!SET\_DEVICE!!!** command:

1. Under Files > ASCII Devices > ASCII Rules create a device type that will initially handle all incoming calls on a particular port (select Find, give it a name – say CALLID – and enter rule #0). These rules are to be assigned to the “Incoming Type” on the remote port job for ASCII Dial-up.
2. Enter numbered rules for this device type to identify what physical device is calling. These rules could attempt to determine the device ID by examining any spontaneous output the device transmits. You could also issue commands or run a script to get it to identify itself. In most cases you will be able to extract a device identifier from the received text – for example, it could be CELL24. Build this identifier in key slots 2-9 using normal slot commands. Classify by site or groups of like formatted devices. If you have several different devices, then in as few lines as possible, determine device format using the **!!!Set\_Device!!!** command.

**WARNING:** Once you use this rule extraction ends.

3. Put the special literal **!!!SET\_DEVICE!!!** in key slot 1, eg, \KL1**!!!SET\_DEVICE!!!** — see Figure M6.17.
4. In the Parameters-Remote Ports screen described on the preceding page, enter the device type created in step 1 in the Incoming Type field. In our example it would be CALLID.
5. On the Files-Dial Up Networks > ASCII Sites > Device screen described on section M6-52:
  - In the Device Type field, enter the actual ASCII rule set to be used with calls from this physical device — for instance, it could be TL1.
  - In the ID Key field, enter the device identifier created in step 2 and 3. In our example, it would be CELL24.

```

          ASCII Device Rules

ASCII DEVICE : GCU          Rule #      : 20          Log Type : STANDARD
Descr : Set ASCII Site          Special  : NONE
                                Ignore   : N

          Pattern Recognition
1 \M^BL
2
3
4
5
6

          Action Extraction
1 \L1!!!SET_DEVICE!!!\L2SITE_KEY
2
3
4
5
6

F>ind, E>dit, D>elete, N>ext, P>rev, M>ove, R>ead, Q>uit :
F4=Debug, F6=Manage, AF6=Import/Export, F10/Esc=Exit

```

Fig. M6.17 - Place the “!!!SET\_DEVICE!!!” command in key slot one that refers to the site shown in Figure M6.18.

```

          ASCII Dialup Device Definition

ASC Site Name: GCU

Description  : GCU'S REPORTING ON CSU'S
Site Name   : GCU
Virtual Addr : 1
Displays    : 1-10
Device Type  : GCU
Time Out    : 30
Incoming Dev :
Id Key       : SITE_KEY

Token #1    :
Token #2    :
Token #3    :
Token #4    :
Token #5    :

F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit :
F1=Pnts, F2=ASCII Actions, F3=Int Alarms, AF1=TL1, AF6=Templates, F10/Esc=Exit

```

Fig. M6.18 - This site is linked to the device rule shown in Figure M6.17 because of the ID Key “SITE\_KEY.”

### Selecting the Device Type Using the \KDlit Command

In the case where there is only one type of incoming device, using this command does not require that messages dialed in from the remote device contain some kind of unique device identification. This command will also work in the case where there are multiple types of incoming devices, as long as the messages contain some kind of unique device identification early in the message. This command will not discard the line containing the unique device identification, which means that this line can be used for further processing. The disadvantage to this command is that the more alarm formats and sites you have, the larger the task of databasing becomes. If this is the case, then DPS recommends assigning each device to its own display on a single site. This would mean only one rule per alarm format as opposed to one rule per alarm format per site.

Using this command will force T/Mon to use the site name contained in “lit,” and the rule set associated with it, if the pattern recognition phase succeeds. In the Action Extraction section, place “\KDlit” as the first command on the line to force the incoming ASCII dial-up device to use the site name, and the rule set associated with it, contained in the “lit” — see Figure M6.16.

```
ASCII Device Rules
ASCII DEVICE : GCU          Rule #      : 5          Log Type : DETAILED
Descr : GCU ALARMS <SET>    Special  : NONE
                               Ignore   : N
Pattern Recognition
1 \MSET\M.\M.\M:
2
3
4
5
6
Action Extraction
1 \KDFRESNO\F1\K5\F6\K3\F1\P1\K1<42,8>\L2:\L4:
2
3
4
5
6
F>ind, E>dit, D>elete, N>ext, P>rev, M>ove, R>ead, Q>uit :
F1=Logging Match. F4=Debug. F6=Manage. AF6=Import/Export. F10/Esc=Exit
```

Fig. M6.19 - Place “\KDlit” as the first command on the line to force the ASCII dial-up device to use the site name, and the rule set associated with it, when recognition phase passes. In this example, “FRESNO” is the “lit” — the name of the site (see Figure M6.20).

## ASCII Dial-Up Definition

To select the ASCII dial-up device definition screen, exit the port definition function and the Parameters menu. Enter the File Maintenance menu, select Dialup Networks and select ASCII Sites. This selection allows you to create alarm equipment polling list at the address level from which T/MonXM will gather information.

```

      ASCII Site Definition
Site Name      : FRESNO
Description    : ASCII Dialup
Remote Site Phone : (559) 454-1600

Polling Type   : PERIODIC
Polling Interval : 60 (mins)
Scheduled Days ---> SUN:   MON:   TUE:   WED:   THU:   FRI:   SAT:
Scheduled Hours :
Scheduled Minute :
Fail Poll Interval: 60 (mins)
Fail Threshold  : 3
Dialout Port    : 0

F)ind, E)dit, D)delete, N)ext, P)revious, Q)uit : _
F1=Device, F10/Esc=Exit
  
```

**Fig. M6.20 - The Remote Site definition screen, ASCII dial-up.**

This screen is reached by selecting by selecting Files > Dialup Networks > ASCII Sites.

**Table M6.T - Fields in the ASCII Dial-Up Site Definition screen**

Fields	Description
Site Name	The name for the site. Up to 10 characters.
Description	The description for the site. Optional. Up to 40 characters.
Remote Site Phone	The phone number that T/MonXM will use to dial the site. Up to 30 digits. Remember to enter 9, or other character to get an outside line if necessary.
Polling Type	Periodic or Schedule. Press Tab for a selection window. Press Tab again to toggle the selection highlight. Press Enter to choose. <ul style="list-style-type: none"> <li>Periodic will call ASCII Device every 60 minutes, or specified time period, all day, every day.</li> <li>Schedule will call the ASCII Device only at the times and on the days specified in the Scheduled Days, Scheduled Hours and Scheduled Minute fields that follow.</li> </ul>
Polling Interval	Amount of time, in minutes between calls to the ASCII Site. 0-9999 minutes. 0=Never. (Applies to periodic only)

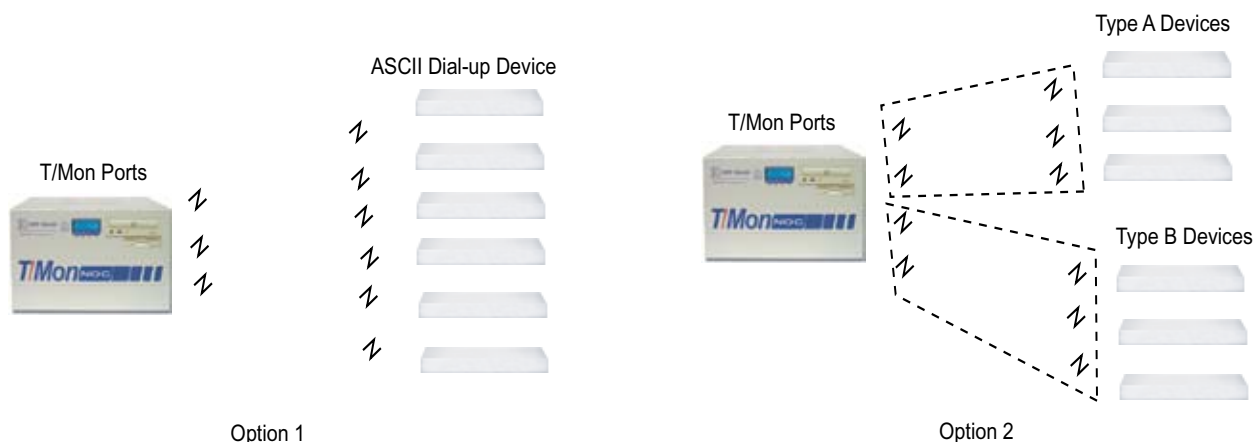
**Note:** Table M6.T continues on the following page

**Table M6.T - Fields in the ASCII Dial-Up Site Definition screen (continued)**

Fields	Description
Scheduled Days	Select Y (do call) or N (don't call) for each day of the week. (Applies to scheduled only)
Scheduled Hours	Select range of hours on the scheduled days to call the ASCII Device. Use 0 to 23. Enter a set (such as 5-8) or individual hours (such as 7, 9, 13, 18, 21). <b>Note:</b> Applies to scheduled only.
Scheduled Minute	Enter the time offset from the hour. <b>Note:</b> Applies to scheduled only.
Dialout Port	Remote port where outgoing calls are made. 0=None (incoming only)

**Table M6.U - Key commands available in the ASCII dial-up site definition screen.**

Function Key	Description
F1	Device. See explanation and table in the following sub section. This hot key is available only after the site has been defined and when the cursor is on the prompt line.
Up Arrow	Move to previous field.
F8	Save. Available only during field editing.
F10/Esc	Exit.



**Fig. M6.21 - Multiple device types can concurrently report alarms to T/Mon**

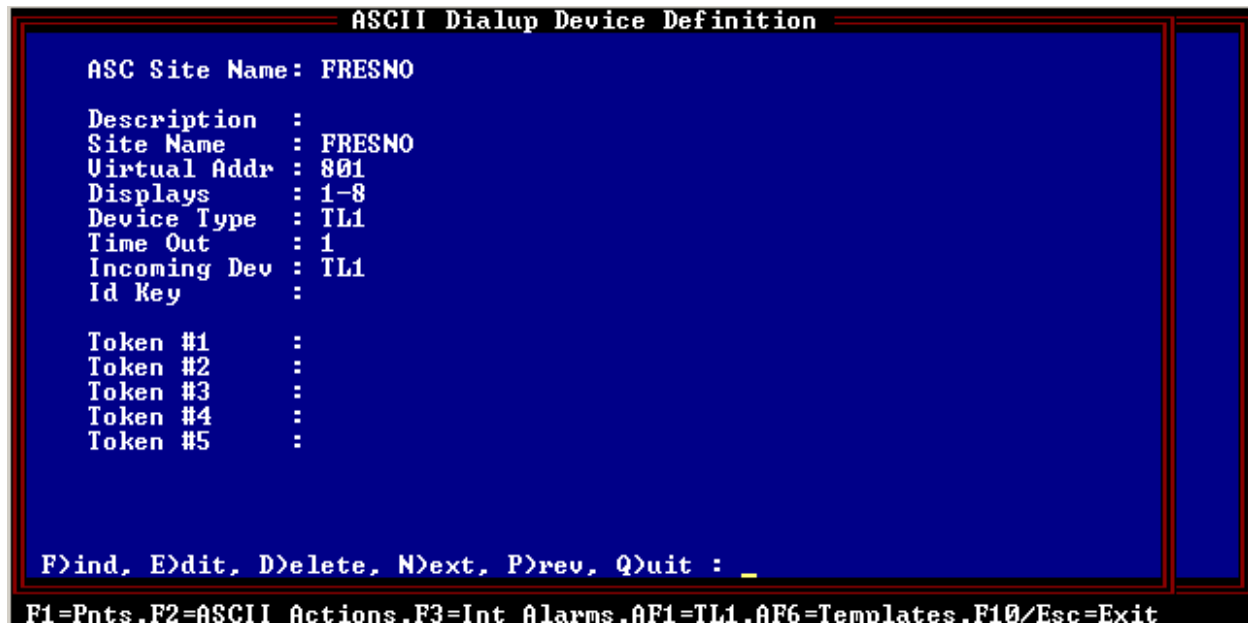


Fig. M6.22 - The Remote Device definition screen, ASCII dial-up. This screen is reached from the Master menu by selecting Files > Dialup Networks > ASCII sites, then select F1=Device after the site has been defined

**Table M6.V - Fields in the ASCII Dial-Up Device Definition screen.**

Field	Description
ASC Site Name	Site Name carried over from the ASC Site Definition screen that this device is being defined under.
Description	An informational description of this device
Site Name	Site Name used for alarm formatting (Master Menu-Parameters-Alarm Format)
Virtual Address	1-999, doesn't matter what it is as long as it does not conflict with a virtual address assigned to any other device in T/Mon. Is used with devices that do not have a true address but need to be referenced by address elsewhere in T/Mon, such as in derived alarms.
Displays	The displays that you wish to allocate for this device under the Virtual Address assigned above. One display holds up to 64 alarms, so you will need as many displays as it takes to hold every possible alarm being reported from this ASCII device. Displays typically start at 1 and continue as needed, up to a maximum of 64. Enter display numbers separated by hyphens or commas. Example: 1-4,7
Device Type	Select the device type that this port will be calling. Press Tab and select from list. Available types are the ASCII devices that have been defined under Files-ASCII Devices-ASCII Rules. This is only used for outgoing calls.
Time Out	The message processor deals with incoming ASCII on a line-by-line basis. If it receives characters with no end-of-line indicator, it will wait for the time specified in this field, assume the line is complete, and proceed with processing. Can be 1 to 30 seconds, usually 1.
Incoming Device	Allows the user to switch the device type and rule set only after a !!!SET_DEVICE!!! has been performed. This is a work around designed to save time databasing.

**Note:** Table M6.V continues on the following page.



**Table M6.V - Fields in the ASCII Dial-Up Device Definition screen (continued)**

Field	Description
Site Name	Site Name used for alarm formatting (Master Menu-Parameters-Alarm Format)
ID Key	Key that will be used to determine device ID for incoming calls. Needed only if using the Incoming Call Device Type Identification process described on section M6-47. If the message processor generates the Id Key entered here, it will use the device type entered on this screen above for subsequent processing of a message called in from this device.
Token #1 - #5	A group of characters that can be included in a command that is sent to an ASCII device. Such commands are defined for generic device types in the message processing section — see highlighted fields in Table M6.A on section M6-8 for LogOn, LogOff, and general polling commands (section M6-37) for scripts. Tokens permit generic commands to be customized for a particular device. In the command definition, to enter the symbol <Tn> where token n=1-5 is to appear, then enter the characters that make up that token here. In short, tokens are used as a way of sending device-specific information to devices as part of ASCII rules. Technically, tokens are the literals that are substituted for variables in log-on, log-off, and command strings.

**Table M6.W - Key commands available in the ASCII Dial-Up Device Definition screen.**

Function Key	Description
F1	Points. This will take you to the Point Definition screen. This is the same point definition screen that is used throughout T/MonXM. Refer to the Point Definition section on page M6-59.
F2	ASCII Actions. This takes you to the ASCII Actions screen. Refer to the ASCII Actions section on page M6-62.
F3	Internal Alarms. ASCII internal alarms are the same as all other device internal alarms in that it allows you to specify alarm points for DEVICE FAILURE & DEVICE OFF LINE situations. Refer to Section 14 (Assigning Internal Alarms) for more information.
F4	Shortcut to the ASCII Rules page
F9	List of all key commands for this window
Alt-F1	TL1 Definition. This option is only available if you've purchased the TL1 Responder Software Module. It will allow you to assign TL1 Attributes to each ASCII alarm. For more information see Software Module 14 (TL1 Responder).
Alt-F4	Shortcut to the ASCII Device menu
Alt-F9	Import/Export to and from a template
F10/Esc	Exit.

## Remote Ports, Dedicated ASCII

- A port numbered 1 to 24 represents a physical T/Mon port.
- A 'port' numbered 30 or higher is called a job and represents a data connection that behaves like a port. For ASCII input, this could be an Ethernet TCP Port, a single channel on an ASCII Mux, etc.
- An ASCII Input port or job can be connected to only one dedicated ASCII device. This is because ASCII messages are not addressable and simply pass back and forth on the communications channel.

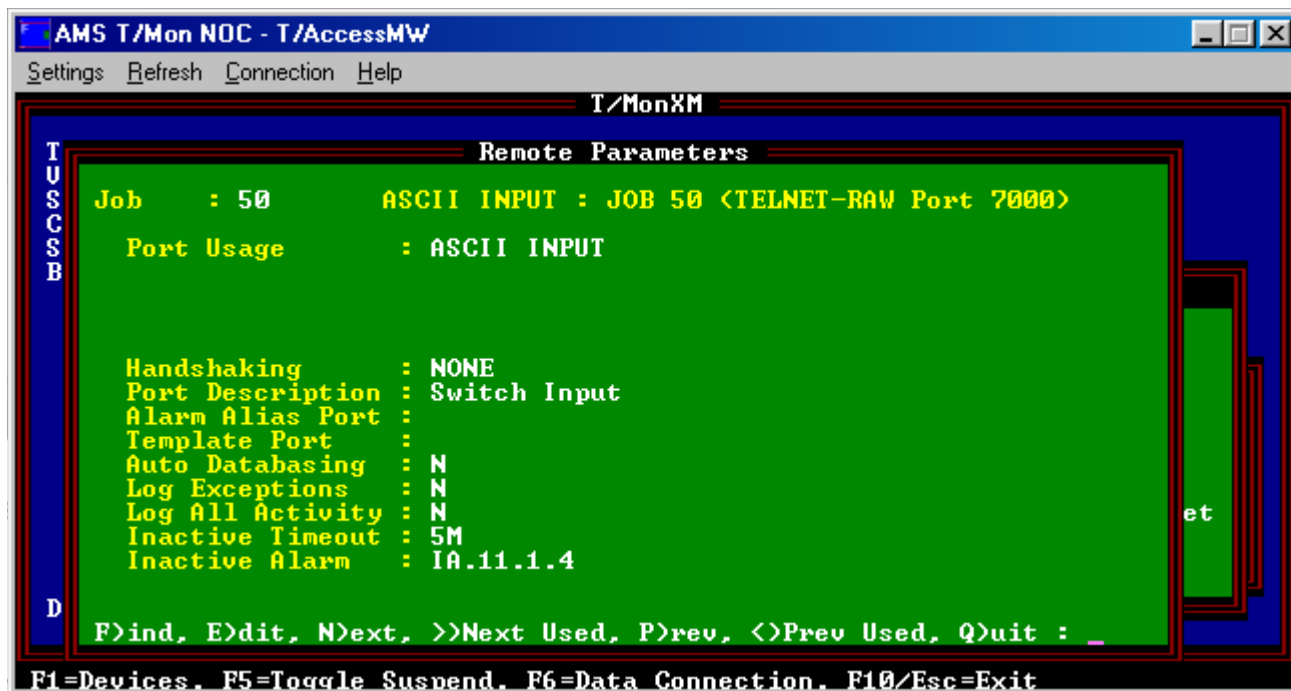


Fig. M6.23 - The Remote Parameters screen, ASCII input usage.

This screen is reached from the Master menu by selecting Parameters-Remote Ports. Use N)ext or P)rev to scroll to the appropriate port or job number, then select E)dit to make entries.

Table M6.X- Fields in the Remote Ports, ASCII Input screen

Field	Description
Port Usage	ASCII INPUT
Serial Format	Baud rate, word length, parity, and stop bits settings.
Handshaking	Select the type of handshaking to use, must match whatever is used by the remote equipment. Valid entries are N (none), X (Xon/Xoff, often called software flow control), or R (RTS/CTS, often called hardware flow control). <b>Note:</b> Only used on ports 1-24.
Port Description	Informational description, used in various places as a name to refer to this port.

**Notes:** Table M6.X continues on the following page.

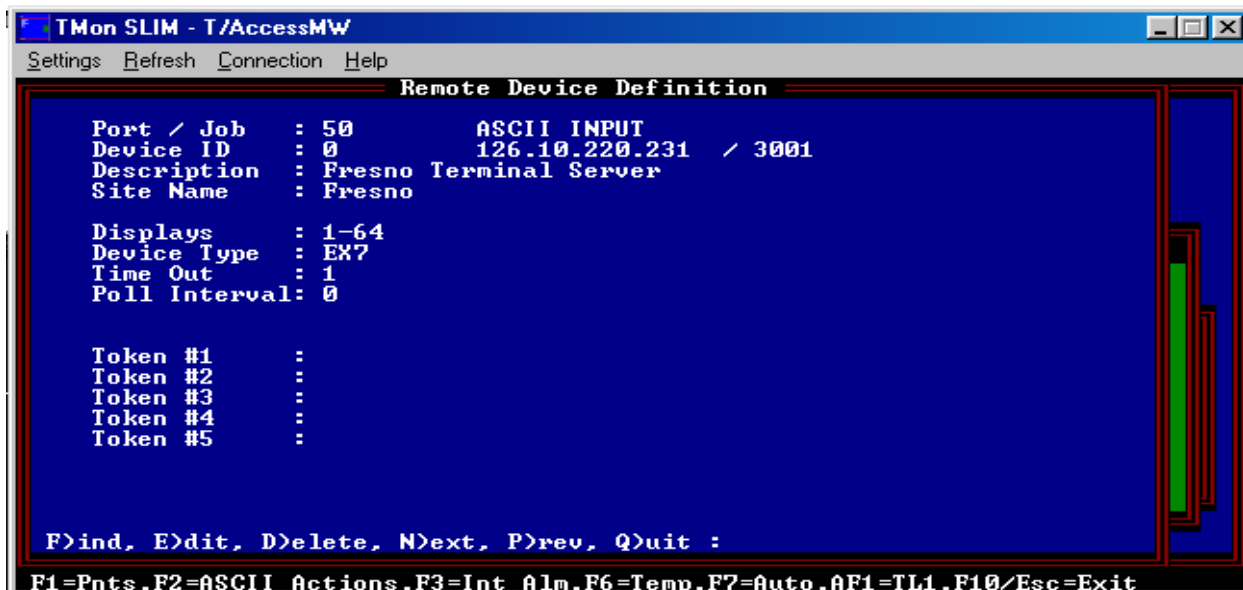
**Table M6.X- Fields in the Remote Ports, ASCII Input screen (continued)**

Field	Description
<b>Select at most one of the following three options, or select none of them if you are manually entering Point Definitions and ASCII Actions.</b>	
Alarm Alias Port	Number of another port whose previously defined data base you wish to use for this port. Leave blank for none. (This option is used only in certain specialized applications when one source of ASCII data provides incomplete or inaccurate information that needs to be supplemented by data from another port. It is usually left blank.)
Template Port	If Point Definitions and ASCII Actions are to be obtained from an ASCII template, enter the Template Port number here (801, 802, or 803). Otherwise leave blank. To define templates see section M6-63. To assign to sites see section M6-64.
Auto Databasing	If Point Definitions and ASCII Actions are to be obtained automatically, enter Yes, otherwise No. See section M6-68 for Auto Databasing instructions. This entry is available only if the ASCII Auto-databasing module is installed.
Log Exceptions	Yes = log all exceptions to a file named AEnum.rep in the directory where T/ Mon is installed, where num is the port number (3 digits with leading zeros).
Log All Activity	Yes = log all incoming ASCII to a file named ALnum.rep in the directory where T/Mon is installed, where num is the port number (3 digits with leading zeros). <b>Note:</b> Usually used in debugging applications. This feature should not be left on indefinitely.
Inactive Timeout	Interval of time without receiving incoming ASCII before the inactivity alarm will be set. To disable the inactivity alarm enter a 0 (zero). Otherwise enter the interval followed by a letter indicating the time units being used. The maximum numeric value is 99. Valid units are M for minutes, H for hours and Q for quarter hours. Example: "10M" = 10 minutes.
Inactive Alarm	The User Internal Alarm which is set if no incoming ASCII is received for the interval defined in the Inactive Timeout field. Enter the User Internal Alarm in the following format PORT.ADD.DISP.PNT (For example IA.11.1.1). Leaving this field blank or setting it to 0 will disable the inactivity alarm.

**Table M6.Y - Key commands available in the Remote Parameters screen, ASCII input**

Function Key	Description
F1	Devices. See explanation and table in the following sub-section. This hot key is available only after the port has been defined and when the cursor is on the prompt line.
F5	Toggle/Suspend. Allows you to define but temporarily halt or suspend this function.
Alt-F5	Move (not visible at bottom of screen). Moves the port definition to another port. A window will appear for you to specify the new port number.
Up Arrow	Move to previous field.
F8	Save port page.
F10/Esc	Exit.

## T/MonXM 6.8 User Manual



**Fig. M6.24 - The Remote Device Definition screen, ASCII input.**

**Table M6.Z - Fields in the ASCII Input Device Definition screen**

Field	Description
Port 1 Job	Port number. Use N)ext and P)rev to scroll to the appropriate port.
Device ID	Always 0 for the first address on a port. One address holds 4096 alarms (64 displays), so you need additional addresses only if your ASCII device reports more than this many different alarms, or has multiple nodes or sites that would work well if separated by address. Subsequent addresses are usually numbered 1,2,3, etc., but addressed used for separate nodes should be spaced address 10, 20, 10, etc. to leave room for multiple addresses per node.
Device Type	Press Tab and select from list. Available types are the ASCII devices that have been defined under <b>Files &gt; ASCII Devices &gt; ASCII Rules</b> . <b>Only appears for address 0.</b> <b>Note:</b> This rule set will be used port wide.
Port Description	Informational description, used in various places as a name to refer to this port.
Displays	The displays that you wish to allocate for this device under the Address assigned above. One display holds up to 64 alarms, so you will need as many displays as it takes to hold every possible alarm being reported from this ASCII device. Displays typically start at 1 and continue as needed, up to a maximum of 64. Enter display numbers separated by hyphens or commas. <b>Example:</b> 1-4,7 <b>Note:</b> Usually left at 1-64.
Site Name	Site Name used for alarm formatting (Master Menu>Parameters>Alarm Format)
IP Address	IP Address of the ASCII device to send commands to CUDP data connection only.
UDP Port	Port of the ASCII device to send commands to CUDP data connection only.

**Note:** Table M6.AA continues on the following page.

**Table M6.Z- Fields in the ASCII Input Device Definition screen. (continued)**

Field	Description
Time Out	The message processor deals with incoming ASCII on a line-by-line basis. If it receives characters with no end-of-line indicator, it will wait for the time specified in this field, assume the line is complete, and proceed with processing. Can be 1 to 30 seconds, usually 1. Entry only appears for address 0.
Poll Interval	Polling interval (1-360 minutes), 0 to disable. Sets the time period between the Logon Connectivity Test commands and Logoff sequences. The poll interval is the time period between sequential Logon commands. Can disable if remote device sends spontaneous alarm messages. Entry only appears for address 0
Send Cmds	Entry appears only on addresses greater than 0. Determines if LogOn, LogOff, and general polling commands will be sent specifically for this address; if so, will use any tokens listed below. Otherwise, commands will not be sent (this is the case if the remote device carries over any such commands that were sent for address 0 to apply to the current address as well).
Token #1 - #5	A group of characters that can be included in a command that is sent to an ASCII device. Such commands are defined for generic device types in the message processing section, section see M6-8 for LogOn, LogOff, and general polling commands (section M6-37) for scripts. Tokens permit generic commands to be customized for a particular device. In the command definition, for enter the symbol <Tn> where token n=1-5 is to appear, then enter the characters that make up that token here.

**Table M6.AA - Key commands available in the ASCII Input Device Definition screen**

Function Key	Description
F1	Points. <b>Note:</b> Use if <b>manually</b> entering Point Definitions and ASCII Actions. Goes to the standard Point Definition screen that is used throughout T/MonXM — see Section 10.
F2	ASCII Actions. <b>Note:</b> Use if <b>manually</b> entering Point Definitions and ASCII Actions. Goes to the ASCII Action Definition screen. See page M6-62
F3	Internal Alarms. Allows internal alarms to be assigned for Device Fail and Device Offline conditions—see Section 14.
F4	Shortcut to the ASCII Rules page
F6	Templates. <b>Note:</b> Select if using <b>templates</b> for Point Definitions and ASCII Actions. See page M6-65
F7	Auto (available only if ASCII Auto Databasing module is installed). <b>Note:</b> Select if using <b>Auto Databasing</b> to enter Point Definitions and ASCII Actions. See Auto Databasing ASCII Module (section M6-68) for detailed information on Auto-Databasing.
F9	List of all key commands for this window
Alt-F1	TL1 (available only if the TL1 Responder module is installed). Select if T/Mon is acting as a TL1 responder reporting to a higher-level monitoring system. See Software Module 14 (TL1 Responder).
Alt-F4	Shortcut to the ASCII Device menu
Alt-F9	Import/Export to and from a template
F10/Esc	Exit

## ASCII Point Definitions

To access the Point definition screen press F1 while in either the ASCII dial-up or ASCII Input Device Definition screen. The table below describes the fields in the Point Definition screen.

**Note:** The names of the second through seventh field are spelled out vertically. The choices for each field appear at the bottom of the window as the cursor is moved to the field.

See Section 10 (Point Definition Tutorial) for detailed information on standard point Definition.

```

Point Definition
Port : 2   Addr: 0   Disp: 2   Display Desc :
P L H L S R
o o s e t v
ASCII INPUT
Pt l g t v s s   Description   Fail   Clear
1 B L H A A N   LINE CARD ONE   F       C
2 B L H A A N   LINE CARD TWO    F       C
3 B L H A A N   LINE CARD THREE  F       C
4 B L H A A N   LINE CARD FOUR   F       C
5 B L H A A N   PRIMARY POWER    OFF     ON
6 B L H A A N   SECONDARY POWER  OFF     ON
7 B L H A A N   CRITICAL ALARM   CRIT    CLR
8 B L H A A N   SUMMARY ALARM    ALARM   CLEAR

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

Message

F10/Esc=Exit

```

Fig. M6.25 - The ASCII Point Definition screen.

Table M6.AB - Fields in the Point Definition screen

Field	Description
Pt	Point. Displays what point you are editing.
Pol	Polarity. Defaults to "B" (Bipolar). <b>Note:</b> "B" posts COS on alarm and clear. "U" (unipolar) posts COS on alarm only.
Log	Printer/File. Entering "L" (Log) allows this point to be logged and entering "N" (No Log) disables logging of this point. [L]
Hst	History. Entering "H" (History) allows point to be logged into history file. Entering "N" (No History) disables logging this point in the history file. [H]
Lev	Level. Select alarm level for this point. Valid options are: a (Most Critical), b, c, d (Least Critical). (Value set in Miscellaneous Parameters)
Sts	Status. Enter "S" (Status) if the alarm doesn't affect the relay card and select "A" (Alarm) if the alarm affects the relay card. [A]
Rvs	Reverse. <b>Note:</b> Not necessary in ASCII, leave as N (normal).

Table M6.AB continues on the following page.

```

Point Definition
Port : 2   Addr: 0   Disp: 2   Display Desc :
P L H L S R
o o s e t v
ASCII INPUT
Pt l g t v s s   Windows   Msg   Qual
1 B L H A A N   7.....   0     0
2 B L H A A N   7         0     0
3 B L H A A N   7         0     0
4 B L H A A N   7         0     0
5 B L H A A N   7,10      4     1
6 B L H A A N   7,10      2     0
7 B L H A A N   5,7       1     0
8 B L H A A N   6,7       3     0

Enter windows. (2-720; 8 max)

Message

```

Up Arrow = Previous Field, F10/ESC = First Field

Fig. M6.26 - ASCII Point Definition screen, Part 2.

Table M6.AB - Fields in the Point Definition screen (continued)

Field	Description
Description	Enter the description (up to 40 characters) of the alarm for this point.
Fail	Enter fail description (up to 8 characters) for point. The fail description allows you to describe the content of the error message. This will default to the settings in the Alarm Format screen.*
Clear	Enter clear status description (up to 8 characters) for point. The clear description allows you to describe the content of error messages. It will also default to the settings in the Alarm Format screen.* <b>Note:</b> Upon entering clear value display advances to show other fields.
Windows	Enter alarm windows (2-90, or greater, depending on options — up to 720) associated with this point. There is a maximum of 8 windows per point. Windows may be sorted by any criteria that has meaning, such as severity, site location, or type of equipment. This gives your system an interface that “makes sense” to users with plain English descriptions that are easily understood.
Msg	Message. Enter the number of the pre-defined message or enter “0” (zero) for No Message. Enter “N” to create a new message. [0] <b>Note:</b> This is an application of “on-the-fly” message creation. <b>Note:</b> Pressing F1 while in this field will open the message search feature.
Qual	Alarm qualification delay. Enter the amount of time in minutes this alarm must be present before it will report. Default is 0 = Immediate.

\*Default alarm formatting is located in the Alarm Format screen under the Parameters menu. From the Alarm Format screen, press F4 to access the Level and Status settings.



**Table M6.AB - Fields in the Point Definition screen (continued)**

Field	Description
Counter	Number of occurrences in a time period before a fault event is declared. 0=None. Enter time (0-99) (M)inutes, (H)ours or (Q)uarters), slash and the number of occurrences. Example: 30M/10 are 10 occurrences in 30 minutes.**
Pager	Enter pager profile number (1-99) for this point.0=None. Tabbing on this field will display a list of pager profiles.The description for the current profile is listed at the bottom of the window. If the selected profile has not been defined, no description is listed — see section M6-75.
<b>Note:</b> While T/MonXM 3.5 and later is backward compatible with the text/message method, Pager Profiles is the preferred method. The pager profiles method provides more capacity and allows the text message to be used as intended. Either or both methods may be used on a particular point.	

\*\* To see more information while in these fields, press F9.

**Table M6.AC - Key commands available in the point definition screen**

Function Key	Description
F1	Moves the cursor to a selected entry point.
F3	Deletes the current point entry.
F4	Toggles between the 2 parts of the Point Definition editing window.
F5	Range function for editing. This is a powerful editing tool that has many more features than can be explained here. Please refer to Section 10 (Point Definition Tutorial) for a thorough explanation.
F6	Read. Allows you to load an existing display of alarm point definitions into the Point Definition Screen. They can then be further edited.
F8	Saves the alarm point entries and returns to the first page of the Point Definitions Editing window.
F9	Displays help for this screen.
F10/Esc	Exit.
Alt-F3	Delete Point. Deletes point under cursor and causes all points below to move up one position.
Alt-F4	Insert Point. Causes point under cursor and all below to move down one position. An undefined point is then inserted at the cursor.
Alt-F5	Block move. Moves a block of points.
Alt-F6	Block Copy. Copies a block of points.



## ASCII Action Definitions

The ASCII action string is the vital link that associates a key generated by the extraction phase of ASCII processing and a particular T/MonXM standard alarm. For each ASCII alarm point you must assign the key that the extraction process would generate when the alarm fails. You would also enter the action key that would be generated when the alarm clears.

For example: if Address 1 point 4 contained

Set: 1LOF, LINE (RED) ALARM

Clear: 1LOF, LINE (RED) OK

and the action key “FRESNO-TOWER-OFF” was generated by the ASCII extraction process then T/MonXM point 1 on address 4 on the appropriate port would be set. Likewise if the “ON” key was received then the alarm would be cleared.

To go to the ASCII Dialup Device Definition screen, go to Parameters > Remote Ports > press F1 (Remote Device Definition screen) > press F2 (ASCII Actions Definition screen).

```

ASCII Dialup Device Definition

ASC Site Name: TNDS

Descr          ASCII Action Definitions
Site
Virtu          Display : 1
Displ
Devic
Time
Point  Type    Action String
-----
Id Re      1    SET    1LOS, LINEALARM
           CLEAR  1LOS, LINEOK
Token      2    SET    1LOS, DTEALARM
Token      CLEAR  1LOS, DTEOK
Token      3    SET    1LOS, CSUALARM
Token      CLEAR  1LOS, CSUOK
Token      4    SET    1LOF, LINE (RED)ALARM
           CLEAR  1LOF, LINE (RED)OK
           5    SET    1BPVALARM
           CLEAR  1BPVOK

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

F10/Esc=Exit
  
```

Fig. M6.27 - The ASCII Action Definitions screen

Table M6.AD - Fields in the ASCII Action Definitions screen.

Field	Description
Display	Indicates display to be edited. There is a one-to-one correspondence between Alarm points and ASCII Actions. If there are 2 displays of alarms, there are 2 displays of ASCII actions. Maximum value is 1-64.
Point	Point to edit which corresponds to the point description in the point editing section. Value is 1-64.
Type	Set or Clear. Each alarm point can have up to two ASCII strings. This field indicates which action string you are defining.
Action String	Up to 50 characters. This is the actual string that must EXACTLY match the output of the extraction section to set or clear the specified alarm.

**Table M6.AE - Key commands available in the ASCII Action Definitions screen.**

Function Key	Description
F1	Copies Action String from the SET section into the CLEAR section.
F3	Blank. Deletes contents of current field.
F8	Save. Saves ASCII action string.
Ctrl-F1	Read. Reads the ASCII action contents from another ASCII action display and copies them into the ASCII action display you are editing. In the case of dedicated ASCII the display that you are copying from MUST be on another port. In the case of dialup the restrictions are reordered such that ASCII the source display must at least be on a different virtual address. After entering this command you will be prompted for the port, address, and display of the display of ASCII action information you wish to copy.
Ctrl-F2	Translate. Replace a portion of an action string with another string. Once this command has been entered a form will allow you to enter: Target- The string you want replaced Replacement - The string to be substituted Type - Allows you to determine which type of strings will be processed. Choices: A: all types (set & clear) S: Set strings only C: Clear strings only Commands can be used to translate abbreviations or place holders into real data. <b>Caution:</b> Be careful to specify a unique enough source string so you don't inadvertently translate more than you intended.
Ctrl-F3	Prefix - Places specified data into the start of the action string.
Ctrl-F4	Append - appends data to the end of the action string.
Ctrl-F5	Read + - Extended read & translate command that will allow you read a display of ASCII actions (copy them) and translate a particular sub-string to another string. This command could be used for example to read a template for a particular device type and replace a dummy site name with the real site name. This command allows ASCII action copy even on the same port by using the translate portion to not duplicate keys.
F10/Esc	Exit.

## ASCII Templates

**Templates can save considerable databasing effort if several different devices report identical alarm information, differing only in details such as location.** For instance, you might have a number of identically-equipped cell sites sending the same alarm messages for particular faults. A template lets you enter alarm information once and share it among sites.

Using templates is a two-phase process. In the first phase, the template itself is built. In the second phase, it is attached to a site – an address on a physical port that is receiving ASCII input.

## Build a Template

1. Access the Remote Device Definition screen by going to Files > ASCII Devices > Templates. It is identical to the ASCII Input Device Definition screen described on page M6-57, but only a few entries are used here:
  - Enter the address (use Find to add addresses, each of which will appear on a new screen). The address, as used here, is logically the equivalent of a site. All alarms at a site must generate the same Site Key during extraction processing; the same alarms at another site would generate a different Site Key, but would share this same address in the template.
  - Enter an optional description.
  - Enter the display numbers that will be defined under this address.
2. Select F1 to manually enter points — see section M6-58. These are entered in the usual manner with one exception: a category C1-C8 can be entered in the pager column. Each category will later be assigned to an actual pager profile, which can be different for the same alarm at different sites.
3. Select F2 to manually enter ASCII Actions in the usual manner — see section M6-61.
4. Save and exit.

**Note:** There can be more than one address in a template. This allows several different sets of alarm points to be defined. Simply refer to the desired address when defining the template site.

```
Remote Device Definition

Port      : 801      ASCII TEMPLATE
Address   : 1
Description : CSU TEMPLATE
Site Name  : PIN TREE

Displays  : 1-64

Send Cmds : N

Token #1   :
Token #2   :
Token #3   :
Token #4   :
Token #5   :

Find, Edit, Delete, Next, Prev, Quit :

F1=Pts,F2=ASCII Actions,F10/Esc=Exit
```

**Fig. M6.28 - Define an ASCII template in the Remote Device definition screen. This screen is reached by selecting Files-ASCII Devices-ASCII Templates, then select template number**

## Template Site Definition

This screen is used to assign templates to addresses on a dedicated ASCII port. Since each address corresponds with a single site, this is equivalent to assigning a template to a site.

### Attach a Template to a Site

1. The template must already have been built, as described on the preceding page.
2. On the Remote Parameters screen, reached by selecting Parameters-Remote Ports from the Master Menu, enter the Template Port number (801, 802, or 803) for the affected ASCII input port or job. Press F1=Devices . Enter through the default values and press F6=Temp to bring up the screen above.
3. The Addr and Site name fields will already be filled out for all addresses that have been defined. For Site Key, enter the key that gets built by the Message Processing extraction rules for this site. (this is the key that is built in Key Slots 10-14).
4. In the Temp Addr (Template Address) field, enter the address in the template that contains the alarms at this site.
5. In the Site Window field, enter a window number that represents this site.
6. If paging, press F7 to assign pager categories to actual pager profiles. (Categories can be assigned in the pager column on the point definition screen when defining templates. Here we are converting those categories to pager profiles, so that different people can be called when the same alarm occurs at different sites).

```

      Ascii Template Site Definition
Port : 21

  Addr  Site      Site      Temp  Site
  Addr  Name      Key      Addr  Window
-----
0      PIN TREE  PINTREE~.....      1      7

Enter site key.

F3=Blank, F7=Paging Categories, F8=Save, F10/Esc=Exit
```

**Fig. M6.29 - Enter the Site Key in the Site Definition screen.**

This screen is reached by selecting Parameters-Remote Ports, then F1=Devices, F6=Temp

## ASCII Analyzer

This screen can be reached by pressing Shift-F7 while in the Alarm Summary screen. The purpose of this screen is to permit analysis of ASCII processing as actual messages are received on ASCII input ports. The upper portion, the ASCII Processor Activity window, shows incoming ASCII and diagnostic messages in various formats depending upon user commands described below. The ASCII Selector window in the lower left corner is used to select the input port and specify a particular rule for detailed examination. It also shows the state of current display options.

## Port and Rule Selection

The screen above comes up when the ASCII Analyzer is first selected. The upper window shows available ASCII ports. The user makes the following entries:

```

      ASCII Processor Activity
    Available ports :
    6) [ASC]
    7) [ASC]
    9) [ASC]
   36) [ASC]

    ASCII Selection
    Channel      : 9
    Rule         : 52.

    Page Index
    > A E I M Q U V : D
      B F J N R V A : P
      C G K O S W S : S
      D H L P T X P:X
    STAND :30   Silenced:0
    COS   :44   Off Line:0

    Up Arrow=Previous Field, F10/Esc=First Field
  
```

Fig. M6.30 - ASCII analyzer screen, port/rule input mode

This screen is reached from the monitor mode alarm summary screen by selecting Shift-F7

Table M6.AF - Port and rule selection

Field	Description
Channel	Port number from which the ASCII input will be obtained.
Rule	A rule number to subject to detailed analysis when the analyzer is being used in RULE mode.

## ASCII Analyzer Display Modes

This setting affects what is seen in the Activity window. The current display mode is reflected in the ASCII Selector window.

When logging is active, whatever is seen in the Activity window is also appended to a text file named ASCLOG.REP. Current state is reflected in the ASCII Selector window as LOG OPEN or CLOSED. Logging is beneficial because most ASCII alarms will generate more text than can be seen on the screen at one time.

Function Key	Description
F1 (Pause)	Halts the Activity display. ASCII processing continues but analysis stops.
F2 (Clear)	Clears the Activity display.
F3 (Text)	Shows incoming ASCII in text form, color-coded to distinguish soft separators (green) and hard separators (yellow). Spaces are indicated by a bar or square. Control characters are not explicitly shown.
F4 (Hex)	Shows incoming ASCII in hex form, color-coded to distinguish soft separators (green), hard separators (yellow), and the line terminator character (red). All characters including control characters are shown.
F5 (Rules)	Shows the result of executing pattern recognition command lines for the selected numbered rule, along with the associated input text. If extraction is successfully completed, general extraction results are also shown regardless of the numbered rule currently selected.
F6	Toggles logging to ASCLOG.REP on and off.
F10/Esc=Edit	Permits channel (port) and selected rule number to be changed.
F10/Esc=Exit	Exits ASCII analyzer mode, terminates logging, returns to the alarm summary screen.



```

ASCII Processor Activity
2A 2A 35 35 20 52 45 50 54 3A 43 45 4C 4C 20 32 32 31 20 41 4C 41 52 40 20 53
43 41 4E 4E 49 4E 47 00 0A 20 20 20 20 20 53 43 41 4E 20 50 4F 49 4E 54 3A 4F
46 46 53 45 54 20 31 2C 20 42 49 54 20 32 00 0A 20 20 20 20 20 41 4C 41 52 40
3A 20 49 4E 54 52 55 53 49 4F 4E 20 41 4C 41 52 40 00 0A 20 20 20 20 20 53 54
41 54 45 3A 20 4F 46 46 20 4E 4F 52 40 41 4C 00 0A 20 20 20 20 20 44 45 56
49 43 45 20 20 20 54 54 59 26 00 0A 00 0A 30 37 2F 32 33 2F 39 36 20 35 35 20
23 38 35 35 36 31 39 00 0A

ASCII Selection
Channel      : 9
Rule         : 52
HEX
LOG CLOSED
500

Page Index
> A E I M Q U V: D
  B F J N R V A: P
  C G K O S W S: S
  D H L P T X P:X
STAND :30 Silenced:0
COS   :44 Off Line:0

F1=Pause, F2=Clear, F3=Text, F4=Hex, F5=Rule, F6=Log, F10/Esc=Edit

```

Fig. M6.32 - Hex mode screen

```

ASCII Processor Activity
[MATCH]      **55 REPT:CELL 221 ALARM SCANNING
[MATCH]      SCAN POINT:OFFSET 1, BIT 2
[MATCH]      ALARM: INTRUSION ALARM
[MATCH]      STATE: OFF NORMAL
[MATCH]      DEVICE - TTY&
[PATTERN LOCK FOR RULE 50]
[PROCESS DIRECTIVE: AUTO>ECPSET]
[RULE 50 KEY] 009000221:1,:2:SET
[FOUND ACTION]
[EXTRACTION PHASE ENDED (1)]
[NOT MATCH] 07/23/96 55 #855619

ASCII Selection
Channel      : 9
Rule         : 52
RULES
LOG CLOSED
500

Page Index
> A E I M Q U V: D
  B F J N R V A: P
  C G K O S W S: S
  D H L P T X P:X
STAND :30 Silenced:0
COS   :44 Off Line:0

F1=Pause, F2=Clear, F3=Text, F4=Hex, F5=Rule, F6=Log, F10/Esc=Edit

```

Fig. M6.33 - Rules mode screen

# Auto-Databasing ASCII

## Overview

Auto-Databasing ASCII is an extension to the standard T/Mon ASCII processing modules. It uses most of the methods and capabilities of standard processing, and you should be familiar with the contents of the ASCII Processor (sections M6-1 to M6-68) before going on to this section of the manual. In particular, everything in the Message Processing phase still applies when using Auto-Databasing—this includes defining ASCII device types and writing rules in the ASCII processing language to recognize and extract text from ASCII messages.

Auto-Databasing ASCII processes alarms in exactly the same way as the standard version: keys are generated from incoming messages, compared with action strings that have been databased for every ASCII alarm in the system, and an alarm is set if a match is found. The difference is in the way alarm definitions and action strings are entered in the first place. In standard databasing they are typed in manually, which can be a massive, expensive, and error-prone undertaking. In Auto-Databasing they are created from incoming messages themselves. If a particular alarm has not yet been entered in the database it is added automatically. Over time, the database populates itself.

Because entire alarms are created, all attributes of an alarm have to be derived from the incoming ASCII text. This includes severity, text messages, paging parameters, and windows in which to display the alarm. There is an added burden on the message processing phase because additional information has to be extracted to define these parameters. To support this, several features are added to the standard message processing capabilities:

- The number of Key Slots is increased from 14 to 30. Slots 1-9 are still Action Slots and 10-14 are Site Slots, but no special meaning is attached to the remaining slots. They temporarily hold text that is being extracted from a message and can be used in any way you want. The additional slots are loaded via the conventional \K commands.
- A number of additional keys are created. These include keys for alarm description, status, level, text message, pager profile, and six different window keys (called categories).
- A matrix is added to copy slot contents into keys in any arbitrary sequence. For instance, an alarm description might be generated from slots 22, 7, and 16, in that order.
- A number of tables are added to assign end results to the various special-purpose keys (these are similar to the standard Action String tables that generate alarms from Action Keys). For instance, a device might report severity as Big Problem, Little Problem, Nuisance, or Ignore. In the Level table, keys based on these values would generate alarm levels A, B, C and D.
- A single directive, \!AUTO, has been added to the ASCII processing language. It makes auto databasing take place when keys are generated.



The only purpose of Auto-Databasing is to create a point definition in the alarm database, much the same as you would when filling out a line in the standard Point Definition screen that is used throughout T/Mon. It only does this when an incoming message gives rise to an alarm that isn't there already. Of course, after that it's there, so none of this processing applies. **Everything described in this module happens only the first time a message triggering a previously un-databased alarm arrives.**

The following pages detail the additional steps required to set up an Auto-Databasing system. See section M6-1 for help in setting up the basic ASCII process.

## Slots and Keys

Slots are temporary holding areas for strings extracted from incoming ASCII messages. Predefined strings (literals) can also be placed in slots by various processing language commands.

Auto-Databasing makes use of the same slots as standard ASCII and adds some additional ones for general-purpose use. The following slots are available:

- Key slots                numbered 1-30, addressed by \K commands. These are divided into:
  - Action slots*        numbered 1-9
  - Site slots*            numbered 10-14
  - Other slots*          numbered 15-30
- Pager slots            numbered 1-9, addressed by \P commands.
- Variable slots        numbered 1-9, addressed by \V commands.

**Keys** are strings derived from an incoming message to express significant parts of the message, usually in highly abbreviated form. They are used to look up associated values. For instance, when you look up a person's number in the phone book, the person's name is the key and the phone number is the value. In ASCII processing, several different keys are created for different purposes. The following are created in standard ASCII processing:

- Action Key            built from Action Slots, value is a particular alarm
- Site Key              built from Site Slots, value is a particular site

Standard ASCII processing can also produce a pager Asc Extract, which is a string built from pager slots and can be included in a pager message.

Auto-Databasing adds the following keys, all of which can be built from any combination of Key Slots. They are used to determine what entries to make in a standard T/Mon point definition line. These tables have, depending on the key type, a maximum of 100-999 entries to restore keys to Alarm field entries. An ASCII table should be used for cases having more than the maximum key to field associations — see section M6-35 (ASCII Tables) for more information.

- Status Key                   value is Alarm or Clear
- Level Key                   value is severity A-D
- Text Message Key       value is a text message number
- Pager Profile Key       value is a pager profile number
- Category Keys           value is a window number – 6 different keys and values are available.

Auto-Databasing also produces an Alarm Description, which is a string built from any combination of Key Slots and goes in the standard Alarm Description field.

Auto-Databasing starts out just like standard message processing. You need to recognize the message and extract significant parts to slots. The only difference is that, using ordinary message processing commands, you need to extract sufficient information to create all of the keys and strings listed above.

- The Action Key is built by concatenating key slots 1-9 in order.
- The Site Key is built by concatenating keys slots 10-14 in order.
- The pager Asc Extract is built by concatenating pager slots 1-9 in order.
- For all the rest, it is sufficient to simply have their components stored in key slots somewhere. One slot can be used in several keys. Just do some bookkeeping to keep track of what's going where — see section A-28 for ASCII Worksheet example. The following pages show how to assemble the keys and values.

## Key Mapping

To reach this page from the Master Menu, select Files > ASCII Devices > ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Key Mapping — see Figure M6.34.

This screen determines how Key Slot contents will be arranged into keys. The Key Slots themselves must be loaded during the extraction phase by using normal \K commands. When extraction is complete and key generation takes place, the processor refers to the mapping defined here to build the various keys needed for Auto-Databasing.

- The column labeled **Type** contains the name of the key being built. It may be necessary to scroll to see all of the available keys.
- The numbers across the top represent sequential positions within a key.
- **Action Keys**, **Site Keys**, and pager **Asc Extracts** do not appear in this table because they are always built in slot order from predesignated slots.

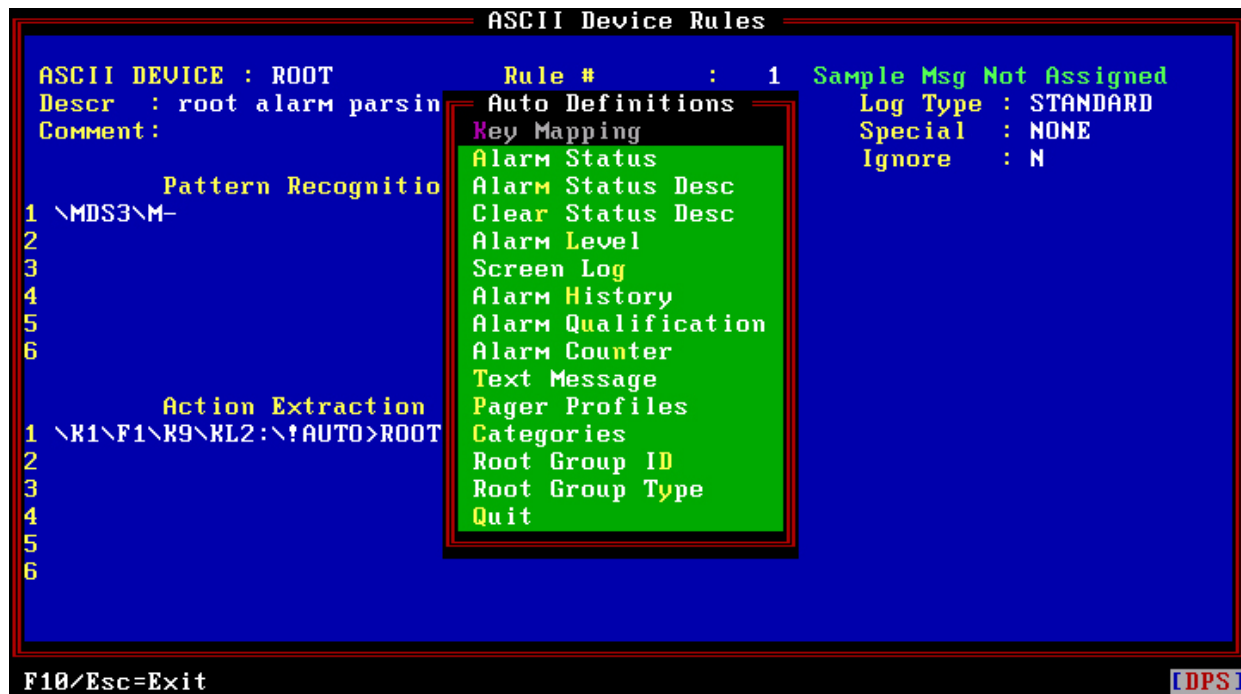


Fig. M6.34 - Press F7 to open the Auto Definitions menu

ASCII Key Map Definition							
Type	#1	#2	#3	#4	#5	#6	#7
Alarm Desc	16	2	1				
Status	5						
Level	15						
Text Message	15						
Category 1	15						
Category 2							
Category 3							
Category 4							
Category 5							
Category 6							

Enter the key number for position 1 (1-30,Blank=None).

F8=Save, F10/Esc=Exit

Fig. M6.35 - ASCII Key Map Definition screen

Table M6.AH – Fields in the ASCII Key Map Definition screen

Field	Description
Key Number	Key Slot number assigned to a particular position within a key. Slot contents are connected together in position order to form their respective keys. Empty slots and unassigned positions are ignored. Slots can be used in more than one key. Example: the Alarm Description built from the screen above would consist of the contents of key slots 16, 2, and 1 connected together in that order.

## Alarm Status

To go to the Auto ASCII Definition–Alarm Status screen go to the Master Menu and select Files-ASCII Devices-ASCII Rules. Then scroll to the header rule (rule 0) for the device type being edited. Press F7 to open the Auto Definitions menu — see Figure M6.34, then select Alarm Status.

The purpose of status is to determine if the Action Key built for an alarm that has not yet been auto databased is an alarm or clear. **Note:** Unlike Alarm Level, Text Message, Pager Profiles, and Categories, the “Alarm Status” does not define part of the point.

The Auto ASCII Definition–Alarm Status screen (see Figure M6. 32) allows you to assign status values to all possible status keys that could be obtained from messages sent by this device type. There are only two possible status values: ALARM and CLEAR. When a status key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, and the state is ALARM, processing continues to add the point to the database and fill out the SET line in the ASCII

Action definition for this point. If it is CLEAR it is ignored – auto points get added only on a SET. See the \!AUTO command, page M6-77, to see how the CLEAR line gets added to the ASCII Actions list.

Entries are compared in numeric order and cannot exceed 100. If more than one match is possible, the processor will stop on the first one it finds. **If no match is found, an ALARM state is assumed.**

Auto ASCII Definition – Alarm Status			
Entry	String	OP	Status
1	SET.....	EQUAL	ALARM
2	CLR	EQUAL	CLEAR
3			
4			
5			
6			
7			
8			
9			
10			
Enter target string			
F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit			

Fig. M6.36 - Auto ASCII Definition–Alarm Status screen.

Table M6.AI - Field names and descriptions for the Auto ASCII Definition–Alarm Status screen

Field	Description
String	A possible status key, as generated by the extraction rules and key mapping.
OP	The type of comparison to be performed between an actual generated status key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Status	ALARM or CLEAR. Use Tab to select.

## Alarm Level

This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Alarm Level

This screen assigns alarm level values to all possible level keys that could be obtained from messages sent by this device type. There are four possible alarm level values: A, B, C, D. When a level key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding level is assigned to point being added.

Entries are compared in numeric order to a maximum 100 entries. If more than one match is possible, the processor will stop on the first one it finds. **If no match is found, the default level A is assigned.**

Auto ASCII Definition - Alarm Level			
Entry	String	OP	Level
1	CR.....	EQUAL	A
2	MJ	EQUAL	B
3	MN	EQUAL	C
4	NA	EQUAL	D
5			
6			
7			
8			
9			
10			
Enter target string			
F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit			

Fig. M6.37 - Auto ASCII Definition-Alarm Level screen

Table M6.AJ - Fields in the Auto ASCII Definition-Alarm Level screen

Field	Description
String	A possible level key, as generated by the extraction rules and key mapping.
OP	The type of comparison to be performed between an actual generated alarm level key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Level	A, B, C, or D (Critical, Major, Minor, or Status)

## Text Message

This screen assigns text message values to all possible text message keys that could be obtained from messages sent by this device type. The value must be the number of a text message that has already been defined under Files – Text/Messages. When a text message key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding message number is assigned to point being added..

Entries are compared in numeric order to a maximum 999 entries. If more than one match is possible, the processor will stop on the first one it finds. **If no match is found, the default 0 (no message) is assigned.**

Auto ASCII Definition – Text Message			
Entry	String	OP	Message Number
1	CR	EQUAL	1
2	.....		
3			
4			
5			
6			
7			
8			
9			
10			
Enter target string			
F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit			

**Fig. M6.38 - Auto ASCII Definition–Text Message screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Text Message.

**Table M6.AK - Fields in the Auto ASCII Definition–Text Message screen**

Field	Description
String	A possible text message key, as generated by the extraction rules and key mapping.
OP	The type of comparison to be performed between an actual generated text message key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Message Number	The number of an existing text message, defined under Files-Text/Message. Leave blank for none.

## Pager Profile

This screen assigns pager profile values to all possible pager profile keys that could be obtained from messages sent by this device type. The value can be any pager profile number 1-99, or 0 for none. When a pager profile key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding pager profile is assigned to the point being added.

Entries are compared in numeric order to a maximum 999 entries. If more than one match is possible, the processor will stop on the first one it finds. **If no match is found, the default 0 (no pager profile) is assumed.**

Entry	String	OP	Pager Profile
1	14*.....	EQUAL	1
2	14**	EQUAL	2
3	14***	EQUAL	3
4			
5			
6			
7			
8			
9			
10			

Enter target string

F1=GOTO, F3=BLANK, AF3=Delete, AF4=Insert, F8=Save, F10/Esc=Exit

**Fig. M6.39 - Auto ASCII Definition–Pager Profile screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Pager Profiles.

**Table M6.AL - Fields in the Auto ASCII Definition–Pager Profile screen**

Field	Description
String	A possible text message key, as generated by the extraction rules and key mapping.
OP	The type of comparison to be performed between an actual generated text message key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Pager Profile	Pager profile number 1-99, or 0 if none.



## Categories (Windows)

This screen assigns windows to all possible category # keys that could be obtained from messages sent by this device type. A single point could appear in several different windows, so six different category keys have been provided. Each key can be assigned to any valid window number on your system. When a category # key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding window is included in the set of windows assigned to the point being added.

Entries are compared in numeric order to a maximum 500 entries. If more than one match is possible, the processor will stop on the first one it finds. **If no match is found, no window is added (all points show in default window 1).**

Entry	String	OP	Window
1	CR.....	EQUAL	2
2	MJ	EQUAL	3
3	MN	EQUAL	4
4	NA	EQUAL	5
5			
6			
7			
8			
9			
10			

Enter target string

F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit

**Fig. M6.40 - Auto ASCII Definition–Category 1 screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, Categories, Category number

**Table M6.AM – Fields in the Auto ASCII Definition–Category # screen**

Field	Description
String	A possible text message key, as generated by the extraction rules and key mapping.
OP	The type of comparison to be performed between an actual generated text message key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Window	A valid window number for your system.

## Screen Log

This screen assigns the point value for logging to the screen. When a log key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding log value is assigned to the point being added. If no match is found, the default log value is set to YES. It will be logged onto the screen.

Entry	String Value	OP	Log
1	NOLOG.....	EQUAL	NO
2	LOG	EQUAL	YES
3			
4			
5			
6			
7			
8			
9			
10			

Enter target string

F1=GOTO, F3=BLANK, AF3=Delete, AF4=Insert, F8=Save, F9=Help, F10/Esc=Exit

**Fig. M6.40 - Auto ASCII Definition–Log To screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Screen Log.

**Table M6.AN – Fields in the Auto ASCII Definition–Log To screen**

Field	Description
String	A possible log key, as generated by the extraction rules and key mapping.
OP	Type of comparison to be performed between an actual generated alarm log key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Log	YES or NO. (selectable by pressing TAB)

## Alarm History

This screen assigns the point value for creating a history log entry. When a history key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding history value is assigned to the point being added. If no match is found, the default history value is set to YES. It will create a history entry.

Entry	String Value	OP	History
1	HISTORY	EQUAL	YES
2	NOHISTORY	EQUAL	NO
3	.....		
4			
5			
6			
7			
8			
9			
10			

Enter target string

F1=GOTO, F3=BLANK, AF3=Delete, AF4=Insert, F8=Save, F9=Help, F10/Esc=Exit

**Fig. M6.41 - Auto ASCII Definition–Alarm History screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Alarm History.

**Table M6.AO – Fields in the Auto ASCII Definition–Log To screen**

Field	Description
String	A possible history key, as generated by the extraction rules and key mapping.
OP	Type of comparison to be performed between an actual generated alarm log key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
History	YES or NO. (selectable by pressing TAB)

## Alarm Qualification

This screen assigns the qualification value for point being added. When a qualification key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding qualification will be assigned to the point being added. If no match is found, qualification will be set to zero.

Entry	String Value	OP	Qualification
1	1MIN	EQUAL	1M
2	20MIN	EQUAL	20M
3	15MIN	EQUAL	10
4	3HOURS	EQUAL	3H
5	.....		
6			
7			
8			
9			
10			

Enter target string

F1=GOTO, F3=BLANK, AF3=Delete, AF4=Insert, F8=Save, F9=Help, F10/Esc=Exit

**Fig. M6.42 - Auto ASCII Definition–Alarm Qualification screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Alarm Qualification.

**Table M6.AP – Fields in the Auto ASCII Definition–Log To screen**

Field	Description
String	A possible qualification key, as generated by the extraction rules and key mapping
OP	Type of comparison to be performed between an actual generated alarm qualification key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Qualification	Qualification value. Format is usually xxM, xxH or xxQ. Note: Press F9 while on this field for more detail.

## Alarm Counter

This screen assigns the counter qualification value for point being added. When a counter key is generated from an incoming message, it is compared with the strings listed on this screen. If a comparison passes, the corresponding counter will be assigned to the point being added. If no match is found, counter will be set to zero.

Entry	String Value	OP	Counter
1	10IN30MIN	EQUAL	30M/10
2	5IN15MIN	EQUAL	10/5
3	1HOUR	EQUAL	1H/1
4	.....		
5			
6			
7			
8			
9			
10			

Enter target string

F1=GOTO, F3=BLANK, AF3=Delete, AF4=Insert, F8=Save, F9=Help, F10/Esc=Exit

**Fig. M6.43 - Auto ASCII Definition–Alarm Counter screen.** This page is reached from the Master Menu by selecting Files-ASCII Devices-ASCII Rules, scroll to the header rule (rule 0) for the device type being edited, select F7=Auto, then select Alarm Counter.

**Table M6.AQ – Fields in the Auto ASCII Definition–Log To screen**

Field	Description
String	A possible counter key, as generated by the extraction rules and key mapping.
OP	Type of comparison to be performed between an actual generated alarm counter key and the string listed on this line. Use Tab to select. EQUAL passes only if the key is identical to the string. CONTAINS passes if the key appears anywhere within the string. STARTS WITH passes if the string begins with the key.
Counter	YES or NO. (selectable by pressing TAB)

# The \!AUTO Command

Table M6.AR - Language Reference—Extraction Phase

The Auto-Databasing module adds the following directive to the standard ASCII Processing Language		
Command	Description	
\!AUTO>tbl	Purpose	<p>Informs the ASCII processor that Auto-Databasing is to take place when keys are generated from the message being processed. tbl is the name of an ASCII table that will be executed after the SET Action String is created. The CLEAR Action String is created from the table result (see next page).</p>
	Result	<p>When keys are generated, if a matching Action String cannot be found in the current alarm database and this message is setting an alarm, a new point will be added to the database after the highest-numbered point in the highest-numbered display already defined for the current port. When the highest display is full (64 points) it will start a new display one number higher. The SET Action String for the new point is assigned the same value as the Action Key that was just generated. Table tbl is then called; it operates on whatever is currently in the slots and modifies them into whatever would be there if a message arrived to clear this same alarm. A new Action Key is generated from the result and is assigned to the CLEAR Action String for the new alarm.</p> <p><b>Note:</b> Auto common does not process auto keys and database points.</p>
	Notes	<p>This command can appear anywhere among extraction commands before key generation starts (key generation normally occurs when extraction is complete, but could also happen in a loop or table). In table tbl, set Gen Key to No (the auto processor will generate the key)</p>
	<b>Example</b>	
	Objective	<p>Use Auto-Databasing with messages being processed under the current rule, using table TL1 to modify the generated SET key into a CLEAR key.</p>
	Command	<p>\F1\K1\K10\KL2:\KL4:\!AUTO&gt;TL1</p>
	Result	<p>If an Action String cannot be found for a SET key generated under this rule, a new point will be added to the database using the Auto-Databasing definitions for this device type</p>

**Notes on the Table referenced in an \!Auto Command:**

The CLEAR Action Key for an auto-database alarm has to be assigned at the same time the SET Action Key is defined because there is otherwise no way to associate a clear message with a particular alarm. The problem is that the ASCII processor does not have a clear message to work from when it is databasing the new point. The solution is to load slots in the usual manner to build the SET key. Then use an ASCII table to modify the slots into whatever they would contain if a corresponding clear message arrived and build the CLEAR key from it. Of course, you need to know what the clear message looks like and what the resultant slot contents would be. Fortunately, much of the time, set and clear messages are identical except for a single word that indicates status. In such a case, put that word in an action slot and use the table to change it from its set value to its clear value. Only a single table entry is required.

ASCII Tables			
Table Name	: EX7SET	Entry #	: 1
Descr	: CHANGES SET KEY TO CLR		
Condition #1			
Key: K5	Type: STRING	OP: =	VALUE: SET
AND Condition #2			
Key:	Type:	OP:	:
TRUE Action			
Key: K5	New Value: CLR	Gen Key: N	
FALSE Action			
Key:	New Value:	Gen Key:	
F)ind, E)dit, D)elite, N)ext, P)rev, M)ove, R)ead, Q)uit : _			
F10/Esc=Exit			

**Fig M6.44 - Table with Set-to-Clear Operation entered**

In a more complex situation, it may take several table entries to accomplish the necessary translation. A workable approach is to:

1. Obtain samples of alarm and clear messages suitable for use with the ASCII debugger.
2. Create the rules to use with each status (in many cases, the same rule will work for both alarm and clear). Also create the table you will use with the \!AUTO command.
3. In the debugger, use the clear message as input and view the resultant action key.
4. In the debugger, use the alarm message as input and view the CLEAR key resulting from auto processing.
5. The results of steps 3 and 4 should be the same. Adjust your rules or table as needed to achieve this result.

## Remote Port Definition

Remote Port Definition is the same under Auto-Databasing as it is under standard ASCII databasing. Refer section M6-55 for more information.

- There should be no entry in the Alarm Alias Port or the Template Port fields.
- Enter Y (yes) in the Auto-Databasing field.

## ASCII Input Device Definition

Remote Device Definition is the same under Auto-Databasing as it is under standard ASCII databasing. Refer to sections M6-57 and M6-58 for more information.

- Note that the device address must be 0 on the first defined device.
- Under Auto-Databasing, an address on the port being databased corresponds to a site, and the site in turn corresponds with one of the possible Site Keys that gets built in key slots 10-14.
- You should define additional devices so there is an address available for each possible Site Key that may be generated.
- In addition, you should define a dummy site and alarm to catch any undefined site keys that may be received. These will 'fall through' all the other sites and be databased immediately after the highest alarm currently defined on the port. Simply create a high address (usually 800) and give it site name UNDEFINED. Then follow instructions for ASCII Actions and Site Keys outlined below.

1. Enter address 800 in the Remote Device Definition screen.

2. Press F7 to show the Auto-ASCII Site Definition screen.

3. Go to address 800 and type in a dummy site key.

4. Assign a high window number.

5. Press F10 to return to the Remote Device Definition screen.

6. Press F2 to show the ASCII Actions (Table) window.

7. Press Edit and enter an Dummy Action String for Point 1, SET.

8. Define window 701 in the Windows Definition screen.

9. Undefined alarms will be reported in Windows 701-705 (using Row/Site).

**Fig. M6.45 - Dummy Address put undefined Site Keys in Address 800.**

**Note:** will add point to first site without a Auto Site key.

### Clear All

All Action keys and points, or partial by address can be deleted by using the following commands:

1. Parameters > Remote Ports > press F)ind and enter the appropriate ASCII port number
2. Press F1 to view device Then press F7 for Auto.
3. Press F6, Toggle Mark, and press F7 ,Toggle Mark all, to select points.
4. Press Alt-F1 to delete the points and actions for the marked address on the ASCII port.



## ASCII Action Definitions

Press F2 while in the Remote Device Definitions screen to view the ASCII Action Definitions screen. (Make sure the Port and Address are correct for the Auto ASCII Device being defined.) The fields in this screen will be automatically filled when ASCII messages are processed (Figure M6.42). It should be empty at this point. Press “D” then “Y” to clear any entries. Press F10 to return to the Remote Device Definition screen.

Notes on ASCII Action Concepts:

1. Action items are maintained by the computer.
2. Do not change or edit any entries.
3. Do not mix Auto ASCII and regular (manual) ASCII in the same display.
4. When the first attempt to program Auto ASCII results in an incorrect action string, delete the display from both the ASCII Action Definitions screen and the Point Definition screen.

**Note:** see section M6-80 for clear all information.

ASCII Action Definitions		
Display : 1		
Point	Type	Action String
1	SET	FRESNO:FRONT DOOR:SET
	CLEAR	FRESNO:FRONT DOOR:CLR
2	SET	
	CLEAR	
3	SET	
	CLEAR	
4	SET	
	CLEAR	
5	SET	
	CLEAR	
F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :		

**Fig. M6.46 - ASCII Action Definitions screen as seen after an Auto ASCII Alarm has been processed.**

## Auto-ASCII Site Definition

This page is reached by selecting function key F7=Auto while on the Remote Device Definition screen.

Address	Site Name	Site Key	Site Window	Window Mode
0	YALE	FRESNO	6	ROW/SITE
1	BAKERSFIELD	BAKFLD	11	ROW/SITE
2	VISALIA	VISALIA	16	ROW/SITE
3	ORANGE COVE	ORGC OV	21	ROW/SITE
4	TERRIBELLA	TERBEL	25	ROW/SITE
5	MERCED	MERCED	31	ROW/SITE
800	UNDEFINED	NEW SITES.....	701	ROW/SITE
801	AUTO DB			
802	AUTO DB			

Enter site key.

F3=Blank, F8=Save, F10/Esc=Exit

Fig. M6.47 - The Site Key is entered in the Auto ASCII Site Definition screen.

Table M6.AS - The Site Key is entered in the Auto ASCII Site Definition screen

Description	
Site Key	The key for this site, as generated by the extraction rules in key slots 10-14. The tilde symbol (~) may be used as a wild card at the end of this entry, so that it will match any extracted key that starts with the entry. Example: if you enter M001~ then keys M001 M001A M001B M001C1 will all show at this site.
Site Window	The window number for all alarms at this site (must also be entered on the Window Definition screen, reached from the Master Menu by selecting Files-Windows)
Window Mode	<ul style="list-style-type: none"> <li>• If NORMAL, all alarms at this site appear in the Site Window assigned above.</li> <li>• If ROW/SITE, all alarms at this site appear in the Site Window assigned above, plus the next 4 windows will receive alarms with severity A, B, C, and D. When using this mode, select a Site Window on the left side of the screen. (Windows must also be entered on the Window Definition screen)</li> </ul>

Alarm Summary				
ALL ALARMS	CRITICAL	MAJOR	MINOR	STATUS
FRESNO...	BAKERSFIELD	VISALIA	ORANGE COVE	TERRIBELLA
TRANQUILITY	HURON	PASO ROBLES	KETTLEMAN CITY	ATASCADERO
SAN LUIS	LOS BANOS	MADERA	YOSEMITE	YOSEMITE FALLS
BAGLEY	OAKDALE	JAMESTOWN	CLOVIS	TOLLHOUSE
ACADEMY	AUBERRY	SHAVER	GRANT GROVE	HUME
COS : 3      STANDING : 3      PRINTER : YES				

Monitor screen using Site Window mode

Alarm Summary				
ALL ALARMS	CRITICAL	MAJOR	MINOR	STATUS
FRESNO...	FRESNO CR	FRESNO MJ	FRESNO MN	FRESNO ST
BAKERSFIELD	BAKERSFLD CR	BAKERSFLD MJ	BAKERSFLD MN	BAKERSFLD ST
VISALIA	VISALIA CR	VISALIA MJ	VISALIA MN	VISALIA ST
ORANGE COVE	ORANGE COVE CR	ORANGE COVE MJ	ORANGE COVE MN	ORANGE COVE ST
TERRIBELLA	TERRIBELLA CR	TERRIBELLA MJ	TERRIBELLA MN	TERRIBELLA ST
COS : 3      STANDING : 3      PRINTER : YES				

Monitor screen using Row/Site Window mode

Fig. M6.48 - Monitor screens are different in Site vs. Row/Site window modes

Point Definition				
Port	Addr	Disp	Display Desc :	
P L H L S R			ASCII INPUT	
o o s e t v				
Pt	l g t v s s	Description	Fail	Clear
1	B L H D A N	FRONT DOOR:NA,OPEN,,":FRESNO		
2				
3				
4				
5				
6				
7				
8				

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

Message

F10/Esc=Exit

Fig. M6.49 - The Site key is entered in the Auto ASCII Site Definition screen

## Point Definition

Press F1 while in the Remote Definition screen to view the Point Definition screen. Make sure the Port and Address are correct for the Auto ASCII device being defined. The fields in this screen will be automatically filled when ASCII messages are processed (Figure M6.41). Description, Status, Level, Text message, and windows will be determined by the Auto ASCII rules. Defaults will be used for POL, LOG, HST, STS and RVS fields. The Fail and Clear fields will be empty. All fields should now be empty. Press “D” then “Y” to clear any entries. Press F10 to return to the Remote Device Definition screen.

## Conclusion

Example is now complete. Press F10 three times <Enter> to return to the Main menu. Perform any other databasing then initialize and monitor.

**This page intentionally left blank.**

# Software Module 7

## E2A Interrogators and Responders

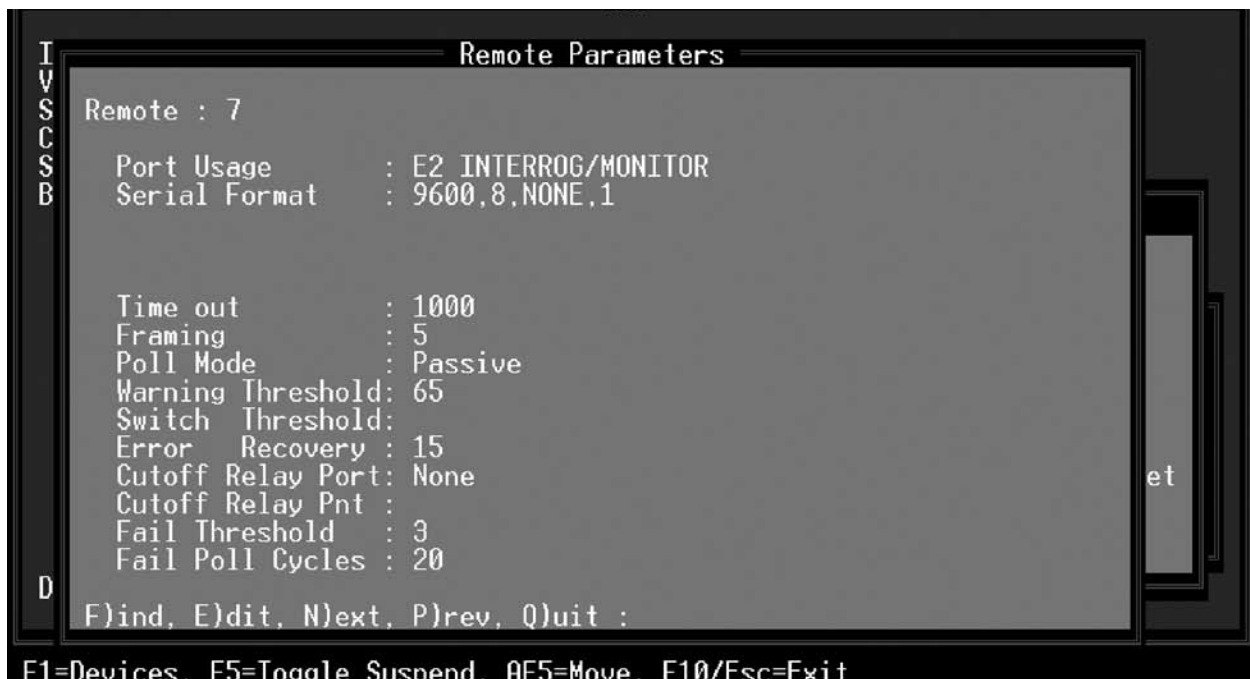
### E2A Interrogators

Interrogators allow data to be brought into the system. With Interrogators, you specify the display list of the items you want to have polled. You can show alarm points on the normal T/MonXM screens under COS windows and Live alarms. In addition, alarm points may also go out responder ports. When you define the data-bases it is important that you define the Interrogators first and then define the Responders.

An E2A Interrogator software module must be installed before you can access the E2A Interrogator. Refer to Section 2 - Software Installation for installation procedures.

To define a remote port for communication to E2A equipment, select Remote Ports from the Parameters menu and then select E2 Interrogator at the Port Usage field.

An example of the Remote Parameters screen defined for E2 Interrogators is illustrated below:



**Fig. M7.1 - Select E2 Interrog/Monitor for the port usage field**

The fields on the Remote Parameters screen are explained as follows:

#### Port usage

Valid port types are E2 Interrogator/Monitor, and Halted. Use Halted (default) if no device is connected to the communication port.

**Serial Format**

Baud rate, word length, parity, and stop bits settings.

**Time Out**

The time T/Mon will wait before failing a poll if there is no response. Acceptable values are 0-9999 milliseconds.

**Framing**

Select either “A” for DPS E2A Converter Shelf or the Dantel 46036 mode E System Interface Card™, or select “5” for the Dantel 46037 mode E System Interface Card™.

**Poll Mode**

Select the poll mode. Valid selections are “P” for Passive only, “M” for Master only, and “C” for Combined polling.

**Note:** Passive Mode will listen for other devices polling E2 remotes and display the status of those remotes, and alarm points. No polling from the T/Mon will occur in Passive Mode.

**Warning Threshold**

The Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds.

**Switch Threshold**

The field is only accessible when combined polling mode is selected. After the switch threshold seconds have gone by without any activity being detected, if defined as “Combined Mode,” T/Mon will switch from Passive to Active polling and assume Master. Valid values are 2-999 seconds.

**Error Recovery**

Enter the recovery time for line abnormalities. Valid entries are 2-99 seconds.

**Cutoff Relay**

Enter the cutoff relay to use. Valid entries are 1-4, and “0” for none

**Fail Poll Cycles**

The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled.

See Table M7.A for default remote parameters and Table M7.B for device part numbers.

**Note:** the Dantel 46036 mode E System Interface Card, and the Dantel 46037 mode E System Interface Card are trademarks of Dantel® Inc.

**Table M7.A - E2A Interrogator/Monitor parameter defaults**

Field	Description
Port usage	E2 INTERROG/MONITOR
Serial Format	9600, 8, None, 1
Time out	1000
Framing	5
Poll Mode	Passive
Warning Threshold	65
Switch Threshold	70
Error Recovery	15
Cutoff Relay	None
Fail Poll Cycles	20

**Note:** E2A operations require some form of external interface device. DPS Telecom offers the E2A Mediation Device card for the Modular Alarm System and the E2A Test Set Software and Interface. See Table M7.B below for model numbers.

**Table M7.B - E2A device part numbers**

Model Number	Description
D-MAS-46033-V2	E2A Mediation Device Module with RS422/485 subassembly
D-MAS-46033-V3	E2A Mediation Device Module with 202 modem subassembly
D-PG-125-10C-00	T/E2 and T/BOS Test Set with Test Interface
D-SW-110-14A-0X	T/E2 Telemetry Test Set Software
D-MAS-46102-10B-04	E2A Converter Shelf with chassis lock
D-MAS-46102-10B-54	E2A Converter Shelf without chassis lock



## Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined E2 Interrogator/Monitors will bring you to the Remote Device Definition screen. An example of the Remote Device Definition screen is illustrated below:



Fig. M7.2 - Remote Device Definition screen

Table M7.C - Fields in the Remote Device Definition screen

Field	Description
Port	Remote Port defined for E2A Interrogator
Address	Address of the Device
Description	Optional Description
Site Name	Site name stamped on every event from remote.
Displays	Valid displays are 1-64.
Poll Mode	Enter the Polling Type. Valid entries are "A" for Alarm, "H" for Hybrid, "S" for Status, and "V" for VGS. <b>Note:</b> The VGS Table appears when VGS is selected and you are requested to enter the group size. Valid group sizes are 0-16.
Refresh Rate	How many polls occur before two status poll used with alarm and hybrid polling.
Verify Rate	The frequency rate at which the alarm will be polled to verify its status. After a specified number of conventional polling cycles, T/MonXM will execute the verification cycle. Valid frequency rates are 0-9999. This field defaults to 0.
Log Undefined	Select Yes or No to log undefined alarms.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]

Table M7.C continues on following page.

Table M7.C - Fields in the Remote Device Definition screen (continued)

Field	Description
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

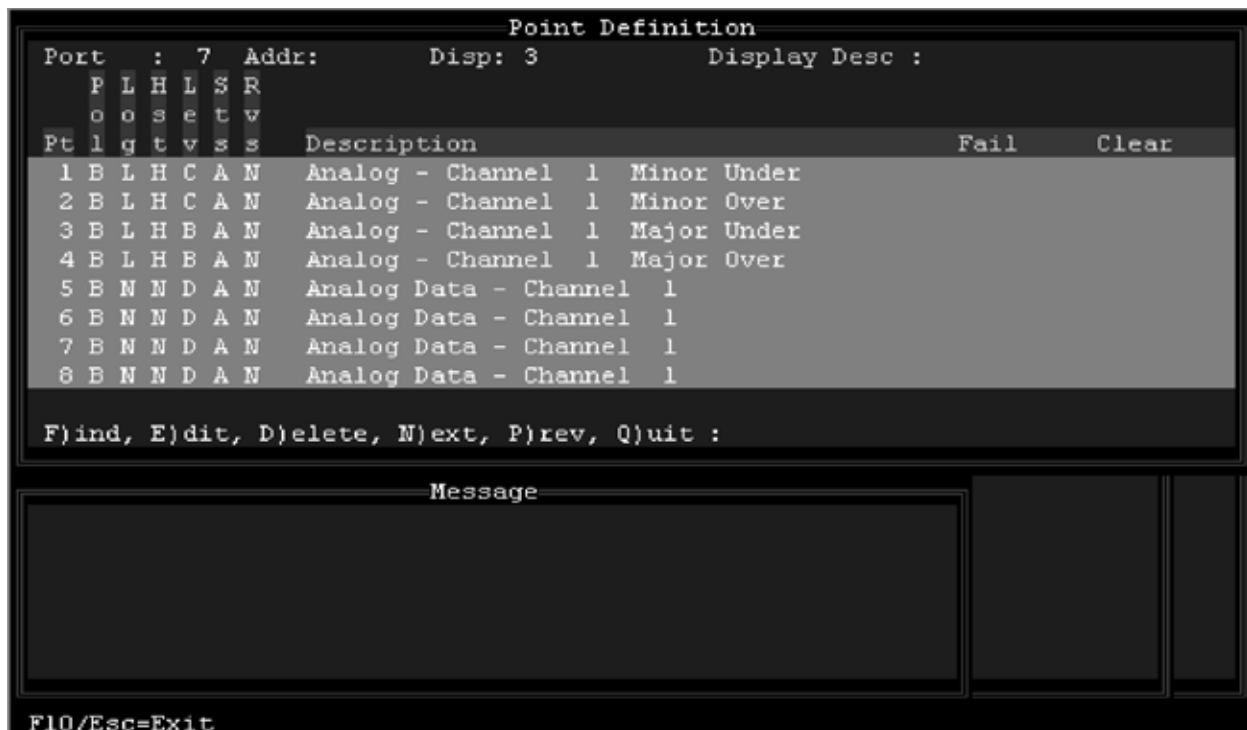


Fig. M7.3 - Point Definition screen

## Point Definition

Pressing F1 (Points) from the Remote Device Definition screen will bring you to the Point Definition screen. Define point attributes for E2A Interrogators in this screen. For more information on Point Definition, see Section 10 (Point Definition Tutorial).

This option allows the user to assign attributes and English descriptions to individual alarm points within the selected displays of the remote. Defining alarm point definitions are done on a display-by-display basis. Begin by entering the remote display number from which the remote stores the alarm point information.

## Internal Alarms

Entering F3 (Internal Alarms) from the Remote Device Definition screen for defined E2 Interrogator/Monitors will bring you to the Device Internal Alarm Assignment screen. An example of the Device Internal Alarm Assignment screen defined for E2A Interrogators is illustrated in Figure M7.4.

For more information on Internal Alarms see Section 14.

```

Device Internal Alarm Assignment

Port : 7

Address Dev      Description                               Fail      Offline
-----
1  ETEL                               11.1.1..  11.1.2

Enter internal point (addr.display.pnt) (blank=none) (address range: 11-13)

F8=Save, F10/Esc=Exit
  
```

Fig. M7.4 - Device Internal Alarm Assignment screen

Table M7.D - Fields in the Device Internal Alarm Assignment screen

Field	Description
Port	The port used by the E2A device.
Address	The address used by the E2A device.
Dev	The E2A device.
Description	The display description (optional).
Fail	This is the internal alarms point that is generated if it doesn't answer or is failed. Enter the internal point (address.display.point) for Fail. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.
Offline	Manually takes an address offline using line mode. This is the alarm you would see. If you don't type anything here you get a standard alarm. Enter the internal point (address.display.point) for Offline. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.

**Note:** You can see the Internal Alarm Assignment from File Maintenance > Internal Alarms > User Defined Alarms. To do this, from the User Defined Internal Alarms screen, define the address and display if not already defined. Then press F1 (Points) to see the Internal Alarm on the Point Definition screen.

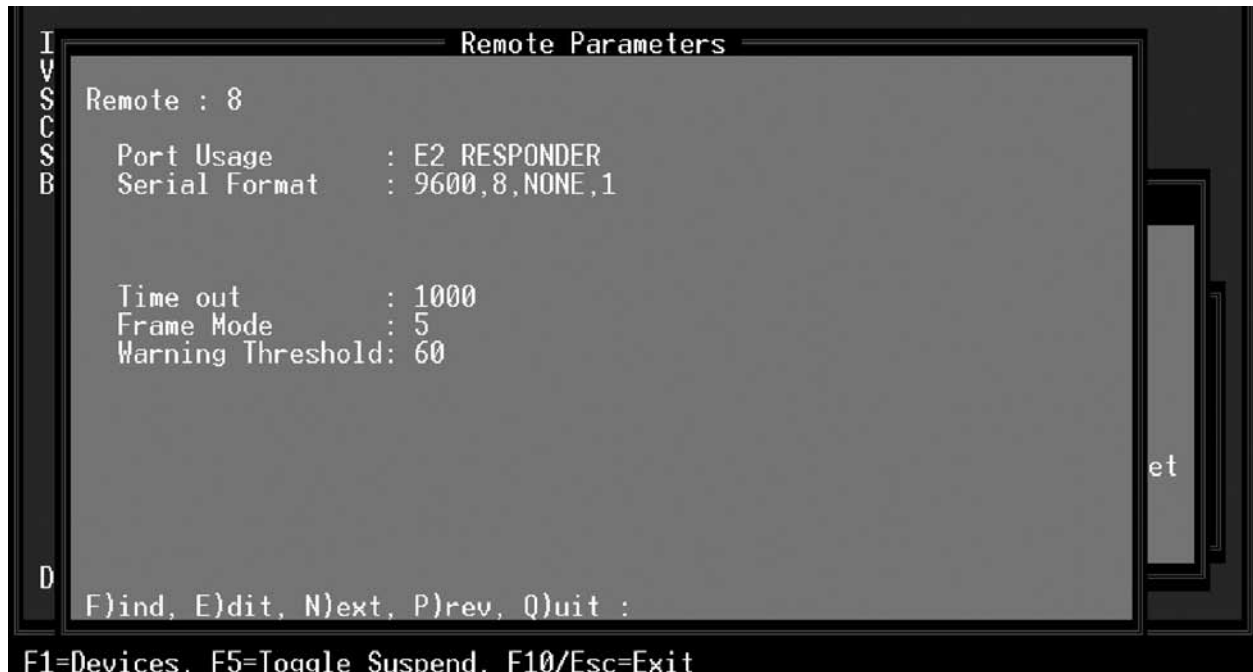


Fig. M7.5 - Remote Parameters screen defined for E2 Responders

## E2A Responders

The E2A Responder software module must be installed before you can access the E2A Responder. Refer to Section 2 - Software Installation for installation procedures.

To define a remote port for communication to E2A equipment, select Remote Ports from the Parameters menu and then select E2A Responder at the Port Usage field.

The fields on the Remote Parameters screen are explained as follows:

### Port Usage

Valid port types are E2 Responder, and Halted. Use Halted (default) if no device is connected to the communication port.

### Serial Format

Baud rate, word length, parity, and stop bits settings. Default values are 9600, 8, None, 1.

### Time Out

The time T/Mon will wait before failing a poll if there is no response. Acceptable values are 0-9999 milliseconds.

### Framing

Select either "A" for DPS E2A Converter Shelf or the Dantel 46036 mode E System Interface Card, or select "5" for the Dantel 46037 mode E System Interface Card.

### Warning Threshold

The Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds. Default value is 60 seconds.

## Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined E2 Responders will bring you to the Remote Device Definition screen.

An example of the Remote Device Definition screen is illustrated below:



Fig. M7.6 - Remote Device Definition screen

Table M7.E - Fields in the Remote Device Definition Screen

Field	Description
Port	The port you are at and the Responder you have defined.
Address	The address used by the E2A device.
Dev	The E2A device.
Description	The display description (optional).
E-Sys Mode	Enables connection to E-System Card Interface. Enter "Y" for Yes, "N" for No.
VGS Table	Enter the Group Size. Valid group sizes are 0-16. The VGS Table is a table of 16 entries (for 16 groups). Each entry can have its own group size. If the system receives a group poll, it will respond with the group size that is listed here.

**Note:** The VGS Table allows you to define the sizes of polling groups. When actively polling, the size of the group determines when the end of a response has been reached. When actively monitoring, the size of the group or the reception of a new command determine when the end of a response has been reached. The units of the group size are words. One word contains 16 bits (or points) which is equivalent to 1/4 of a display.

## Responder Definition

Entering F2 (Responder Displays) from the Remote Device Definition screen will bring you to the Responder Definition screen.

An example of the Responder Definition screen is illustrated below:

```

Remote Device Definition
Port      : 14      E2 RESPONDER
Address   : 1

Responder Definition

-----Interrogator-----
Display  PORT  DEVICE  ADDR  DISPLAY
-----
1....    5      SBP     1      1
2         12      SBP     1      1
3         13      SBP     1      1

Enter Responding Display Number (1-64)

F3=BLANK, F8=Save, F10/Esc=Exit

```

Fig. M7.7 - Responder Definition screen

Table M7.F - Fields in the Responder Definition Screen

Field	Description
Display	Enter the Responding Display Number. Valid entries are 1-64.
Port	Enter the Port Number. Valid entries are 1-500, IA (User Internal).
Device	This field is an address modifier for applicable protocols such as DCM.
Addr	Enter Address Number. Valid entries are 1-255. <b>Note:</b> Enter Address Number 11-12, when IA (User Internal) is selected on the port field.
Display	Enter Display Number. Valid entries are 1-140.

Table M7.G - Key commands available in the Responder Definition screen

Function Key	Description
F3	Blank. Deletes the current entry.
F8	Saves the Responder Definition database.
F10/Esc	Exits without saving any changes that may have been made.

---

## Miscellaneous Interrogator/Responder Notes

For users with T/MonXM version 4.2 and older.

T/MonXM previously indicated channels 1 through 4 (for the T/Mon channels) whenever it listed alarm failures. Now, T/MonXM will always indicate E1 through E4 in order to show 'E' telemetry channels. This is done to eliminate confusion and to distinguish between 'E' channels and remote interrogators. Channels E1 through E4 are 'E' telemetry channels and channels 1-16 are now Remote Access ports.

T/MonXM responders handle control forwards. Controls get reverse mapped so that the controls are returned back to the same location where the alarms originated.

The following shows an example of the responder forwarding controls.

- You have the database set so that you have an interrogator that was polling Port 3 TBOS Display 7.
- You have an E2 responder that is storing this information in display 9.
- If that E2 responder receives a command in Display 9 it will send the control to the TBOS device and will perform whatever protocol translations are necessary.

When you define the databases it is important that you define the Interrogators first and then define the Responders.

- The data that is obtained through the interrogators can either be routed to the normal screen just like an E-telemetry alarm or they can go out to a responder or you can do both.
- The E2 responder maintains display 1 (to indicate new alarms) and 2 (to show which displays have existing alarms). If you have a change of state (COS) in display 7 then point 7 would be seen appropriately in those displays.

# Software Module 8

## DCM Interrogator

### DCM Interrogator Remote Port Definition

Interrogators allow data to be brought into the system. When you use Interrogators, you specify the display list of the items you want to have polled. You can show alarm points on the normal T/MonXM screens under COS windows and Live alarms.

The DCM Interrogator software module must be installed before you can access the DCM Interrogator. Refer to the software module installation section for installation procedures.

To define a remote port for communication to DCM equipment, select Remote Ports from the Parameters menu and then select DCM Interrogator at the Port Usage field.

An example of the Remote Parameters screen defined for DCM Interrogators is illustrated above. Refer to Table M8.A for field descriptions.

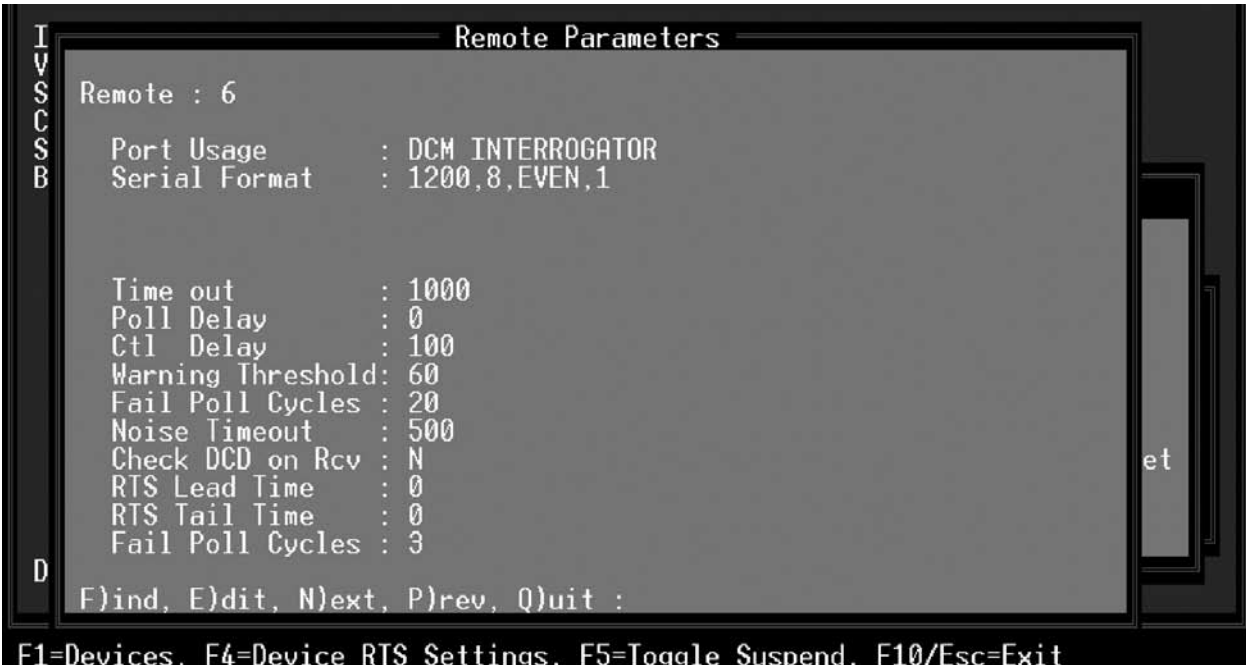


Fig. M8.1 - Remote Parameters screen



**Table M8.A - Fields in the Remote Parameters screen**

Field	Description
Port Usage	Valid port types depend on modules installed in the T/Mon. Use Halted (default) if no device is connected to the communication port.
Serial Format	Baud rate, word length, parity, and stop bits settings.
Time Out	Time out in milliseconds. Acceptable values are 0-9999 milliseconds. [1000]
Poll Delay	The Poll Delay is the time between polls. Acceptable values are 0-9999 milliseconds. [0]
Control Delay	Control Delay is the time delay after issuing controls. Acceptable values are 0-9999 milliseconds. [100]
Warning Threshold	Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds. [60]
Fail Poll Cycles	Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. [20]
Noise Time out	Time out in milliseconds (1 - 9999).
Check DCD on Rcv	Y = Enable DCD checking to validate RCV, N = Disable.
RTS Lead Time	RTS on time in 10 millisecond increments (0 - 2500 ms). Sets default for all devices. Press F4 to customize for a device. (Figure M8.2)
RTS Tail Time	RTS off time in 10 millisecond increments (0 - 2500 ms). Sets default for all devices. Press F4 to customize for a device. (Figure M8.2)
Fail Poll Cycles	Number of polls before a device failure is declared (3 - 20).

**Table M8.B - Key commands in the Remote Parameters screen**

Function Key	Description
F1	Devices
F4	Set individual RTS times for the device types (MAT, CPM, VDM and SBC. Range is 0 - 2500 milliseconds. See Figure M8.2, next page).
F10/Esc	Return to first field or exit to the parameters menu.

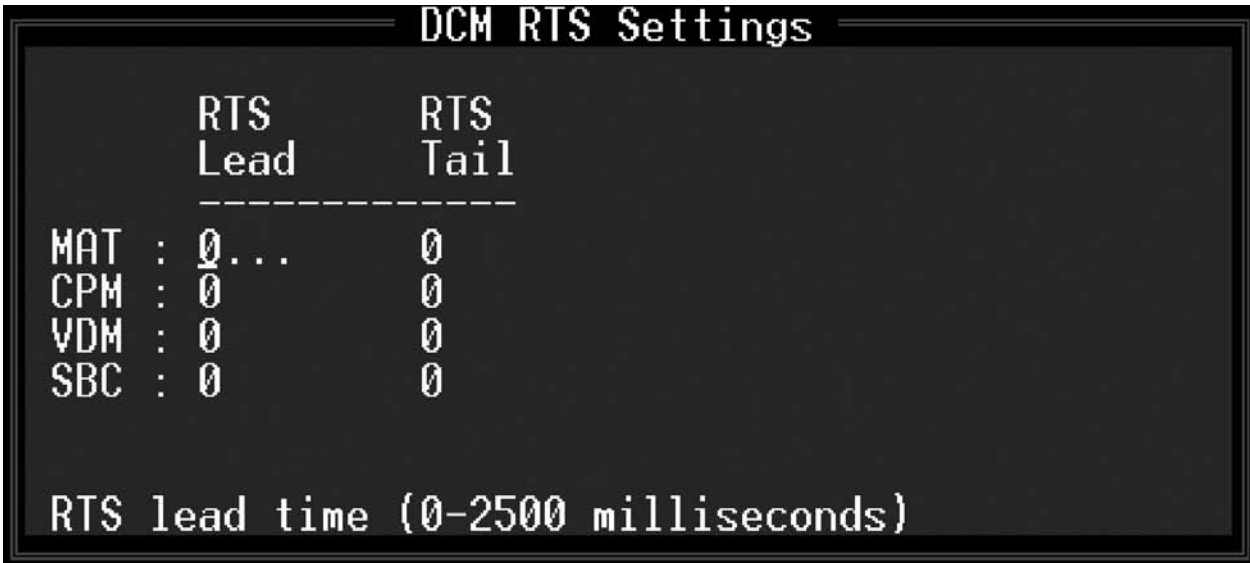


Fig. M8.2 - Press F4 to set RTS Times for Individual Devices

## Remote Device Definition

From the Remote Parameters screen, press F1 to define your remote devices the T/Mon will monitor. Refer to Table M8.C for Field descriptions. Figure M8.3 illustrates a remote device definition for a MAT on port 6 (the DCM Interrogator remote port job). Refer to Table M8.C for field descriptions in the Remote Device Definition screen.



Fig. M8.3 - Device Definition screen, MAT Device

```

Remote Device Definition

Port      : 6          DCM INTERROGATOR
Address   : 2
Device Type : C
Description : Controls
Site Name  : DPS Lab

Short Period : 3
Ext. Period  : 30

┌ CPM Points ────────────┐
Pnt Type Per          Pnt Type Per
 1 E                9 E
 2 S                10 S
 3 S                11 S
 4 M          100    12 L
 5 L                13 L
 6 L                14 M          80
 7 M          130    15 E
 8 E                16 E

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

F1=Pnts,F3=Int Alarms,AF1=TL1,AF6=Templates,F10/Esc=Exit

```

Fig. M8.4 - Device Definition screen, CPM Device

Table M8.C - Fields in the Remote Device Definition screen

Field	Description
Port	The Port number used by the DCM Interrogator. Enter port 1-28.
Address	The Address of the device. Enter Address 1-128 for MAT or CPM, 1-254 for VDM.
Device Type	Enter M for MAT (Figure M8.3), C for CPM (Figure M8.4), V for VDM, S for SBP.
Description	The Description of the device. (Optional)
Site Name	Enter the Site Name. (Optional)
<b>MAT Fields</b> - The following fields appear at the bottom of the Remote Device Definition screen when "M" is entered in the Device Type field. See Figure M8.3	
MAT Points	The MAT Points section allows you to define the level attributes for each alarm point. Select A, B, C or D for each point. Default is D.
<b>CPM Fields</b> - The following fields appear at the bottom of the Remote Device Definition screen when "C" is entered in the Device Type field. See Figure M8.4	
Short Period	"Short" time control points are operated. (1-25.5 sec in 0.1 sec steps)
Ext. Period	"Extended" time control points are operated. (1-25.5 sec in 0.1 sec steps)
CPM Points	The CPM Points section allows you to define the operation attributes for each control point. Attributes are (S)hort period, (E)xtended period, (M)omentary, and (L)atching. If Momentary is selected, another field appears for the time (0 - 255 milliseconds).

Table M8.D - Key commands in the Device Definitions screen

Function Key	Description
F1	Points. Takes you to the Point Definition Screen.
F3	Internal Alarms. This brings up a screen for assigning the device fail and device off-line internal alarm points. Follow screen prompts to specify address, display and point for each device that has been defined (Address must be either 11 or 12.)
Alt-F1	TL1. Refer to the TL1 software module for information.
F10/Esc	Return to first field or exit to the Remote Parameters screen.

## Point Definition

Entering F1 (Points) from the Remote Device Definition screen for defined DCM Interrogators will bring you to the Point Definition screen. Define attributes and English descriptions to individual alarm points within the selected displays. Notice that you must have defined the displays previously in the Remote Device Definition screen. Defining alarm point definitions are done on a display-by-display basis. For detailed information on point definition refer to Section 10, Point Definition Tutorial.

Figure M8.5 illustrates points defined for the MAT.

**Point Definition**

Port : 9 Addr: 1 Disp: MAT Display Desc :

P L H L S R  
o o s e t v  
g t v s s

**DCM INTERROGATOR**

Pt	L	H	A	S	R	Description	Fail	Clear	
1	B	L	H	A	A	N	Fuse	F	C
2	B	L	H	A	A	N	Channel 1-24	F	C
3	B	L	H	A	A	N	Channel 25-38	F	C
4									
5									
6									
7									
8									

Enter polarity. B = bipolar, U = unipolar

**Message**

F1=GOTO.F2=Desc.F3=Blank.F4=Sect.F5=Range.F6=Read.F8=Save.F9=Help.F10/Esc=Exit

Fig. M8.5 - Point Definition screen

## Internal Alarms

Entering F3 (Internal Alarms) from the Remote Device Definition screen for defined DCM Interrogators will bring you to the Device Internal Alarm Assignment screen. See Figure M8.6. For more information on Internal Alarms see Section 14.

The fields on the Device Internal Alarm Assignment screen are described in Table M8.E.

**Device Internal Alarm Assignment**

Port : 9

Address	Dev	Description	Fail	Off line
1	MAT	mux alarms	11.2.5.	11.2.8

Enter internal point (addr.display.pnt) (blank=none) (address range: 11-12)

F8=Save, F10/Esc=Exit

Fig. M8.6 - Device Internal Alarm Assignment screen

Table M8.E - Fields in the Internal Alarms Screen

Field	Description
Port	The port used by the DCM device.
Address	The address used by the DCM device.
Dev	The DCM device.
Description	The display description (optional).
Fail	This is the internal alarms point that is generated if it doesn't answer or is failed. Enter the internal point (address.display.point) for Fail. A blank indicates no Internal Alarm Assignment. Enter either Address 11 or 12.
Offline	Manually takes an address offline using line mode. This the alarm you would see. If you don't type anything here you get a standard alarm. Enter the internal point (address.display.point) for Offline. A blank indicates no Internal Alarm Assignment. Enter either Address 11 or 12.

**Note:** You can see the Internal Alarm Assignment from File Maintenance/Internal Alarms/User Defined Alarms. To do this, from the User Defined Internal Alarms screen, define the address and display if not already defined. Press F1 (Points) to see the Internal Alarm on the Point Definition screen.

# Software Module 9

## TBOS Interrogators and Responders

**Note:** T/MonXM can poll TBOS devices directly, but because of the low point capacity and distribution of TBOS devices DPS recommends the use of RTUs like the KDA or NetMediator to concentrate TBOS alarms.

Interrogators allow data to be brought into the system. With Interrogators, you specify the display list of the items you want to have polled. You can show alarm points on the normal T/MonXM screens under COS windows and Live alarms. In addition to that, alarm points may also go out responder ports. When you define the databases it is important that you define the Interrogators first and then define the Responders.

### TBOS Interrogator

Most TBOS devices use an RS485 interface. Make sure you assign the interrogator to a properly equipped interface.

The TBOS Interrogator software module must be installed before you can access the TBOS Interrogator. Refer to Section 2 - Software Installation for installation procedures.

To define a remote port for communication to TBOS equipment, select Remote Ports from the Parameters menu and then select TBOS Interrogator at the Port Usage field.

An example of the Remote Parameters screen defined for TBOS Interrogators is illustrated below: See Table M9.A on following page for field descriptions.

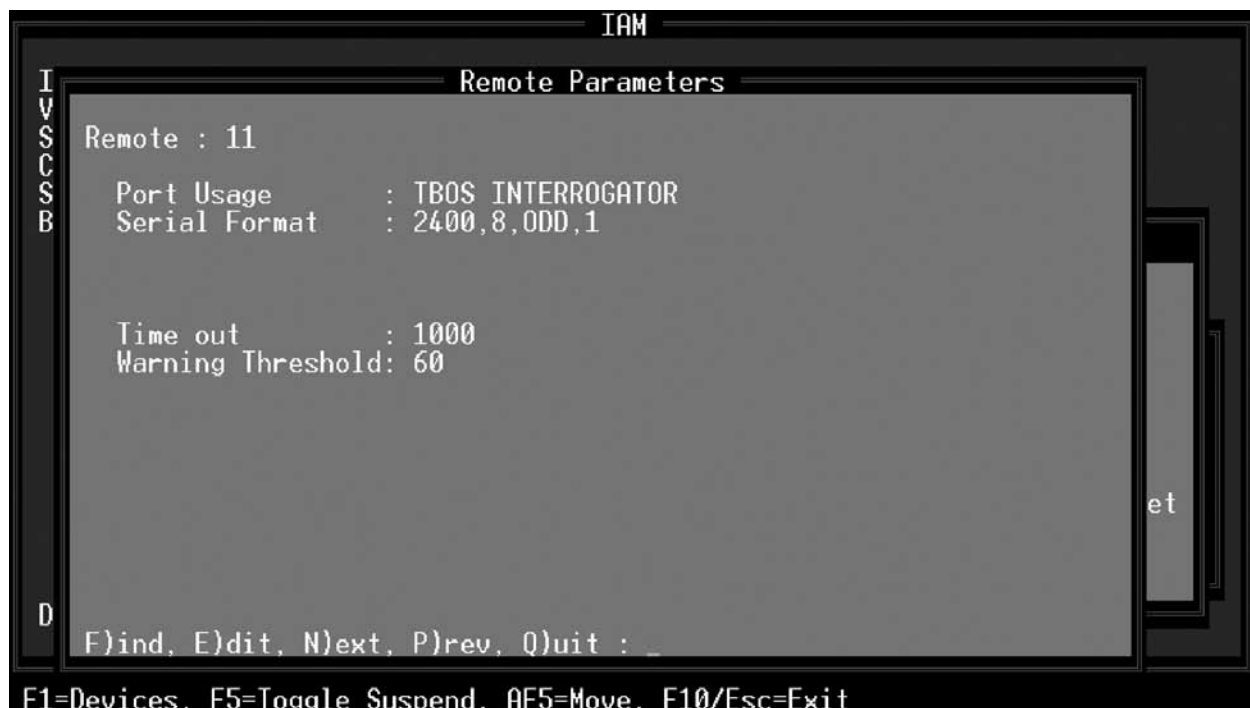


Fig. M9.1 - Remote Parameters screen defined for TBOS Interrogators

The fields on the Remote Parameters screen are explained as follows:

**Table M9.A - Fields in the Remote Parameters screen**

Field	Description
Port Usage	Valid port types are TBOS Interrogator, and Halted. Use Halted (default) if no device is connected to the communication port.
Serial Format	Baud rate, word length, parity, and stop bits settings. Default value is 2400, 8, Odd, 1.
Time out	Time in milliseconds that T/Mon will wait for a response before failing the poll. Acceptable values are 0-9999 milliseconds. Default value is 1000.
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds. Default value is 60.

## TBOS Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined TBOS Interrogators will bring you to the Remote Device Definition screen. For more information about Remote Device Definition refer to Software Module 1 (DCPF Interrogators and Responders).

An example of the Remote Device Definition screen is illustrated below. See Table M9.B on following page for field descriptions.

```

Remote Device Definition
Port      : 11      TBOS INTERROGATOR

Description : TBOS Interrogator used for BAU
Site Name  : Site #1 BAU
Displays   : 1-8
Flip Mode  : Y
Poll Delay : 0
Verify Delay : 0
Log Undefined: N

----- Address Defaults -----
Polarity   : B      Windows      : 3
Logging    : L      Message      : 0
History     : H
Level      : A
Status     : A
Reverse    : N
Description : (Undefined)

F)ind, E)dit, D)elite, N)ext, P)rev, Q)uit : _

F1=Pnts, F3=Int Alarms, AF1=TL1, AF6=Templates, F10/Esc=Exit

```

**Fig. M9.2 - Remote Device Definition screen**

**Table M9.B - Fields in the Remote Device Definition screen**

Field	Description
Port	This is the Port you are at and the Interrogator you have defined. Enter ports 1-28.
Description	The description of the device.
Site Name	Enter the Site Name.
Displays	Enter Displays 1-8.
Flip Mode	Enter "Y" for Yes, "N" for No. This mode will "flip" to the opposite order of normal alarms. Yes is the Default entry. If TBOS alarm point 8 appears in point 1, or vise versa, change flip mode.
Poll Delay	Enter Poll Delay. Acceptable values are 0-5000 milliseconds.
Verify Delay	Enter Verify Delay. Acceptable values are 0-5000 milliseconds.
Log Undefined	Enter "Y" for Yes, "N" for No.

The Address Defaults section is at the bottom of the Remote Device Definition screen. The Address Defaults section allows you to define the point attributes for an undefined alarm point. Refer to the Address and Point Definition sections in to Software Module 1 (DCPF Interrogators and Responders), and Section 9 (Remote Ports and Virtual Jobs) for more information.

The following illustrates the TBOS polling sequence and how the polling and verification fields are applied.

- The first data poll is sent out with the request "I want Display 1, Character 1".
- A response is received and the system waits the Verified Delay time period.
- Then the system sends out a verification poll (which is the same poll as the first poll).
- A response is received and the system waits the Poll Delay time period.
- Then the system sends out the second poll character request "I want Display 1, Character 2" and the sequence continues.



Entering F1 (Points) from the Remote Device Definition screen will bring you to the Point Definition screen. At this screen you are able to define point attributes for TBOS Interrogators. Refer to Section 10 (Point Definition Tutorial) for more information.

This option allows the user to assign attributes and English descriptions to individual alarm points within the selected displays. Notice that you must have defined the displays previously in the Remote Device Definition screen. Defining alarm point definitions are done on a display-by-display basis.

An example of the Point Definition screen is illustrated below:

**Point Definition**

Port : 11 Addr: Disp: 1 Display Desc :

P L H L S R

o o s e t v

Pt l g t v s s

Pt	l	g	t	v	s	s	Description	Fail	Clear
49	B	L	H	A	A	N	Panic Alarm	Set	Clear
50	B	L	H	A	A	N	Door Open	Open	Closed
51	B	L	H	A	A	N	Power Up	Alarm	Normal
52	B	L	H	A	A	N	Relay	Operate	Release
53	B	L	H	A	A	N	Building Occupied	Occupied	Unoccup
54	B	L	H	A	A	N	Illegal Entry	Alarm	Clear
55	B	L	H	A	A	N	Need Configuration	Yes	No
56	B	L	H	A	A	N	Power Loss/Communications Failure	Alarm	Clear

Enter polarity. B = bipolar, U = unipolar

**Message**

F1=GOTO, F2=Desc, F3=Blank, F4=Sect, F5=Range, F6=Read, F8=Save, F9=Help, F10/Esc=Exit

**Fig. M9.3 - Point Definition screen**

## Internal Alarms

Entering F3 (Internal Alarms) from the Remote Device Definition screen for defined TBOS Interrogators will bring you to the Device Internal Alarm Assignment screen. An example of the Device Internal Alarm Assignment screen defined for TBOS Interrogators is illustrated below: For more information on Internal Alarms see Section 14 (Defining Internal Alarms).

**Note:** You can see the Internal Alarm Assignment from File Maintenance/Internal Alarms/User Defined Alarms. To do this, from the User Defined Internal Alarms screen, define the address and display if not already defined. Press F1 (Points) to see the Internal Alarm on the Point Definition screen.

```

Device Internal Alarm Assignment

Port :    1

Address Dev  Description                               Fail      Offline
-----
1.1    TB0$  TB0$ Interrogator used for BAU           12.1.1     12.2.1
1.2    TB0$  TB0$ Interrogator used for BAU           12.1.2     12.2.2
1.3    TB0$  TB0$ Interrogator used for BAU           12.1.3     12.2.3
1.4    TB0$  TB0$ Interrogator used for BAU           12.1.4     12.2.4
1.5    TB0$  TB0$ Interrogator used for BAU           12.1.5     12.2.5
1.6    TB0$  TB0$ Interrogator used for BAU           12.1.6     12.2.6
1.7    TB0$  TB0$ Interrogator used for BAU           12.1.7     12.2.7
1.8    TB0$  TB0$ Interrogator used for BAU           12.1.8..   12.2.8

Enter internal point (addr.disp.pnt) (blank=none) (address range: 11-13)

F8=Save, F10/Esc=Exit

```

Fig. M9.4 - Device Internal Alarm Assignment screen defined for TBOS Interrogators

Table M9.C - Fields in the Device Internal Alarm Assignment screen

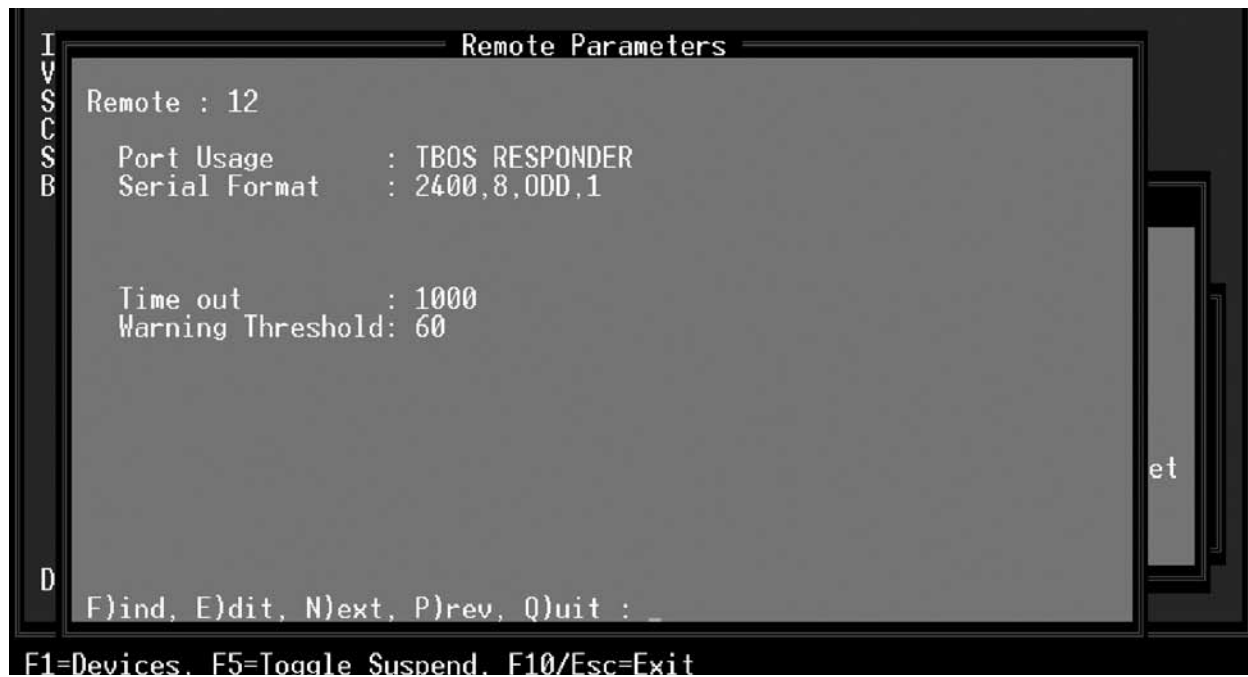
Field	Description
Port	The port used by the TBOS device.
Address	The address used by the TBOS device.
Dev	The TBOS device.
Displays	Enter Displays 1-8.
Flip Mode	This is the internal alarms point that is generated if the TBOS display does not answer or is failed. Enter the internal point (address.display.point) for Fail. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.
Offline	Manually takes an address offline using line mode. This is the alarm you would see. If you do not type anything here you get a standard alarm. Enter the internal point (address.display.point) for Offline. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.

## TBOS Responder

The TBOS Responder software module must be installed before you can access the TBOS Responder. Refer to Section 2 (Software Installation) for installation procedures.

To define a remote port for communication to TBOS equipment, select Remote Ports from the Parameters menu and then select TBOS Responder at the Port Usage field.

An example of the Remote Parameters screen defined for TBOS Responders is illustrated below.



**Fig. M9.5 - Remote Parameters screen defined for TBOS Responders**

**Table M9.D - Fields in the Remote Parameters screen**

Field	Description
Port	Valid port type is TBOS Responder.
Serial Format	Baud rate, word length, parity, and stop bits settings. Default values are 2400, 8, Odd, 1.
Time Out	Time in milliseconds that T/Mon will wait for a response before failing the poll. Acceptable values are 0-9999 milliseconds. Default value is 1000 msec.
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds. Default value is 60 seconds.

## TBOS Responder Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined TBOS Responders will bring you to the Remote Device Definition screen.

An example of the Remote Device Definition screen is illustrated below.



Fig. M9.6 - Remote device Definition screen

Table M9.E - Fields in the Remote device Definition screen

Field	Description
Port	The Port number and description used by the Responder you have defined. Enter ports 1-28.
Description	The Description of the device.
Flip Mode	Enter "Y" for Yes, "N" for No. This mode will "flip" to the opposite order of normal alarms. Yes is the Default entry. If TBOS alarm point 8 appears in point 1, or vice versa, change flip mode.

## TBOS Responder Definition

Entering F2 (Responder Displays) from the Remote Device Definition screen will bring you to the Responder Definition screen.

An example of the Responder Definition screen is illustrated below.

```

Remote Device Definition
Port      : 16      TBOS RESPONDER

Responder Definition

-----Interrogator-----
Display  PORT  DEVICE  ADDR      DISPLAY
-----
1         5         1         1
2        IA        11.
Enter Address Number (11-13)

Up Arrow=Previous Field, F10/Esc=First Field

```

**Fig. M9.7 - Responder Definition screen**

**Table M9.F - Fields in the Responder Definition screen**

Field	Description
Display	Enter the Responding Display Number. Valid entries are 1-8.
Port	Enter the Port Number. Valid entries are 1-500, LC = Local Ctrl, IA, RP, K1, K2, NG, N2.
Device	This field is an address modifier for applicable protocols such as DCM.
Addr	Enter Address Number. Valid entries are 1-255. Note: Enter Address Number 11-12, when IA (User Internal) is selected on the port field.
Display	Enter Display Number. Valid entries are 1-64.

**Table M9.G - Key commands available in the Responder Definition screen**

Field	Description
F3	Blank. Deletes the current entry.
F8	Save. Saves the Responder Definition database.
F10/Esc	Exit. Exits without saving any changes that may have been made.

## M9-8 Software Module Nine - TBOS Interrogators and Responders

# Software Module 10

## FX 8800 Interrogator

### FX 8800 Interrogator

Interrogators allow data to be brought into the system. With Interrogators, you specify the display list of the items you want to have polled. You can show alarm points on the normal T/MonXM screens under COS windows and Live alarms. In addition to that, alarm points may also go out responder ports. When you define the databases it is important that you define the Interrogators first and then define the Responders.

The FX 8800 Interrogator software module must be installed before you can access the FX 8800 Interrogator. Refer to Section 2 (Software Installation) for installation procedures.

To define a remote port for communication to FX 8800 equipment, select Remote Ports from the Parameters menu and then select FX 8800 Interrogator at the Port Usage field. An example of the Remote Parameters screen defined for FX 8800 Interrogators is illustrated below. See Table M10. A and M10.B for field descriptions and key command descriptions.

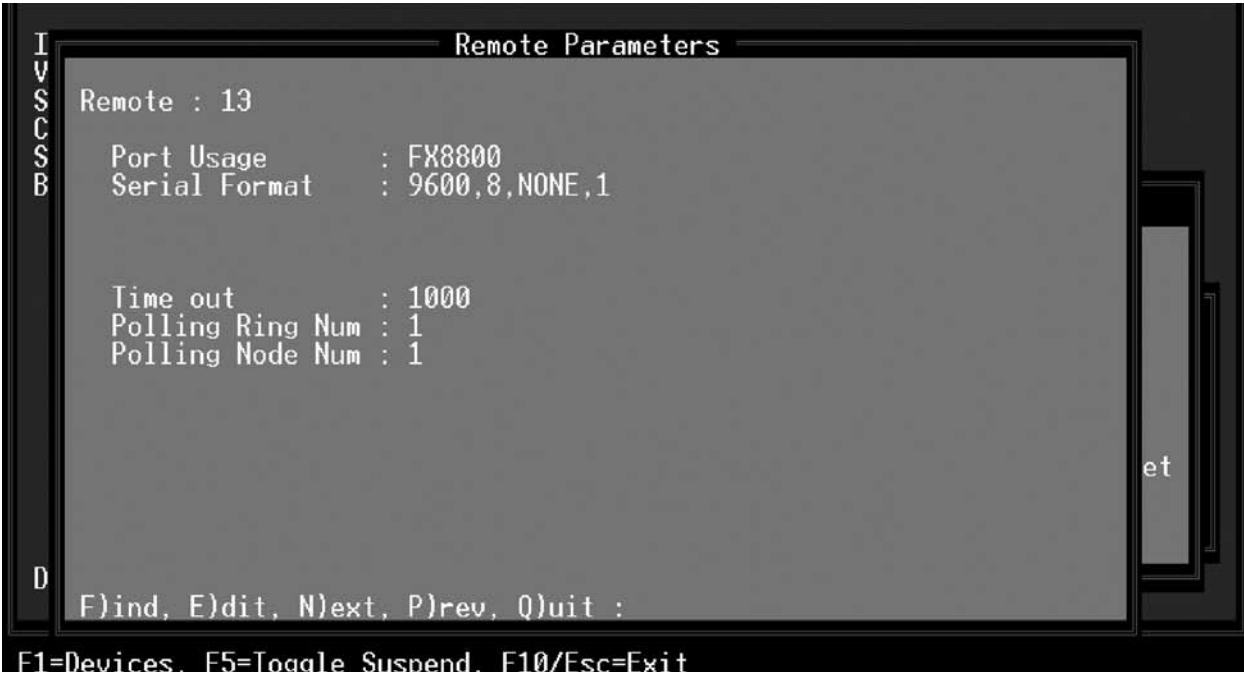


Fig. M10.1 - Remote Parameters screen defined for FX 8800 Interrogators

**Table M10.A - FX 8800 Interrogator Remote Parameters**

Field	Description
Port Usage	FX8800 Interrogator. Valid port types are FX 8800 Interrogator, and Halted. Use Halted (default) if no device is connected to the communication port.
Serial Format	Baud rate, word length, parity, and stop bits settings. [9600, 8, NONE, 1] <b>Note:</b> Due to the amount of information that is transferred from the fiber mux units, it is recommend that you use 9600 Baud.
Time out	Timeout in milliseconds. Acceptable values are 0-9999 milliseconds. [1000]
Polling Ring Num	The Polling Ring Num is the ring number to poll. Acceptable ring numbers are 1-16. [1]
Polling Node Num	The Polling Node Num is the node number to poll. Acceptable node numbers are 1-8. [1]

**Table M10.B - Key commands available in the Remote Parameters screen**

Function Key	Description
F1	Devices. Allows you to access Remote Device Definition screen.
F5	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
F10/Esc	Exit. Leaves the Remote Parameters screen.

## Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined FX 8800 Interrogators will bring you to the Remote Device Definition screen. Refer to Software Module 1 - DCP(F) Interrogators and Responders for more information on remote device definition. This is where you create the Address Definition.

An example of the Remote Device Definition screen is illustrated on the following page.

```

Remote Device Definition

Port      : 13      FX8800
Address   : 1

Description : Port 13 - FX 8800 INT
Site Name  :

Log Undefined: N

----- Address Defaults -----
Polarity   : B      Windows      :
Logging    : L      Message      : 0
History    : H
Level      : A
Status     : A
Reverse    : N
Description : (Undefined)

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

F1=Pnts, F3=Int Alarms, AF1=TL1, AF6=Templates, F10/Esc=Exit

```

Fig. M10.2 - Remote Device Definition screen

Table M10.C - Fields in the Remote Device Definition screen

Field	Description
Port	This is the Port that is assigned to the FX8800 device.
Address	This is the fiber ring Node information. (Range 1-8)
Description	The description of the device (optional).
Site Name	Enter the site name (optional).
Log Undefined	Enter Y for Yes, N for No.

The Address Defaults section is at the bottom of the Remote Device Definition screen. The Address Defaults section allows you to define the point attributes for an undefined alarm point. Refer to the Address and Point Definition sections in Software Module 1 (DCP(F) Interrogator and Responder) and Section 10 (Point Definition Tutorial).

**Note:** When polling fiber rings, there is a limitation of one fiber ring per T/MonXM port. If you wish to poll another fiber ring, use another port. Each node in a fiber ring receives information from all other nodes in that ring. You must define each node in the fiber ring that you wish polling information when defining nodes to poll. You will only receive polling data from nodes you have defined.



## Point Definition

Entering F1 (Points) from the Remote Device Definition screen will bring you to the Point Definition screen. This option allows the user to assign attributes and English descriptions to individual alarm points within the selected displays. This is where you create the Point Definition. Also refer to Section 10 (Point Definition Tutorial) for more information.

An example of the Point Definition screen is illustrated below:

The screenshot shows the 'Point Definition' screen. At the top, it displays 'Port : 17', 'Addr: 1', 'Disp: 1', and 'Display Desc :'. Below this is a table with columns 'Pt', 'l', 'g', 't', 'v', 's', 's', 'Description', 'Fail', and 'Clear'. The table contains 8 rows of data. Below the table, there is a message box with the text 'Enter polarity. B = bipolar, U = unipolar'. At the bottom of the screen, there is a footer with function key definitions: 'F1=GOTO, F2=Desc, F3=Blank, F4=Sect, F5=Range, F6=Read, F8=Save, F9=Help, F10/Esc=Exit'.

Pt	l	g	t	v	s	s	Description	Fail	Clear
1	B	L	H	A	A	N	Power Supply #1	open	closed
2	B	L	H	A	A	N	Power Supply #2	open	closed
3	B	L	H	A	A	N	Audible alarm is active (STAT)	open	closed
4	B	L	H	A	A	N	RESERVED		
5	B	L	H	A	A	N	RESERVED		
6	B	L	H	A	A	N	RESERVED		
7	B	L	H	A	A	N	RESERVED		
8	B	L	H	A	A	N	RESERVED		

Enter polarity. B = bipolar, U = unipolar

Message

F1=GOTO, F2=Desc, F3=Blank, F4=Sect, F5=Range, F6=Read, F8=Save, F9=Help, F10/Esc=Exit

Fig. M10.3 - Point Definition screen

Table M10.D - Fields in the Point Definition screen

Field	Description
Port	The Port number used by the FX 8800 interrogator.
Address	The Address of the device.
Display	The Display used by the device. Enter Display 1-3.
Display Desc	The Description of the device.

## FX 8800 Alarm Output Mapping

Each Node will occupy 3 displays worth of Alarm information. The following tables show the format that should be used for defining the Point Definition screen for Displays 1-3.

**Table M10.E - Display #1**

Point	Description
01	Power Supply #1 failed
02	Power Supply #2 failed
03	Audible alarm is active (STAT)
04	Reserved
05	Reserved
06	Reserved
07	Reserved
08	Reserved
09	Com A - Wrap error
10	Com A - Undefined error
11	Com A - Bypass error
12	Com A - Normal (STAT)
13	Com A - Sync Loss
14	Com A - Com A is Primary (STAT)
15	Com A - LoopBack
16	Com A - Node is ring Master (STAT)
17	Com B - Wrap error
18	Com B - Undefined error
19	Com B - Bypass error
20	Com B - Normal (STAT)
21	Com B - Sync Loss
22	Com B - Com B is Primary (STAT)
23	Com B - LoopBack
24	Com B - Node is ring Master (STAT)
25-64	Reserved

**Table M10.E - Display #2; Ethernet cards 1-8**

Point	Description
01	Card #1 - Sync err
02	Card #1 - Card exists
03	Card #1 - Module taken off line
04	Card #1 - Loop Back
05	Card #1 - Filter Bypassed (STAT)
06	Card #1 – Reserved
07	Card #1 – Reserved
08	Card #1 – Reserved
09-16	Card 2 information
17-24	Card 3 information
25-32	Card 4 information
33-40	Card 5 information
41-48	Card 6 information
49-56	Card 7 information
57-64	Card 8 information

**Table M10.E - Display #3; Ethernet cards 1-8**

Point	Description
01-08	Card 9 information
09-16	Card 10 information
17-24	Card 11 information
25-32	Card 12 information
33-40	Card 13 information
41-48	Card 14 information
49-56	Card 15 information
57-64	Card 16 information

**Note:** If Ethernet cards 9-16 are not used, then display #3 does not have to be included in the displays. The (STAT) notation indicates items that are status information rather than alarm information.

## Internal Alarms

Entering F3 (Internal Alarms) from the Remote Device Definition screen will bring you to the Device Internal Alarm Assignment screen. For more information on Internal Alarms see Section 14.

```

Device Internal Alarm Assignment

Port : 17

Address Dev  Description                               Fail      Offline
-----
1   FX88  Port 17 - FX 8800 INT                             11.1.21.   11.1.22

Enter internal point (addr.disp.pnt) (blank=none) (address range: 11-13)

F8=Save, F10/Esc=Exit

```

**Fig. M10.4 - Device Internal Alarm Assignment screen**

**Table M10.F - Fields in the Device Internal Alarm Assignment screen**

Field	Description
Port	The port used by the FX 8800 device.
Address	The address used by the FX 8800 device.
Dev	The FX 8800 device.
Description	The display description (optional).
Fail	This is the point that is generated if it doesn't answer or is failed. Enter the internal point (address.display.point) for Fail. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.
Offline	Manually takes an address offline using line mode. This is the alarm you would see. If you don't type anything here you get a standard alarm. Enter the internal point (address.display.point) for Offline. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11 or 12.

**Note:** You can see the Internal Alarm Assignment from File Maintenance > Internal Alarms > User Defined Alarms screen.

From the User Defined Internal Alarms screen, define the address and display. Then, press F1 (Points) to see the Internal Alarm on the Point Definition screen.

**This page intentionally left blank.**

# Software Module 11

## Integrated SNMP Agent

The Integrated SNMP Agent was designed to replace the original SNMP Agent TSR to reduce the base memory footprint.

The Integrated SNMP Agent can forward alarms from any alarm point in the T/MonXM system, and it can be configured to send traps to multiple SNMP managers when an alarm point is set or cleared. An SNMP manager or network management system can query the Integrated SNMP Agent for alarm information or send commands to the Agent for the T/MonXM system to perform on alarm points (ack, tag, silence).

The SNMP Agent is SNMP Version 1 and supports all the SNMP Version 1 operations (Get, Set and Get-Next).

The SNMP Manager needs to be running the latest version of the DPS Telecom MIB, which of this writing is version 4.1. This MIB file is included on the T/Mon Resource Disk, and also available at [www.dpstele.com](http://www.dpstele.com).

To configure the SNMP Agent, begin by defining a virtual port for the SNMP Agent. This must be a port numbered 30 or higher.

**Note:** It is recommended that you use Port 50 or higher in order to free jobs 30-50 for remote access connections.

Define the fields in the Remote Parameters screen as shown in Figure M11.1.

### SNMP Agent Configuration

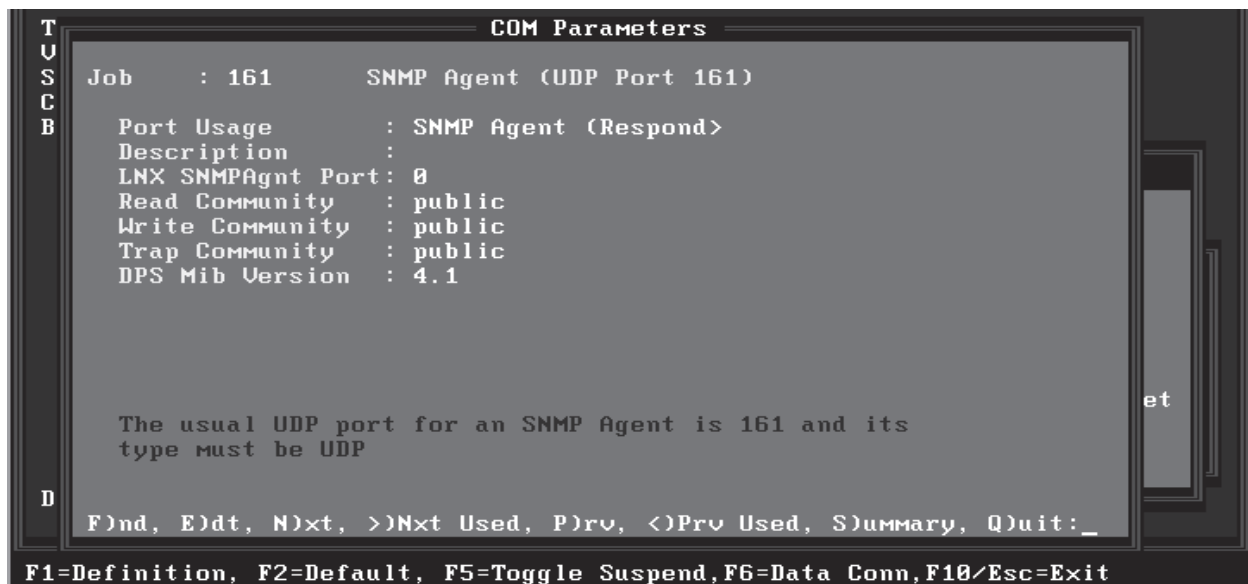


Fig. M11.1 - Remote Parameters screen, SNMP Agent port usage

The port usage must be assigned a data connection. The usual port for the SNMP Agent is 161 and its type must be UDP.

See Table M11.A for a description of the fields in the Remote Parameters screen.

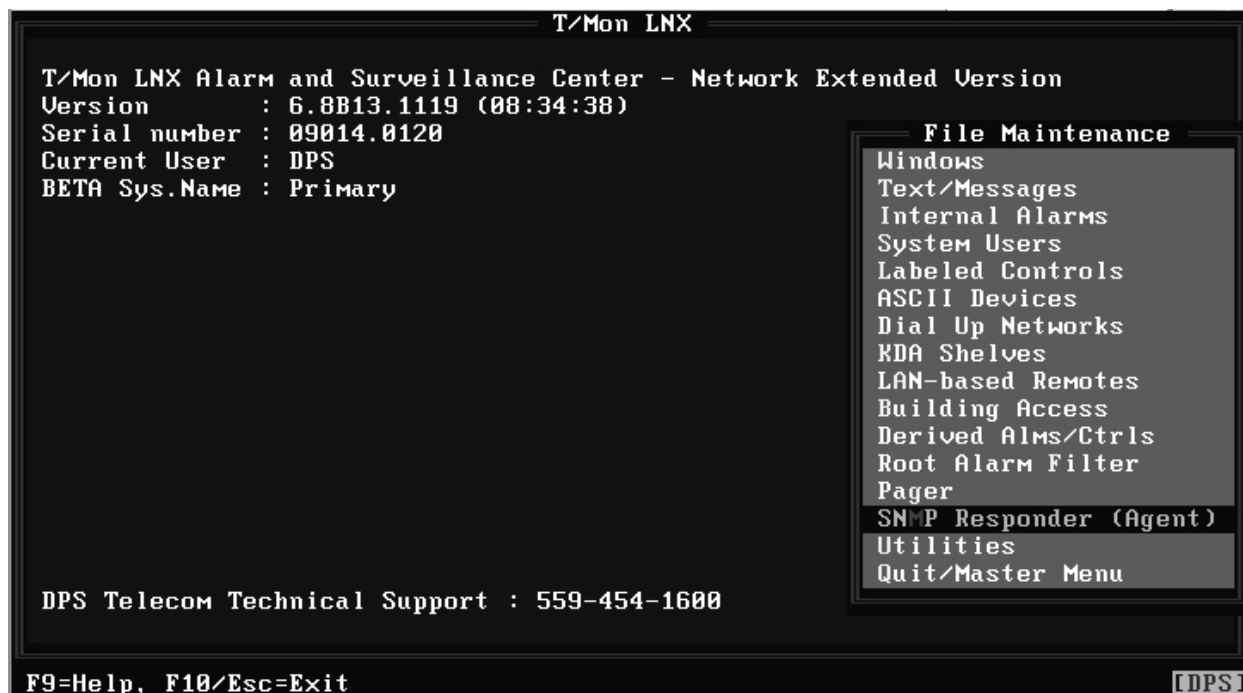
**Tbl M11.A - Fields in the Remote Parameters screen, SNMP Agent port usage**

Field	Description
Description	Optional site description.
LNx SNMPAgnt Port	Internal UDP port for linux side SNMPv3 Agent Process*
Read Community	Password accepted for a Get request received from an SNMP manager.
Write Community	Password accepted for a Set request received from an SNMP manager.
Trap Community	Password sent with SNMP Traps to SNMP managers.

\*LNx SNMP Agnt Port is only available on the T/Mon LNx. The default port is 7504. Use 0 if using only SNMPv1. Use 7504 if sending SNMPv2 or SNMPv3 traps from the T/Mon.

**Note:** The Read Community, Write Community, and Trap Community strings are passwords and should be chosen carefully for security reasons.

After defining the remote port, choose SNMP Responder from the Files menu. This command opens the SNMP Responder Definition screen (Figure M11.3). For an explanation of the fields in this screen,



**Fig. M11.2 - SNMP Responder command**

SNMP Responder (Agent) Definition					
Entry	Description	Window	Source Address	Trap Address	Trap Port
1	NMS 1	2		126.10.230.192	162
2	NMS 2	1	192.168.1.100	192.168.1.117	162
3	NMS 3	3	192.168.2.100	192.168.2.150	162
4	.....				
5					
6					
7					
8					

Enter a description

DPS Telecom Technical Support : 559-454-1600

Quit/Master Menu

F2=Options, F3=Blank, F8=Save, F9=Help, F10/Esc=Exit

Fig. M11.3 - SNMP Responder Definition screen

Tbl M11.B - Fields in the SNMP Responder Definition screen

Field	Description
Description	User-defined description of the SNMP manager.
Window	Window from which alarms will be reported to the SNMP manager. The SNMP Agent will send a trap for each COS alarm that occurs in that window only.
Source Address	User configurable source Agent IP Address included in the SNMP trap from T/Mon. Leave blank to use the default IP Address of the T/Mon. This can be used to override the SNMPv1 source IP address when traps route through the different ethernet interfaces on a T/Mon LNX.
Trap Address	IP address of the SNMP manager that traps are to be sent to.
Trap Port	Port on the SNMP manager to which traps will be sent. The usual port for SNMP managers is 162.



**SNMP Responder (Agent) Definition**

Entry	De	SNMP Responder (Agent) Options Entry 3	Trap Port
1	NM	SNMP Version : <u>SNMPV1...</u>	2
2	NM	UserName :	162
3	NM	EngineID :	162
4		Auth Prot : None	162
5		Auth Pass :	
6		Priv Prot : None	
7		Priv Pass :	
8			

Select the SNMP version for outgoing traps.

Enter a description

DPS Telecom Technical Support : 559-454-1600

Quit/Master Menu

F10/Esc=Exit

Fig. M11.4 - SNMP Responder Definition F2 Options

Tbl M11.C - SNMP Responder Definition Options

Field	Description
SNMP Version	SNMP version of the trap that TMon is to send out for the given entry.
UserName	SNMPv3 only field for the UserName.
EngineID	SNMPv3 only field containing a unique EngineID. Valid values for this field is a string of hex values.
Auth Prot	SNMPv3 only field. Auth Algorithm/Protocol. Selectable values are MD5, SHA or None.
Auth Pass	SNMPv3 only field. Auth Password.
Priv Prot	SNMPv3 only field. Privacy Algorithm/Protocol. Selectable values are DES, AES and None.
Priv Pass	SNMPv3 only field. Privacy Password.

When using SNMPv2 or SNMPv3, make sure the LNX SNMPAgnt Port field on the COM Parameters screen is set to the linux side SNMPv3Agent listening port. Default is 7504.

## Performance/ Stats

After configuring the SNMP Agent, configure your SNMP managers to receive traps from your T/MonXM system.

You can now view the Performance/Stats screen from Monitor Mode to determine the activity of the agent by pressing F6 at the alarm summary screen — see Figure M11.4. Table M15C explains the fields in the Performance/Stats screen.

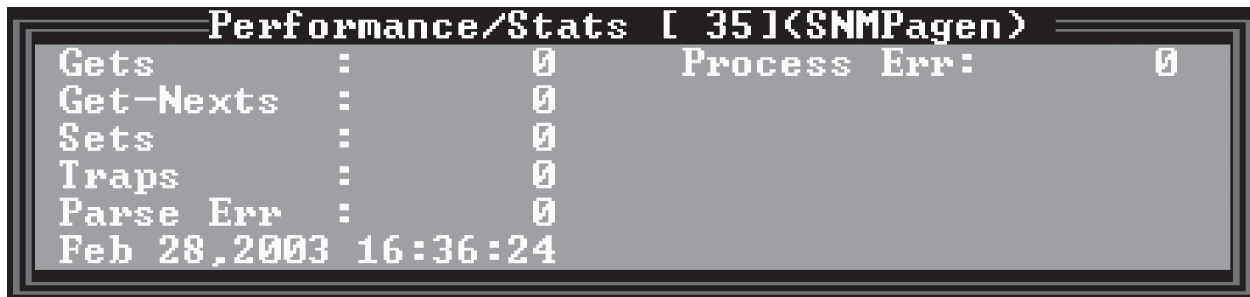


Fig. M11.4 - Performance/Stats screen for SNMP Agent

Tbl M11.C - Fields in the Performance/Stats screen

Field	Description
Gets	Get requests received from SNMP managers.
Get-Nexts	Get-Next requests received from SNMP managers.
Sets	Set requests received from SNMP managers.
Traps	Traps sent to SNMP managers.
Parse Err	Errors that have occurred while parsing a request from an SNMP manager.
Process Err	Errors that have occurred while processing a request from an SNMP manager.

**Note:** All requests from SNMP managers are first parsed to determine the validity of the packet and then processed to determine if the request can be performed.

## SNMP Manager Display

Figure M11.5 shows an example of an SNMP Manager display of alarms from the T/MonXM agent. This illustration is an example only. The appearance of an actual display may be different, depending on the manager being used.

Index	Site	Desc	State	Severity	ChgDate	ChgTime	AuxDesc
1	TEST LAB	Disp 1 Alarm 1	CLR	CR	10/24/02	20:48:37	Aux 1
2	TEST LAB	Disp 1 Alarm 2	ALM	CR	10/25/02	07:12:05	
3	TEST LAB	Disp 1 Alarm 3	ALM	CR	10/25/02	08:23:49	
4	TEST LAB	Disp 1 Alarm 4	CLR	CR	10/25/02	04:46:30	
5	TEST LAB	Disp 1 Alarm 5	ALM	CR	10/25/02	02:19:55	
6	TEST LAB	Disp 1 Alarm 6	ALM	CR	10/25/02	08:34:34	
7	TEST LAB	Disp 1 Alarm 7	CLR	CR	10/25/02	06:32:52	
8	TEST LAB	Disp 1 Alarm 8	ALM	CR	10/25/02	07:07:36	
9	TEST LAB	Disp 1 Alarm 9	ALM	CR	10/25/02	08:08:36	
10	TEST LAB	Disp 1 Alarm 10	ALM	CR	10/25/02	08:31:44	

Fig. M11.5 - Example Of T/Mon Alarms Displayed on a Manager  
(Display appearance varies with the Manager type)

Note: This screen is not part of T/MonXM.

**This page intentionally left blank.**

# Software Module 12

## SNMP Trap Processor

---

### Introduction

The SNMP Trap Processor can process traps from SNMPv1, SNMPv2c, and now SNMPv3 devices.

**Note:** Refer to section M12-16 for an illustration of an SNMP databasing map.

The SNMP Trap Processor module adds the capability of monitoring SNMP traps to T/Mon. This creates a single platform for translating SNMP traps into alarms and may eliminate the need for a separate SNMP trap manager.

With the SNMP Trap Processor, you'll be able to use all the monitoring power of your T/Mon or IAM with your SNMP devices, including event notification, history reports, and monitoring SNMP devices through T/Mon's web browser interface.

### Install or Upgrade the Software

Under normal circumstances installation will only need to be done for software updates or newly ordered modules. The original disks have been supplied with the T/Mon for archival or emergency recovery procedures. See Section 2 (Starting T/MonXM Software) further instructions on upgrading or installing software. preset databasing of internal alarms and analog points for all legacy remotes

### Configuration

After your system has rebooted, verify that the SNMP Trap Processor has been correctly installed by once again choosing Master > Diagnostics > Installable Modules > Installation Status.

Before you can use the SNMP Trap Processor, you must configure your system to map SNMP traps to T/Mon alarm point definitions. This is an essential step. The configuration procedure creates the database by which T/Mon recognizes SNMP traps alarms. This data base is the key to processing SNMP traps with the full capabilities of your T/Mon system. This section contains step-by-step instructions for configuring your system.

Your first step should be to collect the MIB (Management Information Database) files for the devices you want to monitor. A MIB file is a data file containing the information needed to communicate with an SNMP device. The MIB file contains device details, counters, statistics routing tables, and other information. The MIB file is provided by the manufacturer of your SNMP device and can be found on the distribution media that came with your device.

Copy the MIB files for your SNMP devices to a 3 1/2" floppy disk and insert the disk in drive A.

## Step1. - Verify Ethernet Port Assignment

- A. **Verify that Port 28 is assigned to Ethernet I/O.** Your T/Mon system must be configured for Ethernet input and output to receive SNMP traps.
- B. Choose Master > Parameters > Remote Ports > Find.
- C. Type 28 and press Enter. If Port 28 is assigned to Ethernet I/O, go to Step 2. If Port 28 is not assigned to Ethernet I/O, go to Step 1c.
- D. Choose Edit. This command opens the Port Usage list.
- E. Press Tab to select the Port Usage list.
- F. Using the Down and Up arrow keys or Tab and Shift Tab to scroll, highlight Ethernet I/O and press Enter.

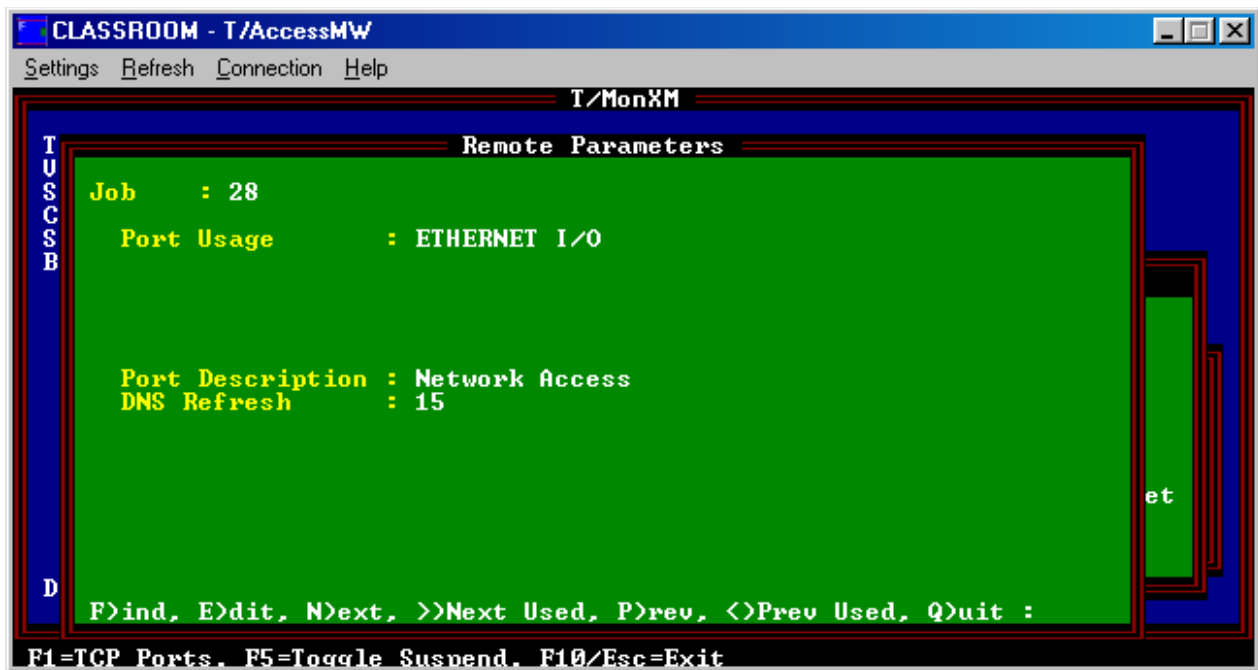


Fig. M12.1 - Port 28 should be assigned to Ethernet I/O

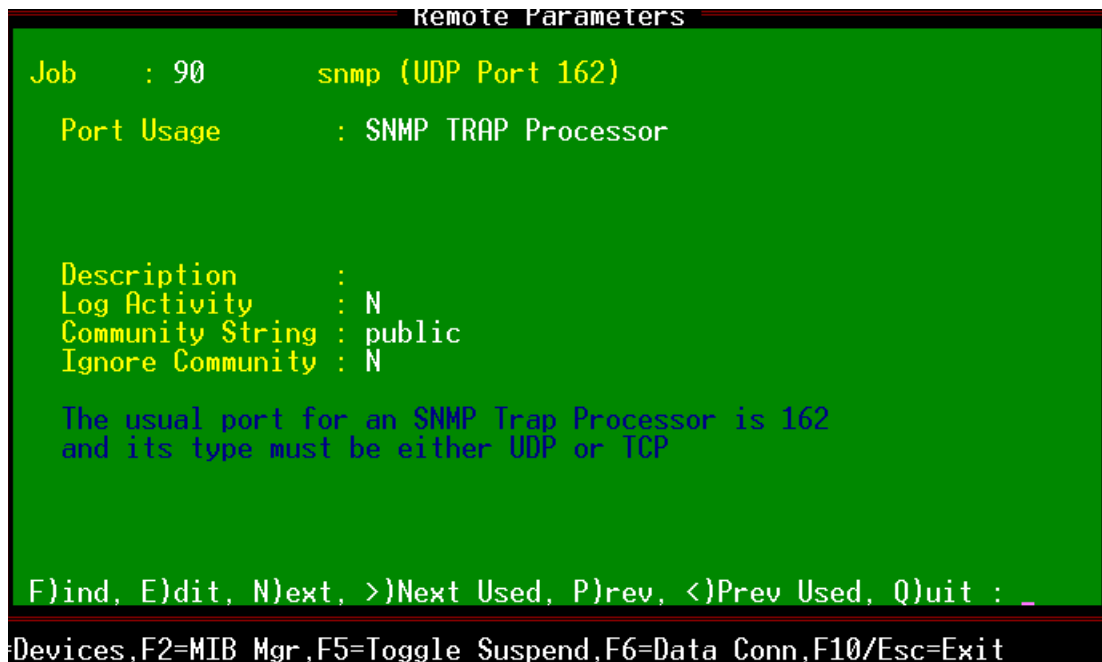


Fig. M12.2 - Assign SNMP Trap Processor to Port 48 or higher

## Step 2. - Assign a Port to the SNMP Trap Processor

**Note:** Only one port should be defined for the SNMP Trap Processor.

- A. **Assign an unused remote port number 48 or higher to the SNMP Trap Processor.** In this step you will assign the remote port through which T/Mon will receive SNMP traps. Assign only one remote port to the SNMP Trap Processor.
- B. Choose Master > Parameters > Remote Ports > Find.
- C. Type a number 48 or higher and press Enter.
- D. Choose Edit to open the Port Usage list.
- E. Press Tab to select the Port Usage list.
- F. Scroll to highlight SNMP Trap Processor and press Enter.
- G. Type a description you will recognize later in the Description field and press Enter.
- H. The Log Activity field will default to N (no). Press Enter. This field can be set to Y (yes) if you wish to log all traps to the file traplog.rep. This is useful when diagnosing unresolved traps. Make sure to set this option to N (no) when you are done to conserve disk space. Note: This can be temporarily overridden by enabling trap logging from within monitor mode.
- I. Fill in the Trap Community field so that it matches the community of your SNMP devices and press Enter.  
**Note:** The community acts as a password.
- J. The Ignore Community field will be set to N (no) by default. Setting this to Y (yes) will process traps without checking the community string.
- K. You may see a message at the top of the Remote Parameters screen that reads <No Data Connection>. This is normal. If you see this message, you must assign a data connection to the port.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	UDP.....		161	SNMP Agent
2	UDP		162	SNMP Trap Processor
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Tab=Defaults, F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit

Fig. M12.3 - The Ethernet TCP Port Definition screen

### Step 3. - Verify Ethernet Port Assignment of SNMP Trap Processor

**Note:** The SNMP Trap Processor can support both UDP and TCP data connection. The UDP data connection is the industry standard for SNMP.

- A. Verify that Ethernet Port 162 has been assigned to the **SNMP Trap Processor** port. Your SNMP devices are configured to report traps to a specific ETHERNET port. The standard port type for an SNMP manager is UDP, and the standard port number is 162. TCP is also supported by T/Mon, but is far less common than UDP.
- B. From the Remote Parameters screen, press F6 to open the Data Connection Assignment screen. Press F1 to open the Ethernet TCP Port Definition screen (Fig. M12.3). Verify that UDP Port 162 is assigned to the SNMP Trap Processor. If the correct port is assigned, then go to Step 4.  
  
If UDP Port 162 has been assigned to another function, assign another UDP port to that function and go to Step 3.C. If UDP Port 162 is unassigned, go to Step 3.C.
- C. Type UDP in the Type field and press Enter.
- D. Type 162 in the TCP Port field and press Enter.
- E. Type a description that you will recognize later in the Description field and press Enter.
- F. Press F8 to save your changes and return to the Data Connection Assignment screen (Fig. M12.4).
- G. Press Tab to select the connection list.
- H. Scroll to highlight the connection you just made for the SNMP Trap Processor and press Enter. You will return to the Remote Parameters screen (Fig. M12.5).



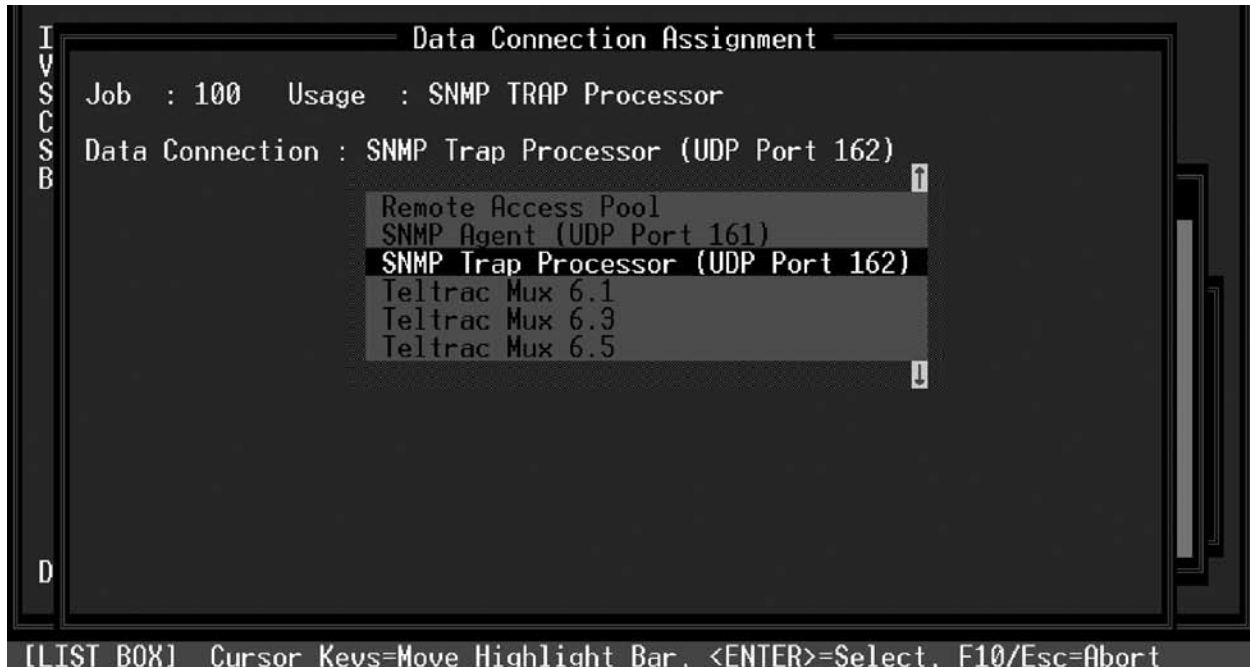


Fig. M12.4 Selecting the new data connection assignment for the SNMP Trap Processor

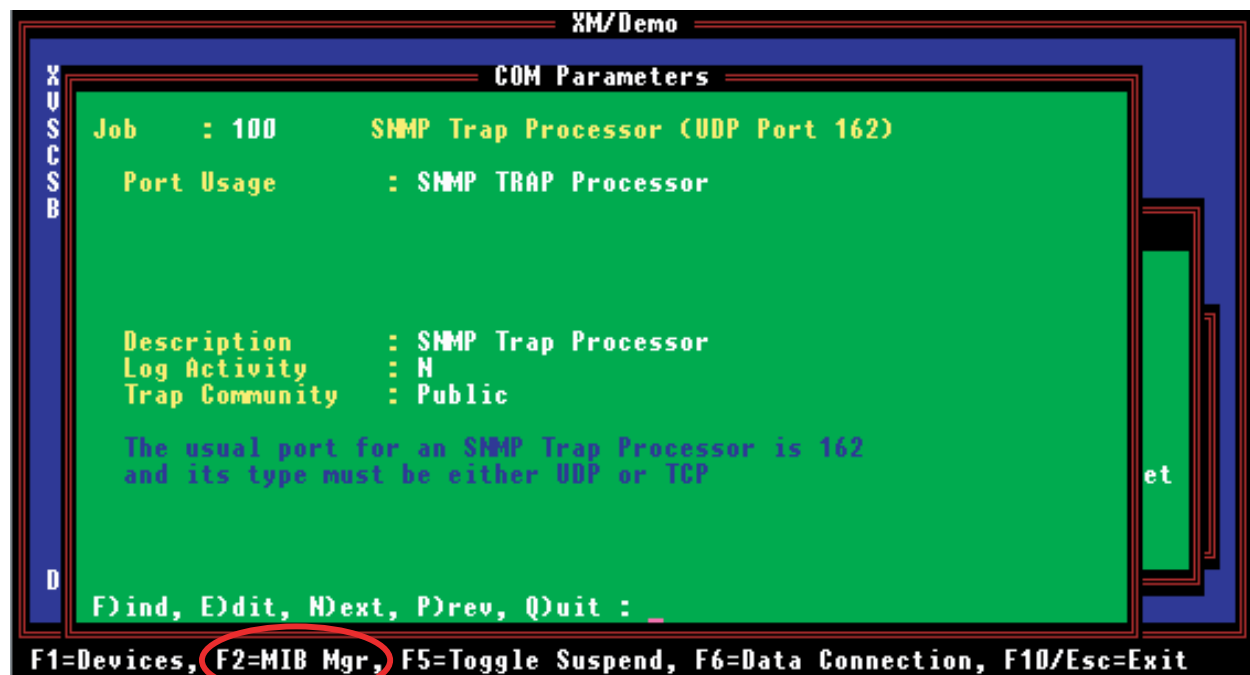


Fig. M12.5 - Press F2 to open the MIB Manager Screen

## Step 4. - Import MIB Files

- A. **Import MIB (Management Information Database) files.** You will need one or more MIB files for each type of device you are monitoring. Many manufacturers write a single MIB file for multiple devices. Make sure that you have the correct MIB file or files for your SNMP devices.
- B. From the Remote Parameters screen, press F2 to open the MIB Manager menu — see Figure M12.5.
- C. Choose Import MIB from the MIB Manager menu — see Figure M12.6. A list of the MIB files available on the floppy disk in drive A will appear.
- D. Press Tab to select the list. Scroll to highlight the MIB file you wish to import, and press Enter.
- E. Repeat Step 6.C as needed to import as many MIB files as you require.
- F. Press F10 or Esc to exit the MIB file list.



Fig. M12.6 - Compile MIBs command

## Step 5. - Compile MIB Files

- A. **Compile MIB files.** The MIB files must be compiled to be used with your T/Mon system.
- B. From the MIB Manager menu, choose Compile MIBs. The status of the compile will be displayed in a message screen — see Figure M12.7.
- C. When the compile is complete, the message line at the bottom of the screen will prompt you to compile more MIB files or quit. Choose Quit to quit the compiler. You will return to the Remote Parameters screen with the SNMP Trap Processor port selected.



Fig. M12-7 - Compiler Message screen

```

Remote Device Definition

Port / Job : 162      SNMP TRAP Processor
Device ID  : 9999
Use Trap Id : Y       126.10.220.168

Description : NetGuardian
Site Name   : NetGuardian
Displays    : 1-64
SNMP Version : 3
Community   :
Device Type :

----- SNMPv3 options -----
User Name   :
Engine ID   :
Auth. Prot. : NONE
Auth. Pass. :
Priv. Prot. : NONE
Priv. Pass. :

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

F1=Pts, F2=Rbld, F3=DvcTyps, AF1=TL1, AF2=SET, AF3=IP, AF5=GET, AF6=Implt, Esc=Ext

```

Fig. M12.8 - Remote Device Definition screen

## Step 6. - Define Devices (SNMP Agents)

- A. **Define devices.** In this step you will define descriptions for your SNMP devices (SNMP Agents), creating the database that T/Mon will use to monitor them. You will also enter descriptions that will allow T/Mon to display detailed information about alarm events.
- B. From the Remote Parameters screen, press F1 to begin defining devices. This command opens the Remote Device Definition screen.
- C. To define a device, choose Find, type the Device ID number of the desired device, and press Enter. The Device ID must be unique for each device. If you select a Device ID that is not currently defined, you will be prompted to add the device.
- D. The Use Trap ID field provides the option of incorporating the Trap IDs into the processing of SNMP trap. Make each Trap OID unique and often results in less databasing. Select the default of Y (yes). Selecting Z will behave the same as Y except it will truncate a zero at the end of the received OID (if one exists) before it is processed.
- E. Type the IP address of the device that will be sending traps, and press Enter. It is not necessary to enter leading zeros.
- F. The Description field is displayed only in this screen and in reports. You can use this field to enter a detailed description of the site, including its street address, what equipment is located there, or any other relevant information. Type a description and press Enter.
- G. The Site Name field displays the site name that will be associated with this device in Monitor Mode. Type a name that will be recognized by your system operators and press Enter.

H. The Displays field determines the number of displays (groups of 64 alarm points) to reserve for this device. The default number is 64 displays of 64 alarm points each. These values can be changed at any time in the future. You can either accept the default by pressing Enter, or type a new value and press Enter.

**Note:** To conserve disk space, define only as many displays as you need for your existing alarm points. Using all 64 displays provides a capacity for 9,096 alarm points from a single IP address-which is probably more than you need and consumes disk resources.

- I. The SNMP Version field is used to define the version of the SNMP device. An optional software module is required to enable SNMPv3.
- J. The Community field will be blank. Enter a community string here to define a device-specific community string. If this field is defined, it will ignore the Community string and Ignore community string settings on the port/job screen.
- K. **For SNMPv3:** The SNMPv3 options at the bottom of the screen will only be enabled if the SNMP Version is set to 3.
- L. Enter the User Name for the SNMPv3 device.
- M. Enter the Engine ID for the SNMPv3 device.
- N. Select an SNMPv3 Authentication Protocol (None or MD5). Password is only required if using MD5. Password field cannot be left blank if using MD5 authentication.
- O. Select an SNMP privacy protocol (none or DES). Password is only required if using DES, and the field cannot be blank if set to DES. Privacy can only be used if Authentication is set.

The screenshot shows the 'Point Definition' screen. At the top, it displays 'Job : 100', 'DevID: 1', 'Disp: 1', and 'Display Desc :'. Below this is a table with columns 'Pt', 'P', 'L', 'H', 'L', 'S', 'R', 'Description', 'Fail', and 'Clear'. The first row shows '1', 'B', 'L', 'H', 'A', 'A', 'N', 'Transmitter A', and '.....'. Below the table is a text input field labeled 'Enter Fail Status Description'. At the bottom, there is a 'Message' box and a legend: 'Up Arrow=Previous Field', 'F1=Trans', 'F10/Esc=First Field'.

Pt	P	L	H	L	S	R	Description	Fail	Clear
1	B	L	H	A	A	N	Transmitter A	.....	
2									
3									
4									
5									
6									
7									
8									

Enter Fail Status Description

Message

Up Arrow=Previous Field F1=Trans F10/Esc=First Field

Fig. M12-9 - Alarm Point Definition screen

## Step 7. - Begin Alarm Point Definition

- A. **Begin alarm point definition.** After defining your SNMP devices, you must define the alarm points associated with the devices. Defining alarm points for SNMP devices involves two different procedures: defining standard T/Mon alarm attributes, which is covered here in Step 7 and in Step 9, “Complete alarm point definition”; and assigning SNMP traps to the fail and clear conditions of the alarm point, which is covered in detail in Step 8, “Associate SNMP traps with alarm points.”
- B. From the Remote Device Definition screen, press F1 to open the Alarm Point Definition screen.
- C. The alarm points are listed in the first column by number. The next six columns list some standard point attributes. You can either accept the default point attributes you defined in Step 6h, or you can specify attributes for this particular alarm. After each entry, press Enter to select the next field.
- D. Type a description for the alarm point in the description field and press Enter.
- E. The Fail field will now be selected. Go to Step 8.

## Step 8. - Associate SNMP Traps with Alarm Points SNMP Traps Defined

Because this is both the most complex and the most crucial step in the configuration process, some explanation is in order.

T/Mon defines each alarm point as having a fail condition and a clear condition. For discrete alarm devices, these conditions are represented by a simple electrical signal-the circuit is either on or off, which represents a fail or a clear.

SNMP devices do not send alarm signals. Instead, they send text messages called traps. The MIB file for an SNMP device lists all the possible traps that the device can send. There is a specific trap for every possible alarm state. A trap message consists of an object identifier (OID), variables, and values. The OID is a number that identifies the trap message. The OID refers to a particular state of a particular device. The device’s MIB file associates the OID with a readable label-for example, the OID “1.3.6.1.4.1.2681.1.2.102” is associated with the label `dpsRTUsumPClr`, which means “DPS Telecom remote telemetry unit, all points clear.” Variables are extensions of OIDs that specify the device state more exactly. Our example trap, `dpsRTUsumPClr`, contains three variables, `sysDescr`, `sysLocation`, and `dpsRTUdateTime`. DPS Telecom remotes send a comprehensive set of bindings to provide detailed alarm information.

Values are possible variable states. Values are typically 1 (true) or 0 (false), or a text string.

A variable-and-value pair is called a variable binding.

In Step 8, you will assign traps to the fail and clear conditions of each of the alarm points of your SNMP devices. This creates the database by which T/Mon recognizes SNMP trap messages as alarm signals. For each alarm point condition, you must specify 1)

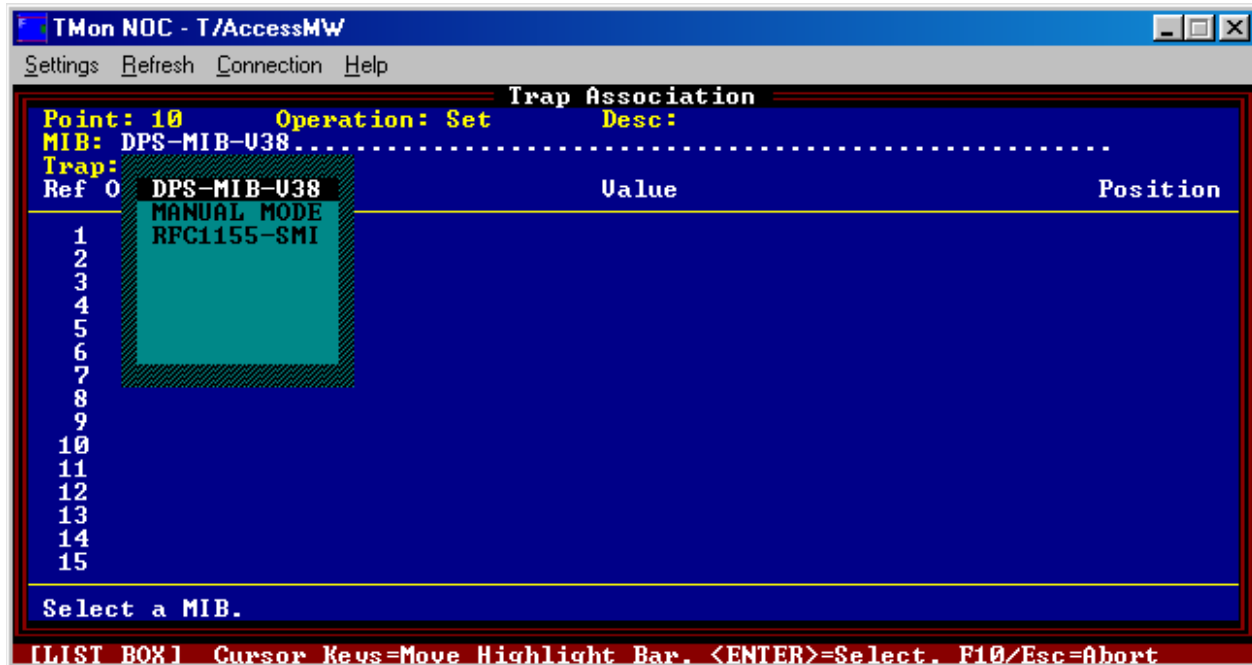


Fig. M12-10 - Selecting a MIB file

the MIB file, 2) the trap, 3) up to 15 variables (optional), and 4) a value for each variable.

**Use the following steps to assign traps using a MIB (recommended method)**

- A. From the Alarm Point Definition screen, press F1 to associate a trap with the fail condition for this alarm point. This command opens the Trap Association screen. Fields at the top of the screen display the number of the alarm point, the operation (alarm condition) being defined—either Set (Fail) or Clear—the description of the alarm point, and the MIB file and trap associated with the alarm point.
- B. A list of the MIB files you compiled in Step 5 will appear. Press Tab to select the list box. Scroll to highlight the MIB file for this type of device and press Enter. To manually enter Traps and OIDs, see section M12-12.
- C. A list of the traps that can be sent by the device specified in the MIB file you selected will appear. Press Tab to select the list box. Scroll to highlight the trap you want to associate with the fail condition for this alarm point and press Enter — see Figure M12-10.
- D. Once you have selected a trap, its OID will be displayed at the bottom of the screen — see Figure M.12-11.
- E. A list of the variables in the selected trap will appear.  
**Note:** Defining variables is not necessary if the MIB defines a unique TRAP for every alarm condition.  
 Press Tab to select the list box. Scroll to highlight the variable you want to define and press Enter.

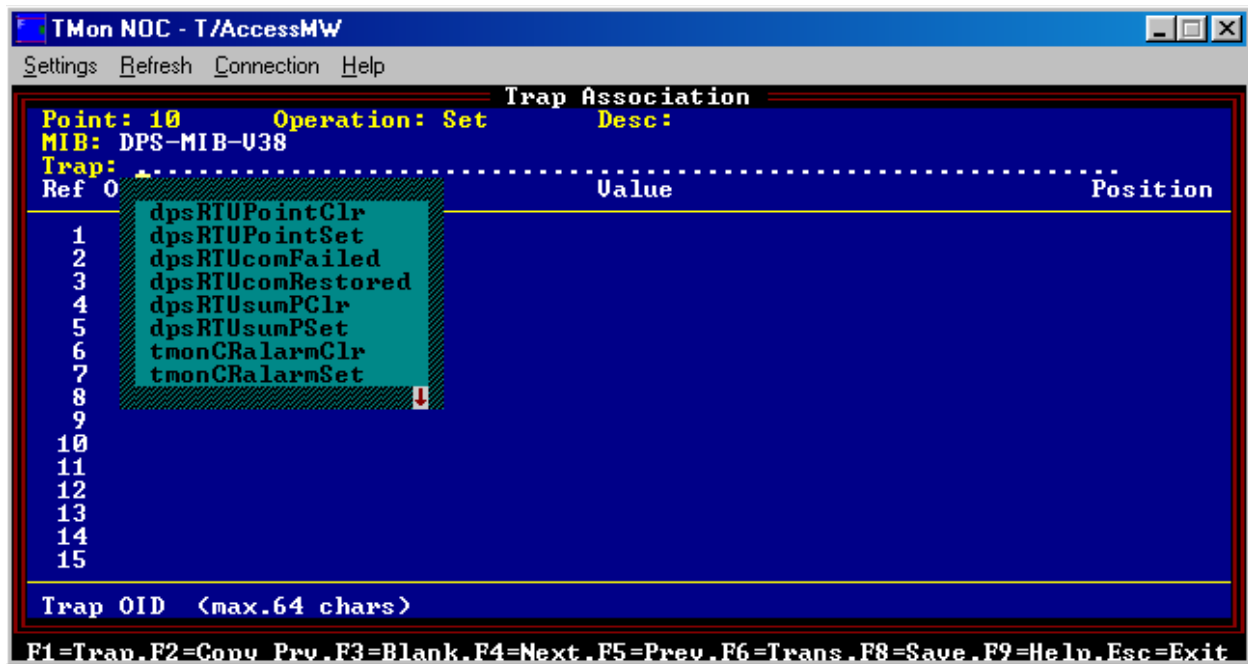


Fig. M12-11 - Selecting a trap to associate with the fail condition of an alarm point

- F. When you have selected a variable, the Value field for that variable will automatically be selected. The message line at the bottom of the screen will display the available value options for the variable, as defined in the MIB. These options will be either an integer value (such as 1 = alarm condition and 0 = clear) or a text string (text strings are not case sensitive). Type the value you want and press Enter.
- G. Repeat Steps 8.E and 8.F for up to fifteen variable bindings for each trap. Undefined variable bindings will be ignored. When you have finished defining variable bindings, press F8 to save your changes, and then press Enter.
- H. The Clear field will now be selected. Repeat Steps 8.A-8.G to associate an SNMP trap with the clear condition for this alarm point. Press F8 to save your changes and press Enter. You will return to the Point Definition screen.

**For shortcut commands used for Step 8, see “Shortcut” Commands” on section M12-13.**

**Use the following steps to assign traps and OIDs manually (advanced method - the potential for error is likely if you are not familiar with what you are doing)**

The TMon supports manually entering the OID of any trap or variable binding from the Trap Associations screen. This is especially beneficial when the manufacturer of the SNMP device has not provided a MIB or you simply wish to database using only traps captured in the trap log.

- A. From the Alarm Point Definition screen, press F1 to associate a trap with the fail condition for this alarm point. This command opens the Trap Association screen. Fields at the top of the screen display the number of the alarm point and the operation
- B. In order to perform manual OID entry you must first set the “MIB” field in the Trap Associations screen to “MANUAL MODE” (see Figure M12-10). This will allow you to enter OIDs in both the “Trap” field and the “OID” fields. Manual mode cannot be used in combination with selecting traps or variable binds from a MIB on any single trap. In other words you cannot database a trap where you enter some OIDs manually and referencing others by name. But you can do some traps completely in manual mode and others completely by referencing a MIB.
- C. Enter a Trap OID you want to associate with the fail condition for this alarm point and press Enter.
- D. Once you have entered a trap OID, the OID will be displayed at the bottom of the screen — see Figure M.12-12.
- E. Enter a variable OID and press Enter.
- F. When you have selected a variable, the Value field for that variable will automatically be selected. Options are either an integer value (such as 1 = alarm condition and 0 = clear) or a text string (text strings are not case sensitive). Type the value you want and press Enter.

**Note:** See Variable Binding Pattern Matching for special commands for text strings.

- G. The “Position” field references the ordering of the variable bindings in the SNMP trap. It is necessary for TMon to know the position of the variable binding in the SNMP trap in order to match on it. When databasing variable bindings using a MIB the position fields are populated automatically as the TMon is able to reference the MIB and determine the ordering. The easiest way to determine the position of any given variable binding, short of looking in the MIB, is to capture the trap in the trap log and look at the “VarBind Position” field associated with each variable binding. This field contains the value you want to enter in the corresponding “Position” field of the Trap Associations screen. — see Figure M.12-12.
- H. Repeat Steps 8.E and 8.G for up to fifteen variable bindings for each trap. Undefined variable bindings will be ignored. When you have finished defining variable bindings, press F8 to save your changes, and then press Enter.
- I. The Clear field will now be selected. Repeat Steps 8.A through 8.I to associate an SNMP trap with the clear condition for this alarm point. Press F8 to save your changes and press Enter. You will return to the Point Definition screen.



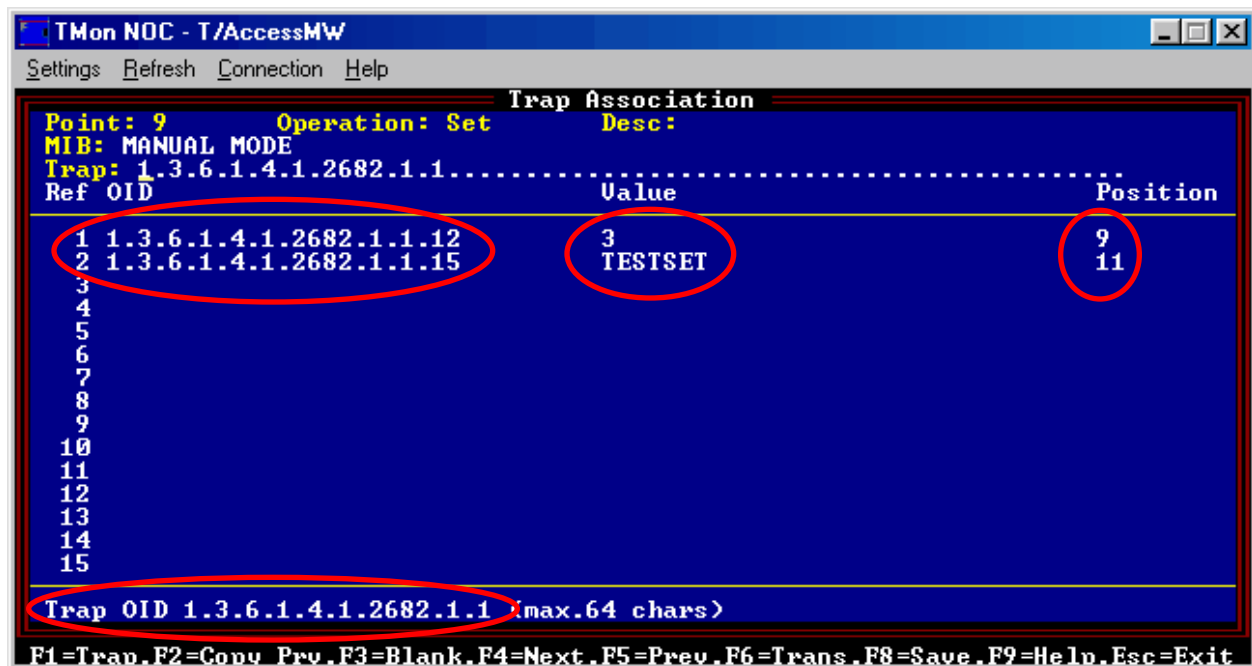


Fig. M12-12 - You will have to manually enter your Trap OID, variable OID, value, and position entries

## Step 9. - Complete Alarm Point Definition

- A. **Complete alarm point definition.** After you have associated SNMP traps with the fail and clear conditions for an alarm point, there are five more fields of standard T/Mon alarm point attributes to define.
- B. In the Windows field type the ID numbers of the windows that will be associated with this alarm point and press Enter.
- C. In the Msg field you can enter a text message that will be associated with this point in Monitor Mode. Type a message, if you wish, and press Enter.
- D. The Qual and Counter fields are used to define event qualification for this alarm point. For a detailed help message on defining these options, press F9. To select the next field, press Enter.
- E. In the Pager field type the number of the pager profile listing the personnel to be notified if this alarm point changes state and press Enter.

## Step 10. - Repeat as Necessary

- A. Repeat as necessary.
- B. Repeat Steps 7-9 for each alarm point associated with a device.
- C. Repeat Steps 6-9 for each device.
- D. Repeat Steps 5-9 for each site. Up to 999 sites can be defined.

**NOTE:** You will save a great deal of time by using the shortcut commands — see “Shortcut Commands” on section M12-19.

## The Trap Log

The trap log is a tool designed to assist in the analysis and databasing of incoming SNMP traps. If logging is enabled then traps received will be saved to a report file called "TRAPLOG.REP" which can be viewed with the standard report viewer. It is also possible to FTP into the system and retrieve the file without exiting monitor mode. The format of the trap log is similar to that of a packet sniffer in that there is both a "raw dump" of the trap and "dissected view" which makes it easy to distinguish the different parts of the trap.

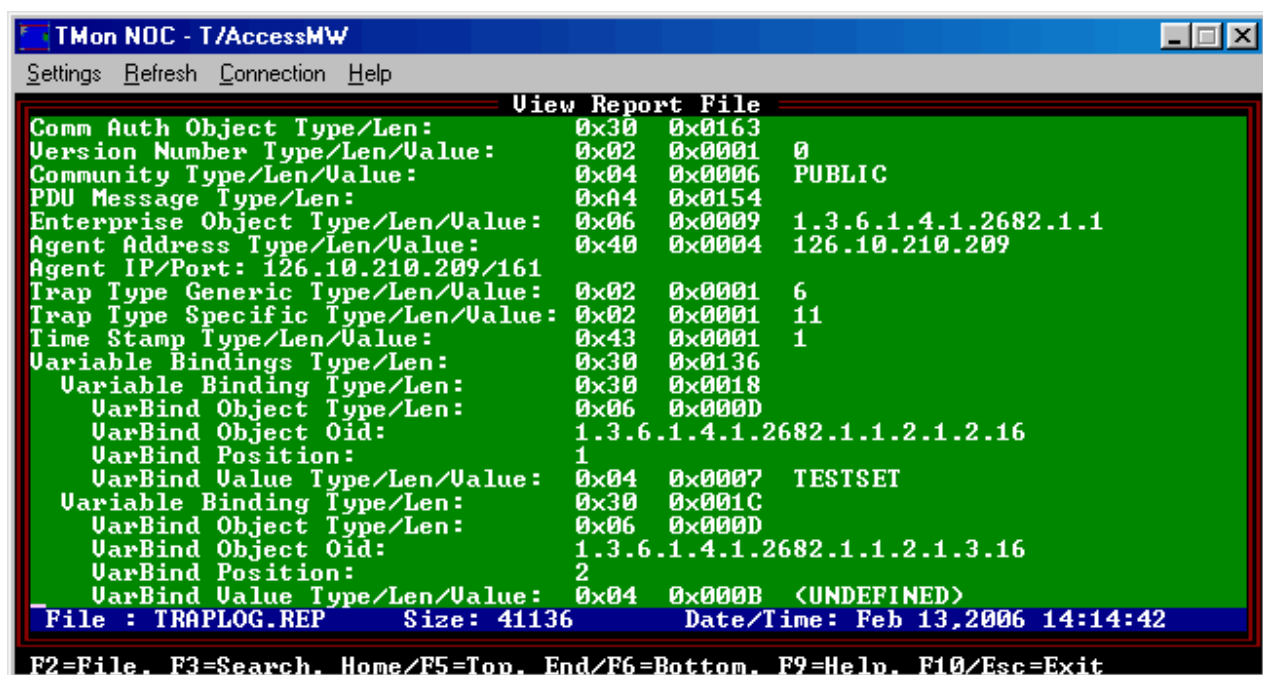


Fig. M12-13 - Trap log report file (TRAPLOG.REP)

Trap logging can be enabled in two different ways. The first way is to enable it from the SNMP Trap Processor job in the Remote Parameters screen by setting the “Log Activity” field to ‘Y’. Setting this field to yes will result in the continuous logging of all incoming SNMP traps. It is important to note that this can use a lot of hard disk space if left on, so it is not the recommended method.

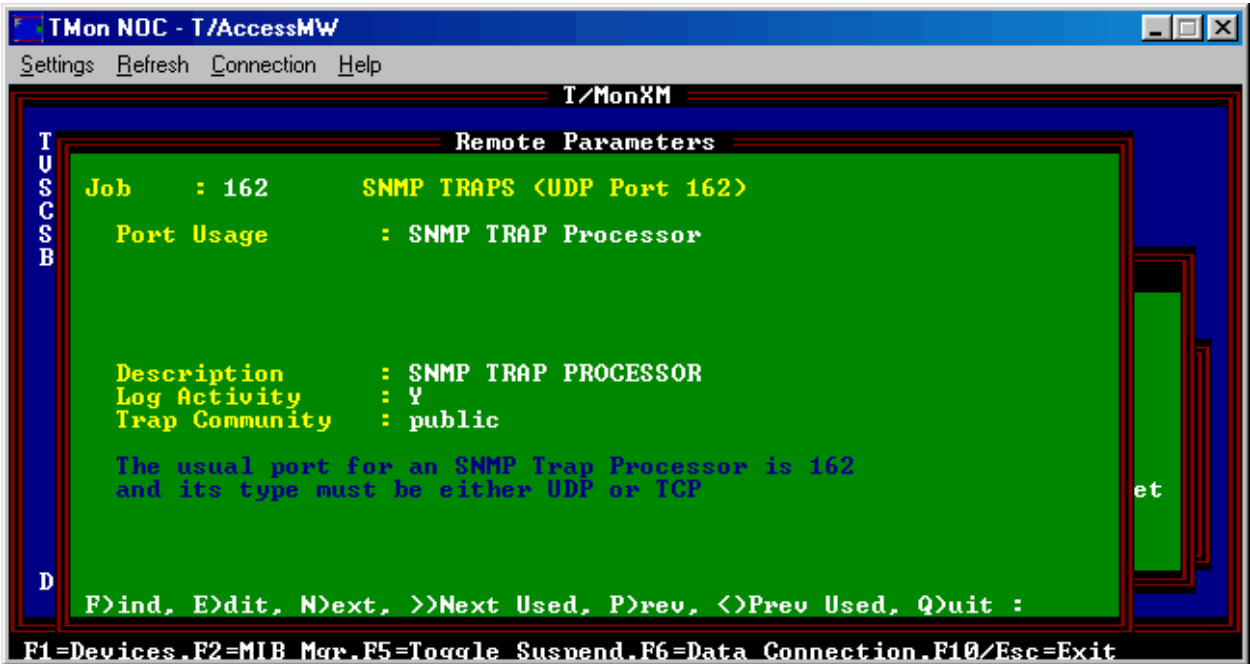
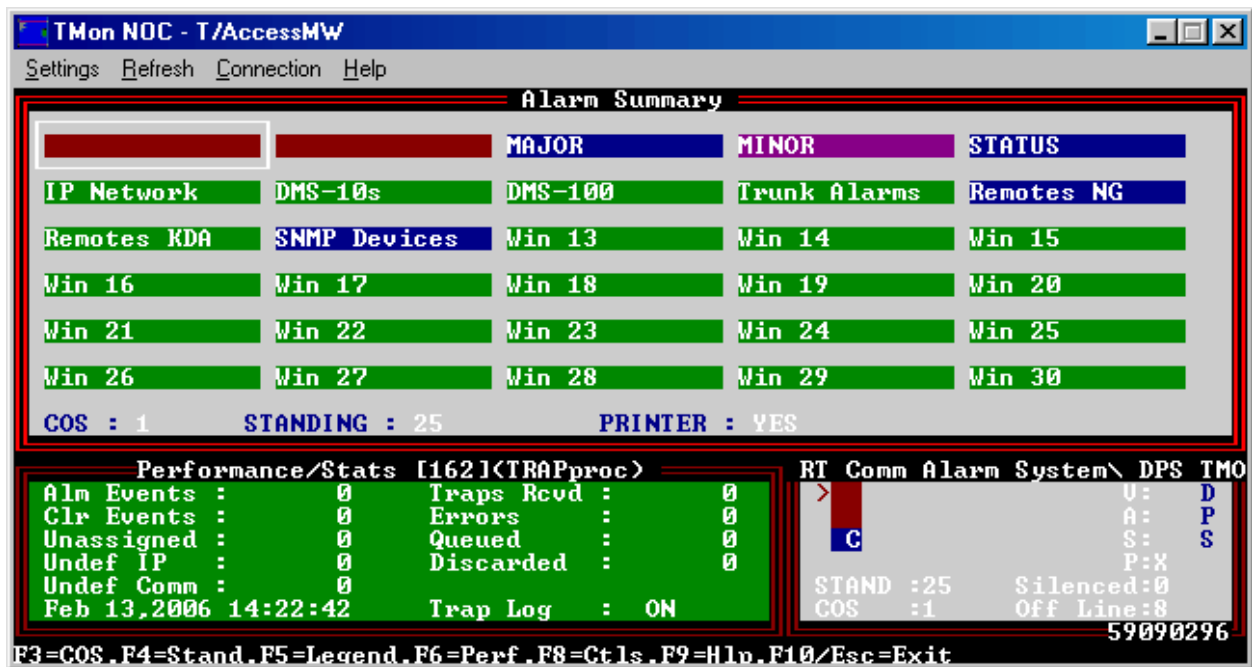


Fig. M12-14 - SNMP Trap Processor job

The second and recommended method for enabling trap logging is performed from the Alarm Summary screen in monitor mode. While in the Alarm Summary screen press “Shift-F9” to toggle the status of trap logging. The status of trap logging can be seen from the Performance/Stats screen of the SNMP Trap Processor by examining the “Trap Log” field. Pressing “Shift-F9” will toggle the status of trap logging regardless of whether the user is viewing the Performance/Stats screen of the SNMP Trap Processor.



**Fig. M12-15 - Alarm Summary**

One thing to remember about enabling or disabling trap logging from monitor mode is that when the system is reinitialized, trap logging will always return to the state of the “Log Activity” field in the Remote Parameters screen (see Figure M12-14). This means that if the “Log Activity” field in the Remote Parameters screen is set to ‘Y’ and you disable trap logging from monitor mode, then trap logging will only remain disabled until you reinitialize the system. The opposite is also true, if the “Log Activity” field in the Remote Parameters screen is set to ‘N’ and you enable trap logging from monitor mode, then trap logging will only remain enabled until you reinitialize the system. This makes it possible to temporarily enable or disable trap logging without exiting monitor mode.

## Manually Acking Alarms

The TMon supports the manual “Acking” (clearing) of alarms created by SNMP traps if the user’s security rights are set accordingly. This is especially beneficial when there is a set trap without a corresponding clear trap. Acking the SNMP alarm will clear the alarm from the Standing Alarms window and generate a clear COS entry in the COS Alarms window.

To assign a user security access to Ack SNMP alarms set the “Ack SNMP Alm” field in the System Users screen to “YES”. This will allow the user to Ack any SNMP alarm that they can see.

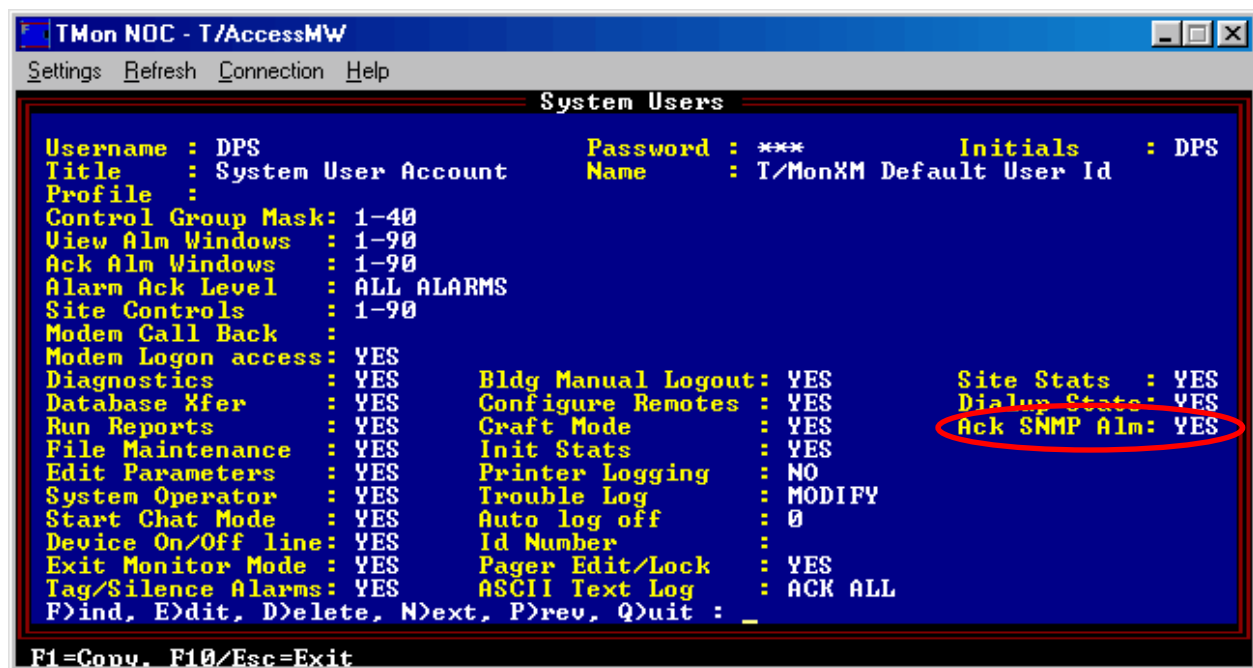


Fig. M12-16 - System users screen

The Acking of SNMP alarms occurs in monitor mode from the Standing Alarms screen. Only SNMP alarms can be Acked. SNMP Alarms can be identified by the 'T' at the beginning of the alarm entry. The 'T' is visible even if the user does not have access to Ack SNMP alarms. Pressing "Alt-F9" while highlighting the SNMP alarm in the Standing Alarms screen will clear the alarm, if the user has sufficient access. Pressing "Alt-F9" from any other screen, including the COS Alarms screen, will not clear the alarm.

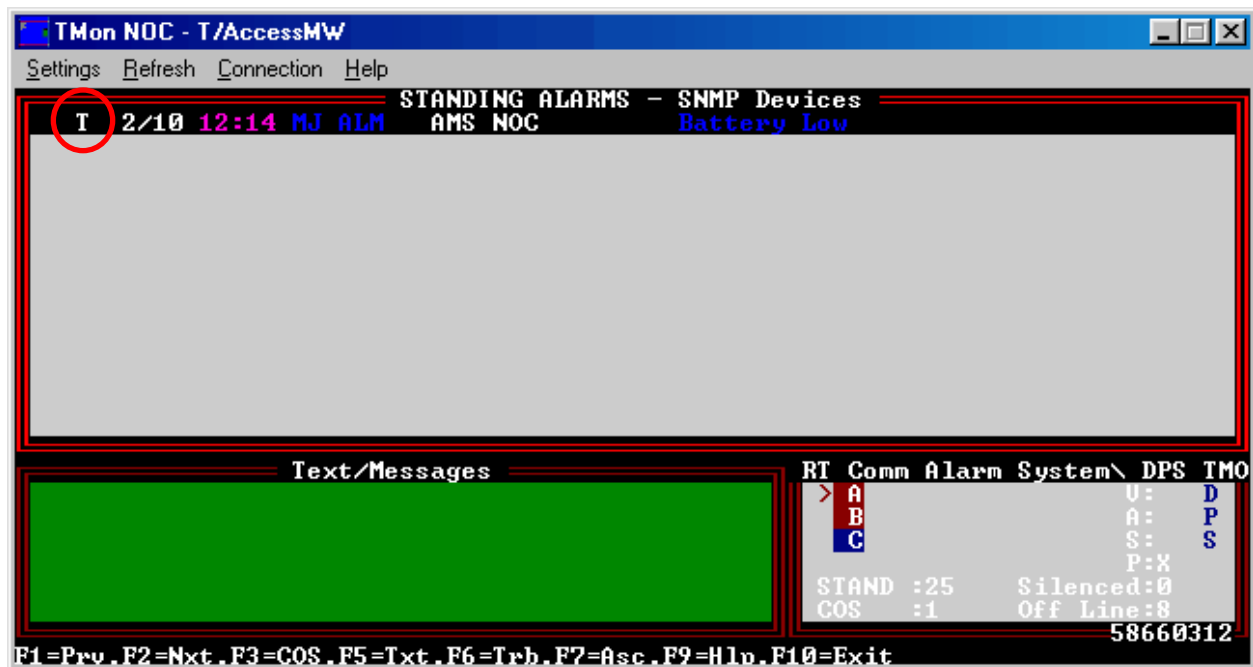


Fig. M12-17 - COS alarm

The following is the COS clear entry which occurred after Acking the SNMP alarm.

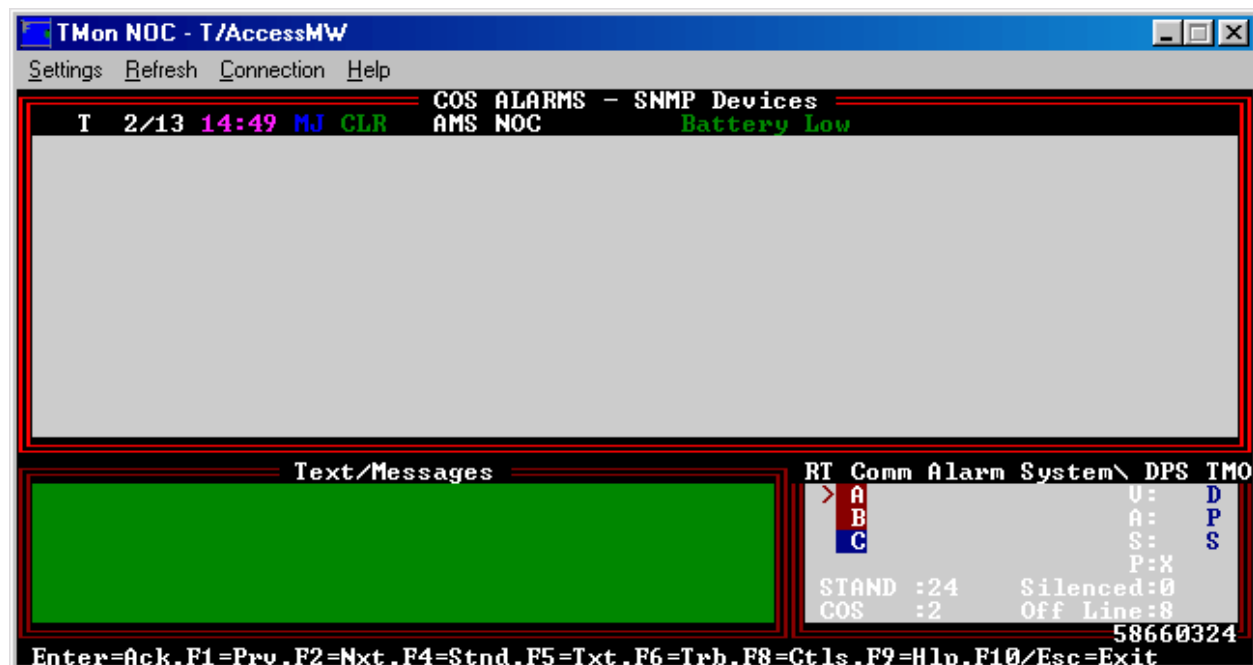


Fig. M12-18 - COS entry acknowledged

# SET and GET Commands

The TMon has support for issuing SNMP GET and SET commands. This allows the TMon to write to SNMP devices that have MIB elements with “read-write” access via an SNMP SET and read from SNMP devices that have MIB elements with “read-only” access via an SNMP GET. SET commands are defined at the device level by pressing “Alt-F2” from the Remote Device Definition screen. GET commands are defined at the device level by pressing “Alt-F5” from the Remote Device Definition screen.

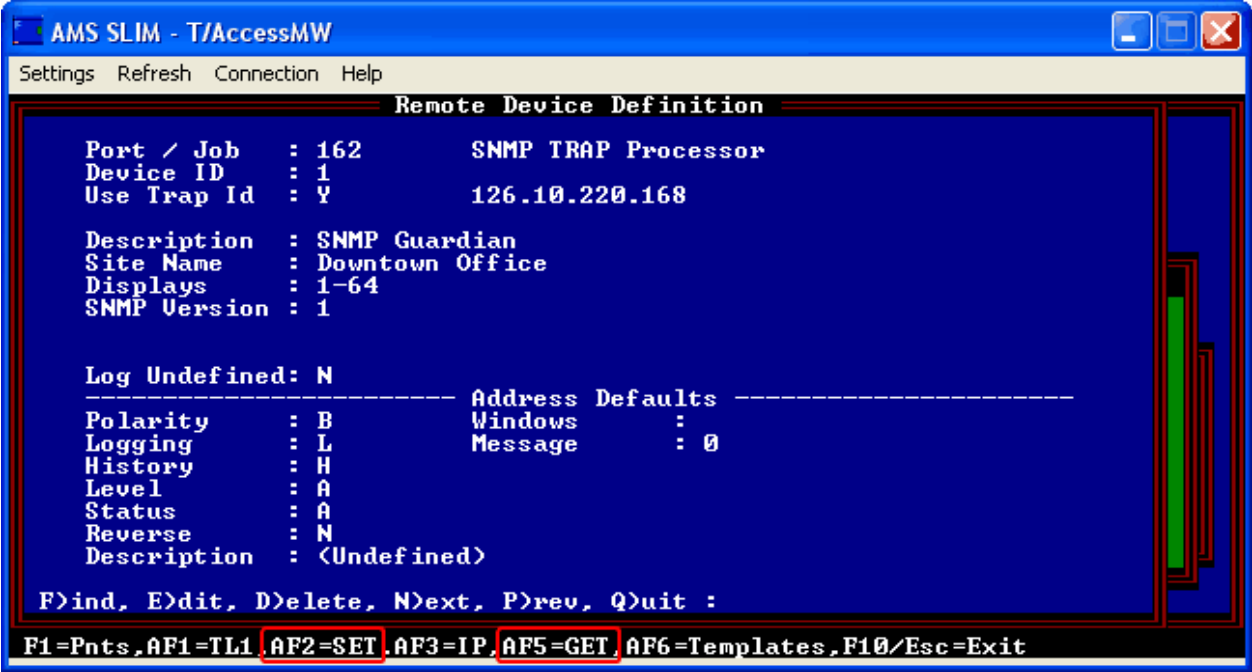


Fig. M12-18 - Remote Device Definition Screen for an SNMP device

Up to 999 SNMP GET and SET commands can be defined per device (999 of each). The device templates (“Alt-F6” from the Remote Device Definition screen) also supports importing and exporting GET and SET commands thereby saving valuable databasing time.

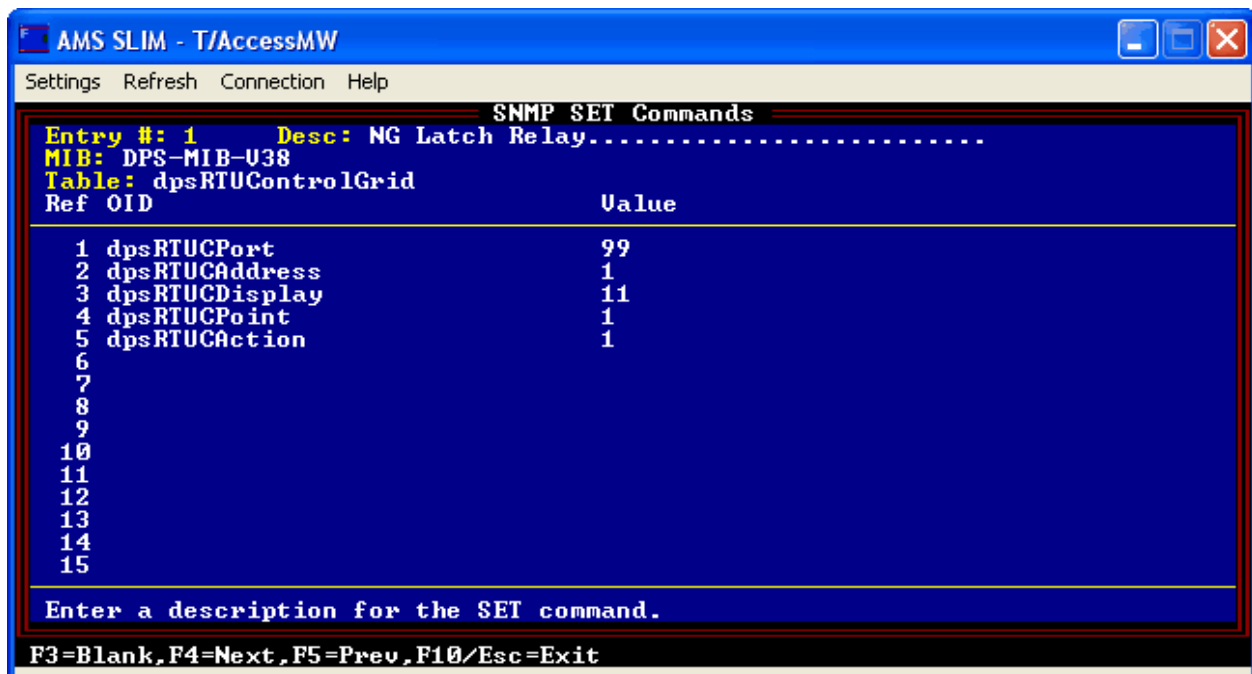


Fig. M12-19 - Databasing an SNMP SET command

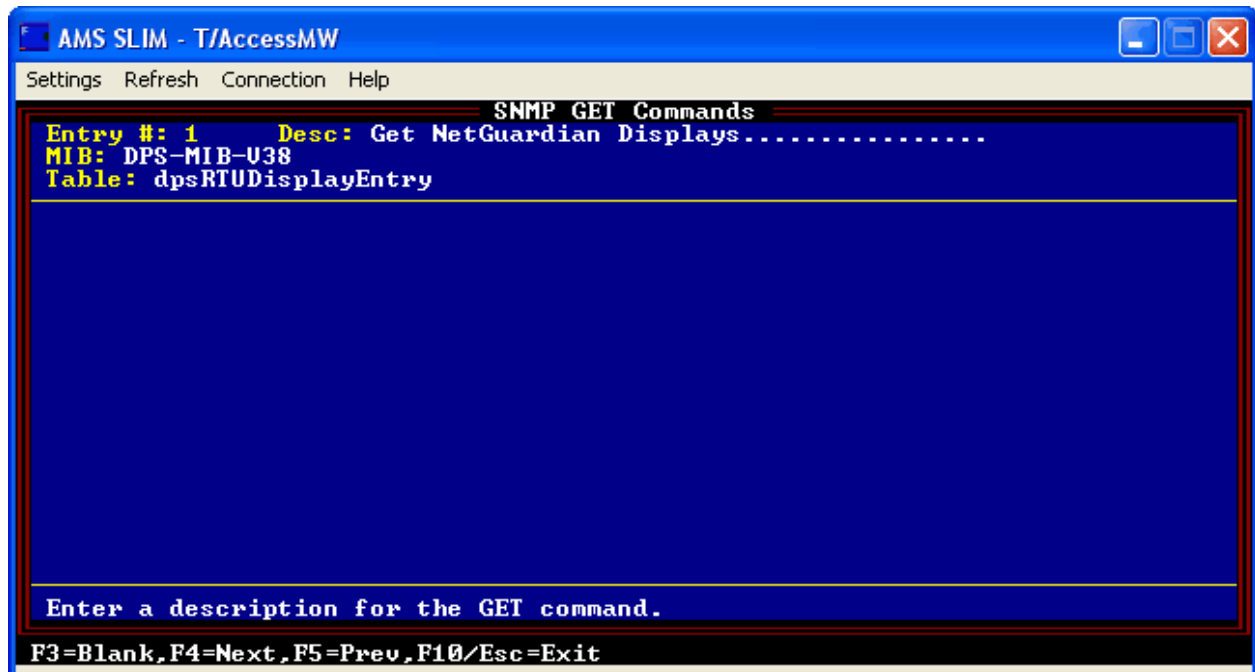
The following is the COS clear entry which occurred after Acking the SNMP alarm.

In order for the TMon to issue an SNMP GET or SET command it must first be defined as an "Entry" (1-999) at the device level.

The steps for defining a SET command are as follows:

1. Press "Alt-F2" from the Remote Device Definition screen to get to the SNMP SET Commands screen.
2. Enter a description of what the SET command will do in the "Desc" field.
3. Select the MIB which contains the table containing the objects you would like to SET on the SNMP device in the "MIB" field.
4. Select the MIB table containing the objects you would like to SET on the SNMP device in the "Table" field.
5. Enter the objects you would like to SET in the "OID" field and the value you would like to write to the object on the "Value" field. You must select one or more objects for the SET command to work.





**Fig. M12-20 - Databasing an SNMP GET command**

The steps for defining a GET command are as follows:

1. Press “Alt-F5” from the Remote Device Definition screen to get to the SNMP GET Commands screen.
2. Enter a description of what the GET command will retrieve in the “Desc” field.
3. Select the MIB which contains the table you would like to GET on the SNMP device in the “MIB” field.
4. Select the MIB table you would like to GET on the SNMP device in the “Table” field.

After creating a GET or SET command it must then be associated with a control point. TMon supports Labeled Controls, Site Controls and Derived Controls, all of which can be associated with SET commands. Because GET commands must be issued manually they can only be associated with Labeled Controls and Site Controls, not with Derived Controls.

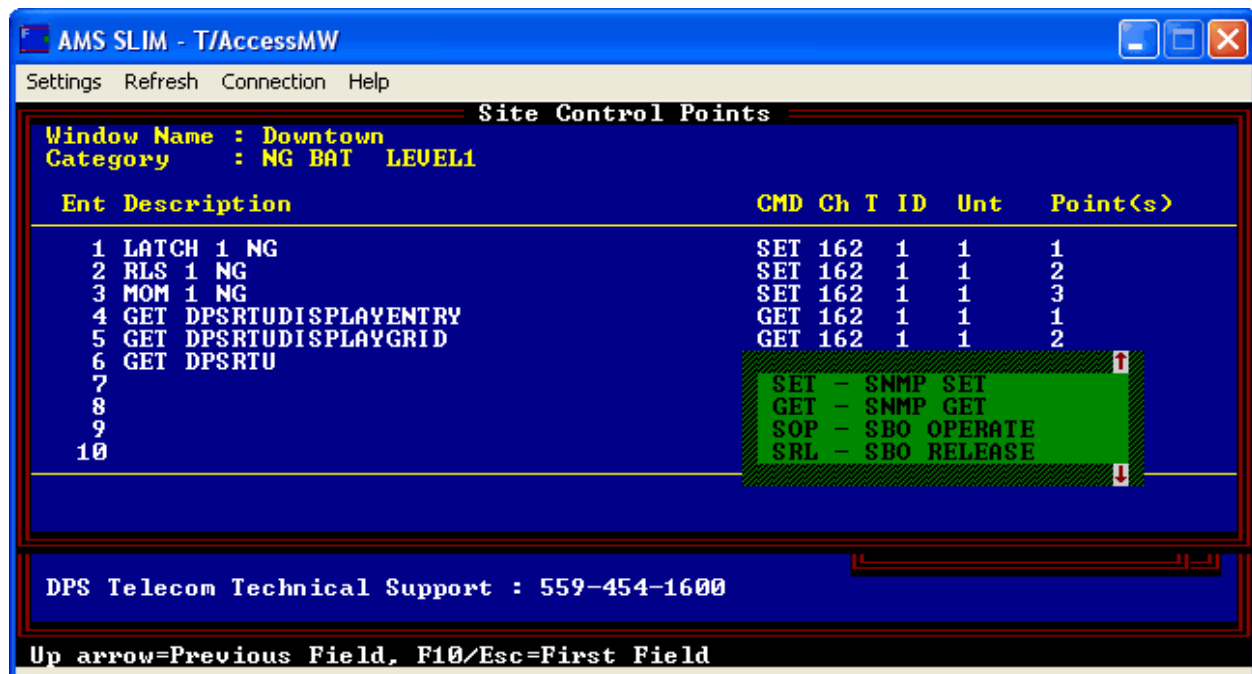


Fig. M12-21 - Associating GET and SET commands with control points

The steps for associating a GET or SET command with a control point are as follows (example with Site Controls):

1. Navigate to the desired Control Points screen (in this case Site Control Point screen).
2. Enter a description of what the control point will do in the "Description" field (same as GET and SET command description).
3. Select the "SET - SNMP SET" or "GET - SNMP GET" control type in the "CMD" field.
4. Enter the job number that you defined the SNMP GET or SET command under in the "Ch" field.
5. Enter the device number that you defined the SNMP GET or SET command under in the "ID" field.
6. Enter the display number that you defined the SNMP GET or SET command under in the "Unt" field. The display is really just a way of breaking up the SNMP command entries into banks of 64. For example:
  - Display 1=SNMP GET or SET command entries 1-64
  - Display 2=SNMP GET or SET command entries 65-128
  - Display 16=SNMP GET or SET command entries 961-999

7. Enter the point number that you defined the SNMP GET or SET command under in the “Point(s)” field. The point is referring to the SNMP GET or SET command’s position with in the bank of 64 entries (see the previous step) which it is assigned to.

For example:

- -SNMP GET or SET command entry 1 = Display 1, Point 1
- -SNMP GET or SET command entry 2 = Display 1, Point 1
- -SNMP GET or SET command entry 64 = Display 1, Point 64
- -SNMP GET or SET command entry 65 = Display 2, Point 1
- -SNMP GET or SET command entry 999 = Display 16, Point 39

Once the SNMP GET or SET command is associated with a control point it can then be issued from monitor mode in the same manner as you would do any other control point.

## Shortcut Commands

### Copy, Next, and Previous

If you are defining alarm points for many SNMP devices, using the shortcut commands will help you work more quickly and easily. The shortcut commands-Copy, Next, Previous, and Translate-are shown in Figure M12.19. By using the shortcut commands you can work with many alarm points without closing the Trap Association screen.

The Copy (F2) command copies the variable binding settings of the previous alarm point to the alarm point that is currently open. This is useful if your trap associations are fairly similar and only a few variable binding settings need to be changed for other alarm points.

Using the Next (F4) and Previous (F5) commands, you can work with the trap associations for successive alarm points without closing the Trap Association screen. The Next command moves from Fail to Clear, to the Fail condition of the next alarm point, and so on. The Previous command moves from Clear to Fail, to the Clear condition of the previous alarm point, and so on.

The Next and Previous commands are also the most efficient way to quickly review and inspect your configuration.

### Translate Command

The Translate (F6) command changes variable binding values for an entire range of alarm points. In the example in Figure M12-20, there are two sites that are almost identical, except for one variable binding. Site 1 will send a trap with a dpsRTUAddress variable binding of 1 and Site 2 will send a trap with a dpsRTUAddress variable binding of 2.

The user need not define an entire database for Site 2 to change this single value. In the example the user has cloned the site definition

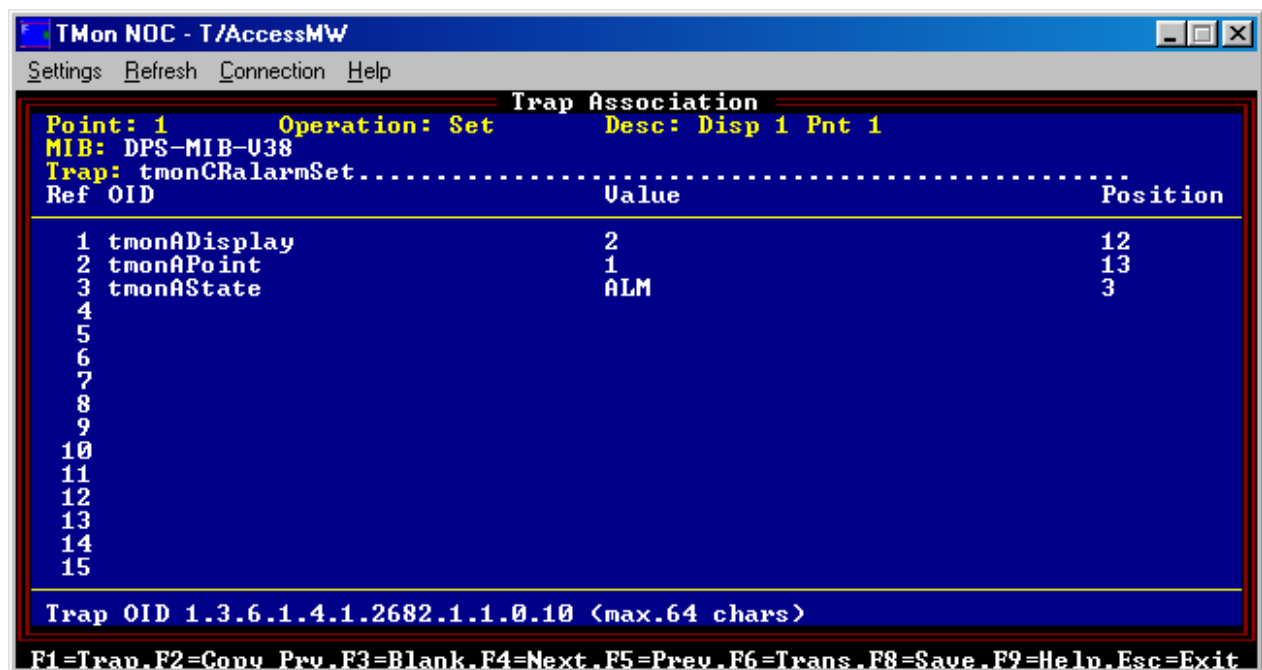
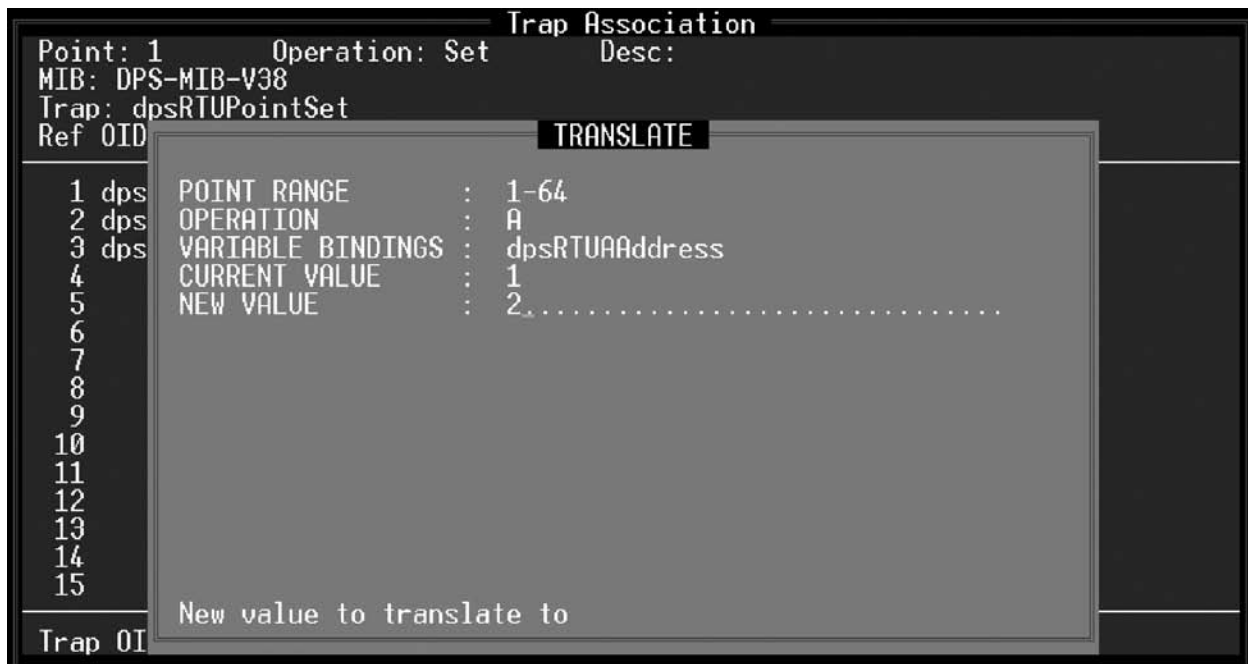


Fig. M12-22 - Copy, Next, Previous, and Translate commands



**Fig. M12-23 - Translate screen**

for Site 1 to Site 2, then used the Translate command to change the dpsRTUAddress variable binding value for all points on Site 2.

To clone a site or display, follow these steps:

1. Choose Master > Parameters > Remote Ports.
2. Choose Devices (F1).
3. Using the Next and Previous commands, select the destination (the port you will be copying to)
4. Choose Points (F1)
5. Choose Edit.
6. Choose Read (F6)
7. Enter the information of the source (the port you will be copying from). The available fields are source port number (1-n or RP for a dial-up port), device number, address number, and display number. The cursor will skip fields that are not applicable to the type of port.
8. The specified source display will be copied to the screen. It may now be modified using the Translate command.

For more information about cloning, see Section 10 (Point Definition Tutorial).

To use the Translate command, press F6 from the Trap Association screen. This command opens the Translate screen. The first four fields in this screen (Point Range, Operation, Variable Bindings, and Current Value) define which values will be changed. The last field, New Value, defines the new value that will be applied to the

value specified in the previous fields.

The fields in the Translate screen are:

**Point Range:** Enter the alarm points you wish to change. Ranges may be entered using dashes and commas without spaces. Valid alarm point ranges are 1-64. Only alarm points in the selected range will be changed.

**Operation:** Valid entries are A (change values for both fail and clear conditions of the alarm points selected); S (change values only for the set, or fail, condition of the alarm points selected); or C (change values only for the clear condition of the alarm points selected).

**Variable Bindings:** When this field is selected, a list of the variable bindings that have been defined for this alarm point will appear. Press Tab to select the list box, scroll to the desired variable binding, and press Enter. Only the variable binding you have selected will be changed by the Translate command.

**Current Value:** This field displays which values will be changed. If this field is left blank, the value entered in the New Value field will be applied to all values. If you wish to change only a particular value, enter it here.

**Note:** Each of the entries you make in these fields successively narrows the scope of the Translate command. Choose your entries carefully. If you enter exactly the range of values that you wish to change, you can save yourself a great deal of repetitive editing, but be careful to only change the values you want to change.

**New Value:** Enter the new value for the variable binding.

After each entry, press Enter to select the next field. When the cursor is at the last field, press Enter to execute translation and close the Translate screen.

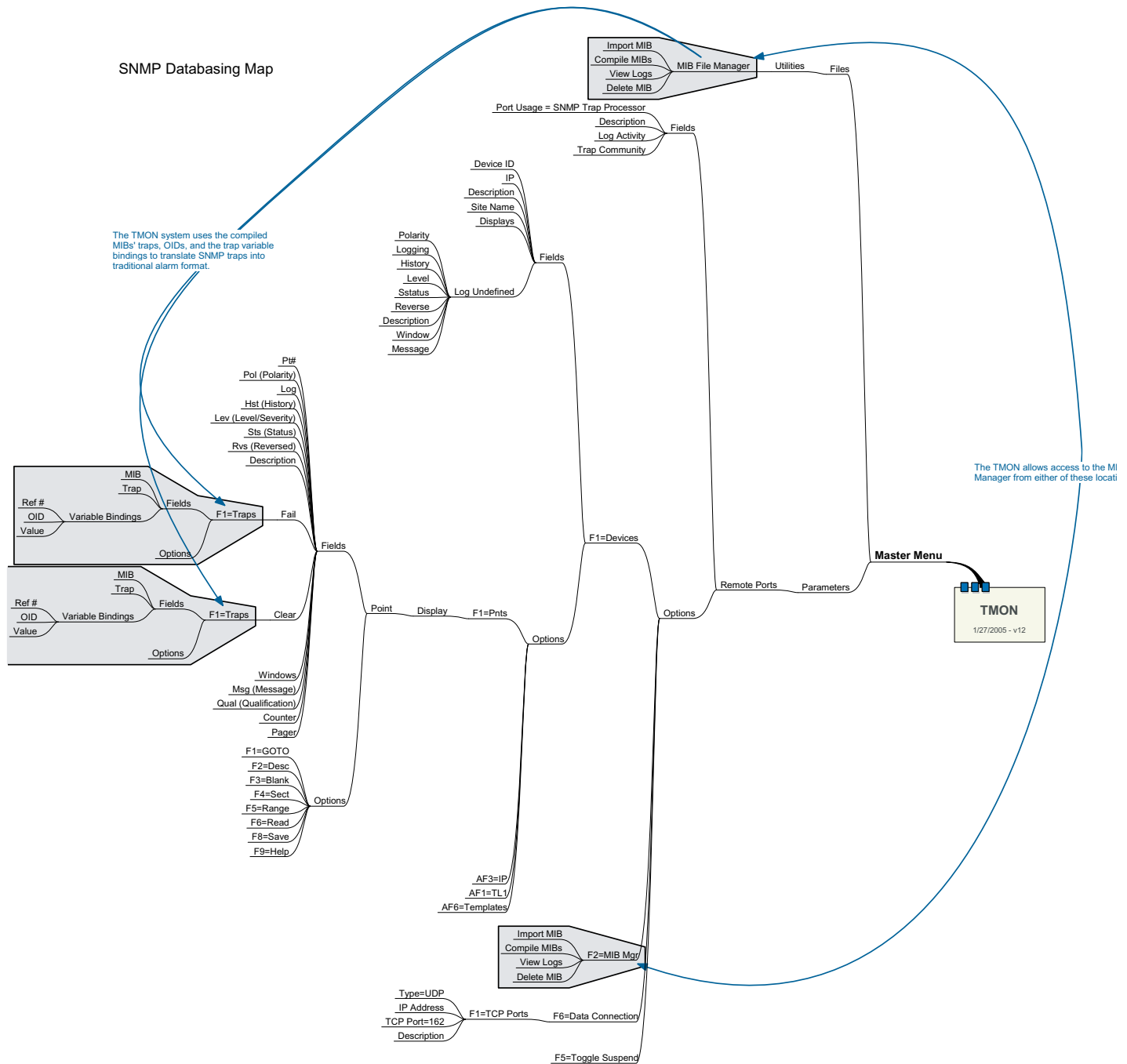


Fig. M12-24 - SNMP Databasing Map

## Variable Binding Pattern Matching

The SNMP Trap Processor allows partial matches of variable binding values by using special commands. This will search for a substring with the received value and will only work with text type variable bindings.

Commands must be entered on the Variable Binding Value field and must uppercase.

### Hex Octet containing non-ASCII characters.

Command	Description	
#OS1_	Summary	<p>This will convert decimal values into a hex octet string. Each decimal value must be separated by dots and can only be between 0 and 65535.</p> <p>#OS1_ must be entered as uppercase characters to be detected as a special command.</p> <p>Each decimal value will be converted to 2 bytes.</p>
	Syntax	#OS1_###.###.###
	Where	## are numerical values.
	Example	
	Input	#OS1_1.2.3
	Matching Variable Binding Value	0x00010002003
	Input	#OS1_4660.22136
	Matching Variable Binding Value	0x12345678 Where 1234h=4660 5678h=22136



**Case-Sensitive Text**

Command	Description	
<b>#CS1_</b>	Summary	This will preserve lowercase characters entered in the variable binding value field.
	Syntax	#CS1_CaseSensitive
	Where	CaseSensitive is case sensitive text.
	<b>Example</b>	
	Input	#CS1_Apple
	Matching Variable Binding Value	Apple *Will not match on "apple"

**Pattern Matching Text**

Command	Description	
#PM%	Summary	<p>This will allow matching of a substring. The percent sign is used as the wildcard character and can be replaced with any character.</p> <p>The entered text is case sensitive and must match exactly.</p>
	Syntax	#PM%_Text1%
	Where	<p>% is a wildcard and Text1 is the text that we are trying to match on.</p> <p>To match Text1 at the start of the line, include the wildcard after the text.</p> <p>To match Text1 in the middle of the line, include the wildcard before and after the text.</p> <p>To match Text 1 at the end of the line, include the wildcard before the text.</p>
	<b>Example</b>	
	<b>Match text on start of line.</b>	
	Input	#PM%_Start%
	Matching Variable Binding Value	<p>"Start Line"</p> <p>*Will not match on "Line Start"</p>
	<b>Match on a string somewhere in the middle of the line.</b>	
	Input	#PM%_ %Middle%
	Matching Variable Binding Value	<p>"Line Middle Line"</p> <p>*Will not match the following:</p> <p>"Middle Line"</p> <p>"Line Middle"</p>
	<b>Match on a string at the very end of the line.</b>	
	Input	#Pm_ %End
	Matching Variable Binding Value	<p>"Line End"</p> <p>*Will not match the following:</p> <p>"End Line"</p> <p>"Line End Line"</p>
	<b>Combinations of more than one substring on the same line.</b>	
	Input	#PM%_ %Egg%Chicken%
	Matching Variable Binding Value	<p>"Line Egg Chicken Line"</p> <p>*Egg must come before Chicken. And both must show up.</p>
	Input	#PM%_Start%End
	Matching Variable Binding Value	<p>"Start Line End"</p> <p>*Start must be at start and End at end.</p>

**Pattern Matching Text Cont.**

Command	Description	
#INT_	Summary	<p>Can be used to allow processing of variable binding integer values to be within a specific range.</p> <p>The first numerical value of the received variable binding will be processed as an integer. The rest of the value will be ignored. If the received value starts with a non-numerical character, this will always fail.</p>
	Syntax	#INT_Range
	Where	Range contains a start and end value "1-10", greater than ">10" or less than "<10". The received integer value must be within the specified range to match the trap.
	<b>Example</b>	
	<b>Match on integer values between 90 to 100. Including 90 and 100.</b>	
	Input	#INT_90-100
	Matching variable binding Value	<p>"59"</p> <p>"63 alarm"</p> <p>*Will not match on the following:</p> <p>"30"</p> <p>"alarm 86"</p>
	<b>Match on integer values less than 27. Not including 27.</b>	
	Input	#INT_<27
	Matching variable binding value	<p>"20"</p> <p>*Will not match on the following:</p> <p>"27"</p> <p>"30"</p>
	<b>Match on integer values greater than 30. Not including 30.</b>	
	Input	#INT_>30
	Matching variable binding value	<p>"59"</p> <p>"63 alarm"</p> <p>*Will not match on the following:</p> <p>"30"</p> <p>"alarm 86"</p>

## AutoSNMP

SNMP Traps can be processed to automatically define and generate alarm points with Autodatabasing SNMP Device types. AutoSNMP Device Types can be assigned to regular SNMP devices. This will allow all unassigned traps to run through a set of rules similar to AutoASCII and automatically database a new point.

AutoSNMP Device Types can be defined on the Remote Parameter screen by navigating to the SNMP Trap Processor and pressing F3. From the Main Master Menu, press P for parameters. Press R for remote ports. Press F for find. Enter the SNMP Trap process job number. Or press < and > to navigate through all defined jobs. Then press F3 to enter the AutoSNMP Device Types window.

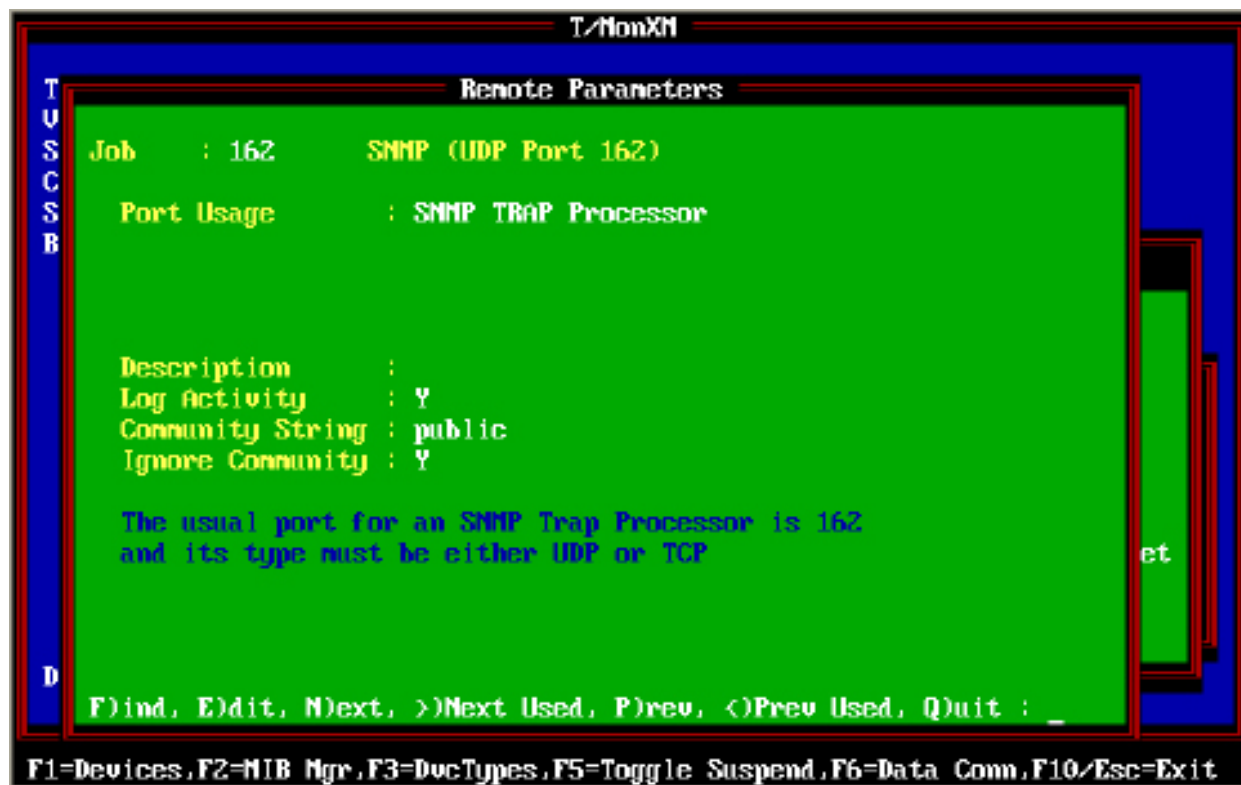


Fig. M12-25 - Setting up AutoSNMP at the Remote Parameters screen

Define a new AutoSNMP device by pressing F for find and entering a Device ID number. This number will be associated with a 6 character Device Name. Make sure this name is unique and not already assigned as an AutoASCII device or as an AutoSNMP device.

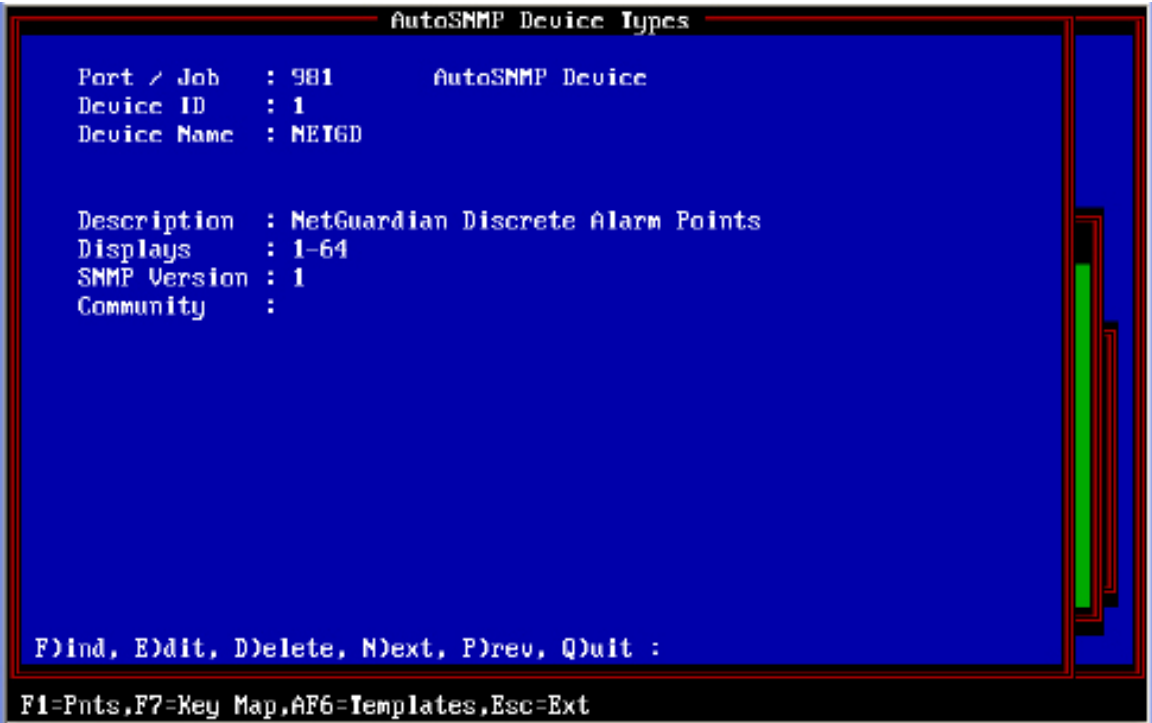


Fig. M12-26 - AutoSNMP device types

Enter the Description, displays, SNMP Version and Community setting. Default values should work for most cases.

Press F1 to enter the Point Definition screen. This is where we will enter our SNMP Trap rules. The screen will look and behave like any other Point Definition screen.



Fig. M12-27 - Entering AutoSNMP Trap rules

Define a new point. The values entered here will be used as the default when creating new AutoSNMP points.

After the point has been defined go back through the line and stop on the Fail and Clear fields. Press F1 to enter the Trap Association screen. AutoSNMP rules will be defined here. F1 on Fail will define the SET trap associations. F1 on Clear will define the CLEAR trap associations.

AutoSNMP Trap Association			
Point: 1		Operation: Set	Desc: NetGuardian Point
MIB: DPS-MIB-MGD-U10			
RTrip: dpsRTUp8001Set*		MTRP:A	
Ref	OID	Value	Position
1	dpsRTUAPoint		7
2	dpsRTUAState	ALARM:	9
3	dpsRTUDateTime		3
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Reference Trap OID 1.3.6.1.4.1.2682.1.2.0.8001 <max.64 chars>

F1=Trap, F2=Copy Prev, F3=Blank, F4=Next, F5=Prev, F6=Trans, F8=Save, F9=Help, Esc=Exit

Fig. M12-28 - Entering SET and CLEAR trap associations

Unassigned traps will only be processed against the SET trap association. If the unassigned trap matches the SET rules, it will process the associated CLEAR to create the CLEAR trap association.

Start by entering a MIB. Selecting a MIB other than MANUAL MODE will allow selection of variable names for the Trap OID and variable binding OIDs.

Enter the Trap OID by either selecting it from the drop down list or manually entering a value. The drop down list will only be populated if a MIB was selected in the MIB field. This field may contain a numerical Trap OID, a trap OID variable name (from the MIB), a wildcard character "\*" or an offset. The offset value can only be entered for CLEAR trap associations. Entering a value of "+1000" will adjust the received Trap OID's last value by adding 1000. "-1000" will subtract 1000.

Use the wildcard if you are going to process the same variable bindings against several traps with different Trap OIDs.

Use a specific Trap OID if the set of rules should only be processed against a specific trap.

Entering an "\*" symbol at the end of the Trap OID indicates a wildcard and will process all unassigned traps against this point's variable binding rules but will also populate the variable binding OID

drop down lists with data. This makes databasing easier if the traps you want to run the rule against has the same format as the selected trap but may not necessarily always be the same trap OID.

Enter “A” or “R” in the MTRP field to match all traps (wildcard) or match only on the reference trap.

Enter the Variable Binding section. The first 15 variable bindings are used to match on received trap data. An AutoSNMP point will not be generated if any of the defined variable bindings between 1 and 15 do not match the received data. Variable bindings 16 through 30 are used to store constants for use with building the AutoSNMP point definition.

The OID field can hold a wildcard “\*” character to match any received OID. The Variable Binding position will determine which received data needs to be processed.

The value field for AutoSNMP Device Types will have 2 parts that are separated by a pipe symbol “|”. The first part is the matching portion. Pattern Matching can be used in this field. Leaving this part blank will match on any received value.

The second part of the Value field is the extraction value. This is the value that will be stored in the trap association when creating new AutoSNMP points. Leaving this part blank will store the received value in the trap association.

All defined variable bindings between 1 and 15 will be transferred over to the AutoSNMP point.

Variable bindings 16 to 30 allows matching of OIDs and variable binding positions. If the OID is defined and exists in the received trap, it will use the value from the matching variable binding as the constant. If the OID is not defined or doesn’t exist in the received trap, it will check for the variable binding position. If the position is defined and found in the received trap, the value from the matching variable binding will be used as the constant. If the position is not defined or was not found in the received trap, it will use the value entered in the Value field as the constant. These constants are used for key mapping.

If you wish to resolve an integer value to the text description given in the MIB, select OID and enter “#INTLOOKUP” in the value field. This will only work with variable bindings 16-30.

The CLEAR trap association works the same as the SET except all of the matching is ignored. The CLEAR trap association is only used to determine which variable bindings needs to be used for the AutoSNMP point and what values to store.

Entering a specific Trap OID value in the CLEAR trap association will store the entered value on the AutoSNMP CLEAR trap association. This value will not be used to filter the received trap.

After entering the SET and CLEAR rules, press F8 to save and go back to the AutoSNMP Device Types window.

Define the key mapping by pressing F7. Select Key Mapping to define the alarm point definition. This behaves the same as AutoASCII except the values that are entered here corresponds with a variable binding instead of a key slot. Entering a value between 1 and 15 will use the received value from the received variable binding. Entering a value between 16 and 30 will use a predefined constant.

AutoSNMP also only allows one table to be associated with each device. The table name is the same as the device name and gets processed after matching on the AutoSNMP device and before creating the new SNMP point.

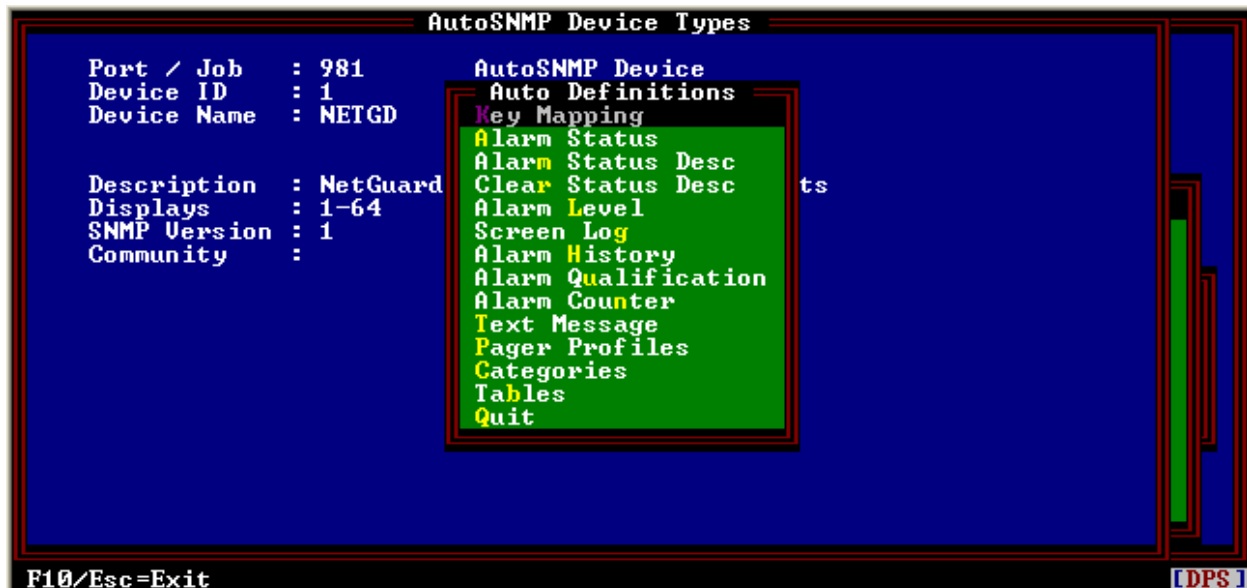


Fig. M12-29 - Key Mapping

Save the AutoSNMP Device Type and assign it to an SNMP Device.

Navigate back to the Remote Parameter window and press F1 for Devices.



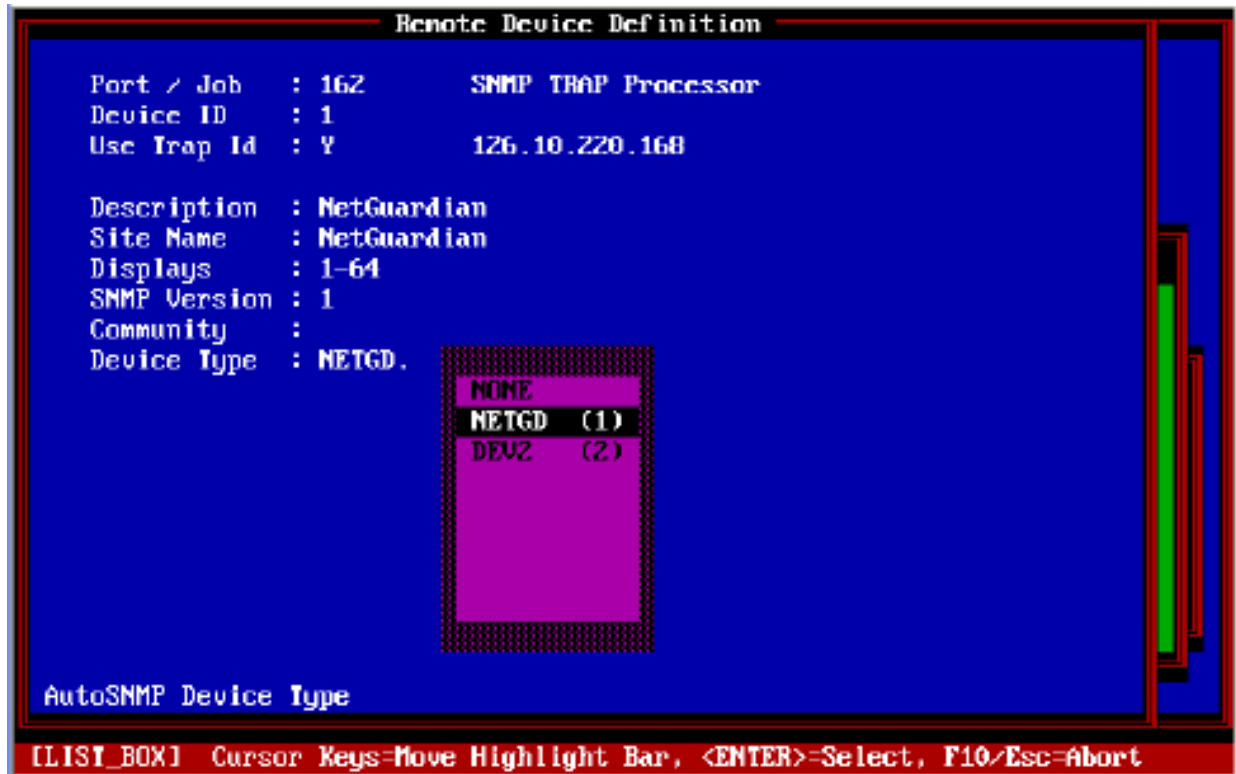


Fig. M12-30 - AutoSNMP devices

Press E for edit and enter down to the Device Type field. Press TAB and select an AutoSNMP Device Type for handling unassigned traps. The value next to the device name indicates the Device ID.

Pressing F3 on the Remote Device Definition screen will jump to the AutoSNMP Device Types screen.

## Import/Export of AutoSNMP Device Types

Press Alt+F6 on the AutoSNMP Device Types screen to display the Import/Export menu.

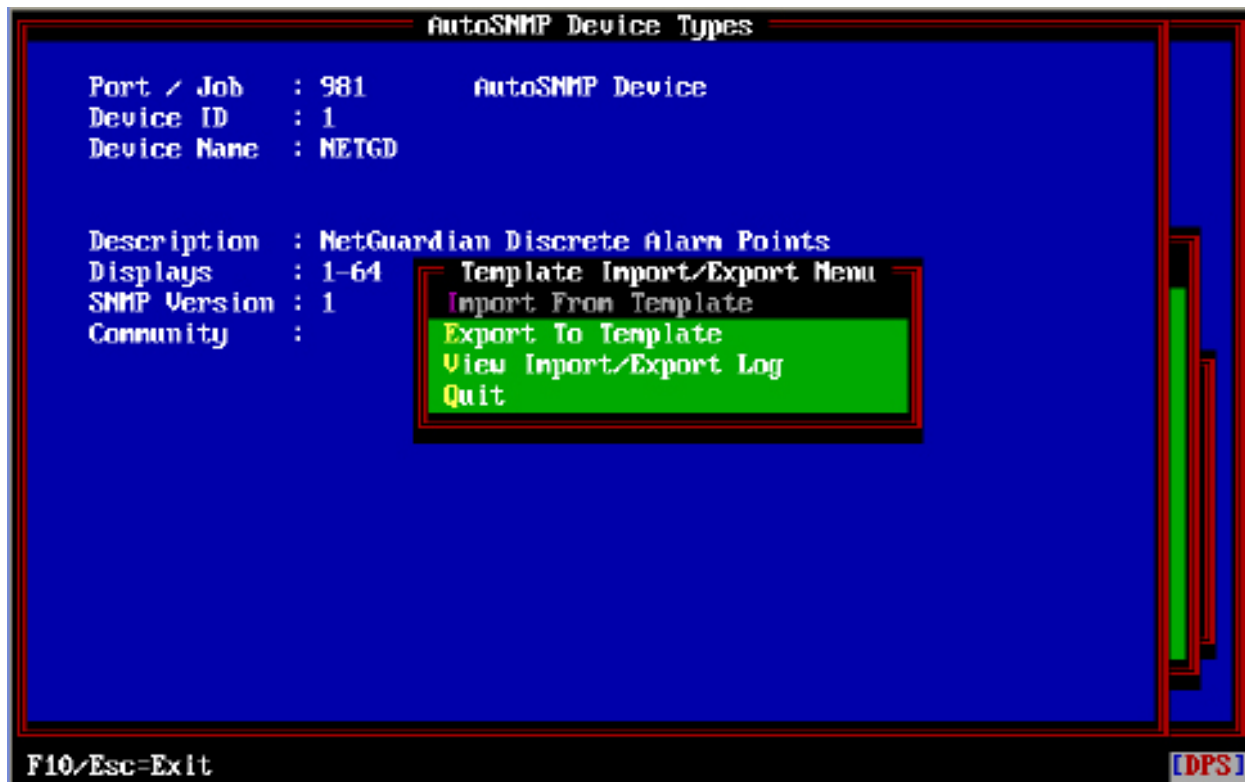


Fig. M12-31 - Import/Export Screen

Select Export To Template to export the selected device. This will export the point definition and the key mapping data.

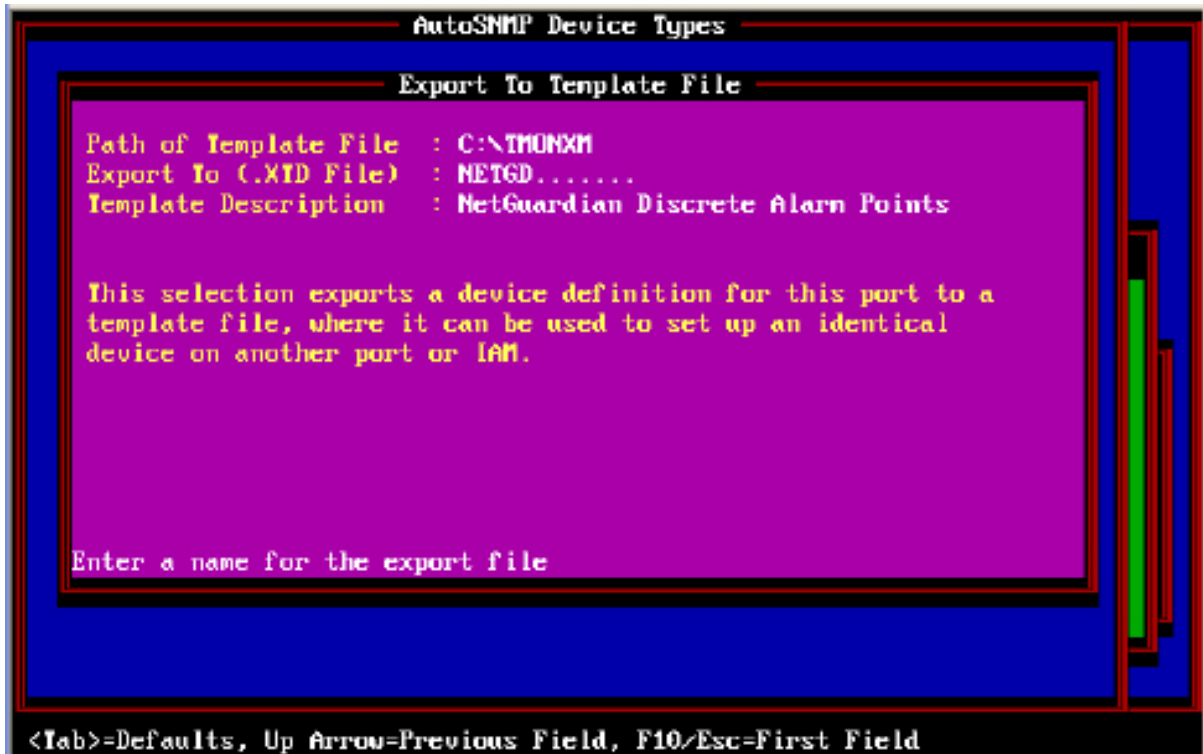


Fig. M12-32 - Export Point Definition and Key Mapping Data

Import by selecting Import From Template file. Make sure to create a new AutoSNMP Device Type before importing. Do not Import over an existing AutoSNMP Device Type with valid data.

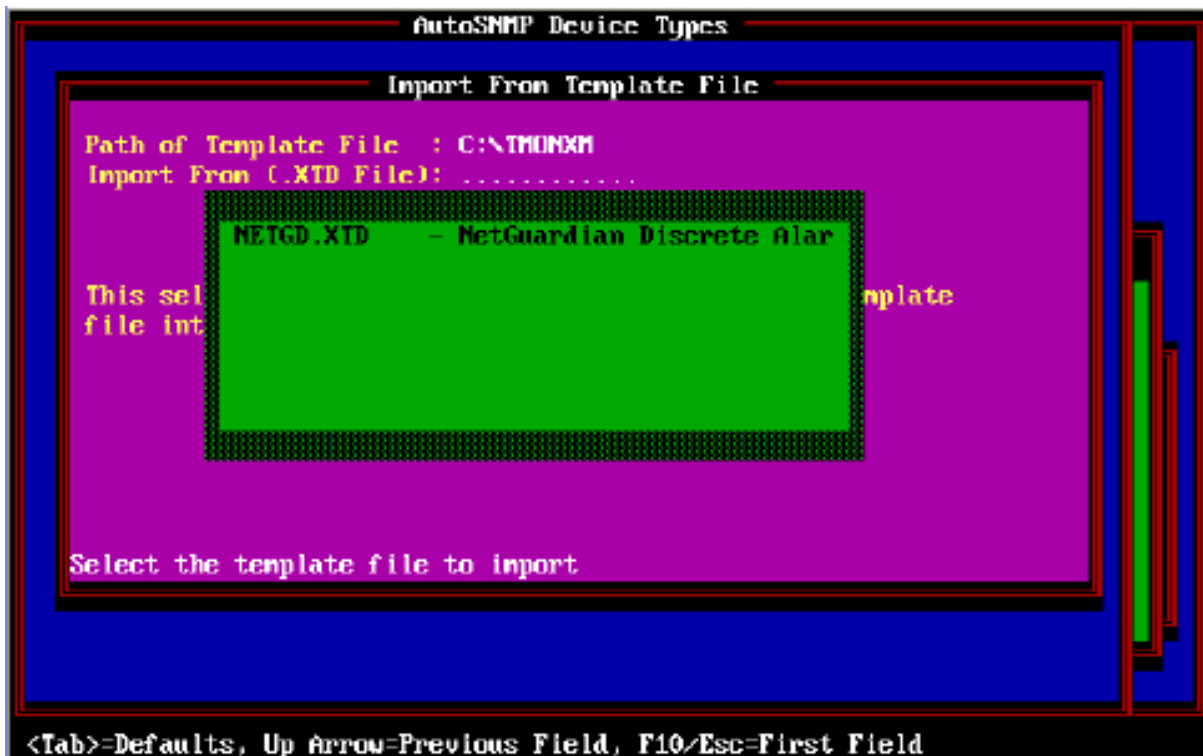


Fig. M12-33 - Import From Template

### Example

This example will show how to use AutoSNMP Device Types to automatically database NetGuardian discrete alarm points.

1. Define a new AutoSNMP Device Type by pressing F to find an available Device ID. It will prompt to add to the data base. Select Y for yes.
2. Enter NETGD as the Device Name. Enter a description and leave the rest with the default values.

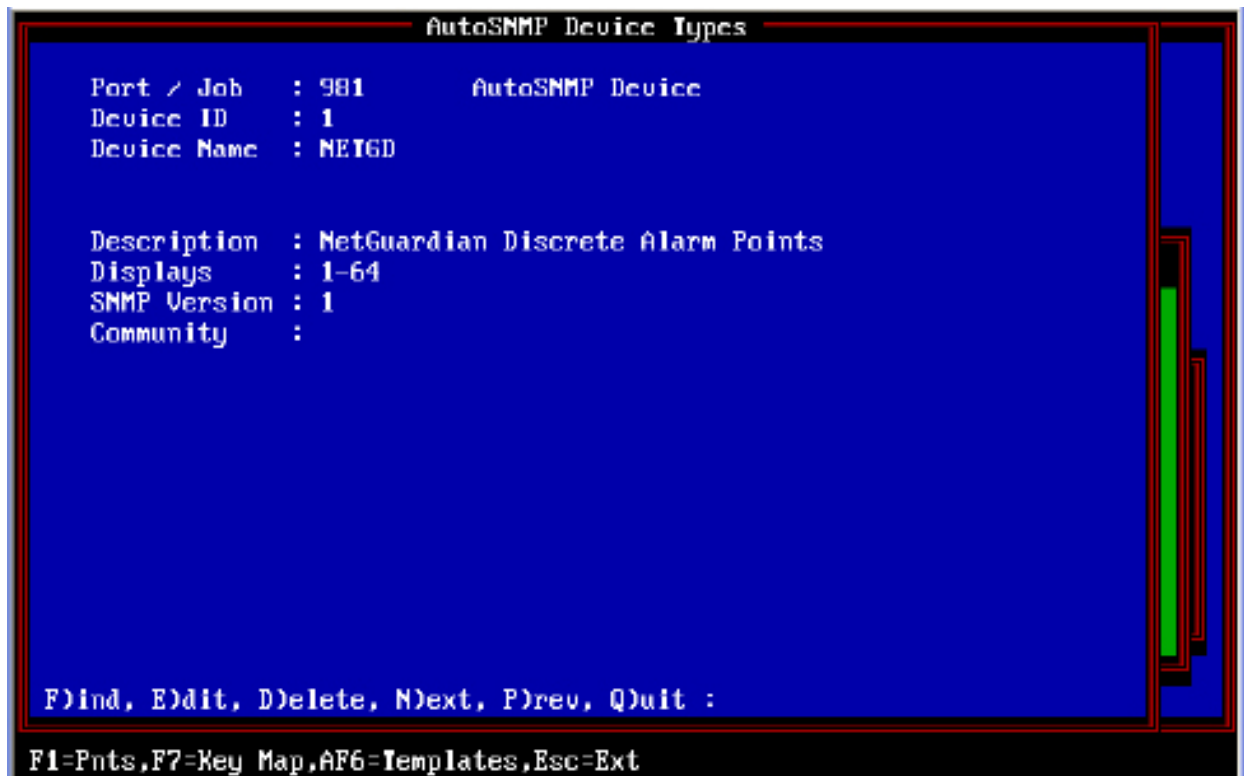


Fig. M12-34 -Defining a new AutoSNMP device

3. Press F1 to enter the Point Definition screen.

Point Definition

Job : SD    DuID: 1    Disp: 1    Display Desc :

P L H L S R

o o s e t u

Pt l g t u s s

AutoSNMP Device

Pt	Description	Fail	Clear
1	B L H A A N    NetGuardian Point		
2			
3			
4			
5			
6			
7			
8			

Enter Fail Status Description

Message

Up Arrow=Previous Field, F1=Traps, F10/Esc=First Field

Fig. M12-35 -Point Definition

4. Create a new display by pressing E for edit. Enter 1. It will prompt to add to the database. Select Y for yes.
5. Create a new point with default values. Enter all the way through the line.
6. Go back to the point we just defined and press F1 on the  
Fail field. This will bring up the AutoSNMP Trap Association window.

AutoSNMP Trap Association

Point: 1    Operation: Set    Desc: NetGuardian Points

MIB: DPS-MIB-NGD-V10

Trap: dpsRTUp8001Set\*

Ref	OID	Value	Position
1	dpsRTUAPoint		7
2	dpsRTUASState	ALARM	9
3	dpsRTUADisplay	1	6
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Trap OID 1.3.6.1.4.1.2682.1.2.0.8001 (max.64 chars)

F1=Trap,F2=Copy Prev,F3=Blank,F4=Next,F5=Prev,F6=Trans,F8=Save,F9=Help,Esc=Exit

Fig. M12-36 -Defining a new AutoSNMP device

7. Select the MIB DPS-MIB-NGD-V10.
8. Select dpsRTUp8001Set for the Trap OID.
9. Press F1 to go back to the Trap OID field and enter a "\*" at the end. This will catch all Trap OIDs but will allow us to select variable names for our variable bindings.
10. Select dpsRTUAPoint for the first variable binding. Enter "[" for the value without the quotes. Enter 7 for the position. This should already be filled in. Entering "[" means that we will match any value for this variable binding and we will store whatever value we had received. The OID must exist in the received trap for it to match. This will use the received point value and store it on the AutoSNMP point.
11. Select dpsRTUAState for the second variable binding. Enter "ALARM]" on the value field and 9 for position. We want to match on ALARM states only. Leaving the second part blank means we will store whatever we had received, which should be ALARM.
12. Select dpsRTUADisplay for the third variable binding. Enter "1]" on the value field and 6 for position. This is just to make sure that we don't match on anything from display 2 or 11. Display 1 is for discrete points.
13. Press down until you get to variable binding 16.
14. Select dpsRTUAPntDesc and enter "UNDEFINED" on the value field. This will use Undefined if the NetGuardian sends a blank description.

**AutoSNMP Trap Association**

Point: 1      Operation: Set      Desc: NetGuardian Points

MIB: DPS-MIB-NGD-V10

Trap: dpsRTUp8001Set\*

Ref	OID	Value	Position
16	dpsRTUAPntDesc	Undefined	8
17		Point	0
18		:	0
19			0
20			0
21	dpsRTUAAddress		0
22	dpsRTUADisplay		0
23	dpsRTUAPntDesc		0
24	dpsRTUAPoint		0
25	dpsRTUAPort		0
26	dpsRTUAState		0
27	dpsRTUDateTime		0
28			0
29			0
30			0

OID (max. 64 chars)

F1=Goto Trap, F3=Blank, F8=Save, F9=Help, F10/Esc=Exit

Fig. M12-37 - Defining discrete alarm points

15. Enter variable binding 17 and leave the oid field blank. Enter “Point ” in the value field and 0 for position.
16. Enter variable binding 18 and leave the oid field blank. Enter “:” in the value field and 0 for position.
17. Press F8 to save.
18. At the Point Definition screen, go to the Clear field and press F1.

The screenshot shows the 'AutoSNMP Trap Association' screen. At the top, it displays 'Point: 1', 'Operation: Clear', and 'Desc: NetGuardian Point'. Below this, it shows 'MIB: MANUAL MODE' and 'Trap: +1000'. A table lists variable bindings with columns for 'Ref', 'OID', 'Value', and 'Position'. The table contains three entries: Ref 1 with Value 'CLEAR' and Position 9; Ref 2 with Value '|' and Position 7; and Ref 3 with Value '|' and Position 6. The bottom of the screen shows a status bar with function key definitions: F1=Trap, F2=Copy Prv, F3=Blank, F4=Next, F5=Prev, F6=Trans, F8=Save, F9=Help, Esc=Exit.

Ref	OID	Value	Position
1	*	CLEAR	9
2	*		7
3	*		6
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Trap OID +1000 (max.64 chars)

F1=Trap, F2=Copy Prv, F3=Blank, F4=Next, F5=Prev, F6=Trans, F8=Save, F9=Help, Esc=Exit

**Fig. M12-38 - After pressing F1 at the Point Definition screen**

19. Enter MANUAL MODE in the MIB field.
20. Enter “+1000” in the Trap field. This will adjust the received trap by adding 1000 to the last number.
21. Enter \* in the oid field on the first variable binding. Enter “|CLEAR” for the value and 9 for position. This will store the OID in variable binding position 9 and store the value “CLEAR”. This variable binding should have come through as ALARM but the clear trap has the value CLEAR.
22. Enter \* in the second oid field and enter “|” for the value. Enter 7 for position. This will create an entry for variable binding 7 and store the received value.
23. Enter \* in the third oid field and enter “|” for the value. Enter 6 for the position.
24. Press F8 to save.
25. Then F8 to save again. And exit out of the Point Definition screen.
26. Press F7 at the AutoSNMP Device Types screen and select Key Mapping.

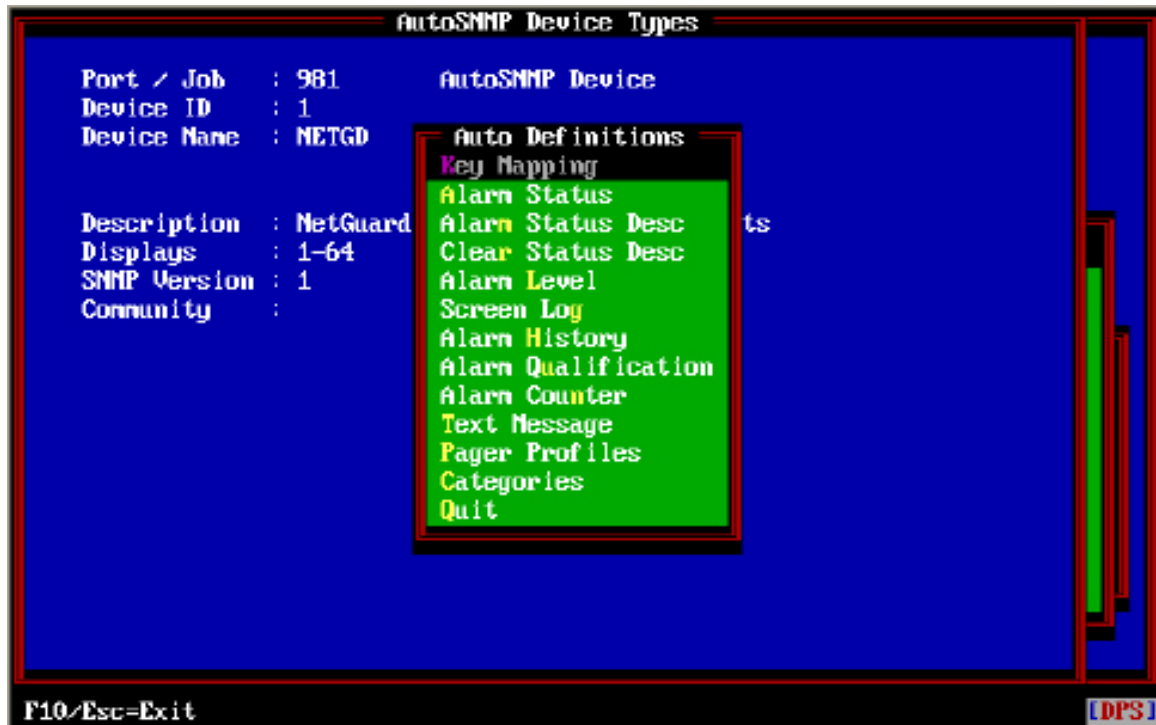


Fig. M12-39 - Back to Key Mapping screen

27. Enter 17, 1, 18 and 16 on Alarm Desc. This build the following string for the point description: "Point " + the received point number + ": " + received point description.

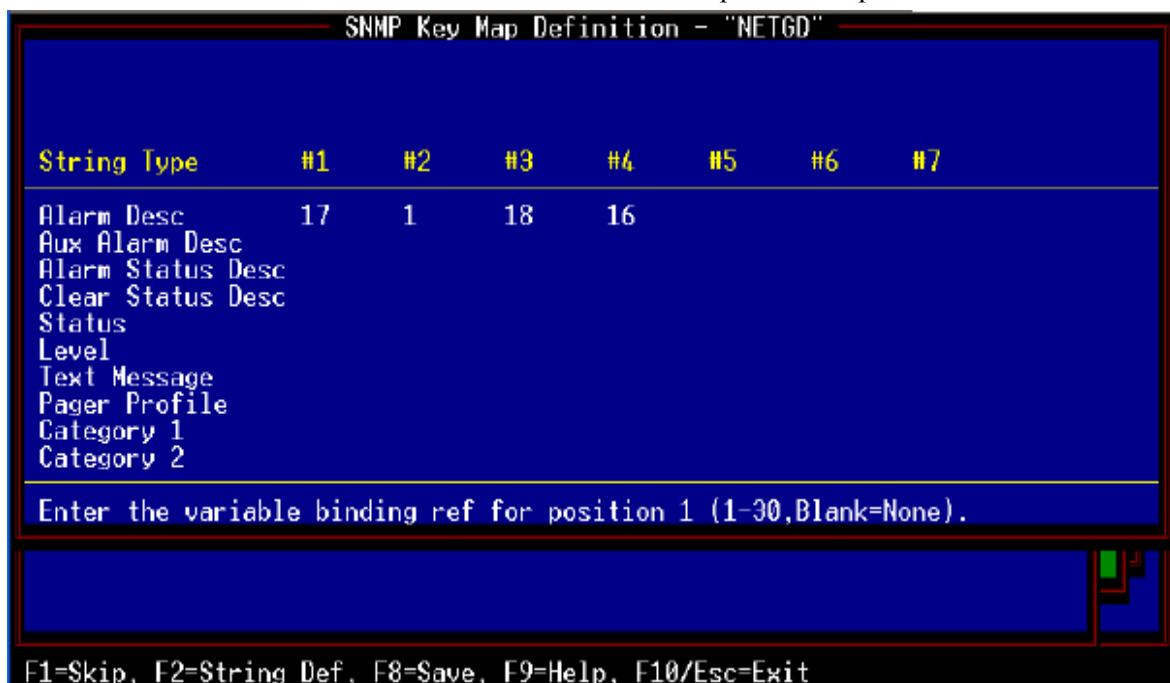


Fig. M12-40 - String for Point Definition

28. Press F8 to save.
29. Navigate back to the Remote Parameters screen. From the Main Master Menu, select Parameters -> Remote Ports. Then find the SNMP Trap Processor job.





Fig. M12-41 - Located SNMP Processor Job

30. Press F1 to view devices.

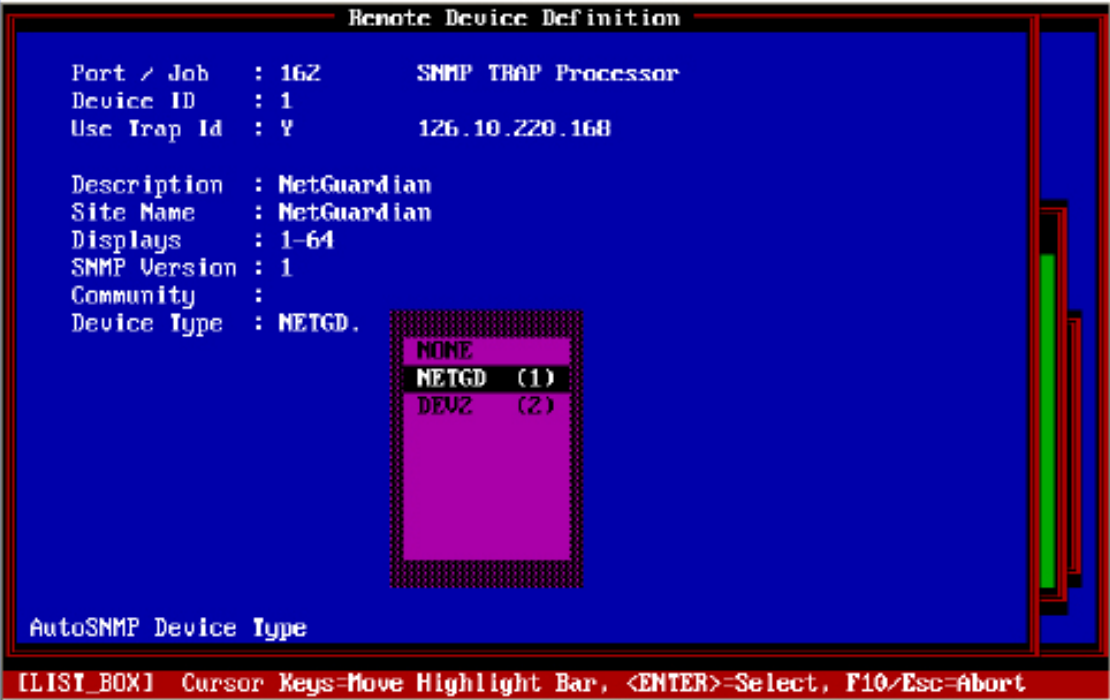


Fig. M12-42 - Viewing AutoSNMP devices

31. Create a new device and enter the IP of the NetGuardian where we want to receive our traps from.
32. On the Device Type field, press TAB. Select NETGD. Press Enter.
33. The SNMP Processor should now be set to automatically database discrete alarms from the NetGuardian.

Toggling discrete points 1, 7 and 12 on the NetGuardian will give the following result on T/Mon's SNMP Processor job.

Point Definition

Job : 162 DoID: 1 Disp: 1 Display Desc :

P L H L S R  
o s e t v  
i g i v s

SNMP TRAP Processor

PI	Position	Description	Fail	Clear
1	B L H A A N	Point 1: LOGIN USER4		
2	B L H A A N	Point 7: ALARM POINT7		
3	B L H A A N	Point 12: Undefined		
4				
5				
6				
7				
8				

Enter polarity. B = bipolar, U = unipolar

Message

F1=GOTO, F2=Desc, F3=Blank, F4=Sect, F5=Range, F6=Read, F8=Save, F9=Help, F10/Esc=Exit

Fig. M12-43 - T/Mon's SNMP Processor Job after toggling discrete points 1, 7, & 12.

This is the point definition screen for the SNMP device that we set up in step 31.

Point 1 on the NetGuardian was defined as LOGIN USER4, point 7 was ALARM POINT 7, and point 12 was not defined.

The set trap association for point 1 would look like this:

Trap Association

Point: 1 Operation: Set Desc: Point 1: LOGIN USER4

MTB: MANUAL MODE

Trap: 1.3.6.1.4.1.2682.1.2.0.8001.....

Ref	OID	Value	Position
1	1.3.6.1.4.1.2682.1.2.5.1.4	1	7
2	1.3.6.1.4.1.2682.1.2.5.1.6	Alarm	9
3	1.3.6.1.4.1.2682.1.2.5.1.3	1	6
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			

Trap OID 1.3.6.1.4.1.2682.1.2.0.8001 (max.64 chars)

F1=Trap, F2=Copy Prev, F3=Blank, F4=Next, F5=Prev, F6=Trans, F8=Save, F9=Help, Esc=Exit

Fig. M12-44 - Set Trap Association for Point 1

The clear trap association for point 1 would look like this:

Trap Association			
Point: 1	Operation: Clear	Desc: Point 1: LOGIN USER4	
MIB: MANUAL MODE			
Trap: 1.3.6.1.4.1.2682.1.2.0.9001.....			
Ref	OID	Value	Position
1	1.3.6.1.4.1.2682.1.2.5.1.6.99>	CLEAR	9
2	1.3.6.1.4.1.2682.1.2.5.1.4.99>	1	7
3	1.3.6.1.4.1.2682.1.2.5.1.3.99>	1	6
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
Trap OID 1.3.6.1.4.1.2682.1.2.0.9001 (max.64 chars)			
F1=Trap,F2=Copy Prv,F3=Blank,F4=Next,F5=Prev,F6=Trans,F8=Save,F9=Help,Esc=Exit			

Fig. M12-45 - Clear Trap Association for Point 1

The set trap association for point 7 would look like this:

Trap Association			
Point: 2	Operation: Set	Desc: Point 7: ALARM POINT7	
MIB: MANUAL MODE			
Trap: 1.3.6.1.4.1.2682.1.2.0.8007.....			
Ref	OID	Value	Position
1	1.3.6.1.4.1.2682.1.2.5.1.4	7	7
2	1.3.6.1.4.1.2682.1.2.5.1.6	Alarm	9
3	1.3.6.1.4.1.2682.1.2.5.1.3	1	6
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
Trap OID 1.3.6.1.4.1.2682.1.2.0.8007 (max.64 chars)			
F1=Trap,F2=Copy Prv,F3=Blank,F4=Next,F5=Prev,F6=Trans,F8=Save,F9=Help,Esc=Exit			

Fig. M12-46 - Set Trap Association for Point 7

The clear trap association for point 7 would look like this:

Trap Association			
Point: 2	Operation: Clear	Desc: Point 7: ALARM POINT7	
MIB: MANUAL MODE			
Trap: 1.3.6.1.4.1.2682.1.2.0.9007.....			
Ref	OID	Value	Position
1	1.3.6.1.4.1.2682.1.2.5.1.6.99>	CLEAR	9
2	1.3.6.1.4.1.2682.1.2.5.1.4.99>	7	7
3	1.3.6.1.4.1.2682.1.2.5.1.3.99>	1	6
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
Trap OID 1.3.6.1.4.1.2682.1.2.0.9007 (max.64 chars)			
F1=Trap,F2=Copy Prev,F3=Blank,F4=Next,F5=Prev,F6=Trans,F8=Save,F9=Help,Esc=Exit			

Fig. M12-47 - Clear Trap Association for Point 7

# Software Module 13

## TL1 Responder

---

### TL1 Responder

Reference Bellcore  
FR-NWT-000439  
Vol. 8, Sub-section  
TR-NWT-000833.

The TL1 responder gives T/MonXM the ability to report alarms in Transaction Language 1 (TL1). This support includes autonomous messages (Logger messages that report when an alarm fails or clears) as well as response to queries from the Operational System, host or from an ASCII terminal.

As with other T/MonXM responders, the user has the ability of choosing which displays of alarm information are associated with a given TL1 port. The TL1 responder also allows individual control over which points in a display will be treated as TL1 points.

Prior to dealing with this function it is recommended that you become familiar with the TL1 Tutorial. Even if you are well acquainted with TL1, the tutorial can help explain specific features of T/MonXM.

The TL1 Responder software module must be installed before you can access the TL1 Responder. Refer to Section 2 - Software Installation for module installation procedures.

References at the end of this section give TL1 Commands, Messages and Codes, TL1 Performance Statistics, Configuration Tables, and a TL1 Glossary. Refer to these tables for supporting data when preparing the database.

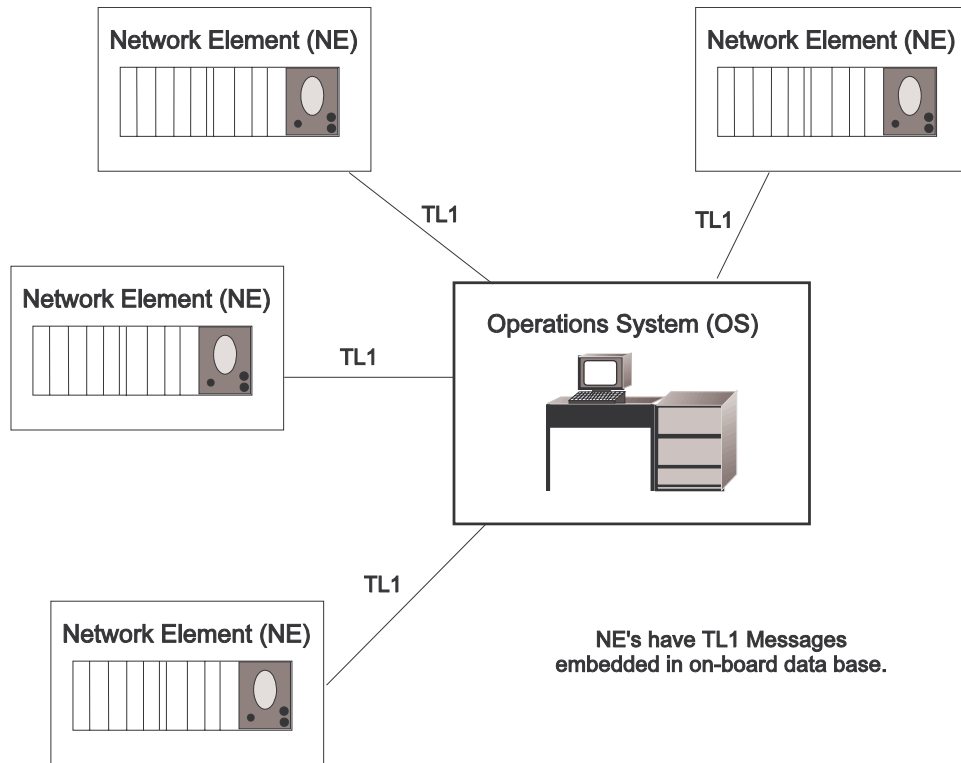
---

### TL1 Tutorial

**Transaction  
Language 1 (TL1)**

Transaction Language 1 (TL1) is a Bellcore-established alarm reporting language designed to standardize alarm messages produced in equipment manufactured for use in the Public Switched Telephone Network (PSTN). By following TL1 guidelines a manufacturer may embed a set of alarm messages in any network element (NE) that will be compatible with a TL1-based operational system (OS). These messages are written in ASCII, allowing monitoring on any dumb terminal. The message may then be read by anyone familiar with the cryptic rules of TL1 language.

The T/MonXM TL1 Responder software module enables the TMon to act as a TL1 network element. By applying the TL1 attributes to alarms coming from non-TL1 network elements T/MonXM performs a mediation function. The power of the TMon makes it possible to interface virtually



**Fig. M13.1 - TL1 Network Elements Report to an Operations System**

any alarm source to a TL1 OS, whether it uses TBOS, DCP(F), DCM, ASCII, TABS, Datalok or a number of other protocols. (Refer to Figure M13.2.)

The T/MonXM TL1 Responder Module also allows all alarms to be displayed on the T/MonXM WorkStation in the normal fashion. Only the alarms that are defined in the database for TL1 reporting are passed on to the OS.

TL1 sets very specific guidelines for assembling the message. T/MonXM asks for only the basic information in clearly identified screen fields. T/MonXM then assembles the message according to the TL1 guidelines making it easy for both administrator and system operator.

## SIDs and AIDs

TL1 defines two parameters that must be created in the T/MonXM database, the SID and the AID. These two parameters are known as “dynamic” because they can be created and/or changed by the database administrator. They are used to identify alarm sources, similar to using street names and address numbers to identify locations in a city. In addition to the SID and AID there is one other dynamic parameter and seven fixed parameters that are used to further describe the alarm, its state and level.

The SID\*, which stands for Source IDentifier, is a source parameter. The SID is associated with a display under a port and address, and is created in a TL1 SID definition screen. Up to 20 alpha/numeric characters may be used. The SID may be unique to

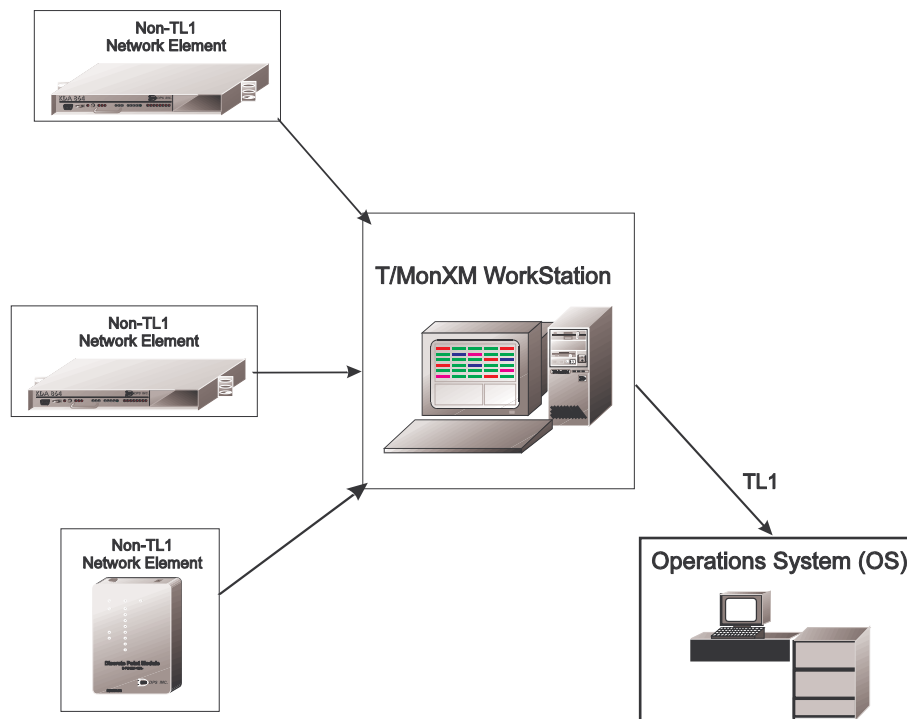
each display or may be used again on any number of displays and under other ports and addresses. (The AID and other dynamic and fixed parameters serve to further identify alarms that have the same SID.) The SID may be likened to a street name.

The AID, which stands for Access Identifier, is an access parameter. The AID is associated with an alarm point and is created in a TL1 Alarm Point Definition screen. Up to 44 alpha/numeric characters may be used. The AID may be unique to each point or may be used again on any number of points and under other SIDs. (The other dynamic parameter and seven fixed parameters serve to further identify alarm points that have the same AID.) The AID may be likened to a house address and the other parameters may be items within the house, such as doors, windows or appliances.

The TL1 Responder software module records all dynamic and fixed parameters in tables that can be accessed during database preparation. This assures standardization across the system and reduces the time required for database preparation. Editing functions that allow point definitions to be easily blocked copied or moved also eases database preparation.

Database administrators need to determine before beginning database preparation how the SIDs and AIDs will be used to identify alarms. Consult Bellcore documentation as well as information supplied by network element manufacturers.

**\*Note:** The term TID, which stands for Target Identifier, is also used as a source parameter in Bellcore literature. Only the term SID is used in T/MonXM.



**Fig. M13.2 - T/MonXM Serves as a Network Element**

---

## TL1 Responder Setup Procedure

The T/MonXM database for the TL1 Responder is prepared in two parts:

- 1) Define the TL1 points (overlay TL1 attributes over the interrogated database);
- 2) Define the TL1 responder port (determine which displays to use in responder).

Part one is done in the definition screens for the interrogator ports that are bringing in the alarms which will be converted to TL1.

Perform the following steps:

- a) Select Parameters from the Master Menu.
- b) Select Remote Ports
- c) Find the first port to be defined by using the “N” or “P” keys or press “F”, type in the port number and press Enter. This will bring up the Remote Parameters screen. See note below.
- d) Refer to Defining TL1 Source Interrogators section (M13-5) to define the SID’s.
- e) Refer to Defining TL1 Alarm Points section (M13-7) to define the AIDs and other alarm point parameters.
- f) Refer to Defining TL1 Control Points section (M13-13) to define control points.
- g) Repeat for other ports.

Part two is done in the definition screens for the responder port that is sending the TL1 alarms to the Operations System. Perform the following steps:

- a) Select Parameters from the Master Menu.
- b) Select Remote Ports
- c) Find the port to be defined as the TL1 Responder by using the “N” or “P” keys or press “F”, type in the port number and press Enter. This will bring up the Remote Parameters screen. See note below.
- d) Refer to Defining TL1 Responders section (M13-15) to define the port
- e) Refer to Remote Device Definition section (M13-16) to define the device.
- f) Refer to Responder Definition section (M13-18) to define the responder.
- g) Repeat if other responder ports are to be defined.

**Note:** TL1 definitions can be entered into the data base after normal port, device and point definitions are completed or at the same time. However, device displays must be assigned in the Remote Device Definition screen before they will appear on the SID Definition screen



After all of the interrogation sources have been entered, you may initialize the data and proceed to Monitor Mode.

## Defining TL1 Source Interrogators

As mentioned in the above Setup section, the first step in configuring your T/MonXM platform to report TL1 data is to determine which of your interrogators contain points that you wish to report TL1. To do this go to the Remote Device Definition screen by pressing F1 at the Remote Parameters screen and select the appropriate interrogation source device. This is going to be the source data that you wish to convert and send out as TL1.

From the Remote Device Definition screen, press Alt-F1 (TL1) to take you to the TL1 SID Definition screen for that particular interrogation device. Once in this section, all displays that were defined for the device in the Remote Device Definition section will be displayed on this screen along with any SIDs that were previously assigned to that display.

To assign a SID to a display, just use the cursor keys to get to the position you want to modify and enter the SID you wish to use. If it has not already been used, you will have the opportunity to add it to the SID table. Once the SID has been entered, you have the option of either defining Alarm Points (F2) or Control Points (F4).

**Note:** TL1 definitions can be entered into the data base after normal port, device and point definitions are completed or at the same time. However, device displays must be assigned in the Remote Device Definition screen before they will appear on the SID Definition screen

**Sid Definition**

Port : 1      Address : 3

Display	SID
1	P#NXSTH.
2	P#NXNRH
3	MESAZA
4	CARSON
5	SOANX
33	.....

Enter Sid

Description : (Undefined)

F1=GOTO,F2=Alm Pnts,F3=Blank,F4=Ctr1 Pnts,F8=Save,F9=Hlp,F10/Esc=Ext

Fig M13.3 - SID Definition screen

## SID Definition Screen

An example of the SID Definition screen is illustrated in Figure M13.3. The fields in the SID Definition Screen are explained in the Table M13.A. The command line keys for the SID Definition screen are explained in the Table M13.B.

**Table M13.A - Fields in the SID Definition Screen**

Field	Description
Display	The corresponding interrogator display that you wish to report TL1.
SID	The source identifier name for the corresponding display. Up to 20 characters. <b>Note:</b> A SID may be used more than once.

**Table M13.B - Key commands available in the SID Definition Screen**

Function Key	Description
F1	Go to Entry Point
F2	Enter Alarm Points Screen
F3	Deletes current entry
F4	Enter Control Points Screen
F8	Exit and Save polling list
F9	SID Definition help screen.

To assign a SID to a display use the cursor keys to get to the position you want to modify and enter the SID. If it has not already been used, you can add it to the SID table. Once the SID has been entered, you have the option of either defining Alarm Points (F2) or Control Points (F4).

To display the SID table press Alt F9.

A T/MonXM TL1 Responder can emulate multiple TL1 devices by assigning more than one SID.

```

Sid Definition
Port : 1   Address : 3

TL1 ALARM Points
Port: 1   Addr: 3   Disp: 33   SID: TRYING

Point AID                      Eqt      Cond                      Lv Dn Locn Eff Type
1  CHAN BK #1                  EQPT     STEPUP                     CR AZ NEND SA  A
2  CHAN BK #2                  EQPT     STEPUP                     CR AZ NEND SA  A
3  SRV UNIT A                  EQPT     STEPUP                     CR AZ NEND SA  A
4  SRV UNIT B                  EQPT     STEPUP                     CR AZ NEND SA  A
5  MUX-RING                    EQPT     STEPDOWN                   CR AZ NEND SA  A
6  ENTRY 2.                    T7X1     STEPDOWN                   CR AZ NEND SA  A
7  ENTRY 3.....
8
9
10

Enter Aid Attribute

F1=GOTO,F3=Blank,F5=Range,F6=Read,F8=Save,F9=Help,AltF7-9=Table,F10/Esc=Exit

```

Fig. M13.4 - TL1 Alarm Points Definition screen

## Defining TL1 Alarm Points

The TL1 Alarm Points screen is used to define the alarm points associated with the current interrogator display. To define points, move the cursor to the desired entry number in the SID Definition list (using the Up & Down arrow keys) and press the F2 function key. Then fill in the attribute Fields in each point to be defined. An example of the TL1 Alarm Points screen, with data in it, is illustrated in Figure M13.4.

### Alarm Point Definition Keys

The following keys are used to move between fields and are only available while in the Point Definitions screen.

Table M13.C - Key commands available in the Point Definitions screen

Function Key	Description
PgUp, PgDn	Move up/down to the next page with a defined entry.
Home, End	Move to first/last page with a defined entry.
Ctrl-Enter	Move to previous field.
Ctrl-F	Move to first field (no save).
Ctrl-L	Move to last field (no save).
Ctrl-Q	Save the cursor position and insert mode (no save).
Ctrl-PgUp	Move to vertically (up) to the previous defined entry.
Ctrl-PgDn	Move to vertically (down) to the next defined entry.

## TL1 Alarm Point Attributes

The TL1 alarm point attributes shown below are either fixed or dynamic. A fixed attribute entry has a fixed entry table associated with it and the value entered must be in the table. fixed entry tables cannot be changed. However, dynamic attributes are user definable entries and are saved to a table.

When you first define dynamic entries for point attributes, T/MonXM will ask if you wish to add the entries to the entry table. If you answer with a “No”, T/MonXM will go to the next entry in the table (if any entries are present) and display it. If you answer with a “Yes”, the entry will be accepted and added to the entry table.

**Note:** On most fields, Alt-F9 will show the fixed or dynamic Tables. An item may be selected from a table as follows: With the cursor in the field to be entered press Alt F7. The first table item or next higher (previous) table item will appear in the field. Press Alt F7 to continue moving up in the table until the desired item is entered in the field. If the computer beeps, the top of the table has been reached. Press Alt F8 to move down in the table. Press Enter to accept the item and move to the next field.

See Table M13.D for valid values for the point attributes.

**Table M13.D - Valid Point Attributes**

Attribute	Value
AID	User defined Access ID entry. Max length is 44 characters. (Dynamic) NOTE: Only 16 characters will show on the screen for all but the point being edited.
Eqt	See Table M13.Q - TL1 Equipment Table on page M13-22. (Fixed)
Cond	User defined Condition entry. Max length is 14 characters. (Dynamic)
Lv	Level Table entry. Valid values are CR, MJ, MN, NA, NR. (Fixed) See Table M13.R - Level Table on page M13-23.
Dn	Direction Table entry. Valid values are AZ, ZA, NA. (Fixed) See Table M13.S - Direction Table on page M13-23.
Locn	Location Table entry. Valid values are NEND, FEND. (Fixed) See Table M13.T - Location Table on page M13-23.
Eff	Effect Table entry. Valid values are SA, NSA. (Fixed) See Table M13.U - Effective Table on page M13-23.
Type	Enter “A” for Alarm or “E” for Environmental

## Alarm Definition Commands

The following commands are for defining and editing TL1 alarm point definitions:

**Table M13.E - TL1 alarm point command definitions**

Function Key	Description
F1	Goto Point
F3	Blank
F5	Range Functions
F6	Read
F8	Save
F9	Help
Alt-F3	Delete Point
Alt-F4	Insert Point
Alt-F5	Block Move
Alt-F6	Block Copy
Alt-F7	Moves down table list
Alt-F8	Moves up table list
Alt-F9	Show table list
F10/Esc	Exit

See Table M13.I for additional details of the above table of commands. Note that these commands can only be invoked when the cursor is at the AID field. Pressing Alt-F7, Alt-F8, and Alt-F9 will work in any field except the Alarm Type field.

The following commands are only available when editing in the Alarm Point or Control Screen and are described as follows:

**Table M13.F - Key commands available in the Alarm Point or Control screen**

Function Key	Description
F1	Goto Point. This function allows the user to go directly to any point in the current defined display.
F3	Blank Point. "Blanks out" (deletes) the attributes of the current point. (The current point is the one that has the cursor in its "AID" field).
F5	Range Functions. The Range Function will allow the user to use several field editing features that will greatly enhance all point editing. You may define several points at one time or change certain parameters for a range of points, all in a few short keystrokes.

Once the Range function is invoked, the commands available are listed in Table M13.G.

Refer to Table M13.H for examples of range parameters that are acceptable.

**Table M13.G - Fields in the Range**

Command	Description
AID	Use to set the AID attributes for the range specified.
EQT	Use to set the EQT attributes for the range specified.
COND	COND. Use to set the COND attributes for the range specified.
LV	Use to set the LV attributes for the range specified.
DN	Use to set the DN attributes for the range specified.
LOC	Use to set the LOC attributes for the range specified.
EFF	Use to set the EFF attributes for the range specified.
TYP	Use to set the TYP attributes for the range specified.
COPY	Copy Point. This will ask for the point to be copied and then the range of points to copy it to. Note: When using the Copy feature the range will default to previously set range parameters. After the range is set, this will be the new default range.
DELETE	Delete Points. This will ask for the range of points to delete. The range will default to the previously set range parameters. After the range is set, this will be the new default range.
RANGE	Prompts the user to specify the range parameters to be involved in the editing process.

**Table M13.H - Range parameters**

Range	Point Specified
30	30
5-10	5, 6, 7, 8, 9, 10
43, 45, 50	43, 45, 50
20-30, 35, 37	20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 35, 37

**Table M13.I - Key commands available in the Range function**

Function Key	Description
F6 (Read)	Reads the point definitions from another polling list entry and copies them into current point definitions. This command can copy definitions from any other TL1 Alarm Point definition. Select the Read function (F6). Enter the Port, Device Type, Address and display number to read and insert to the current definition. An example of the Read Display window is shown in Figure M13.5.
F8 (Save)	Saves any and all changes to the point definitions and returns to the Polling List screen.
F9 (Help)	Brings up the Help screen that explains these commands.
Alt-F3 (Delete Point)	This command will delete the point definition that the cursor is currently on and cause all points below it to move up one position.
Alt-F4 (Insert Point)	This command causes points under the current cursor position to move down one position so that a new point definition can be added. The last point will roll off the end of the definition list.
Alt-F5 (Block Move)	<p>The Block Move command uses a Start point, End point and Destination point to cut a block of point definitions and paste it in another location within the point definitions list. (Example: Start point of 7 and end point of 10 with a destination point of 17 moves points 7 through 10 to points 17 - 20.) After selecting the block move function the Block Move window appears (See Figure M13.6).</p> <p><b>WARNING!</b> Make sure when using the “Block Move” feature that the destination points are points that you want to overwrite. Parameters for the Block Move window: Start Point = The first point of the block to be moved; End Point = The last point of the block to be moved; Destination Point = The start of the new location for the block.</p> <p><b>Note:</b> The selected destination block must be large enough to receive the entire source block. (Example: The block starting at point 1 and ending at point 10 could not be moved to a block starting at point 60 since there are only 5 positions available beginning at point 60). This rule also applies to Block Copy.</p>
Alt-F6 (Block Copy)	The Block Copy command uses a Start point, End point and Destination point to copy a block of point definitions and paste it in another location within the point definitions list. Warning! Make sure when using the “Block Copy” feature that the destination points are points that you want to overwrite.
Alt-F7 (Scroll Down Table List)	This function allows the user to scroll down the table listing of predefined entries for the current field.
Alt-F8 (Scroll Up Table List)	This function allows the user to scroll up the table listing of predefined entries for the current field.
Alt-F9 (Show Table List)	Pressing this command will display a table list of all predefined entries available for the current field.

Sid Definition					
Port : 1		Address : 3			
T11 ALARM Points					
Port: 1		Addr: 3		Disp: 33	SID: TRYING
Point	AID	Read Points		cn	Eff Type
1	CHAN	Port Number	: ..	ND	SA A
2	CHAN	Device Type	:	ND	SA A
3	SRV U	Address Number	:	ND	SA A
4	SRV U	Display Number	:	ND	SA A
5	MUX-R			ND	SA A
6	ENTRY			ND	SA A
7	ENTRY			ND	NSA A
8		Enter port number 1-29, IA, RP			
9					
10					

F10/ESC = Exit

Fig. M13.5 - Read Display window

Sid Definition					
Port : 1		Address : 3			
T11 ALARM Points					
Port: 1		Addr: 3		Disp: 33	SID: TRYING
Point	AID	BLOCK MOVE		Dn	Locn Eff Type
1	CHAN BK #1	START POINT	: ..	AZ	NEND SA A
2	CHAN BK #2	END POINT	:	AZ	NEND SA A
3	SRV UNIT A	DESTINATION POINT	:	AZ	NEND SA A
4	SRV UNIT B			AZ	NEND SA A
5	MUX-RING			AZ	NEND SA A
6	ENTRY 2.			AZ	NEND SA A
7	ENTRY 3			AZ	FEND NSA A
8		Enter starting point (1-64)			
9					
10					

F10/ESC = Exit

Fig. M13.6 - Block Move window



## Defining TL1 Control Points

The TL1 Control Points Screen is used to define the control points associated with the current polling list entry. The same key commands that were available for defining the Alarm Points are used for defining the control points. The TL1 Alarm Points screen is used to define the alarm points associated with the current interrogator display.

To define control points, select the port, press F1, find the device and press Alt F1 to reach the SID Definition screen. Move the cursor to the desired entry number in the SID Definition list (using the Up & Down arrow keys) and press the F4 function key. Then fill in the attribute Fields in each control point to be defined. An example of the TL1 control points screen, with data in it, is illustrated in Figure M13.7.

Key commands, command definitions and range functions apply to defining control points in the same way they do for alarm points. Refer to the appropriate tables in this section.

```

Sid Definition
Port : 1   Address : 3

T11 CONTROL Points
Port: 1   Addr: 3   Disp: 1   SID: P#NXSTH.
Point AID                      Eqt      Cond
1    bjh.....              EQPT      up
2    bjh                      EQPT      dn
3    bjh                      EQPT      54
4
5
6
7
8
9
10

Enter Aid Attribute

F1=GOTO,F3=Blank,F5=Range,F6=Read,F8=Save,F9=Help,AltF7-9=Table,F10/Esc=Exit

```

Fig M13.7 - TL1 Control Points Definition screen

Table M13.J - Valid control point attributes

Attribute	Value
AID	User defined Access ID entry. Max length is 44 characters. (Dynamic) <b>Note:</b> Only 16 characters will show on the screen.
Eqt	See Table M13.Q - TL1 Equipment Table on page M13-22. (Fixed)
Cond	User defined Condition entry. Max length is 14 characters. (Dynamic)

The TL1 OPR/RELEASE COMMAND structure is as follows:

**Command:SID:AID:c::Cond,e** (Part “c” is defined as CTAC.)

The TL1 control commands supported are as follows:

- |                                |   |
|--------------------------------|---|
| <b>Command: OPR-EXT-CONT</b>   | OPERATE-EXTERNAL-CONTROL instructs T/MonXM operate an external control such as a relay in a KDA remote. Operation can be either latching or momentary, depending on the duration (DUR) portion of the TL1 message. DUR is part “e” of the message and can be either CONTS for latched or MNTRY for momentary. All other parts of the message are normal TL1.  |
| <b>Command: RLS-EXT-CONT</b>   | RELEASE-EXTERNAL-CONTROL instructs T/MonXM release a latched external control such as a relay in a KDA remote. Release can be either continuous or momentary (returns to the latched state after the time period set in the remote), depending on the duration (DUR) portion of the TL1 message. DUR is part “e” of the message and can be either CONTS for continuous or MNTRY for momentary. All other parts of the message are normal TL1. |
| <b>Command: RTRV-ATTR-CONT</b> | RETRIEVE-ATTRIBUTE-CONTROL obtains attributes from the T/MonXM database for the control point specified in the other parts of the TL1 message. This information includes the SID, AID, Eqt, Cond and other data about the point.  |
| <b>Command: SET-ATTR-CONT</b>  | SET-ATTRIBUTE-CONTROL sends attributes for the control point or points specified in the other parts of the TL1 message to the T/MonXM database . This information includes the SID, AID, Eqt, Cond and other data about the point.  |

These commands can be issued to T/MonXM via the TL1 Responder port from an ASCII terminal or P.C. operating as a terminal emulator. The addressed device will respond according to the instructions in the TL1 message. The following example TL1 message will latch control point 1 defined in Figure M13.7:

**OPR-EXT-CONT:P#NXSTH:bjh:::up,CONTS**

The following example will release the same point:

**RLS-EXT-CONT:P#NXSTH:bjh:::up,CONTS**

**Note:** TL1 messages are case sensitive. Observe this when entering messages via an ASCII terminal.

## Defining TL1 Responders

After all of your interrogators have been set up to report TL1 it is time to route these out to the TL1 Responder Out port. This is done by going to the Remote Parameters screen and finding an unused port. Edit the port and select “TL1 RESPONDER OUT” for the port usage. At this time you will need to define the appropriate baud, parity, word length, stop bits, echo input and null aids allowed. The Remote Parameters screen defined for TL1 Responder Out is illustrated in Figure M13.8.

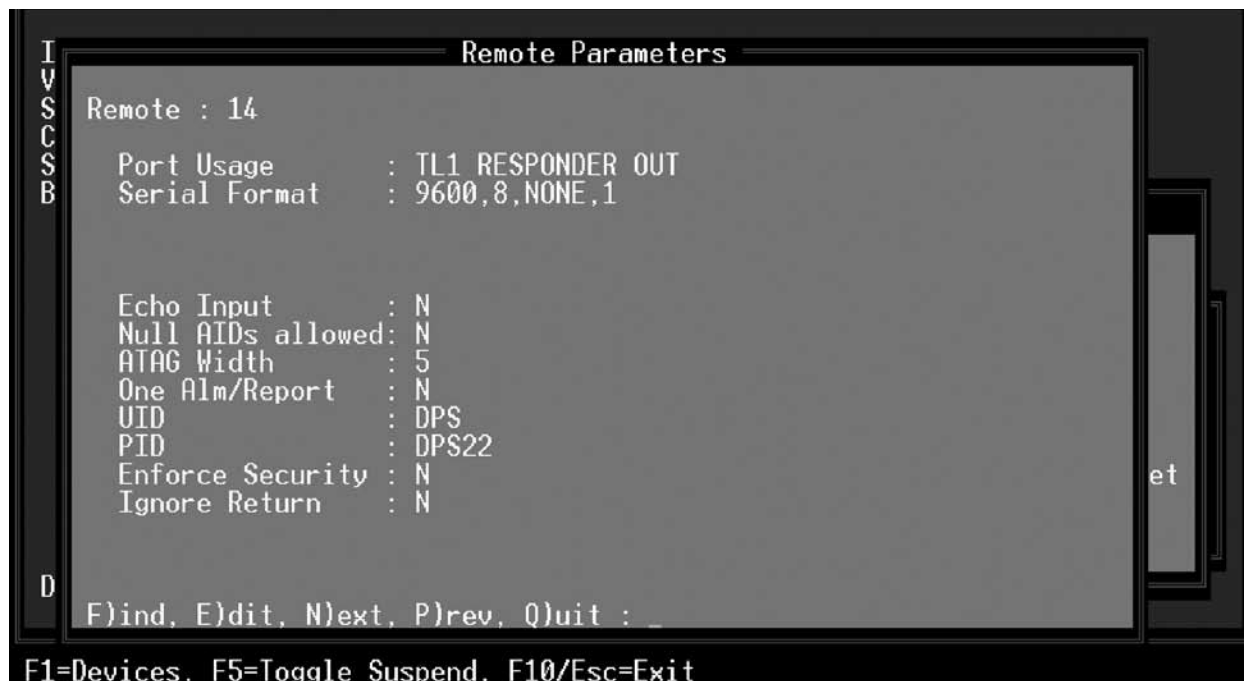


Fig. M13.8 - Remote Parameters screen defined for TL1 Responder Out

**Table M13.K - Fields in the Remote Parameters screen**

Field	Description
Port Usage	Valid port types are TL1 Responder Out and Halted. [TL1]
Serial Format	Baud rate, word length, parity, and stop bits settings.
Echo Input	If set to "Y", T/MonXM will echo back all commands/characters that are received. Set to "N" if you are connected to another computer. [N]
Null Aids Allowed	"N" forces users to enter AIDs with TL1 commands . "Y" allows null (omitted) AIDs with TL1 commands (as allowed in Bellcore 833) [N]
ATAG Width	Number of characters to output for ATAG (4-10).
One Alm/Report	For autonomous reports: Y=One alarm per header; N=Multiple alarms.
UID	User Identification. Used when TL1 OSS or other interrogating device queried with an ACT-USER command. The ACT-USER command is used for setting up a session when logging on to an external device (i.e.: switch, radio, multiplex channel, DPM, etc.). Use up to 10 alphanumeric characters. If left blank, cursor skips to Enforce Security field.
PID	Private Identifier or password. This field is entered only if a UID has been entered. It is also used in conjunction with the ACT-USER command, as explained above. Use at least 2 non-alpha characters in the string.
Enforce Security	Y = Require correct UID/PID (as entered above) with an ACT-USER command. N = Don't match UID/PID with an ACT-USER command.
Ignore Return	Y or N, Ignore carriage return.

## Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined TL1 Responders will bring you to the Remote Device Definition screen. Enter a description for the port. An example of the Remote Device Definition screen is illustrated in Figure M13.9.

```

Remote Device Definition

Port      : 9          TL1 RESPONDER OUT

Description : MAIN MONITORING CENTER (TL1)

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :
F2=Responder Displays, F10/Esc=Exit
  
```

Fig. M13.9 - Remote Device Definition screen

The fields on the Remote Device Definition screen are described in the following table.

Table M13.L - Fields in the Remote Device Definition screen

Field	Description
Port	The Port you are at and the Responder you have defined.
Description	The Description of the device.

Table M13.M - Key commands in the Remote Device Definition screen

Function Key	Description
F2	Responder Displays (see section later in this module)
F10/Esc	Exit

## Responder Definition

Entering F2 (Responder Displays) from the Remote Device Definition screen will bring you to the Responder Definition screen. On the Responder Definition screen, enter each interrogation port and display that you want to redirect out as TL1. (Max entries = 4000) An example of the Responder Definition screen is illustrated above.

```

Remote Device Definition
Port      : 9      TL1 RESPONDER OUT

Responder Definition

-----Interrogator-----
PORT      DEVICE  ADDR      DISPLAY  SID
-----
1          1       3         1        P#NXSTH.
1          1       3         2        P#NXNRH
1          1       3         3        MESA2A
..

Enter Port Number (1-29), IA=User Internal, LC=Local Control, RP=Modem
F3=BLANK, F8=Save, F10/Esc=Exit

```

Fig. M13.10 - Responder Definition screen

Table M13.N - Fields in the Responder Definition screen

Field	Description
Port	Enter the Port Number. Valid entries are 1-500, IA (User Internal).
Addr	Enter Address Number. Valid entries are 1-255. <b>Note:</b> Enter Address Number 11-12 when IA (User Internal) is selected on the port field.
Display	Enter Display Number. Valid entries are 1-99.
SID	Echoes the SID of the interrogator source display.

Table M13.O - Key commands available in the Responder Definition screen

Function Key	Description
F3	Blank. Deletes the current entry.
F8	Save. Saves the Responder Definition database.
F10/Esc	Exits without saving any changes that may have been made.

## TL1 User Input Command Errors

An “A” error code is the additional error information that will appear in the error response. A “B” error code explains more detail about the message. A “C” error code will contain an example that illustrates the error.

### IDNV - Input, Data Not Valid

- a) Error in command modifier.
- b) Third part of command modifier was not valid.
- c) RTRV-ALM-ENZ would cause this error since ENZ is not a valid modifier (Should be ENV).
- a) “PARAMNAME” invalid formal parameter name/incorrectly positioned.
- b) Occurs when a formal parameter is incorrectly used.
- c) LOCA=NEND is invalid because LOCA is not the formal parameter name. If a formal parameter is used it should be LOCN=NEND.
- a) Data for parameter “PARAMNAME” is mandatory.
- b) Occurs when a data field is explicitly required for a command and has been omitted from the command request.
- c) Currently, there are no data parameters that we implement that have this requirement, but there may be in the future.
- a) “PvalStr” invalid value for “RealPname” parameter
- b) User attempted to use a value for a value that was not permitted.
- c) LOCN=XEND is not valid because XEND is not contained in the acceptable range of ‘NEND’ or ‘FEND’.
- a) “PvalStr” invalid value for “RealPname” parameter. Must be CONTS or MNTRY.
- b) A specific error message that occurs with OPR-EXT-CONT and RLS-EXT-CONT when an invalid duration selection is made.
- c) OPR-EXT-CONT:TID:AID:TAG::COND,DLON;DLON is not valid because it is not CONTS or MNTRY.

### ICNV - Input, Command Not Valid

- a) None.
- b) Occurs when the TL1 responder encounters a command that it did not understand. This could be either a invalid TL1 command, or a TL1 command that is not in our implementation set.
- c) INV-CMD:SID:AID; Would cause this error since INV-CMD is not a valid TL1 command.

### IISP - Input, Invalid Syntax or Punctuation

- a) Missing/Expected semicolon.
- b) Occurs when we were expecting a semicolon to terminate the command and none was received.
- c) RTR-ATTR:SID:AID:CTAG- would cause this error since the command was not properly terminated.

## TL1 Commands, Messages and Codes

For more details refer to TL1 Command Overview sub-section in this Module, section M13-24 through M13-32.

### TL1 Commands

The following commands are supported:

ACT-USER  
SET-ATTR-ENV  
SET-ATTR-CONT  
SET-ATTR  
RTRV-ATTR-ENV  
RTRV-ATTR-CONT  
RTRV-ATTR  
RTRV-ALM-ENV  
RTRV-EXT-CONT  
RTRV-ALM  
RTRV-COND  
OPR-EXT-CONT  
RLS-EXT-CONT  
RTRV-HDR

### Notes:

- <Ctrl>R - Will restore the current input line
- <Ctrl>X - Abort current input line
- Command echo is disabled on the TL1 KDA master port, but is enabled from the local terminal mode.

### TL1 Messages

The following Automatic messages are supported :

REPT ALM  
REPT ALM ENV  
REPT EVT

**Notes:** The automatic messages will sort the alarms by level of severity and alarm state before displaying them. The highest priority message will be at the top of the message and its corresponding priority will appear in the header (for reports that have a level).

The KDA-TL1 will report one alarm event per autonomous message.

### Error Codes and Meanings

If an undefined TL1 point failure occurs in a TL1 DISPLAY that is being reported, the point will be reported as an event with the following designation : “##-###-#####-##” where the data is interpreted as “PORT-ADDRESS-DISPLAY-POINT”, which is the source location (T/MonXM Interrogator where the data originated).

When the TL1 responder encounters an error with a user request, it will respond with an error message that contains the standard 4 character TL1 Error code, followed by the expanded format of the error message. Wherever possible the T/MonXM TL1 responder will attempt to provide additional information that will clarify either the nature or location of the error.

The error messages are explained as follows: First, the Error code & expanded code will form the header of a section. Since multiple causes can exist for some messages they will be grouped under the section they occur in and have (A, B, C) codes assigned to them.



**IIITA - Input, Invalid Target Identifier**

- a) “xxx” Not found in SID table.
- b) The SID that was in the TL1 Request and was not defined in the T/MonXM TL1 database. Double check that you entered it correctly.
- c) Rtrv-attr:BADSID;- would be an error if BADSID was not defined in T/MonXM.
- a) SID is mandatory for this command.
- b) Occurs when the user omitted an SID on a command that required it.
- c) Currently there are no commands that fit into the category.

**IIAC - Input, Invalid Access Identifier**

- a) “xxx” Not found in AID table
- b) The AID that was in the TL1 Request, was not defined in the T/MonXM TL1 database. Double check that you entered it correctly.
- c) Rtrv-attr:SID:BADAID;- would be an error if BADAID was not defined in T/MonXM.
- a) Aid is mandatory for this command.
- b) Occurs when the user omitted an AID on a command that required it. All T/MonXM commands, with the exception of RTRV-HDR, require an AID. However, T/MonXM does have an option while defining the operation characteristics of the TL1 Responder that permits you to relax this restriction.
- c) RTRV-ALM:SID; - Is invalid because no AID was specified.

**IICT - Input, Invalid Correlation Tag**

- a) “Tag” is more than 6 characters in length.
- b) Occurs when the correlation tag is too long.
- c) RTRV-ATTR:SID:AID:TAGTOLONG;

**SROF - Status, Request Operation Failed**

- a) None
- b) Occurs when the specified control point could not be found. This probably means the CONTTYPE field specified did not correlate with the specified AID.
- c) OPR-EXT-CONT:SID:AIDX:TAG::SPRINKLER,CONTS; where the CONTTYPE for AIDX was defined to something other than SPRINKLER.

**Note:** Names surrounded by Quotation Marks will be replaced with actual Parameter, Symbols, SID, Tokens etc.

**Table M13.P - TL1 performance stats**

Message	Meaning
Crit Msg	Number of automatic critical alarm messages reported.
MajorMsg	Number of automatic major alarm messages reported.
MinorMsg	Number of minor messages reported.
EventMsg	Number of event messages reported.
Envirn Msg	Number of environmental messages reported.
Inp CmdOK	Number of successful command requests.
Inp Cmd Bad	Number of command requests that contained errors.

**Note:** The message counts are counted by the highest alarm level in a message. If a message has both a Critical alarm and a Major alarm, it would count the message as a single critical.

## Configuration Tables

Refer to Table M13.Q for TL1 Equipment table list.

**Table M13.Q - Equipment Table**

EQPT	T1	T4X8	T7X
LINE	T1C	T4X9	T7X1
TRK	T1X	T5X	T7X2
PLK	T1Z	T5X1	T7X3
SLK	T2	T5X2	T7X4
TST	T2X	T5X3	T7X5
COM	T3	T5X4	T7X6
ALL	T3X	T5X5	T7X7
DATA	T3X1	T5X6	T7X8
MEM	T3X2	T5X7	T7X9
PTO	T3X3	T5X8	TOT
PTOX	T3X4	T5X9	TOTS
PT1	T3X5	T6X	VT1
TO	T4	T6X1	VT2
TOX	T4X	T6X2	VT3
TOXA	T4X1	T6X3	VT6
TOXAS	T4X2	T6X4	OC1
TOXB	T4X3	T6X5	OC3
TOXBS	T4X4	T6X6	OC9
TOXC	T4X5	T6X7	OC12
TOXCS	T4X6	T6X8	OC18
TOXD	T4X7	T6X9	OC24
OC36	OC48	STS1	STS3C
OC96			

**Table M13.R - Level Table**

<b>ntfcncde</b>	
CR	Critical Alarm, reported via REPORT ALARM
MJ	Major Alarm, reported via REPORT ALARM
MN	Minor Alarm, reported via REPORT ALARM
NA	Not Alarmed, reported via REPORT EVENT
NR	Not Reported, but alarm retained for subsequent RTRV-ALARM command
<b>condeff</b>	
CL	Standing Condition Cleared
SC	Standing Condition Raised
TC	Transient Condition

**Table M13.S - Direction Table**

AZ	A to Z
ZA	Z to A
NA	Not Applicable

**Table M13.T - Location Table**

NEND	Near End
FEND	Far End

**Table M13.U - Effective Table**

SA	Service Affecting
NSA	Not Service Affecting

---

## TL1 Glossary

**Table M13.V - TL1 terms**

<b>Term</b>	<b>Description</b>
SID	Source IDentification number
Addr	Address
AID	Access IDentification entry
COND	CONDition on point entry
Lv	Alarm Level table entry
Dn	Direction table entry.
Locn	Location table entry.
Eff	Effect on service table entry.
Eqt	Equipment type.
Dur	Duration table entry.

## TL1 Command Overview

The TL1 command set gives you a powerful way to view and control your network. In many ways it is similar to a database query language. It allows you to view alarms by several criteria. For example, with the RTRV-ALM (Retrieve alarm command), you could do such things as: view all alarms, view all critical alarms, view all service affecting alarms at a particular device, or view problems with a particular type of alarm. When you specify selection criteria, the TL1 processor will select the “intersection” of the data, which is only those points that meet ALL the specified criteria.

The TL1 command syntax consists of a set of rules that must be followed before a command can be accepted. TL1 commands are positional in nature. This means that the various elements of a command must be in a specified order. TL1 uses special characters such as “.” and “,” to both separate fields and maintain place holders for data that is not used.

### Notations

- [ ] - Fields enclosed by square brackets are optional and may or may not be used.
- ^ - Denotes a space
- CR - Carriage return
- LF - Line feed

### General Command Syntax

TL1-CMD[-Mod]:[TID]:AID:[CTAG]:Data1,Data2...

#### Where

TL1-CMD - Is the TL1 command that you wish to issue.

#### Examples

RTRV-HDR                      RTRV-ALM      OPR-EXT-CONT

### Mod

Verb Modifier. Depending on the command, this field can have one of three meanings.

None - Some commands do not require them and therefore should not be used.

Eqpt - Equipment type. Several TL1 commands allow you to restrict a search to a particular type of equipment (i.e.: OC48). This equipment type works very similar to the TL1 attributes that are located in the data area of the command, except that it is positioned earlier in the command because it is frequently used and increases the likelihood of command short-cuts. If you do not use this field in a command that supports it, then the TL1 processor will interpret this as “ALL” equipment types.

Extensions -Some commands use these simply as part of the command.

Examples : RTRV-ALM-ENV    OPR-EXT-CONT.

Extensions may not be omitted from commands that use them.

Examples: ‘OPR-EXT’ by itself would cause a command error.

**Technical Note:** RTRV-ALM by itself, is a different command than RTRV-ALM-ENV and will be processed, as such.

<b>TID</b>	Identifies a particular Network element, site or piece of equipment. If TID block is left blank, TL1 defaults to “ALL.”
<b>AID</b>	Access Identifier. This allows you to specify a particular alarm or control point to select. This field may not be omitted, however you may specify “ALL” to select all AIDs.
<b>CTAG</b>	Correlation Tag. This field is used to correlate responses to the commands that created them. The value that you supply with this command will be echoed in the response. This field may be either alpha or non-numeric, up to 6 characters.
<b>ATAG</b>	Autonomous messages create their own numeric TAG, that increments for each new message.
<b>Data parameters</b>	These parameters are typically point attributes that allow you to select which part of the TL1 data set that is to be operated on. The quantity and meaning of the data parameters vary depending on the TL1 command. For most data parameters if the field is omitted, it will exclude that field from consideration when querying the database. This is equivalent to saying, “accept any or all values for this field.”

Each data parameter is positional, which means that it must be in a given relative position in the parameter block. A field can only be omitted provided the trailing “,” separator is retained.

Example:

```
pos1    pos2    pos3
□        □        □
Data1,Data2,Data3
```

where Data1, Data2, Data3 are the valid parameters, and if you do not wish to use Data2;

**Wrong Way:**

```
pos1    pos2
□        □
Data1,Data3
```

would be incorrect because TL1 would attempt to process Data 3 in Data 2’s position.

**Correct Way:**

```
pos1    pos2
□        □
Data1,Data3
```

The additional comma holds the place of Data2.

Parameters used by the DPS TL1 Responder include:

**almcde** (alarm code) - \*C = Critical Alarm  
 \*\* = Major Alarm  
 \*^ = Minor Alarm  
 A^ = Autonomous Message (comes in when an alarm clears or when a non-alarm “event” is reported).

**ntfcncde** (notification code) same as alarm level, see Table M13.R.

**condtype** (condition type) This is a dynamic parameter, defined in the TL1 Alarm Points screen, Condition field.

**almtype** (alarm type) Same as condtype, but related to environmental alarms only.

**conttype** (control type) This is a dynamic parameter, defined in the TL1 Control Points screen, Condition field.

**srveff** (service effecting) - see Table M13.U

**locn** (location) - see Table M13.T.

**dirn** (direction) - see Table M13.S.

**\”status\”** A free-form text message used only by the DPS TL1 Responder in REPT EVT messages.

**condeff** (condition effect) - like ntfcncde, used only in REPT EVT messages - see Table M13.R.

**uid** (user identifier) This is a dynamic parameter, defined in the Users screen, UID field.

**pid** (private identifier) This is a dynamic parameter, defined in the Users screen, PID field.

**Note:** The uid and pid parameters used in the DPS TL1 Responder are not subject to the same character limitations as specified in the Bellcore documentation.

**constate** (control state)      OPER = Operated  
    RLS = Released  
    NA = Not Applicable

**dur** (duration) - Time duration of a control  
    CONTS = Continuous (latched)  
    MNTRY = Momentary (default)

## ; (semi colon)

A semi colon marks the end of a TL1 message. It is a very important part of the TL1 syntax, and must be used to terminate every command. The TL1 responder also uses it to finish every response it issues.

## Short cuts

The TL1 input syntax supports several shortcuts that eliminate the need for unnecessary key strokes.

Early command termination - Once you have entered all the parameters that are required for your task, you do not have to enter the remainder of the parameters that are supported by the command. Simply enter the ‘;’ at the point you wish to terminate the command, all remaining parameters will be ignored.

This not only saves keystrokes, but is simpler because you don't have to count all the parameters that are used in the command.

Long Way : RTRV-ALM:TID:AID:CTAG::CR,,,;

Short Cut : RTRV-ALM:TID:AID:CTAG::CR;

Long Way : RTRV-HDR:::CTAG;

Short Way : RTRV-HDR;

Note: The “;” can terminate blocks (sections surrounded by “:”) just as easily as it can with data parameters.

## TL1 Command Definitions

Refer to Table M13.W for TL1 Command descriptions.

**Note:** Table continues on the following page.

**Table M13.W - TL1 Command Descriptions**

Command	Description	
RTRV-ALM	RETRIEVE-ALARM - This command will retrieve all points in the system that are in ALARM and match the selection criteria.	
	Formal Input	RTRV-ALM-[EQPT]:[tid]:aid:ctag::[ntfcncde],[condtype],[srveff],[lo cn],[dirn]
	Example Input Command	RTRV-ALM:FRESNO:ALL:305;
		Very general form of the command that will report all alarms that are in the FRESNO TID. The 305 is the CTAG field that will be echoed in the response to the command.
		RTRV-ALM:FRESNO:ALL:306::MJ; -This command will retrieve all major alarms that are in Fresno.
	Formal Output	RTRV-ALM:FRESNO:RECTIFIER:307::CR,DOWN,SA,NEND;
		(This is a very specific command that could only identify a single alarm point, assuming that it is in a failed state.)
		<CR> <LF> <LF>
		^^^tid^date^time <CR> <LF>
		M^^ctag^COMPLD <CR> <LF>
		^^^"aid:ntfcncde,condtype,srveff,,,lo cn" <CR> <LF>
		(multiple lines of the above may appear in the message)
		;
	Example Output	FRESNO 04-01-27 18:30:33
		M 305 COMPLD
		"RECTIFIER:CR,DOWN,SA,,,NEND,NA"
		;
	<b>Note:</b> Many of the input parameter fields also appear in the output format. All attributes for the selected points that are defined in the TL1 database will be included in the response independent of whether the attribute was specified in the input command.	

**Table M13.W - TL1 Command Descriptions (continued)**

Command	Description
RTRV-ALM-ENV	RETRIEVE-ALARM-ENVIRONMENT - This command retrieves specific outstanding environmental alarms. This command can also be used to retrieve information to update an OS environmental alarm database if autonomous message (REPT ALM ENV) was not received or processed correctly.
	Formal Input: RTRV-ALM-ENV:[tid]:aid:ctag::[ntfcncde],[almtype];
	Example Input Command: RTRV-ALM-ENV:FRESNO:ALL:308::CR,FANOUT;
	Formal Output: <CR> <LF> <LF> ^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ^^^"aid:ntfcncde,almtype" <CR> <LF> ;
	Example Output: FRESNO 04-05-16 10:41:43 M 308 COMPLD "AIR CONDITIONER:MJ,FANOUT" ;
RTRV-ATTR	RETRIEVE-ATTRIBUTE - This command retrieves attributes associated with non-environmental alarms. Note: This command does not determine whether or not an alarm is in existence, it simply shows what non-environmental alarm points are defined in the database.
	Formal Input: RTRV-ATTR[-EQPT]:[tid]:aid:ctag::[ntfcncde],[condtype],[locn],[dirn];
	Example Input Command: RTRV-ATTR:FRESNO-T4X8:PRIMARY POWER SYSTEM:309::CR,OUT,NEND,NA; This is a very specific command that could only identify a single alarm associated with this type of command input.
	Formal Output: <CR> <LF> <LF> ^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ^^^"aid:ntfcncde,condtype,locn,dirn, <CR> <LF> ;
	Example Output: FRESNO 04-05-16 10:41:43 M 309 COMPLD PRIMARY POWER SYSTEM:CR,OUT,NEND,NA ;



Table M13.W - TL1 Command Descriptions (continued)

Command	Description	
RTRV-ATTR-CONT	RETRIEVE-ATTRIBUTE-CONTROL - This command retrieves the TL1 attributes associated with an external control. <b>Note:</b> This command does not determine whether or not a control is operated, it simply shows which control points are defined in the database.	
	Formal Input:	RTRV-ATTR-CONT:[tid]:aid:ctag::[condtype];
	Example Input Command:	RTRV-ATTR-CONT:FRESNO:ALL:310::TXASTBY, RUN;
	Formal Output:	<CR> <LF> <LF> ^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ^^^"aid:condtype" <CR> <LF> ;
	Example Output:	M FRESNO 04-05-16 10:41:43 310 COMPLD "GENERATOR:RUN" ;
RTRV-ATTR	RETRIEVE-ATTRIBUTE-ENVIRONMENT: -This command retrieves attributes associated with environmental alarms. Note: This command does not determine whether or not an alarm is in existence, it simply shows what environmental alarm points are defined in the database.	
	Formal Input:	RTRV-ATTR-ENV:[tid]:aid:ctag::[ntfcncde],[almtype];
	Example Input Command:	RTRV-ATTR-ENV:FRESNO:AIR CONDITIONER:311::CR; This example will return a list of all critical alarm types associated with the air conditioner at Fresno.
	Formal Output:	<CR> <LF> <LF> tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ^^^"aid:ntfcncde,almtype" <CR> <LF> ;
	Example Output:	M FRESNO 04-05-16 10:41:44 311 COMPLD "AIR CONDITIONER:CR,FANOUT" "AIR CONDITIONER:CR,COMPOUT" ;

**Table M13.W - TL1 Command Descriptions (continued)**

Command	Description	
RTRV-COND	RETRIEVE-CONDITION - This command retrieves the current standing condition and/or state of specified equipment, facility, interfaces, lines, etc.	
	Formal Input:	RTRV-COND[-EQPT]:[tid]:[aid]:ctag::[condtype],[locn],[dir n],,,;
	Example Input Command:	RTRV-COND:FRESNO:ALARM POINT 2:312::DOWN,NEND,NA;
	Formal Output:	<CR> <LF> <LF> ^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ^^^"aid,ntfcncde,locn,dirm: <CR> <LF>
	Example Output:	M FRESNO 04-05-16 10:41:43 312 COMPLD "ALARM POINT 2:CR,NEND,NA,,; ;
RTRV-ATTR	RETRIEVE-EXTERNAL-CONTROL - This command sends an external control state to the user. This command can also be used to audit a result of an OPERATE-EXTERNAL-CONTROL or RELEASE-EXTERNAL-CONTROL.	
	Formal Input:	RTRV-EXT-CONT:[tid]:aid:ctag::[condtype];
	Example Input Command:	RTRV-EXT-CONT:FRESNO:GENERATOR:313::START;
	Formal Output:	<CR> <LF> <LF> ^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ^^^"aid:condtype,dur,constate" <CR> <LF>
	Example Output:	M FRESNO 04-05-16 10:41:43 313 COMPLD "GENERATOR:START,CONTS,OPER" ;

Table M13.W - TL1 Command Descriptions (continued)

Command	Description	
RTRV-HDR	RETRIEVE-HEADER - This command is typically used to verify the existence of a particular network element or to generate a list of all network elements on the network. In order to test for a particular element simply specify its TID. Otherwise all other elements will be returned.	
	Formal Input:	RTRV-HDR:[tid]::ctag;
	Example Input Command:	RTRV-HDR:FRESNO::314;
	Formal Output:	<CR> <LF> <LF> @^^^tid^date^time <CR> <LF> @M^^ctag^COMPLD <CR> <LF> @;
	Example Output:	FRESNO 04-05-16 10:41:43@M314 COMPLD@;
RTRV-ATTR	OPERATE-EXTERNAL-CONTROL - This command will operate a control. In the case of the TL1 Responder card the control can be either of the two internal relays or it can be mapped to a TBOS point on the 8-Port TBOS Collector.	
	Formal Input:	OPR-EXT-CONT:[tid]:aid:ctag::[condtype],[dur] Special Syntax Note: @CONDTYPE - A null value for this field results in all controls defined under the selected AID to be executed.
	Example Input Command:	OPR-EXT-CONT:FRESNO:FRONTDOOR:315::ACCESS,MNTRY; This command will open the door at the Fresno site. Since the MNTRY period was specified the door latch will energize for a period of time and then automatically de-energize. OPR-EXT-CONT:FRESNO:FRONTDOOR:316; This command will perform the exact function as the previous command because the CONDTYPE will default to ALL and the DUR field will default to MNTRY. OPR-EXT-CONT:FRESNO:FRONTDOOR;317::,CONTS; This command would latch on the air conditioner until such time a RLS-EXT-CONT command is issued. Please note that the “,” before the CONTS is a place holder for the CONDTYPE field and must be present. Failure to include the comma will result in the DUR field being processed as the CONDTYPE field.
	Formal Output:	<CR> <LF> <LF> ^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF>

**Note:** the OPR-EXT-CONT command can issue control commands to any interrogator port, as long as the port supports control issuance, and the control is defined as a TL1 control.

**Table M13.W - TL1 Command Descriptions (continued)**

Command	Description
ACT-USER	ACTIVATE-USER (SESSION) - This command is used for setting up a session when logging on to an external remote device (i.e., switch, radio, multiplex channel, DPM, etc.). A personal identification (PID) and user identification (UID) should be provided by the user.
	Formal Input: ACT-USER:[tid]:uid:ctag::pid;
	Example Input Command: ACT-USER:FRESNO:C.HARMON:319::45556;
	Formal Output: <CR> <LF> <LF> ^^^<TID>^date^time <CR> <LF> M^^<ctag>^COMPLD <CR> <LF> ^^^"uid>:user date^user time,attempts" ; Note: User Date and User Time was the last time that user logged on. Attempts" is the number of invalid logon attempts since last session.
	Example Output: M FRESNO 04-05-16 10:41:43 319 COMPLD "C.HARMON:96-05-24 13:20:20,01" ;
RLS-EXT-CONT	RELEASE-EXTERNAL-CONTROL - Releases relay momentarily or continuously. Opposite of OPR-EXT-CONT command.
	Formal Input: RLS-EXT-CONT:[tid]:aid:ctag::[condtype],{dur};
	Example Input Command: RLS-EXT-CONT:FRESNO:FRONTDOOR:318::LOCK;
	Formal Output: <CR> <LF> I f^^^tid^date^time <CR> <LF> M^^ctag^COMPLD <CR> <LF> ;
	Example Output: M FRESNO 04-05-16 10:41:43 318 COMPLD ;

**Table M13.X - TL1 Automatic Messages**

Command	Description
ACT-USER	REPORT ALARM - This message reports the occurrence of alarmed events. There are alarms that have immediate impact on operation and condition. Effort is required to restore normal operation and performance.
	Formal Input: (None)
	Formal Output: <CR> <LF> <LF> ^^^tid^date^time <CR> <LF> almcde^atag^REPT^ALM^EQPT <CR> <LF> ^^^aid:ntfcncde,condtype,srveff,,,locn,dirn" <CR> <LF> ;
	Example Output: FRESNO 04-05-22 08:02:29 *C 000038 REPT ALM T4X8 "PRIMARY POWER SYSTEM:CR,OUT,A,,,NEND,NA" ;
RLS-EXT-CONT	Messages may be correlated with other messages generated by actions of a Network Element. Related messages are RETRIEVE-ALARM, RETRIEVE-CONDITION, and REPORT EVENT.
	Formal Input: (None)
	Formal Output: <CR> <LF> <LF> ^^^tid^date^time <CR> <LF> almcde^atag^REPT^ALM^ENV ^^^aid:ntfcncde,almtype,, " <CR> <LF> ;
	Example Output: FRESNO 04-05-22 08:02:29 ** 000038 REPT ALM ENV "AIR CONDITIONER:MJ,FANOUT,, " ;
	This message uses the "Condition" field in the TL1 Alarm Point screen for the "ALMTYPE" parameter.
REPT EVT	REPORT EVENT - This message reports the occurrence of non-alarmed events. Any event that is reported can be attributed to the change of an irregular, or unsuitable event. This may be a non-severity occurrence, but can indicate a performance condition.
	Formal Input: (None)
	Formal Output: <CR> <LF> <LF> ^^^tid^date^time <CR> <LF> A^atag^REPT^EVT^EQPT <CR> <LF> ^^^aid:condtype,condeff,,,locn,dirn:,,\'status\'" <CR> <LF> ;
	Example Output: FRESNO 04-05-22 08:02:29 A 000038 REPT EVT EQPT "PRIMARY POWERSYSTEM:NOISY,SC,,,NEND, NA:,,\'EVENT TRUE\'" ;

**Note:** Automatic Messages are created in response to an alarm status change, not in response to used commands.

**This page intentionally left blank.**

# Software Module 14

## TABS Responder

The TABS Responder software module reports alarms collected by T/MonXM to another master using TABS protocol. This application is chiefly used for mediating alarms from other protocols, such as DCP, TBOS, and ASCII, into TABS.

If you ordered the TABS Responder with a new T/MonXM system, it will be factory-installed. If you are installing the TABS Responder on an existing system, follow the instructions for installing new modules in Section 2, Software Installation.

### Protocol Mediation Steps

The protocol mediation function of the TABS Responder occurs in three steps:

1. T/MonXM collects alarms from reporting devices in their native protocol.
2. The alarm data is mapped onto the TABS display defined by the user.
3. The mediated TABS data is reported to the TABS master.

Configuration of the TABS Responder consists of three steps:

1. Defining a remote port.
2. Defining the TABS master that T/MonXM will report to.
3. Mapping alarm points from the devices to be collected to the TABS display.

### TABS Responder Setup

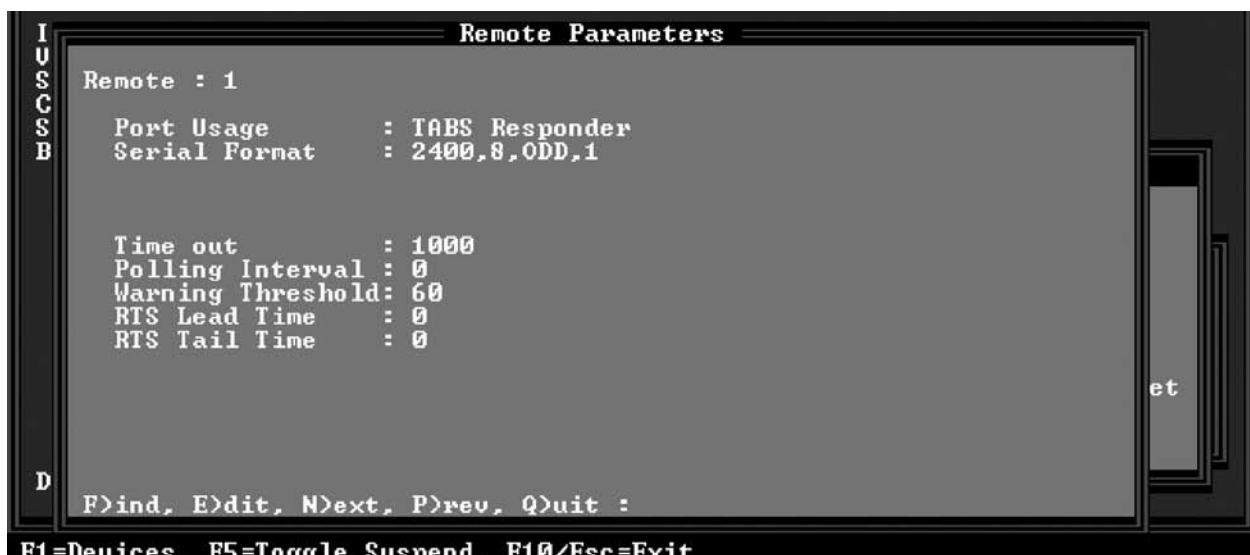


Fig. M14.1 - Remote Port defined for TABS Responder

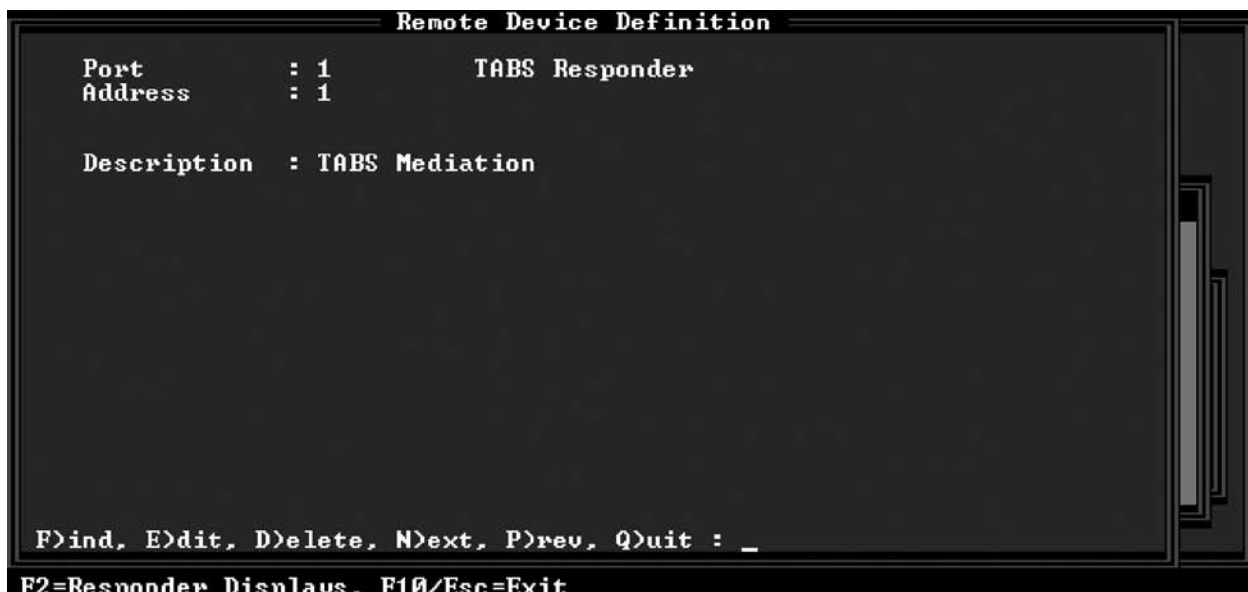
#### Defining the Remote Port

1. From the Master menu, select Parameters > Remote Ports.

2. Using the F)ind, P)revious, or N)ext commands, navigate to an unused remote port.
3. Choose E)dit.
4. Press Tab to select the list box and choose “TABS Responder” from the list of available port usages.
5. Enter appropriate values in the other fields in the Remote Parameters screen. See Figure M14.1 on page M24-2 for a picture of the Remote Parameters screen and Table M14.A for an explanation of the fields.

**Table M14.A - Fields in the TABS Responder Remote Parameters screen**

Field	Description
Port Usage	TABS Responder
Serial Format	Baud rate, word length, parity, and stop bits settings. Note: Make sure these settings match those of the TABS master T/MonXM will report to.
Time Out	Time out in milliseconds.
Polling Interval	Time between polls in milliseconds.
Warning Threshold	Seconds of no activity before a device failure is declared.
RTS Lead Time	RTS on time.
RTS Tail Time	RTS off time.

**Fig. M14.2 - Defining TABS address in the Remote Device Definition screen**

### Defining the TABS Master

1. Press F1 to open the Remote Device Definition screen.
2. Enter the TABS address that T/MonXM will report to and a description. (See Figure M14.2.)



### Mapping Devices to the TABS Display

1. From the Remote Device Definition screen, press F2 to open the Responder Definition screen.
2. Enter the port, address and display information of the devices to be mediated. See Figure M14.3 for a picture of the Responder Definition screen and Table M14.B for an explanation of the fields.

```

Remote Device Definition
Port      : 1      TABS Responder
Address   : 1

Responder Definition

-----Interrogator-----
Display   PORT    DEVICE  ADDR    DISPLAY
1         K1      1        1        1
2         NG      1        1        1
.....

Enter Responding Display Number <0-65535>

F3=BLANK  F8=Save  F10/Esc=Exit

```

**Fig. M14.2 - Mapping mediated devices in the Responder Definition screen**

In the example shown in Figure M14.3, the interrogating device will see alarms from KDA site 1 display 1 on TABS display 1, and alarms from Net Guardian site 1 display 1 on TABS display 2.

**Table M14.B - Fields in the Responder Definition screen**

Field	Description
Display	The display of the TABS master that the mediated devices will be mapped to. Up to 65,535 displays can be defined.
Interrogator	The fields under the Interrogator banner define the devices that will be mediated by T/MonXM.
Port	Port of the mediated device. (Relevant to DCM jobs only)
Device	Device ID of the mediated device.
Address	Address on the mediated device to be mapped to this TABS display.
Display	Display of the mediated device to be mapped to this TABS display.

**This page intentionally left blank.**

# Software Module 15

## FTP Server

The FTP (File Transfer Protocol) Server provision in T/MonXM provides for the capability of connecting to a T/MonXM as an FTP server using a standard Windows or other FTP client. This allows communicating machines of different types and operating systems to transfer information to and from T/MonXM.

Using the FTP Server, users are able to easily backup their systems, without exiting Monitor Mode, by simply transferring a copy of the database to a different terminal over LAN. Additionally, users are able to transfer MIB files and install T/MonXM updates remotely.



Fig. M15.1 - Transfer MIB files and T/MonXM updates via the FTP Server

## Set up a FTP Server

This section is a step by step procedure for configuring T/MonXM to use the FTP Server.

The following outlines the FTP Server configuration steps:

1. Setup a FTP Server Job
2. Setup a FTP Data Transfer Job
3. Test the FTP Connection

### Setup a FTP Server Job

1. Choose Master > Parameters > Remote Ports.
2. Press F (Find) and enter a port above 48. Press E (Edit) to edit the port parameters.
3. Press Tab to enter the list box. Select FTP Server and press Enter.
4. Enter a description — see Figure M15.2 for example.
5. Enter the maximum number of simultaneous connections.



**Fig. M15.2 - Establish an FTP Server job**

6. Press F6 to open the Data Connection Assignment screen — see Figure M15.3.
7. Press Tab to enter the list box. The usual TCP port for an FTP Server is 21 and its type must be TCP.

Entry	Type	IP Address	TCP Port	Description
1	TCP		21	FTP Server Socket
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Tab=Defaults, F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit

Fig. M15.3 - The FTP Server job must be on port 21

- 8. If no suitable data connection is available, press F1 to open the Ethernet TCP Port Definition screen and define a TCP connection on Port 21.
- 9. Press F8 to save your changes and return to the Data Connection screen.
- 10. From the Data Connection Screen, press Tab to enter the list box and select TCP Port 21. Press Enter to complete data connection assignment and return to the Remote Parameters Screen.

Data Connection Assignment	
Job : 67	Usage : FTP Server
Data Connection : FTP Server Socket (TCP Port 21)	
<div><div>NONE</div><div>FTP Server Socket (TCP Port 21)</div></div>	

I  
V  
S  
C  
S  
B

D

Fig. M15.4 - Assign TCP Port 21 to the FTP Server

**Setup a FTP Data Transfer Job**

1. Choose Master > Parameters > Remote Ports. Press F (Find) and enter a port above 48.
2. Press E (Edit) to edit the port parameters. Press Tab to enter the list box and select FTP Data Transfer.
3. Enter a description — see Figure M15.5 for example.

**Fig. M15.5 - Establish an FTP data transfer job**

4. Press F6 to open the Data Connection Assignment screen. Press Tab to enter the list box. The usual TCP port for an FTP Data Transfer is 20 and its type must be TELNET-RAW — see Figure M15.6.
5. If no suitable data connection is available, press F1 to open the Ethernet TCP Port Definition screen and define a TCP connection on Port 20. In the IP Address field of Port 20, enter the IP address of the T/Mon's IP Address.
6. Press F8 to save your changes and return to the Data Connection screen.
7. From the Data Connection Screen, press Tab to enter the list box and select TELNET-RAW Port 20.
8. Press Enter to complete data connection assignment and return to the Remote Parameters Screen — see Figure M15.7.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	TCP		21	FTP Server Socket
2	TELNET-RAW	126.10.220.12	20	FTP Data Transfer Socket
3	.....			
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				

Tab=Defaults, F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit

Fig. M15.6 - The FTP Data Transfer job typically uses TCP port 20

Remote Parameters	
Job : 68	FTP Data Transfer Socket (TELNET-RAW Port 20)
Port Usage :	FTP Data Transfer
Description :	FTP Data Transfer Socket
The usual TCP port for a FTP Data Transfer is 20 and its type must be TELNET-RAW	
F)ind, E)dit, N)ext, P)rev, Q)uit :	

F5=Toggle Suspend, F6=Data Connection, F10/Esc=Exit

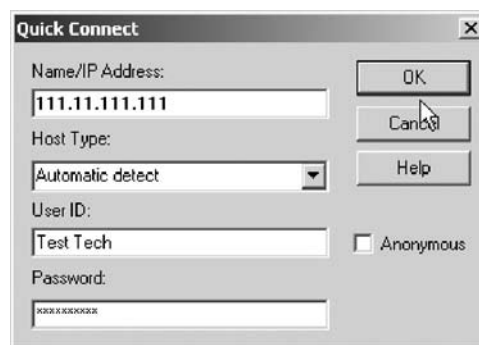
Fig. M15.7 - Completed FTP Data Transfer Job

### Test the FTP Connection

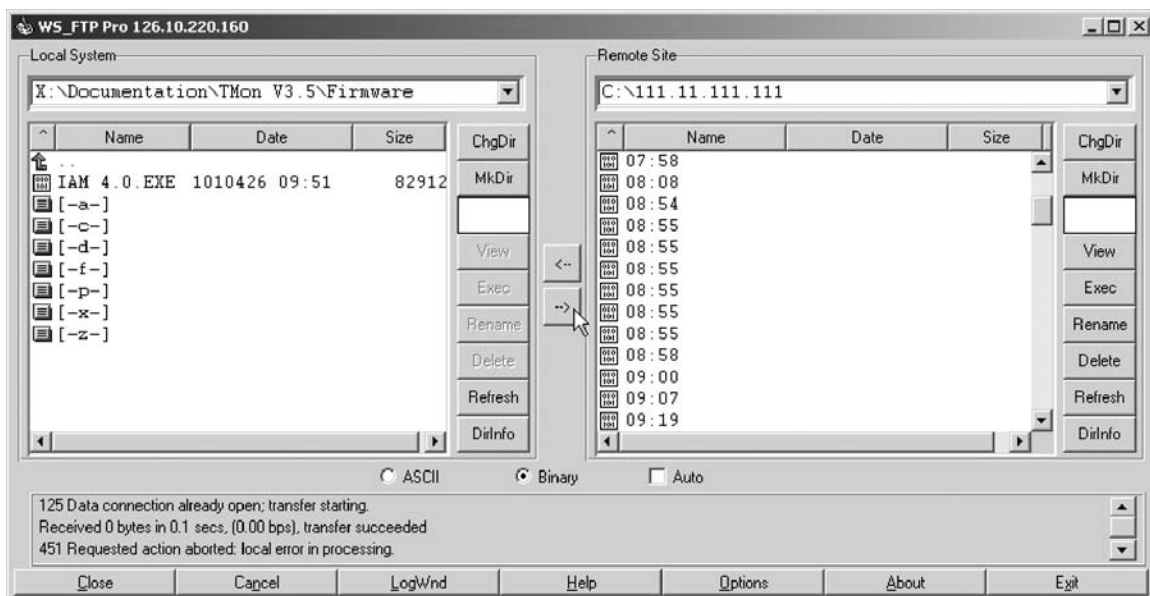
FTP connection interfaces will vary depending which FTP client you are using. Refer to your FTP client for instructions. The example below will likely not be identical to your FTP client.

A typical FTP client requires the IP Address of the T/MonXM system and the user name and password in order to establish a connection — see figure M15.8. Once a connection is established, files may be transferred to or from the T/MonXM system.

Figure M15.9 illustrates an example of transferring an IAM version 4.0 firmware upgrade.



**Fig. M15.8 - Enter the IP Address of the T/MonXM system and your user name and password**



**Fig. M15.9 - Example FTP IAM firmware upgrade**



# Software Module 16

## Pulsecom Datalok Interrogator

### Overview

The Datalok Interrogator is compatible with Pulsecom Datalok Models

- 10A
- 10AM
- 10D
- 10DM
- 10L
- 10

### Datalok Operational Summary

T/MonXM allows multiple protocols on multiple ports (up to 24 serial ports) in the same system. So you can have Datalok remotes on one or more ports and still have the capacity to expand your network with other remote alarm gathering devices on other ports. This is the ideal solution if your plans call for an integration of new remote gathering equipment into your existing Datalok network. T/MonXM's multi-protocol capabilities allow it to do tasks that would otherwise require multiple systems and screens to be placed in the alarm monitoring center.

*"Pulsecom" and "Datalok" are trademarks of the Pulsecom Division of Hubbell Inc.*

#### Network Design

Allocate how many remote access ports you want to use (dialup or direct) and put them on the first ports in the systems — see Figure M16.1.

Allocate which ports to use as direct connect 10A.

Allocate your dialup ports for 10Ds. Determine which lines should be Input/Output and which should be input only.

The 10A units are polled continuously. Each individual address has its own status refresh frequency. A status refresh can be requested at any time.

The 10D ports are capable of receiving an incoming call at any time (except when the line is already in use). The 10D will originate a call in three cases: Units are powered up, an alarm/control/Analog point changes status on a point that was designated as a dial in point, the no contact timer expired. T/Mon will dial Dataloks at a user specified time period (defined individually for each site). The user can also force a call to a site.

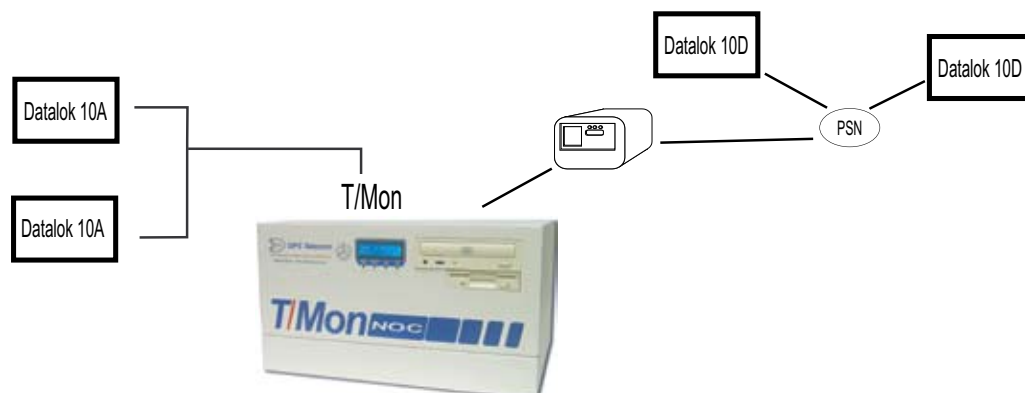


Fig. M16.1 - Application showing the current Datalok possibilities

## Provisioning 10A Units

You must create a remote port job on T/Mon to poll your 10A units. Use the following steps to create a remote port job:

- 1) Go to the Main menu > Parameters > Remote Ports option and create a 10A port job — see Figure M16.2 and Table M16.A for field descriptions.
- 2) Press F1. The Remote Device Definition screen will appear. Fill in the fields with the appropriate information — see Figure M16.3 and Table M16.B for field descriptions.

**Note:** The 10A units are polled continuously. Each individual address has its own status refresh frequency. A status refresh can be requested at any time.



Fig. M16.2 - Default remote parameters for Datalok 10A

Table M16.A - Fields in the Remote Parameters screen

Field	Description
Port Usage	Datalok 10A
Serial Format	Baud rate, word length, parity, and stop bits settings. <b>Note:</b> Be sure these settings match those of the 10A.
Time Out	Time interrogator will wait for a response before failing the poll (200-9999 milliseconds).
Poll Delay	Time between polls in milliseconds (0-9999).
Fail Threshold	Number of polls before device failure is declared (3-20)
Fail Poll Cycles	Polling loop cycles before failed devices are polled (0-255).
Check DCD on Rcv	Y = Enable DCD checking to validate Rcv. N = Disable. [N]
RTS Lead	RTS Lead is the time carrier is turned on before data is sent (0-2500 milliseconds, in 10 millisecond increments). [0]
RTS Tail	RTS Tail is the time carrier is left on after the last byte is sent (0-2500 milliseconds, in 10 millisecond increments). [0]

## Remote Device Definition

Refer to Figure M16.2 and Table M16.B for completing the Remote Device Definition screen. Table M16.B continues on following page.

```

Remote Device Definition

Port      : 21      DATALOK 10A
Address   : 1

Description :
Site Name  :
Unit Type  : 10 AM/L
Displays   : 1-35
Cards      : 0
Refresh Rate : 531
Log Undefined: N
Emulation On : N

KDA Mode   : N
Latched Rlys :
Skip Ctl stat:

----- Address Defaults -----
Polarity    : B      Windows :
Logging      : L      Message  : 0
History      : H
Level        : A
Status       : A
Reverse      : N
Description   : <Undefined>

F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit :

F1=Prints, F3=Int. Alarms, D10=, F4=Print, F5=Ctl, F6=Alarms, AF1=TL1, AF5=Move, F10/Esc=Exit

```

Fig. M16.2 - The Remote Device Definition screen

Table M16.B - Fields in the Remote Device Definition screen

Field	Description
Port	Remote Port defined for 10A Interrogator.
Address	Address of the Device. (must be unique to other units on same polling leg)
Description	Optional Description.
Site Name	Site name stamped on every event from remote.
Unit Type	Select type of unit: 10 AM/L, 10, 10A, 10A.1
Displays	Valid displays are 1-35.
Cards	Enter the number of expansion cards (0-3)
Refresh Rate	How many polls occur before two status poll used with alarm and hybrid polling.
Log Undefined	Enter "Y" for Yes, "N" for No.
Emulation On	Select Y for Emulation Mode and N for Native mode (downloadable). <b>Note:</b> This should be set to 'Y' if you have an old model 10A or 10D, or wish to run a current 10AM or 10DM in emulation mode. It should be set to 'N' if you wish to have T/Mon download the Datalok. Even though no configuration is required to be downloaded for emulation mode Dataloks, you should still define the analog threshold so T/Mon can still declare alarms.
KDA Mode	Select Y (Yes) if the unit is a KDA remote or N (No) if the remote is not a KDA remote.
Latched Rlys	Number of latched relays (0,5,10). <b>Note:</b> Indicates the number of latched relays that must match BOTH the physical amount of latched relays on the Datalok and the quantity of latched relays manually programmed into the unit. THIS FIELD IS ONLY APPLICABLE if emulation mode is ON.
Skip Ctl stat	Select Y (Yes) to skip control status or N (N) to perform exhaustive control refresh.

**Table M16.B - Fields in the Remote Device Definition screen (continued)**

Field	Description
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

**Table M16.C - Key commands in the Remote Device Definition screen**

Key	Command	Description
F1	Pnt	Opens the Point Definition screen. Use this screen to define points for reporting to T/Mon.
F3	Int Alarms	Define internal alarms for Datalok unit. Device failure/Device offline.
F4	Pnt	Opens the D10 Point Definition screen. Use this screen to provision alarm points.*
F5	Ctl	Opens D10 Control Point Provisioning screen. Use this screen to provision control points.*
F6	Alg	Opens D10 Analog Points Definition screen. Use this screen to define analog points.*
Alt-F1	TL1	Opens Sid Definition screen. Use this screen to define internal alarms.
Alt-F5	Move	Opens Move Address screen. Use this screen to move database to another port or address. Valid ports are 1-29. Only available if TL1 Responder Module is installed.
F10/Esc	Exit	Leaves the database screen without saving any changes that have been made.

\* = Provisioning downloaded to RTU.

## Point Definition

To go to the Point Definition screen, press F1 in the Remote Device Definition screen. This screen is used to define your Datalok's units for reporting alarm events to the T/Mon. Refer to Tables M16.D and M16.E for field descriptions and key commands. Refer to section M16-22 through M16-24 for point display mapping. See Section 10 (Point Definition Tutorial) for more information on defining points.

**Point Definition**

Port : 2 Addr: 1 Disp: 1

P L H L S R

o o s e t v

DCP(F) INTERROGATOR

Pt	l	g	t	v	s	s	Description	Fail	Clear
1	B	L	H	A	A	N	OPEN DOOR	OPEN	CLOSED
2	B	L	H	A	A	N	HIGH TEMP	HI	NORM
3	B	L	H	A	A	N	LOW TEMP	LO	NORM
4	B	L	H	A	A	N	BEACON	OUT	NORM
5	B	L	H	A	A	N	EAST RADIO	FAIL	NORM
6	B	L	H	A	A	N	WEST RADIO	FAIL	NORM
7	B	L	H	A	A	N	PRIMARY SWITCH	FAIL	NORM
8	B	L	H	A	A	N	SECONDARY SWITCH	FAIL	NORM

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

Message

F10/Esc=Exit

**Fig. M16.3 - The Point Definition screen**

**Table M16.D - Fields in the Point Definition screen**

Field	Description
Polarity	Enter "B" for Bipolar, "U" for Unipolar
Logging	Enter "L" for Log, "N" for No log.
History	Enter "H" for History, "N" for No history.
Level	Enter the default alarm level. Valid entries A, B, C, D.
Status	Enter "A" for Alarm, "S" for Status.
Reverse	Enter "R" for Reverse, "N" for No Reverse.
Description	Enter the default point description. This field is initially "Undefined."
Windows	Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

**Note:** Table M16.D continues on following section.

**Table M16.D - Fields in the Point Definition screen (continued)**

Field	Description
Qualification	Enter the duration alarm qualification time setting followed by a letter indicating the time units being used. The maximum numeric value is 99. Valid units are M for minutes, H for hours, and Q for quarter hours. <b>Example:</b> "10M" means 10 minutes.
Counter Qualification	Enter counter alarm qualification setting. In counter qualification, the alarm qualifies when a specified number of occurrences of the alarm occur in specified amount of time.  For no counter qualification enter a 0. Otherwise enter the qualification time followed by a letter indicating the time units being used. Follow this with a slash and the number of occurrences that will cause the alarm to qualify.  The maximum value for the period length is 99. Valid time units are M = minutes, H = hours, and Q = quarter hours. The maximum value for occurrences is 250. <b>Example:</b> 30M/10 MEANS 10 occurrences in 30 minutes.
Pager	Pager Profile Number (1-99)    0 = none

**Table M16.E - Key commands in the Point Definition screen**

Key	Command	Description
F1	GOTO	Go directly to a point.
F3	Blank	Blanks out a point definition.
F4	Attribute Section	Displays next section of attributes.
F5	Range Functions	Access commands that operate a range of points (e.g. translations, copies).
F6	Read	Reads point definitions from another display or address.
F8	Save	Save point definitions and return to polling list.
F10/Esc	Exit	Leaves the database screen without saving any changes that have been made.
Alt-F3	Delete Point	Deletes point under cursor and all below to move down one positions. And undefined point is then inserted at the cursor.
Alt-F4	Insert Point	Inserts an undefined point above cursor.
Alt-F5	Block Move	Moves a block of points within a display.
Alt-F6	Block Copy	Copies a block of points within a display.
Ctrl-F6	Extended Read	Reads in a portion of another display to a starting point in the current display.

**Note:** Vertical editing is available in the point editing section via the CTRL-PGUP and CTRL-PGDN keys. (Press Ctrl-H for more help on this).

## Device Internal Alarm Assignment

Provision your Datalok's internal alarms in the Device Internal Alarm Assignments screen. To go to this screen, press F4 in the Remote Device Definition screen. For more information on internal alarms, see Section 14 (Define Internal Alarms).

**Note:** Internal alarms must have an address of 11-13 only.

Address	Dev	Description	Fail	Off line
1	D10A	Jonestown	11.1.1.	11.2.1

Enter internal point (addr.display.pnt) (blank=none) (address range: 0-13)

F8=Save, F10/Esc=Exit

Fig. M16.4 - The Device Internal Alarm Assignments screen

Table M16.F - Fields in the Device Internal Alarm Assignments screen

Field	Description
Port	The port used by the device.
Address	The address used by the device.
Dev	The device name (D10)
Description	Site name
Fail	This is the internal alarms point that is generated if it doesn't answer or is failed. Enter the internal point (address.display.point) for Fail. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11, 12, or 13.
Offline	If a user takes an RTU offline, this is the alarm you would see. If you don't type anything here you get a standard alarm. Enter the internal point (address.display.point) for Offline. A blank entry indicates no Internal Alarm Assignment. Enter either Address 11, 12, or 13.

## D10 Alarm Point Definition

Provision your alarm points by pressing F4 in the Remote Device Definition screen. The D10 Alarm Point Definition screen will appear — see Figure M16.5. See Table M16.G for field descriptions.

**D10 Alarm Point Definition**

Port : 21      Address : 1

Alm Pnt	Point Type	Delay Qualify
1	Normal	
2	Delay	....
3		
4		
5		
6		
7		
8		
9		
10		

Delay Time in secs <1-1200>

Description : <Undefined>

Up Arrow=Previous Field, F10/Esc=First Field

Fig. M16.5 - The D10 Alarm Point Definition screen

Table M16.G - Fields in the Device Internal Alarm Assignments screen

Field	Description
Alm Pnt	Alarm point on the unit to be defined.
Point Type	Determines the characteristics of a point. Select one of the following: Normal: Alarms are declared immediately Delay: Alarms declared after a qualified (specified) amount of time Accum: Alarms declared after a number of transitions
Delay/Qualify	Determines the time delay/accumulation count for "Delay" and "Accum" types. <b>Note:</b> this is on the Datalok unit and is cumulative with T/Mon Qual.
Call on COS	Gives the alarm point call in priority. (10D unit only)

Table M16.H - Key commands in the Device Internal Alarm Assignments screen

Key	Description
F1	GOTO. Moves the cursor to a selected entry.
F3	BLANK. Deletes the current entry.
F8	Saves the database.
F9	Online help files.
F10/Esc	Leaves the database screen without saving any changes that have been made.



## D10 Control Point Definition

**Note:** Refer to section M16-25 for Control Point display mapping

The 80 control points are divided into four groups of twenty.

1. Only the first 10 points of each group may be latching.
2. All latching control definitions must precede other types of controls.
3. A latching point disqualifies other points from being used — see Table M16.I.

**Note:** See Table M16.H for descriptions of command keys available in the D10 Control Point Definition screen.

**D10 Control Point Definition**

Port : 1    Address : 1

Ctl Pnt	Point Type	Duration
1	Momen	5
2	Normal	
3	Normal	
4	Normal	
5	Normal	
6	Normal	
7	Normal	
8	Normal	
9	Normal	
10	Normal	

Point type: N=Normal, M=Momen, L=Latched, U=Undef

Description : (Undefined)

F1=GOTO, F3=BLANK, F8=Save, F9=Help, F10/Esc=Exit

Fig. M16.6 - The D10 Control Point Definition screen

Table M16.I - Latching points and disqualified points

Latching Point	Point, and all points below cannot be used
1	20
2	19
3	18
4	17
5	16
6	15
7	14
8	13
9	12
10	11

**Note:** These settings must correspond with the relay hardware connected to the Datalok.

## D10 Analog Point Definition

Define your Datalok analog points by pressing F6 in the Remote Device Definition screen. The D10 Analog Point Definition screen will appear — see Figure M16.7. Refer to Table M16.J for field descriptions and see Table M16.H for key commands descriptions.

**Note:** Refer to section M16-26 through M16-27 for point display mapping.

Telemetry Pnt	Description	Call 00L	Call RTN	Scale Factor	Disp Scale	Disp Offset	Low Thresh	High Thresh	Disp Unit	Sig Dig
1	TEMPERATURE....			3.0	1.00000	0.00000	35.15	60.00	T	2
2	HUMIDITY				1.00000	0.00000	0.00	20.00	°H	2
3										
4										
5										
6										
7										
8										

Description of telemetry point

Fig. M16.7 - The D10 Analog Point Definition screen

Table M16.J - Fields in the D10 Analog Point Definition screen

Field	Description
Description	The analog description that gets displayed on real time analog display screen.
Call 00L	Gives analog point call in priority when the voltage goes out of limits. (10D only).
Call RTN	Gives analog point call in priority when the voltage returns to normal range. (10D Only)
Scale Factor	The voltage scaling factor that must correspond to hardware settings. This is only applicable for the first analog point on the base unit and each expansion card. Values are: 1.0, 1.5, 3.0
Disp Scale, Disp Offset	Values used to calculate the analog value that will be displayed on the monitor mode screen: $\text{DISPLAYED VALUE} = (\text{VOLTAGE} \times \text{DISP\_SCALE}) + \text{DISP\_OFFSET}$ <b>Note:</b> while editing the Disp Scale field, you can press F6 to bring up a worksheet to test or calculate these values — see section M16.11.
Low Threshold	Any voltage under this value will cause a threshold alarm to occur. To enter the value in displayed units instead of volts, press F6 while the cursor is at this field.
High Threshold	Any voltage over this value will cause a threshold alarm to occur. To enter the value in displayed units instead of volts, press F6 while cursor is at this field.
Disp Unit	Text that will be displayed next to the analog value on the Monitor Mode screen. For example: psi, lbs, etc.
Sig Dig	Number of digits after the decimal point that will be displayed on the Monitor Mode screen.

```

D10 Analog Point Definition
Port : 21    Address : 1

Te Pn
Analog Display Worksheet
Sig Dig
2

Use this form to calculate or test different values for Display
Scale and Display Offset. The numbers in brackets show
(voltage * Display Scale) + Display Offset.

Display Scale           : 1.00000
Display Offset          : 0.00000
Sig Dig                 : 2

Value displayed for lowest voltage : -19.844    [-19.84]
Value displayed for highest voltage : 20.0000    [ 20.00]

En
Enter display scale <cannot be 0>

F8=Save, F10/Esc=Exit

```

Fig. M16.8 - Change the analog reference scale in the Analog Display Worksheet screen

**Note:** This operation is optional for users who want to change the analog reference scale so that the displayed analog values correspond to real world values.

### Analog Display Worksheet

To define your analog reference scale, press F6 from the Analog Provision screen. The Analog Display Worksheet screen is used to convert the analog voltage and current readings into meaningful measurements and units. The analog inputs actually measure either voltage or current. The values must be converted to their actual units by determining the scale and offset for each input. By entering in a few simple values, T/Mon will make the conversion calculations automatically. Each field and its function are described below.

#### Call OOL

Gives that analog point call in priority when the voltage goes out of limits. (10D only)

#### Call RTN

Gives that analog point cal in priority when the voltage returns to normal range. (10D only)

#### Scale Factor

The voltage scaling factor that must correspond to hardware settings. This is only applicable for the first analog point on the base unit and each expansion card. Values are 1.0, 1.5, 3.0.

#### Disp Scale, Disp Offset

Values used to calculate the analog value that will be displayed on the Monitor Mode screen:

$$\text{DISPLAYED VALUE} = (\text{VOLTAGE} * \text{DISP\_SCALE}) + \text{DISP\_OFFSET}$$

**Note:** while editing the Disp Scale field, you can press F6 to bring up a worksheet to test or calculate these values.

#### Low Threshold

Any voltage under this value will cause a threshold alarm to occur. To enter the value in displayed units instead of volts, press F6 while

the cursor is at this field.

#### High Threshold

Any voltage over this value will cause a threshold alarm to occur. To enter the value in displayed units instead of volts, press F6 while the cursor is at this field.

#### Disp Unt

Text that will be displayed next to the analog value on the Monitor Mode screen. For example: psi, lbs, etc.

#### Sig Unt

Number of digits after the decimal point that will be displayed on the Monitor Mode screen.

Define Datalok alarm points for TL1 reporting in the Sid Definition screen. Press Alt-F1 in the Remote Device Definition screen to go to the Sid Definition screen. For detailed information and instructions, refer to Section 13 (TL1 Responder).

**Note:** Requires TL1 Responder software module. TL1 Responder software module sold separately.

Move your remote device definition from one port or address to another by pressing Alt-F5. The Move address screen will appear — see Figure M16.9. Enter the destination port or address.

**Note:** Valid ports are 1-29 and valid addresses are 1-999.

## Define Points for TL1 Alarm Reporting

## Move Address

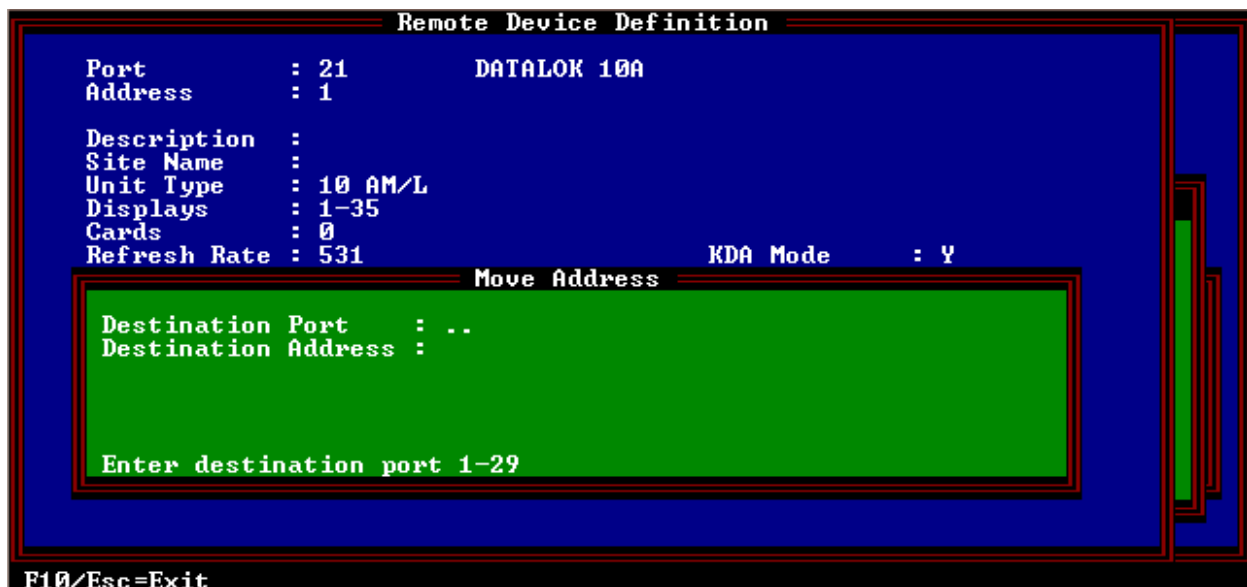


Fig. M16.9 - Move your remote device definition from one port or address to another

## Provisioning 10D Units

The following is an overview of the recommended steps to provision your 10D unit. Detailed instructions and information are continued on the following sections:

- 1) Create 10D remote port job in the Parameters > Remote Port screen — see Figure M16.10.
- 2) Go to the Master Menu > Files Maintenance menu.
- 3) Select Dial Up Networks.
- 4) Select Datalok Devices.
- 5) Enter the appropriate site information.
- 6) Press F1 to go to the virtual address definition (Datalok 10 Device Definition) screen.
- 7) Enter the appropriate address information.
- 8) Press F1 to define all applicable points.
- 9) On the Address screen, provision the Datalok units by doing the following:
  - F4- Define Points
  - F5- Define Controls
  - F6- Define Analogs
  - F7- Define Modem Information

## Define Remote Parameters

Use the following steps to create a remote port job for polling your Datalok 10D units:

1. Go to the Main Menu > Parameters > Remote Ports sub-menu option.
2. Press F (Find) and enter a port number.
3. Refer to Figure M16.10 and Table M16.K for field descriptions.

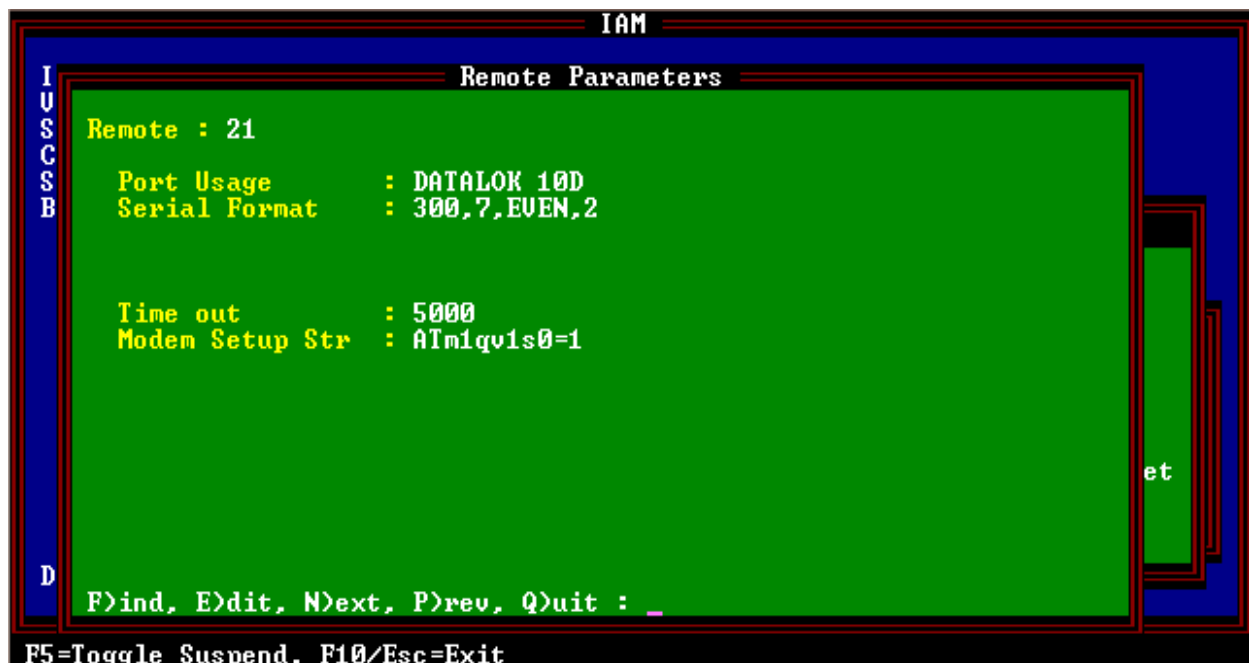


Fig. M16.10 - Default Remote Parameters

**Table M16.K - Fields in the Remote Parameters screen**

Field	Description
Port Usage	Datalok 10D
Serial Format	Baud rate, word length, parity, and stop bits settings. <b>Note:</b> Be sure these settings match those of the 10D unit.
Time Out	Time interrogator will wait for a response before failing the poll (200-9999 milliseconds).
Modem Setup Str	String that is sent to an "AT" style modem to configure the modem. [ATm1qv1s0=1]

## D10 Site Definition

Use the following steps to define your D10 Site:

1. Go to the Main menu > Files > Dial Up Networks sub-menu option. The D10 Site Definition screen will appear — see Figure M16.11.
2. Enter the appropriate information in each field. Refer to Table M16.L for field descriptions.

```

D10 Site Definition

Site Name      : YOUR SITE
Description    : Enter a description here
Remote Site Phone : 1112223333
Connect Timeout : 15

Polling Type   : PERIODIC
Polling Interval : 60  (mins)

Scheduled Days ---> SUN:    MON:    TUE:    WED:    THU:    FRI:    SAT:
Scheduled Hours :
Scheduled Minute :

Dialout Port   : 0.

Remote port where outgoing calls are made. 0=none

Up arrow=Previous Field, F10/Esc=First Field

```

**Fig. M16.11 - The D10 Site definition screen****Table M16.L - Fields in the D10 Site definition screen**

Field	Description
Site Name	Enter modem site name.
Description	Description of site.
Remote Site Phone	Phone number at remote site.
Connect Timeout	Number of seconds before aborting outgoing connection (10-99). [15]

Table M16.L continues of following section.

Table M16.L - Fields in the D10 Site definition screen (continued)

Field	Description
Polling Type	Select Periodic or Schedule from the sub-menu by pressing the Tab key. If Periodic is selected, the cursor will skip to the Polling Interval field. If schedule is selected, the cursor will skip to the Scheduled Days field.
Polling Interval	The number of minutes T/Mon will wait since the last scheduled poll before T/Mon will automatically call the site. Periodic polling only — 0-9999 minutes. (0=never) <b>Note:</b> skips out of edit mode after entering value.
Scheduled Days	Schedule polling only. For each day of the week enter Y (Yes) to activate polling or N (No) to deactivate.
Scheduled Hours	Enter the whole number of each hour (24 hour clock) to place a polling call (0-23, where 0=midnight). <b>Example:</b> 0,8-16 polls at midnight and every hour from 8AM to 4PM.
Scheduled Minutes	Enter the whole number of offset from the hour each call is to be made (0-59 where 0= on the hour). <b>Example:</b> 30 polls at half past the hour.
Dialout Port	Enter the remote port where outgoing calls are made. (0=none). The port specified must have been previously defined in the Parameters > Remote Ports sub-menu option. If you are defining a Datalok site, then the remote port job must be defined as a Datalok Dialup port.

## Datalok 10D Device Definition

Define your 10D units by pressing F1 in the D10 Site Definition screen. Refer to Figure M16.12 and Table M16.M for field descriptions and options.

```

Datalok 10D Device Definition

D10 Site Name: DPS
D10 Address : 1

Description :
Site Name :

Displays : 1-10
Cards : 0
Virtual addr : 1
Log Undefined: N
Emulation On : N
KDA Mode : N
Latched Rlys :

----- Address Defaults -----
Polarity : B
Logging : L
History : H
Level : A
Status : A
Reverse : N
Description : <Undefined>

F1>ind, E>dit, D>elete, N>ext, P>rev, Q>uit :
F1=Prints, F3=Int Alarms, D10=, F4=Print, F5=Ctrl, F6=Alarms, F7=Menu, AF1=Title, F10/Esc=Exit

```

Fig. M16.12 - The Datalok 10 Device Definition screen

**Table M16.M - Fields in the Datalok 10 Device Definition screen**

Field	Description
Port	Remote Port defined for 10D Interrogator
Address	Address of the Device.
Description	Optional field to describe site.
Site Name	Site name stamped on every event from remote.
Displays	Valid displays are 1-35. [1-10]
Cards	Enter the number of expansion cards (0-3). [0]
Virtual Address	Enter virtual address (1-999).
Log Undefined	Enter Y (Yes) to log undefined points using address default settings, or N (No) to ignore undefined points. <b>Note:</b> information entered in the Point Definition screen will override address default settings.
Emulation On	Select Y for Emulation Mode and N for Native mode (downloadable). <b>Note:</b> This should be set to 'Y' if you have an old model 10A or 10D, or wish to run a current 10AM or 10DM in emulation mode. It should be set to 'N' if you wish to have T/Mon download the Datalok. Even though no configuration is required to be downloaded for emulation mode Dataloks, you should still define the analog threshold so T/Mon can still declare alarms.
KDA Mode	Select Y (Yes) if the unit is a KDA remote or N (No) if the remote is not a KDA remote.
Latched Rlys	Number of latched relays (0,5,10). <b>Note:</b> Indicates the number of latched relays that must match BOTH the physical amount of latched relays on the Datalok and the quantity of latched relays manually programmed into the unit. THIS FIELD IS ONLY APPLICABLE if emulation mode is ON.
Skip Ctl stat	Select Y (Yes) to skip control status or N (N) to perform exhaustive control refresh.
<b>Address Defaults</b>	If an alarm occurs in a reported RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Enter "B" for Bipolar, "U" for Unipolar
Logging	Enter "L" for Log, "N" for No log.
History	Enter "H" for History, "N" for No history.
Level	Enter the default alarm level. Valid entries A, B, C, D.
Status	Enter "A" for Alarm, "S" for Status.
Reverse	Enter "R" for Reverse, "N" for No Reverse.
Description	Enter the default point description. This field is initially "Undefined."
Windows	Enter the default windows. Valid windows are 2-90 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

See Table M16.N on the following page for key commands and descriptions.



**Table M16.N - Key commands in the Datalok 10 Device Definition screen**

Key	Command	Description
F1	Pnt	Opens the Point Definition screen. Use this screen to define points for reporting to T/Mon.
F3	Int Alarms	Define internal alarms for Datalok unit.
F4	Pnt	Opens the D10 Point Definition screen. Use this screen to provision alarm points.*
F5	Ctl	Opens D10 Control Point Provisioning screen. Use this screen to provision control points.*
F6	Alg	Opens D10 Analog Points Definition screen. Use this screen to define analog points.*
Alt-F1	TL1	Opens Sid Definition screen. Use this screen to define internal alarms. <b>Note:</b> only if TL1 Responder Module is installed.
Alt-F5	Move	Opens Move Address screen. Use this screen to move database to another port or address. Valid ports are 1-29.
F10/Esc	Exit	Leaves the database screen without saving any changes that have been made.

\* = This information will be downloaded to RTU.

## Point Definition

From the Datalok 10 Device Definition screen, press F1. The Point Definition screen will appear — refer to section M16-5 for further instructions and illustrations. Also, see Section 10 Point definition Tutorial for more information.

## Internal Alarms Definition

Pressing F3 in the Datalok 10 Device Definition screen will bring up the Device Internal Alarm Assignment screen. Refer to section M16-7 for field and key command descriptions.

## D10 Alarm Point Definition

To provision your Datalok 10D alarm points, press F4 from the the Datalok 10 Device Definition screen. Refer to section M16-8 for field and key command descriptions.

## D10 Control Point Definition

To provision your Datalok 10D control points, press F5 from the the Datalok 10 Device Definition screen. Refer to section M16-9 for field and key command descriptions.

## D10 Analog Point Definition

Pressing F6 in the Datalok 10 Device Definition screen will bring up the D10 Analog Point Definition screen. Provision your analog points and settings. Refer to section M16-10 for further details.

## D10 Modem Point Definition

Define backup phone numbers your Datalok will attempt to dial T/Mon in the D10 Modem Point Definition screen. Press F7 in the Datalok 10 Device Definition screen. The D10 Modem Point Definition screen will appear. Refer to Table M16.O for field descriptions.

**D10 Modem Point Definition**

Port : RP      Address : 1

Primary Phone Number	Secondary Phone Number	Call Timer DTMF
		HR MN
.....		

The first phone number Datalok will call. "0-9,T,P"

Description : <Undefined>

F1=GOTO, F3=BLANK, F8=Save, F9=Help, F10/Esc=Exit

Fig. M16.13 - The D10 Modem Point Definition screen

Table M16.O - Fields in the D10 Modem Point Definition screen

Field	Description
Primary phone number	The backup phone number the Datalok will attempt to call T/Mon. Valid digits are 0-9 plus the following special control characters: "T" wait for dial tone, "P" for pause. Formatting characters "( ) -" and spaces are permitted but will not be downloaded to the Datalok. "E" is not permitted but will be sent to the Datalok.
Secondary phone number	The backup phone number the Datalok will attempt to call if the primary number is not successful. The format of this number is the same as the primary number.
No Call Timer: (Hours and minutes)	The amount of time the Datalok will wait without any contact with this master, before the Datalok will initiate a call. Note: any value less than 20 minutes will result in this feature being disabled. A disabled timer will be denoted by "— —".
DTMF	Selects the type of dialing the Datalok will perform. "Y" indicates DTMF, "N" indicates pulse.

Table M16.P - Key commands in the D10 Modem Point Definition screen

Key	Description
F1	GOTO. Moves the cursor to a selected entry.
F3	BLANK. Deletes the current entry.
F8	Saves the database.
F9	Online help files.
F10/Esc	Leaves the database screen without saving any changes that have been made.

## Define Points for TL1 Alarm Reporting

Define Datalok alarm points for TL1 reporting in the Sid Definition screen. Press Alt-F1 in the Remote Device Definition screen to go to the Sid Definition screen. For detailed information and instructions, refer to Section 13 (TL1 Responder).

**Note:** Requires TL1 Responder software module. TL1 Responder software module sold separately.

---

## Labeled Controls

All labeled controls are issued to displays 4 and 5. In the case of 10A units, use the remote port number connected to the 10A address. For 10D units, you must use the “RP” followed by 10D virtual address. For more information see Section 12 (Configure Controls).

---

## Internal Device Failures

Internal user alarms provide an enhanced method to report device failures compared to the generic default method that the system uses. Using internal device failures you can assign an internal alarm to represent a device failure. This gives you the ability to customize your alarm attributes such as alarm description and the windows that you want to define the alarm to go to (ie., group the device failure with the rest of that site’s alarms).

For both direct connect and dialup devices, enter the internal alarms section by pressing F3 on the address definitions screen.

**Note:** The address definition screen for direct connect devices is located on the Parameters > Remote Ports menus. The address screen for dialup devices is under Files > Dialup Devices > Device type sub menu. Once selected, enter the soft alarm you wish to use into the device offline section. Later, you must go to the Files > Internal Alarms > User Defined Alarm screen and set the attributes for the point you just specified — see Section 14 (Define Internal Alarms).

---

## 10A Statistic Explanations

Table M16.Q explains the statistics for 10A Units.

The lower left of the stat window contains the Time of Day, the lower right corner contains the address and the mode that is currently being polled.

**Note:** Press F6 to get to this screen in Monitor Mode.

---

## 10D Dialup Stats

These stats are standard dial-out stats. Calls made, Calls busy, Call Errs, Hang-up Err, Calls Rcvd are self explanatory.

**Special note regarding HANGERR:** If hangerr gets incremented every time you try to make a call, then you either have a bad modem, or an improper connection between the workstation and the modem.

---

## Monitor Mode Options

Monitor Mode options from alarm summary screen are described below.

### Shift-F4: Dialup Site Monitor

Shows the current status of all dialup sites. (Indicates if the site is waiting to call, the cause of the call, device status and time of last call.) See Table M16.R for hot keys you can access from this screen.

**Table M16.Q - Fields in 10D Dialup Statistics**

Field	Description
MODE	Tells you if the modem is "WAITING", placing an "OUTGOING" call, or accepting an "INCOMING" call.
Site Name	Will contain the name of the site the modem is connected to. This is providing, of course, the modem is not in the "WAITING" state.
No Tone Err	Indicates that no dial tone was present when the system wanted to make a call. This can happen from time to time during incoming and outgoing call collisions. If this number is large, there may be a problem with the connection to the phone line, or somebody else may be on that line.

**Table M16.R - Fields in 10A Statistics (F6)**

Field	Description
Polls Sent	# of polls (commands) sent to Datalok.
Polls Ok	# of polls that the Datalok responded to.
Ctrl's Sent	# of Labeled controls that were issued.
Ctrl's Ok	# of controls that the Datalok accepted.
Downloads	Number of times the Datalok was downloaded.
No Response	Number of times no response was received from the Datalok.
No Response	Number of times no response was received from the Datalok.
Time Out	Number of times that only a partial response was received from the Datalok.
Hdr Error	There was an error with the header of the response received. Either wrong address or wrong format.
Misc Error	General Catch all error. The specific cause of the error is probably not important as they are all generally due to a noisy communications environment. However you can get a specific description by selecting the English view window.
	CMD ERR      Datalok rejected previous command.
	Invalid ART      An invalid character was received where at the ART position of the frame.
	Invalid PNT Except      An invalid point number was received in a COS alarm packet.
	Invalid CTL Except      An invalid control point was received in the control section of frame.
	Invalid ALG Except      An invalid analog point was received in the control section of frame.
	Invalid ctrl Cfg      Did not find the control section in a response where one was expected.
	Bad Analog      There was an error in the analog portion of the frame.
	Alog Data not valid      A specific portion of the analog field was not as expected.

**Note:** Table M16.R continues to following section.

**Table M16.R - Key commands available in the Dial-Up Site Monitor screen (continued)**

Field	Description	
Dsp Not Mon	This field tells you that data was received from the Datalok that T/Mon was not told to monitor. To find out which displays, to into English and watch for:	
	(NOT MON)	Data display not monitored (Displays 1-3).
	(CTL NOT MON)	Status update Controls not monitored (Disp 4-5).
	(CR1 NOT MON)	Cos Update for ctrls not monitored (Disp 4-5).
	(AT NOT MON)	Analog Threshold alarm not monitored (Disp 6)
	(AV NOT MON)	Analog Voltage not monitored (Disp 7-10).

**Table M16.S - Key commands available in the Dial-Up Site Monitor screen (Shift-F4)**

Key	Description
F1	Force Call, Mark the Datalok for an immediate call.
F2	Undo force call - Removes the site from the immediate call list. (Assuming the call is not in progress).
F3	Forces a call and unit will be downloaded.
F4	Online- puts a dialup device back in the calling list.
F5	Offline- Removes a dialup device from the calling list.
Cursor Keys	Select site (Up/Dn Arrow, Pg Up/Dn, Home/End)

**Shift-F6: Site Statistics**

Shows the Address, device type, site name, polls, ok and fail status.

**Table M16.T - Key commands available in Site Statistics screen**

Key	Description
F1	Init stats - Resets all Poll/OK/Fail stats to 0.
F2	Online - Puts the highlighted site on line.
F3	Offline - Takes the highlighted site off line.
F4	Status Poll - Forces the highlighted site to be status polled next time through the polling site.
F5	Reconfig - Forces the highlighted site to be downloaded next time through the polling site.
Cursor Keys	Select site (Up/Dn Arrow, Pg Up/Dn, Home/End)

**Shift-F8: View analogs**

Use the cursor keys to select the analog page you want to see.

Initially the screen will show the last analog value polled. The analog display for Dataloks display 16 channels at a time. Pressing F4 will toggle the next bank of 16 channels. Most users will not need to use F4, as there are seldom more than 16 analogs (2 expansion cards) in the typical Datalok. When the analog is in alarm, the analogs values will be displayed with RED background and have an Up or Down arrow. Normal analogs will be display in green.

10A Devices will continuously update.

10D Devices will NOT automatically update alarm status until the

## Configuration Tables

user presses F5 to initiate an analog update dialing sequence. Prior to pressing F5 the user is warned that the analog display is static.

T/MonXM is a display-based (64 pt) alarm monitoring system. Therefore, Datalok information is mapped into T/Mon Displays — see Table M16.U.

**Table M16.U - Display Overview for Datalok information**

Display	Description
Displays 1-3	Alarm points 1-144
Displays 4-5	Control Points 1-80
Display 6	Under/Over Analog Threshold alarms. These are internally generated by T/Mon.
Displays 7-10	Analog image data.

## Point Display Mapping

### Datalok Alarm Points to T/MonXM Display Conversion

Datalok alarm points are mapped to Displays 1 and 2 in T/MonXM. Refer to Tables M16.V–M16.Z for alarm point mapping information.

**Table M16.V - Base Unit (Alarms 1-36)**

Datalok Type/Point	T/MonXM Display.Point	Datalok Type/Point	T/MonXM Display.Point
Alm Pt 1	1.1	Alm Pt 19	1.19
Alm Pt 2	1.2	Alm Pt 20	1.20
Alm Pt 3	1.3	Alm Pt 21	1.21
Alm Pt 4	1.4	Alm Pt 22	1.22
Alm Pt 5	1.5	Alm Pt 23	1.23
Alm Pt 6	1.6	Alm Pt 24	1.24
Alm Pt 7	1.7	Alm Pt 25	1.25
Alm Pt 8	1.8	Alm Pt 26	1.26
Alm Pt 9	1.9	Alm Pt 27	1.27
Alm Pt 10	1.10	Alm Pt 28	1.28
Alm Pt 11	1.11	Alm Pt 29	1.29
Alm Pt 12	1.12	Alm Pt 30	1.30
Alm Pt 13	1.13	Alm Pt 31	1.31
Alm Pt 14	1.14	Alm Pt 32	1.32
Alm Pt 15	1.15	Alm Pt 33	1.33
Alm Pt 16	1.16	Alm Pt 34	1.34
Alm Pt 17	1.17	Alm Pt 35	1.35
Alm Pt 18	1.18	Alm Pt 36	1.36

**Table M16.X - Expansion Card #1 (Alarms 37-72)**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Alm Pt 37	1.37	Alm Pt 55	1.55
Alm Pt 38	1.38	Alm Pt 56	1.56
Alm Pt 39	1.39	Alm Pt 57	1.57
Alm Pt 40	1.40	Alm Pt 58	1.58
Alm Pt 41	1.41	Alm Pt 59	1.59
Alm Pt 42	1.42	Alm Pt 60	1.60
Alm Pt 43	1.43	Alm Pt 61	1.61
Alm Pt 44	1.44	Alm Pt 62	1.62
Alm Pt 45	1.45	Alm Pt 63	1.63
Alm Pt 46	1.46	Alm Pt 64	1.64
Alm Pt 47	1.47	Alm Pt 65	2.1
Alm Pt 48	1. 48	Alm Pt 66	2.2
Alm Pt 49	1.49	Alm Pt 67	2.3
Alm Pt 50	1.50	Alm Pt 68	2.4
Alm Pt 51	1.51	Alm Pt 69	2.5
Alm Pt 52	1.52	Alm Pt 70	2.6
Alm Pt 53	1.53	Alm Pt 71	2.7
Alm Pt 54	1.54	Alm Pt 72	2.8

**Table M16.Y -Expansion Card #2 (Alarms 73-108)**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Alm Pt 73	2.9	Alm Pt 91	2.27
Alm Pt 74	2.10	Alm Pt 92	2.28
Alm Pt 75	2.11	Alm Pt 93	2.29
Alm Pt 76	2.12	Alm Pt 94	2.30
Alm Pt 77	2.13	Alm Pt 95	2.31
Alm Pt 78	2.14	Alm Pt 96	2.32
Alm Pt 79	2.15	Alm Pt 97	2.33
Alm Pt 80	2.16	Alm Pt 98	2.34
Alm Pt 81	2.17	Alm Pt 99	2.35
Alm Pt 82	2.18	Alm Pt 100	2.36
Alm Pt 83	2.19	Alm Pt 101	2.37
Alm Pt 84	2.20	Alm Pt 102	2.38
Alm Pt 85	2.21	Alm Pt 103	2.39
Alm Pt 86	2.22	Alm Pt 104	2.40
Alm Pt 87	2.23	Alm Pt 105	2.41
Alm Pt 88	2.24	Alm Pt 106	2.42
Alm Pt 89	2.25	Alm Pt 107	2.43
Alm Pt 90	2.26	Alm Pt 108	2.44

**Table M16.Z - Expansion Card #3 (Alarms 109-144)**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Alm Pt 73	2.9	Alm Pt 91	2.27
Alm Pt 74	2.10	Alm Pt 92	2.28
Alm Pt 75	2.11	Alm Pt 93	2.29
Alm Pt 76	2.12	Alm Pt 94	2.30
Alm Pt 77	2.13	Alm Pt 95	2.31
Alm Pt 78	2.14	Alm Pt 96	2.32
Alm Pt 79	2.15	Alm Pt 97	2.33
Alm Pt 80	2.16	Alm Pt 98	2.34
Alm Pt 81	2.17	Alm Pt 99	2.35
Alm Pt 82	2.18	Alm Pt 100	2.36
Alm Pt 83	2.19	Alm Pt 101	2.37
Alm Pt 84	2.20	Alm Pt 102	2.38
Alm Pt 85	2.21	Alm Pt 103	2.39
Alm Pt 86	2.22	Alm Pt 104	2.40
Alm Pt 87	2.23	Alm Pt 105	2.41
Alm Pt 88	2.24	Alm Pt 106	2.42
Alm Pt 89	2.25	Alm Pt 107	2.43
Alm Pt 90	2.26	Alm Pt 108	2.44

**Datalok Housekeeping Mapping**

Housekeeping bits are mapped to Display 3 points 57-64 and are interpreted differently depending on the Datalok type:

**Table M16.AA - Datalok 10A housekeeping Mapping**

<b>Display</b>	<b>Point</b>	<b>Description</b>
3	57	Path Failure Proof Occurred
3	58	Memory Error
3	59	Latched Control Failure
3	60	Power Recovery
3	61	Unprogrammed (needs download)
3	62	Unused
3	63	Station Locked Out
3	64	Reserved

**Table M16.AB - Datalok 10D Housekeeping Mapping**

<b>Display</b>	<b>Point</b>	<b>Description</b>
3	57	Path Failure Proof Occurred
3	58	Memory Error
3	59	Dial Retry
3	60	Power Recovery
3	61	Unprogrammed (needs download)
3	62	Station Security Call In
3	63	Station Locked Out
3	64	Reserved



**Control Point Mapping**

Datalok control points are mapped to Display 4. Refer to Tables M16.AC–M16.AE for point display mapping information.

**Table M16.AC - Base Unit; Controls 1-20**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Ctrl Pt 1	4.1	Ctrl Pt 11	4.11
Ctrl Pt 2	4.2	Ctrl Pt 12	4.12
Ctrl Pt 3	4.3	Ctrl Pt 13	4.13
Ctrl Pt 4	4.4	Ctrl Pt 14	4.14
Ctrl Pt 5	4.5	Ctrl Pt 15	4.15
Ctrl Pt 6	4.6	Ctrl Pt 16	4.16
Ctrl Pt 7	4.7	Ctrl Pt 17	4.17
Ctrl Pt 8	4.8	Ctrl Pt 18	4.18
Ctrl Pt 9	4.9	Ctrl Pt 19	4.19
Ctrl Pt 10	4.10	Ctrl Pt 20	4.20

**Table M16.AD - Expansion Card #1; Controls 21-40**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Ctrl Pt 21	4.21	Ctrl Pt 31	4.31
Ctrl Pt 22	4.22	Ctrl Pt 32	4.32
Ctrl Pt 23	4.23	Ctrl Pt 33	4.33
Ctrl Pt 24	4.24	Ctrl Pt 34	4.34
Ctrl Pt 25	4.25	Ctrl Pt 35	4.35
Ctrl Pt 26	4.26	Ctrl Pt 36	4.36
Ctrl Pt 27	4.27	Ctrl Pt 37	4.37
Ctrl Pt 28	4.28	Ctrl Pt 38	4.38
Ctrl Pt 29	4.29	Ctrl Pt 39	4.39
Ctrl Pt 30	4.30	Ctrl Pt 40	4.40

**Table M16.AE - Expansion Card #2; Controls 41-60**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Ctrl Pt 41	4.41	Ctrl Pt 51	4.51
Ctrl Pt 42	4.42	Ctrl Pt 52	4.52
Ctrl Pt 43	4.43	Ctrl Pt 53	4.53
Ctrl Pt 44	4.44	Ctrl Pt 54	4.54
Ctrl Pt 45	4.45	Ctrl Pt 55	4.55
Ctrl Pt 46	4.46	Ctrl Pt 56	4.56
Ctrl Pt 47	4.47	Ctrl Pt 57	4.57
Ctrl Pt 48	4.48	Ctrl Pt 58	4.58
Ctrl Pt 49	4.49	Ctrl Pt 59	4.59
Ctrl Pt 50	4.50	Ctrl Pt 60	4.60

**Expansion Cards 2 and 3 Analog Point Mapping**

The Datalok Expansion cards' analog alarm points are mapped to Display 6. Refer to Tables M16.AF–M16.AG for point display mapping information.

**Table M16.AF - Expansion Card #2; Analogs 17-24**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Analog #17 Over	6.33	Analog #21 Over	6.41
Analog #17 Under	6.34	Analog #21 Under	6.42
Analog #18 Over	6.35	Analog #22 Over	6.43
Analog #18 Under	6.36	Analog #22 Under	6.44
Analog #19 Over	6.37	Analog #23 Over	6.45
Analog #19 Under	6.38	Analog #23 Under	6.46
Analog #20 Over	6.39	Analog #24 Over	6.47
Analog #20 Under	6.40	Analog #24 Under	6.48

**Table M16.AG - Expansion Card #3; Analogs 25-32**

<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>	<b>Datalok Type/Point</b>	<b>T/MonXM Display.Point</b>
Analog #25 Over	6.49	Analog #29 Over	6.57
Analog #25 Under	6.50	Analog #29 Under	6.58
Analog #26 Over	6.51	Analog #30 Over	6.59
Analog #26 Under	6.52	Analog #30 Under	6.60
Analog #27 Over	6.53	Analog #31 Over	6.61
Analog #27 Under	6.54	Analog #31 Under	6.62
Analog #28 Over	6.55	Analog #32 Over	6.63
Analog #28 Under	6.56	Analog #32 Under	6.64

**Analog Image Alarm Mapping**

T/Mon stores analog data in Displays 7-10. T/Mon uses this space for calculating threshold alarms, and to forward information out to responders. Although the user need not ever access this area, the mapping details are as follows:

**Table M16.AH - Base Unit; Analogs 1-8**

<b>Datalok Type/Point</b>	<b>T/MonXM</b>	
	<b>Display</b>	<b>Point</b>
Analog #1	7	1-8
Analog #2	7	9-16
Analog #3	7	17-24
Analog #4	7	25-32
Analog #5	7	33-40
Analog #6	7	41-48
Analog #7	7	49-56
Analog #8	7	57-64

**Table M16.AI - Extension Card #1; Analogs 9-16**

Datalok Type/Point	T/MonXM	
	Display	Point
Analog #9	8	1-8
Analog #10	8	9-16
Analog #11	8	17-24
Analog #12	8	25-32
Analog #13	8	33-40
Analog #14	8	41-48
Analog #15	8	49-56
Analog #16	8	57-64

**Table M16.AJ - Extension Card #2; Analogs 17-24**

Datalok Type/Point	T/MonXM	
	Display	Point
Analog #17	9	1-8
Analog #18	9	9-16
Analog #19	9	17-24
Analog #20	9	25-32
Analog #21	9	33-40
Analog #22	9	41-48
Analog #23	9	49-56
Analog #24	9	57-64

**Table M16.AK - Extension Card #3; Analogs 25-32**

Datalok Type/Point	T/MonXM	
	Display	Point
Analog #25	10	1-8
Analog #26	10	9-16
Analog #27	10	17-24
Analog #28	10	25-32
Analog #29	10	33-40
Analog #30	10	41-48
Analog #31	10	49-56
Analog #32	10	57-64

**This page intentionally left blank.**

# Software Module 17

## DTMF On-Call

**Note:** This module requires external hardware — either DPS T/Mon DTMF Voice Interface or Black Box DTMF-ASCII Converter™.

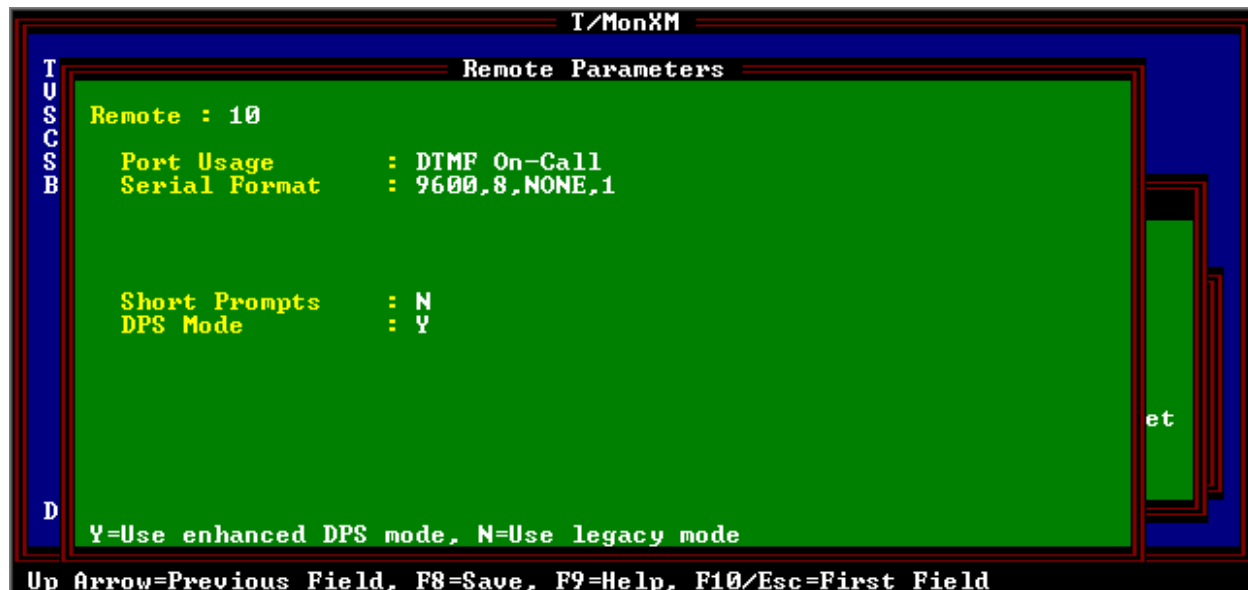
Black Box DTMF-ASCII converter is a trademark of Black Box Corporation.

## Setup

The DTMF On-Call software allows alarms to be acknowledged and tagged from a touch-tone phone (e.g., POT, cellular, PLS).

The DTMF On-Call software module must be installed before you can use the DTMF On-Call functions of T/MonXM. Refer to section 2, Installation for installation procedures.

1. Connect the DB9 cable from the converter's back panel craft port to an available port on your T/Mon NOC.
2. Go to the Master menu > Parameters > Remote Ports option to define the remote parameters.
3. In the port usage field, press the Tab key and select DTMF On-Call from the list box.
4. Set the Baud rate to 9600. Then set the Parity to 8; set the Word length to None; and set the Stop bits to 1 — see Figure M17.1.
5. In the Short Prompts field, select Y (Yes) to select short prompts. Two messages have shorter versions: "Enter your item number followed by pound" will be shortened to "Enter



**Fig. M17.1 - Set the port usage on the Remote ports screen to DTMF ON-Call**

item number” and “Enter your transaction number followed by pound” will be shortened to “Enter transaction number”. Select N (No) to enable standard message formatting.

6. In the DPS Mode field, select Y (Yes) to enable enhanced DPS operation mode. This mode is more responsive than legacy mode and is only supported by the T/Mon DTMF Voice Interface Adapter. Select N (No) for legacy mode. Default setting is N.

**Note:** DPS Mode also features the use of the \* key for quick hang-up. If your transactions are finalized, you may enter the \* key or just hang-up the receiver.

#### Barge-In Feature (Bypass Automated Menu Prompts)

Selecting DPS Mode in the Remote Parameters screen enables support for the Barge-In feature. This feature allows you to skip a recorded menu message by pressing \*. Then enter your item number and the # key.

**Note:** You may press the \* key, and then the # key to hang-up any time after a menu prompt.

## Pager Carrier Response Options

Once you have set the remote parameters, configure your pager carriers for monitoring options. Response options for each pager carrier can be set in the Pager Carriers screen.

1. Go the Master menu > File Maintenance menu > Pager sub-menu > Pager Carriers option.
2. Highlight the pager carrier you want to modify and press F1. The Response Options screen will appear. Assign the response options allowed for each pager carrier — see Figure M17.2.

The screenshot shows the 'Pager Carriers' screen with a list of carriers and a 'Response Options' dialog box overlaid on the list.

Pag	Int	Na	Response Options		ID/Delay
1	AGP	ALP	Name	:WILL TOTTEN	0  4002990 4002991 10 4002562 3223322 10  1689433 1857412 6572348 10 10
2	TWR	TOW	Initials	:WDT	
3	BGP	BET	Ack Single Alarm	: Y	
4	CRS	CLI	by Reply	: Y	
5	TMC	TOM	Ack Site	: Y	
6	KJ	KIM	Tag Single Alarm	: Y	
7	AJK	AL			
8	TRD	TER			
9	MRD	MAC			
10	GGP	GAM			
11	WDT	WIL	Include AckAlarm link (Y/N)		
12	RIS	RAY			
13	AJM	A. J. MACINTYRE	2	448-9632	
14	FRG	FRANK GUILDER	N	448-9632	
15	PEM	PHIL MONTGOMERY	N	448-3872	

F8=Save, F10/Esc=Exit

Fig. M17.2 - Response options are set in the Pager Carrier screen

## Operation - How to Ack/Tag Alarms

Once you have completely installed the converter, operating the converter takes a simple six-step process.

1. You will receive an eight digit “Item Number” with each alphanumeric page. The Item Number is used to identify the pager carrier and the alarm to be acted on. The format of the Item Number in the pager message is “ITEM->XXXX-XXXX”.
2. After you receive a page, you can use a touch-tone phone to call the <PRODUCT>.
3. The converter requests the item number. Enter the item number followed by the pound sign (#).

**Note:** The item number is 8 digits followed by the pound (#) sign. Do not enter any dashes between digits. If you have enabled DPS Mode in T/Mon (see Section 6), you may use the Barge In feature and skip to the next menu level — refer to section 6.1. If you make a mistake, you can press the \* to reset your entry.

4. After a valid item number has been entered, the converter will request a transaction number. The transaction number indicates what you want to do with the alarm.

The following are the valid transaction numbers:

- 1 = ack the alarm
- 2 = tag the alarm
- 19 = ack all alarms for the site. This is based on the site name of the alarm.

5. After entering a valid transaction number, you will hear a transaction response. Valid responses include:
  - “Ack Accepted”
  - “Tag Accepted”
  - “Ack All Accepted”

**Note:** Invalid transactions will prompt a problem message — see section 7.1 (Errors - What Are the Problem Messages?) for message descriptions.

6. Finally, you will be prompted to enter another Item Number. At this point, you may enter another item or press the \* key, and then the # key to hang-up.

**Note:** You may press the \* key, and then the # key to hang-up any time after a menu prompt.

## Problem Message Numbers

If errors occur during data entry, they are reported to the user by the word “problem” followed by a number. Refer to Table M17.A for descriptions.

**Tbl. M17.A - Problem Message descriptions and numbers**

Problem	Description	Problem Number
Timeout	Too much time (20 seconds) has passed without any data being entered. Note: In DPS Mode this time is extended to 30 seconds.	1
Unexpected Keys	Touch-tone keys have been pressed	2
Line Noise	Line noise is causing data to be garbled	3
Invalid Trans	An invalid transaction number has been entered	4
Unallowed Trans	A transaction number has been entered that is not allowed for the user	5
Too Many Digits	More than the expected number of digits has been entered by the user	6
Too Many Errors	More than 3 consecutive errors have been made by the user	7



# Software Module 18

## 21SV Interrogator



Fig. M18.1 - Remote Port defined for 21SV Interrogator

The 21SV Interrogator software module supports polling the NEC 21SV remote telemetry unit. This software module fully supports all the functions of the 21SV, plus it offers two advantages over using the 21SV's original NEC-made master: with this software module, T/MonXM can poll the 21SV directly, bypassing the need for a hard master; and you can use all of T/MonXM's advanced alarm notification and processing functions with the 21SV.

If you ordered the 21SV Interrogator with a new T/MonXM system, it will be factory-installed. If you are installing the 21SV Interrogator on an existing system, follow the instructions for installing new modules in Section 2, Software Installation.

Configuration of the 21SV Interrogator consists of three steps:

1. Defining a remote port.
2. Defining 21SV remote devices.
3. Defining alarm points.

### Defining the Remote Port

1. From the Master menu, select Parameters > Remote Ports.
2. Using the F)ind, P)revious, or N)ext commands, navigate to an unused remote port.
3. Press E (Edit) to edit the port parameters.
4. Press Tab to select the list box and choose "21SV Interrogator" from the list of available port usages.
5. Enter appropriate values in the other fields in the Remote

## 21SV Interrogator Setup

Parameters screen. See Figure M18.1 on section M18-2 for a picture of the Remote Parameters screen and Table M18.A for an explanation of the fields.

**Table M18.A - Fields in the 21SV Interrogator Remote Parameters screen**

Field	Description
Port Usage	21SV Interrogator
Serial Format	Baud rate, word length, parity, and stop bits settings. Normally 1200, 7, O, 1. <b>Note:</b> Be sure these settings match those of the 21SV remotes.
RTS Lead/Tail	RTS on and off time (0-2500 msec)
Time Out	Time out in milliseconds (200-9999)
Poll Delay	Time between polls in milliseconds (0-9999).
Protocol	Select between A series and B series remotes. A Series: 32 discrete alarms and 6 controls per remote. Expandable to 544 discrete alarms and 128 controls B Series: 32 discrete alarms, 6 controls, and 4 TBOS ports
Fail Threshold	Number of bad polls before a device failure is declared (3-20).
Fail Poll Cycles	Polling loop cycles before failed devices are polled (0-255).
Check DCD on Rcv	Y = Enable DCD checking to validate Rcv. N = Disable.
Immediate Retries	Number of retries before proceeding with next address..

```

Remote Device Definition

Port      : 3      21SV Interrogator
Address   : 1

Description : NEC 21SV Device
Site Name  : NEC 21SV Remote

Displays   : 1-36
Refresh Rate : 411

Log Undefined: N
-----
Polarity    : B      Address Defaults -----
Logging     : L      Windows      :
History     : H      Message      : 0
Level       : A
Status      : A
Reverse     : N
Description  : (Undefined)

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit : _

F1=Ports, F3=Int Alarms, AF1=TL1, AF6=Templates, F10/Esc=Exit

```

**Fig. M18.2 - Remote Device Definition screen for 21SV Interrogator**

### Defining 21SV Remote Devices

1. Press F1 to open the Remote Device Definition screen.
2. Enter appropriate information in the fields. See Figure M18.2 for a picture of the Remote Device Definition screen and Table M18.B for an explanation of the fields.
3. Define a different address for each 21SV site.

**Table M18.B - Fields in the 21SV Interrogator Remote Device Definition screen**

Field	Description
Port	This port number.
Address	Address of this 21SV remote site. (Matches the RTU.)
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Displays	Number of displays to be reserved for collection. The default setting is 1–36, which should never be changed.
Refresh Rate	Number of poll cycles before a refresh cycle occurs.
Log Undefined	Select Yes to log undefined alarms.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear.
Message	ID number of text message associated with alarms from this site.

### Define Alarm Points

1. From the Remote Device Definition screen, press F1 to open the Point Definition screen.
2. Define fail and clear points for your NEC Devices.

### Point Mapping

When defining 21SV remote devices, note the following relationships between T/MonXM displays and the alarm and control points of the 21SV remote.

Refer to Section 10 (Point Definition Tutorial) for more information on defining points.

**Table M18.C- NEC display points in T/MonXM**

NEC Device	NEC Type	T/Mon Display	T/Mon Points
21SV/RA	32 DI	1	Points 1-33
21SV/EXP 1	64 DI	1	Points 33-64
21SV/EXP 1	64 DI	2	Points 1-33
21SV/EXP 2	64 DI	2	Points 33-64
21SV/EXP 2	64 DI	3	Points 1-33
21SV/EXP 3	64 DI	3	Points 33-64
21SV/EXP 3	64 DI	4	Points 1-33
21SV/EXP 4	64 DI	4	Points 33-64
21SV/EXP 4	64 DI	5	Points 1-33
21SV/EXP 5	64 DI	5	Points 33-64
21SV/EXP 5	64 DI	6	Points 1-33
21SV/EXP 6	64 DI	6	Points 33-64
21SV/EXP 6	64 DI	7	Points 1-33
21SV/EXP 7	64 DI	7	Points 33-64
21SV/EXP 7	64 DI	8	Points 1-33
21SV/EXP 8	64 DI	8	Points 33-64
21SV/EXP 8	64 DI	9	Points 33-64
21SV/EXP 9	32 AI	9	Points 33-64
21SV/EXP 10	32 AI	10	Points 33-64
21SV/EXP 11	32 AI	11	Points 33-64
21SV/EXP 12	32 DO	12	Points 33-64
21SV/EXP 13	32 DO	13	Points 33-64
21SV/EXP 14	32 DO	14	Points 33-64
21SV/EXP 15	32 DO	15	Points 33-64
		16	Unused
21SV/RA	System Alarms	17	Points 1-64

### Provision the NEC 21SV Device

**Note:** T/Mon can remotely provision the NEC Devices as they would be the front panel.

1. From the Remote Device Definition screen, press F2 to open the 21SV Provision menu.
2. Use your arrow keys to highlight and press Enter to select the NEC device you wish to provision.

### Step 5 - General provision.

From the 21SV Provision menu, highlight the General option, and press Enter. See figure M18.3 screen capture and Table M18.D for field descriptions.

**Note:** General provision is only available for the 21SV/RA. If you have any 21SV expansion units you only need to provision control and monitor points, see the following pages. There can be one base unit (21SV/RA) and 14 expansion units (21SV/EXP) under one address. The 21SV/EXP (32AI) is not currently supported.

```

Remote Device Definition
Port      : 3      21SV Interrogator
21SV/RA Provisioning - General

Port: 3   Address: 1   Site Name:

Alarm Qualifier A      : 100..
Alarm Qualifier B      : 500
Alarm Qualifier C      : 1000
Alarm Qualifier D      : 1600
Mom Control Pulse Duration A : 100
Mom Control Pulse Duration B : 500
Mom Control Pulse Duration C : 1000
Mom Control Pulse Duration D : 1600
21SV/EXP (64DI)        : 0
21SV/EXP (32DO)        : 0

Alarm qualification time A (100-25500 msec in 100 msec increments)

F8=Save, F9=Help, F10/Esc=Exit
  
```

Fig. M18.3 - Default settings in the General provision screen for 21SV Interrogator.

Table M18.D - Fields in the 21SV Interrogator Remote Access General provision screen

Field	Description
Alarm Qualifier A thru D	The amount of time an alarm point must be set or cleared before it will change state (100–25500 milliseconds). Each alarm point will be assigned a qualifier A thru D.
Mom Control Pulse Duration A thru D	The amount of time a relay will stay latched during a momentary pulse control (100–25500 milliseconds). Each control point will be assigned a pulse A thru D.
21SV/EXP (64DI)	Number of 21SV/EXP 64 point discrete input expansion units daisy chained to the 21SV/RA (0 to 8).
21SV/EXP (32DO)	Number of 21SV/EXP 32 point discrete output expansion units daisy chained to the 21SV/RA (0 to 4).

**Table M18.E - Key commands available in the General Provision screen**

Function Key	Description
F8	Saves the remote configuration database.
F9	Displays help screen.
F10/Esc	Leaves the remote configuration database screen without saving any changes that may have been made.

Remote Device Definition			
Port : 3 21SV Interrogator			
21SV/RA Provisioning - Monitor Points			
Port: 3 Address: 1 Site Name:			
Point	Level	Polarity	Qualification
1	MAJOR	NORMAL	A <100 msecs>
2	MAJOR	NORMAL	A <100 msecs>
3	MAJOR	NORMAL	A <100 msecs>
4	MAJOR	NORMAL	A <100 msecs>
5	MAJOR	NORMAL	A <100 msecs>
6	MAJOR	NORMAL	A <100 msecs>
7	MAJOR	NORMAL	A <100 msecs>
8	MAJOR	NORMAL	A <100 msecs>
9	MAJOR	NORMAL	A <100 msecs>
10	MAJOR	NORMAL	A <100 msecs>
Monitor point level			
Tab=Defaults, F8=Save, F9=Help, F10/Esc=Exit			

**Fig. M18.4 - Default settings in the Monitor Points provision screen for 21SV Interrogator.****Monitor Points Provision**

From the 21SV Provision menu, highlight the Monitor Points option, and press Enter. See Figure M18.4 for screen capture and Table M18.F for field descriptions.

**Table M18.F - Fields in the 21SV Interrogator Remote Access Monitor Points provision screen**

Field	Description
Point	ID number of the monitor point (1–32). <b>Note:</b> This field is not editable.
Level	Select MAJOR, MINOR, or STATUS to set the severity level.
Qualification	Select alarm qualification time for this monitor point.

### Provision Control Points

1. From the 21SV Provision menu, highlight the Control Points option, and press Enter. See figure M18.5 for screen capture and Table 16.G for field descriptions.
2. Use the Tab key edit choices.

```

Remote Device Definition
Port      : 3      21SV Interrogator
21SV/RA Provisioning - Control Points

Port:    3      Address: 1      Site Name:

Point    Type    Polarity    Duration
33       LATCH   NORMAL      A <100 msec>
34       LATCH   NORMAL      A <100 msec>
35       LATCH   NORMAL      A <100 msec>
36       LATCH   NORMAL      A <100 msec>
37       LATCH   NORMAL      A <100 msec>
38       LATCH   NORMAL      A <100 msec>

Control point mode

Tab=Defaults. F8=Save. F9=Help. F10/Esc=Exit
[DPS]

```

Fig. M18.5 - Default settings in the Control Points provision screen for 21SV Interrogator.

Table M18.G - Fields in the 21SV Interrogator Remote Access Control Points provision screen

Field	Description
Point	ID number of the control point (33-38). <b>Note:</b> This field is not editable.
Type	Select LATCH or PULSE to set the control type.
Polarity	Select NORMAL or REVERSE polarity.
Duration	Select pulse duration for this control point. <b>Note:</b> This field is only editable if the Type is set to PULSE.

Table M18.H - Key commands available in the Control Points screen

Function Key	Description
F8	Saves the remote configuration database.
F9	Displays help screen.
F10/Esc	Leaves the remote configuration database screen without saving any changes that may have been made.

**Define Controls for the 21SV/RA or 21SV/EXP 32 DO**

1. To define controls you must exit the NEC 21SV provision screen and go to the Master Menu > File Maintenance Menu > Windows Definition screen.
2. Use the Up/Down Arrow keys to select the line of the window you would like to issue the controls from and press F4. The Site Controls Category Definition screen will appear.
3. Enter a name and press Tab.
4. Enter a description for your controls and press Enter. The Site Control Points screen will appear.
5. Use Table M18.I to define your control points.

**Note:** For more information on site controls refer to Section 12 or press F9 for help online.

**Table M18.I - 21SC control points display in T/MonXM**

NEC Device	NEC Type	Controls	T/Mon Display	T/Mon Points
21SV/RA	6 DO	1-6	17	Points 1-6
21SV/EXP 12	32 DO	1-32	12	Points 33-64
21SV/EXP 13	32 DO	1-32	13	Points 33-64
21SV/EXP 14	32 DO	1-32	14	Points 33-64
21SV/EXP 15	32 DO	1-32	15	Points 33-64



# Software Module 19

## Modbus Interrogator

The Modbus Interrogator software module enables T/MonXM to monitor any Modbus device. You will need to install the Modbus Interrogator software module into your T/Mon unit, see Part One. The Modbus Interrogator software module fully supports the following features: discrete inputs, analog inputs and control relays. All Modbus protocols are supported. (ASCII, RTU, and TCP)

### Part One

#### Install or Upgrade the Software

Under normal circumstances installation will only need to be done for software updates or newly ordered modules. The original disks have been supplied with the T/Mon for archival or emergency recovery procedures. See Section 2 of the T/MonXM user manual for further instructions on upgrading or installing software.

### Part Two

#### Configure the Modbus Interrogator

The Modbus Interrogator is configured in eight steps. The initial three steps differ slightly between LAN-based and Dialup remotes.

1. Define a remote port for the Modbus Interrogator.
2. Create a data connection for polling remotes over the LAN.(For virtual port users only)
  - If configuring a Modbus dialup remote, you will define your Modbus remote's site See Alternate Step 2: Dialup Configuration
3. Define Modbus remote device.
4. Define alarm points.
5. Define internal alarms.(optional)
6. Define Modbus Addressing.
7. Define T/MonXM analog thresholds for analog inputs. (optional)
8. Import/Export Modbus templates.(optional)

#### Step One

##### Define the Remote Port

1. From the Master menu, select Parameters > Remote Ports.
2. Using the F)ind, P)revious, or N)ext commands, navigate to the remote port number for the port that is connected to the Modbus remote.
3. Choose E)dit.
4. Press Tab to select the list box and choose "Modbus Interrogator" from the list of available port usage, or, if using a Modbus dialup remote, choose Modbus Int Dialup.
5. Enter appropriate values in the other fields in the Remote Parameters screen. See Figure M19.1 for an example of the Remote Parameters screen and Table M19.A for an explanation of the fields. If configuring for dialup, see figure M19.2 for an example of the Remote Parameters screen and Table M19.B for an explanation of the fields.

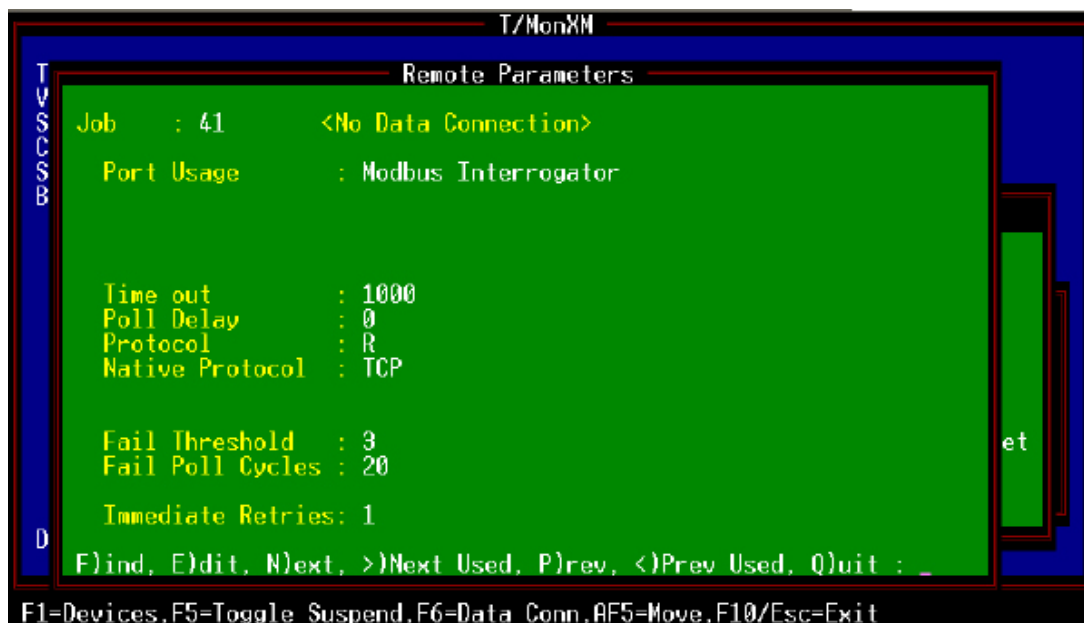
**Step Two Create a Data Connection (Virtual Port Jobs)**

**Note:** This step is only for users who already have a Ethernet TCP port defined. If configuring a modbus dialup remote, skip to the Alternate Step 2: Dialup Configuration section, starting on the following page.

1. From the Remote Ports screen press F6 to open the Data Connection screen.
2. Press F1 to open the Ethernet TCP Ports Definition screen.
3. Press Tab to select Telnet-Raw as the port type.
4. Enter your TCP port number, a description, and an IP number.

**Note:** The port and IP can be anything for the moment—they will be defined in a later screen.

5. Press F8 to save your changes and return to the Data Connection Assignment screen.
6. From the Data Connection Assignment screen, press Tab to select the List Box. Select the Telnet-Raw port you just defined for the data connection. Then return to the Remote Parameters screen.



**Fig. M19.1 - Remote Port defined for Modbus Interrogator.**

**Table M19.A - Fields in the Modbus Interrogator Remote Parameters screen**

Field	Description
Port Usage	Modbus Interrogator.
Time Out	Time out in milliseconds (200-9999).
Protocol	Protocol Mode <R =RTU Mode or A=ASCII Mode>Note: If using a virtual port then RTU mode is default and cannot be edited. Selecting a virtual port will automatically activate TCP.
Poll Delay	Time between polls in milliseconds (0-9999).
Fail Threshold	Number of polls before device failure is declared (3-20)
Immediate Retries	Number of retries before proceeding with next address..
Native protocol	Top or dedicated. Only applies to a virtual port. If dedicated selected, it will send modbus protocol RTU or ASCII as it would over serial. TCP will enable TCP mode. Use dedicated if going over LAN proxy to a serial device.



Fig. M19.2 - Remote Port defined for Modbus Dialup Interrogator.

Field	Description
Port Usage	Modbus Int Dialup
Serial Format	The settings for your Modbus remote's modem
RTS Lead / Tail	RTS lead and tail time in 10 millisecond increments. Use defaults unless otherwise specified.
Description	Input a description for the remote job
Time Out	Time out in milliseconds (200-9999).
Protocol	Protocol Mode <R =RTU Mode or A=ASCII Mode>Note: If using a virtual port then RTU mode is default and cannot be edited. Selecting a virtual port will automatically activate TCP.
Modem Setup Str	Any specific modem settings for your phone system.
Native protocol	Top or dedicated. Only applies to a virtual port. If dedicated selected, it will send modbus protocol RTU or ASCII as it would over serial. TCP will enable TCP mode. Use dedicated if going over LAN proxy to a serial device.

**Alternate Step 2: Configure your Modbus Site**  
**Dialup Configuration:** **Note:** These steps are for users configuring the Modbus Interrogator for dialup remotes. If not polling your remote via dialup, skip this step.

1. Return to the Master Menu.
2. Select **Files> Dial Up Networks>Modbus Dial Sites**
3. Enter information in the appropriate fields to configure your site (see table M19.C for field descriptions).

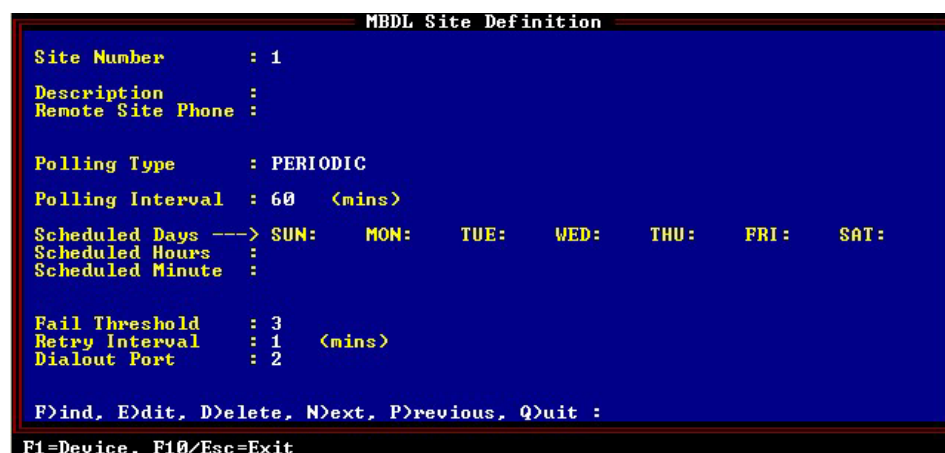


Figure M19.3 - The Modbus Site Definition Screen

**Table M19.C - Fields in the Modbus Dial-Up Site Definition screen**

<b>Fields</b>	<b>Description</b>
Site Name	The name for the site. Up to 10 characters.
Description	The description for the site. Optional. Up to 40 characters.
Remote Site Phone	The phone number that T/MonXM will use to dial the site. Up to 30 digits. Remember to enter 9, or other character to get an outside line if necessary.
Polling Type	Periodic or Schedule. Press Tab for a selection window. Press Tab again to toggle the selection highlight. Press Enter to choose. <ul style="list-style-type: none"> <li>Periodic will call ASCII Device every 60 minutes, or specified time period, all day, every day.</li> <li>Schedule will call the ASCII Device only at the times and on the days specified in the Scheduled Days, Scheduled Hours and Scheduled Minute fields that follow.</li> </ul>
Polling Interval	Amount of time, in minutes between calls to the ASCII Site. 0-9999 minutes. 0=Never. (Applies to periodic only)
Scheduled Days	Select Y (do call) or N (don't call) for each day of the week. (Applies to scheduled only)
Scheduled Hours	Select range of hours on the scheduled days to call the ASCII Device. Use 0 to 23. Enter a set (such as 5-8) or individual hours (such as 7, 9, 13, 18, 21). <b>Note:</b> Applies to scheduled only.
Scheduled Minute	Enter the time offset from the hour. <b>Note:</b> Applies to scheduled only.
Dialout Port	Remote port where outgoing calls are made. 0=None (incoming only)

**Step Three Define Modbus Remote Device**

1. From the Remote Ports screen (or the Dialup Site Definition screen if configuring a dialup remote) press F1 to open the Remote Device Definition screen.

If Configuring a dialup remote, you will have to enter an address for the remote

2. Enter appropriate information in the fields. For LAN-based remotes, see Figure M19.4 for a screen capture of the Remote Device Definition screen, and see Table M19.D for an explanation of the fields. For dialup remotes, see figure M19.5 and table M19.E
3. Define a different address for each Modbus site.

```

Remote Device Definition
Port / Job      : 41      Modbus Interrogator
Device ID      : 41      0.0.0.0..... / 0

Description    :
Site Name     :
Device Type    : Testset
Displays      : 1-80
Poll Type     :
Refresh Rate  : 340
Firmware Ver  :
Log Undefined  : N

----- Address Defaults -----
Polarity      : B      Windows      :
Logging       : L      Message      : 0
History       : H
Level         : A
Status        : A
Reverse       : N
Description    : <Undefined>

RTU IP Address <i.e. 192.168.63.14>

F10/Esc=Exit

```

Fig. M19.4 - Remote Device Definition screen for Modbus Interrogator

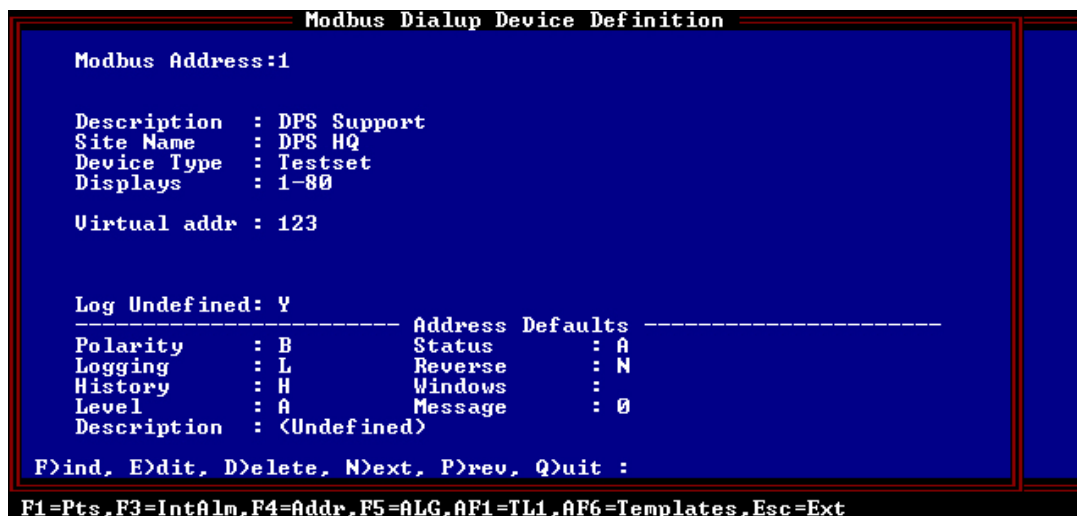
Table M19.D - Fields in the Modbus Interrogator Remote Device Definition screen

Field	Description
Port/Job	This port number.
Device ID	Enter Device ID (1-247)
RTU IP Address	Address of this Modbus RTU site (Matches the RTU).
TCP Port	Should match RTU (1-65535)
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode.
Device Type	Testset is default. You may select JACE 5XX for Jace 500 series remotes. For all other devices use Testset.
Displays	Number of displays to be reserved for collection.
Poll Type	Leave blank
Refresh Rate	Number of poll cycles before a refresh cycle occurs.
Firmware Ver	Firmware version (optional)
Log Undefined	Select Yes to log undefined alarms.

**Note:** Table M19.B continues on following section.

**Table M19.D(continued) - Fields in the Modbus Interrogator Remote Device Definition screen**

Field	Description
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear.
Message	ID number of text message associated with alarms from this site.

**Table M19.5(continued) - Fields in the Modbus Interrogator Remote Device Definition screen****Table M19.E - Fields in the Modbus Dialup Device Definition screen**

Field	Description
Modbus Address	Enter the unit's Device ID
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode.
Device Type	Testset is default. You may select JACE 5XX for Jace 500 series remotes. For all other devices use Testset.
Displays	Number of displays to be reserved for collection.
Virtual addr	A three digit number T/Mon will use to sort dialup devices. T/Mon will notify you if you choose a number already in use.
Log Undefined	Select Yes to log undefined alarms.
Polarity	Bipolar(B) or Uni-polar(U), [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]

**Table M19.E (Continued) - Fields in the Modbus Dialup Device Definition screen**

Field	Description
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear.
Message	ID number of text message associated with alarms from this site.

**Step Four Define Alarm Points**

From the Remote Device Screen press F1 to go to the Point Definition screen where you can define your alarm points (See Figure M19.6). Table M19.F explains the fields in this screen.

**Note:** You will find that the analog points have been databased automatically on displays 65–80. You must manually database discrete alarm points on displays 1–64.

Press E)dit and edit your alarm point definitions. See Table M19.G for more Point Edit help.

Figure M19.4 shows the extended definitions for each point. For an explanation of each field see Table M19.G.

**Point Definition**

Job : 41 DoID: 1 Disp: 65 Display Desc :

Pt	l	g	t	u	s	s	Description	Modbus Interrogator	Fail	Clear
1	B	L	H	C	A	N	Analog - Channel 1	Minor Under		
2	B	L	H	C	A	N	Analog - Channel 1	Minor Over		
3	B	L	H	B	A	N	Analog - Channel 1	Major Under		
4	B	L	H	B	A	N	Analog - Channel 1	Major Over		
5	B	N	N	D	A	N	Analog Data - Channel 1			
6	B	N	N	D	A	N	Analog Data - Channel 1			
7	B	N	N	D	A	N	Analog Data - Channel 1			
8	B	N	N	D	A	N	Analog Data - Channel 1			

F>ind, E>dit, D>elete, N>ext, P>rev, Q>uit : \_

**Message**

F10/Esc=Exit

**Fig. M19.6 - Press F1 to define your alarm points.**

**Point Definition**

Job : 41 DuID: 1 Disp: 65 Display Desc :

Pt	Log	Th	St	Rev	Windows	Msg	Qual	Counter	Pager
1	B	L	H	C	A	N	0	0	0
2	B	L	H	C	A	N	0	0	0
3	B	L	H	B	A	N	0	0	0
4	B	L	H	B	A	N	0	0	0
5	B	N	N	D	A	N	0	0	0
6	B	N	N	D	A	N	0	0	0
7	B	N	N	D	A	N	0	0	0
8	B	N	N	D	A	N	0	0	0

Enter windows. <2-720; 8 max>

**Message**

Ilb Arrow=Previous Field. F10/Esc=First Field

Fig. M19.7 - Extended definitions for alarm points.

Table M19.F - Fields in the Definition Points screen

Field	Description
Point	This port number.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Enter a description that best describes the alarm point. This field is initially "Undefined."
Fail	Enter Fail Status description. If left blank then the setting from the alarm formatting screen will be used.
Clear	Enter Clear Status description. If left blank then the setting from the alarm formatting screen will be used.
Windows	Window in Monitor Mode in which alarms from this site will appear.
Message	ID number of text message associated with alarms from this site.
Qualification	Enter the duration alarm qualification time setting followed by a letter indicating the time units being used. The maximum numeric value is 99. Valid units are M for minutes, H for hours, and Q for quarter hours. <b>Example:</b> "10M" means 10 minutes

**Note:** Table M19.C continues on following page.



**Table M19.F (continued) - Fields in the Definition Points screen**

Field	Description
Counter Qualification	Enter counter alarm qualification setting. In counter qualification, the alarm qualifies when a specified number of occurrences of the alarm occur in specified amount of time. For no counter qualification enter a 0. Otherwise enter the qualification time followed by a letter indicating the time units being used. Follow this with a slash and the number of occurrences that will cause the alarm to qualify. The maximum value for the period length is 99. Valid time units are M = minutes, H = hours, and Q = quarter hours. The maximum value for occurrences is 250. <b>Example:</b> 30M/10 MEANS 10 occurrences in 30 minutes.
Pager	Pager Profile Number (1-99) 0 = none

**Note:** Duration qualification and counter qualification can both be enabled for a particular point. When both types of qualification are active, the alarm will qualify when either of the qualification conditions become true. The alarm will clear when BOTH qualification conditions become false.

**Table M19.G - Fields in the Base Unit Provision — Points screen**

Key	Command	Description
F1	GOTO	Go directly to a point.
F3	Blank	Blanks out a point definition.
F4	Attribute Section	Displays next section of attributes.
F5	Range Functions	Access commands that operate a range of points (e.g. translations, copies).
F6	Read	Reads point definitions from another display or address.
F8	Save	Save point definitions and return to polling list.
F10/Esc	Exit	Leaves the database screen without saving any changes that have been made.
Alt-F3	Delete Point	Deletes point under cursor and all below to move down one positions. And undefined point is then inserted at the cursor.
Alt-F4	Insert Point	Inserts an undefined point above cursor.
Alt-F5	Block Move	Moves a block of points within a display.
Alt-F6	Block Copy	Copies a block of points within a display.
Ctrl-F6	Extended Read	Reads in a portion of another display to a starting point in the current display.

**Note:** Vertical editing is available in the point editing section via the CTRL-PGUP and CTRL-PGDN keys. (Press Ctrl-H for more help on this).

**Step Five Define Internal Alarms (Optional)**

User Defined Internal Alarms originate from remote port device failures or derived alarms. These alarms must be assigned in Remote Ports - Device Definition or in Derived Alarms. For information on Internal Alarms refer to Section 14.

**Step Six Define Modbus Addressing**

From the Remote Device Definition screen press F4 to define your Modbus addresses. See Table M19.H for field descriptions. If the remote device has discrete inputs, analog inputs, or control relays then the T/Mon or IAM must be databased to know the addressing of the Modbus remote. Refer to the documentation on your Modbus remote as to how it is addressed.

For more information on the Modbus addressing model see the latest version of the “Modbus Application Protocol specification” available at <http://www.modbus.org>.

The following information in Sections i, ii, and iii are aspects on Modbus addressing taken from the MODBUS Application Protocol Specification V1.1 user manual (available at <http://www.modbus.org>).

- i. MODBUS bases its data model on a series of tables that have distinguishing characteristics. The four primary tables are:

**Table M19.H - Modbus data model.**

Primary tables	Object type	Access type	Description
Discrete Input	Single bit	Read-Only	Type of data can be provided by an I/O system.
Coils	Single bit	Read-Only	Type of data can be alterable by an application program.
Input registers	16-bit word	Read-Only	Type of data can be proved by an I/O system.
Holding registers	16-bit word	Read-Write	Type of data can be alterable by an application program.

The distinctions between inputs and outputs, and between bit-addressable and word-addressable data items, do not imply any application behavior. It is perfectly acceptable, and very common, to regard all four tables as overlaying one another, if this is the most natural interpretation on the target machine in question.

For each of the primary tables, the protocol allows individual selection of 65536 data items, and the operations of read or write of those items are designed to span multiple consecutive data items up to a data size limit which is dependent on the transaction function code.

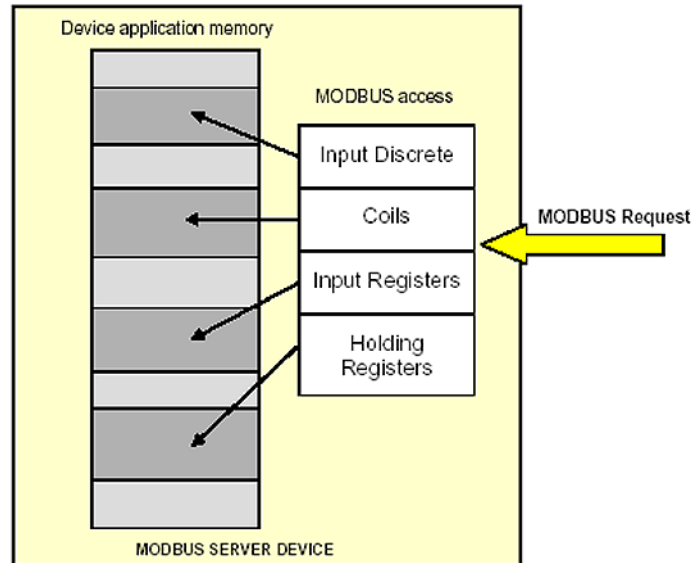
It's obvious that all the data handled via MODBUS (bits, registers) must be located in device application memory. But physical address in memory should not be confused with data reference. The only requirement is to link data reference with physical address.

MODBUS logical reference number, which are used in MODBUS functions, are unsigned integer indices starting at zero.

- ii. The examples below show two ways of organizing the data in device. There are different organizations possible, all are not described in this document. Each device can have its own organization of the data according to its application

**Example 1 :** Device having 4 separate blocks

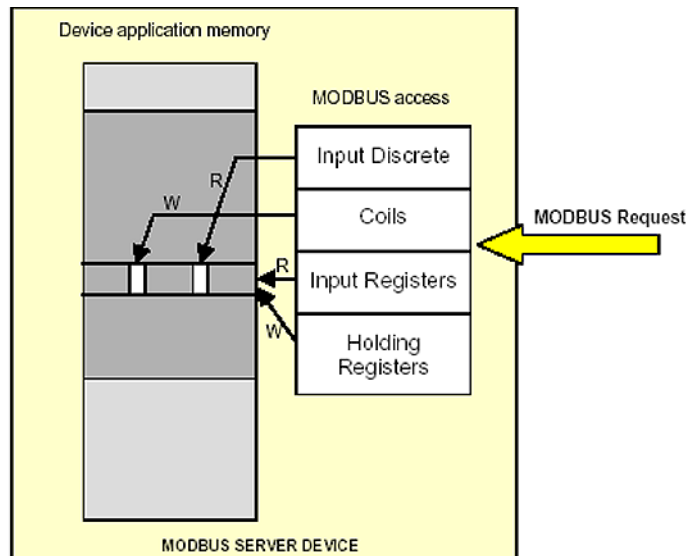
The example below shows data organization in a device having digital and analog, inputs and outputs. Each block is separate from each other, because data from different block have no correlation. Each block is thus accessible with different MODBUS functions.



**Fig. M19.8 - Modbus Data Model with separate block.**

**Example 2:** Device having only 1 block

In this example, the device have only 1 data block. A same data can be reached via several MODBUS functions, either via a 16 bits access or via an access bit.



**Fig. M19.9 - Modbus Data Model with only 1 block.**

### iii. Modbus Addressing Model.

The Modbus application protocol defines precisely PDU addressing rules.

**In a Modbus PDU each data is addressed from 0 to 65535.**

It also defines clearly a Modbus data model composed of 4 blocks that comprises several elements numbered from 1 to n.

**In the Modbus data Model each element within a data block is numbered from 1 to n.**

Afterwards the Modbus data model has to be bound to the device application ( IEC 1131 object, or other application model).

**The mapping between the Modbus data model and the device application is totally device specific.**

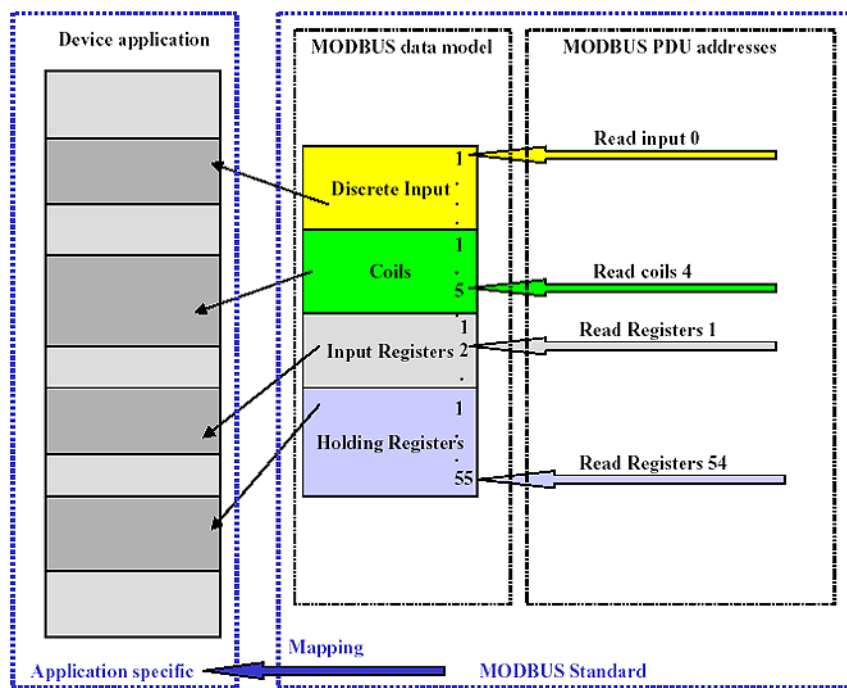


Fig. M19.10 - Modbus addressing model.

```

Remote Device Definition
Port / Job      : 41      Modbus Interrogator
Device ID      : 1      192.163.63.14 / 1

Description    : Test
Site Name     : DPS Documentation
Device Type    : Testset

Modbus Addressing

DISCRETE Data Type: 2 <Input Discretes>
DISCRETE Address  : 0
DISCRETE Total    : 64
ANALOG Data Type  : 4 <Input Registers>   Reg Type: 0 <Integer>
ANALOG Address    : 0
ANALOG Total      : 16
CONTROL Data Type : 5 <Coils>
CONTROL Address   : 0
CONTROL Total     : 8

Discrete points data type <1-4>

Tab=Defaults, F8=Save, F9=Help, F10/Esc=Exit

```

Fig. M19.11 - Modbus device with 64 discrete alarm of data type Input Discrete, 16 analog inputs of data type Input Register, and 8 control relays of data type coil

Table M19.1 - Fields in the Remote Device Definition > Modbus Addressing screen.

Field	Description
DISCRETE Data Type	Modbus data type for discrete alarm points. <b>Coils:</b> 1-bit (Read/Write Access) <b>Input Discretes:</b> 1-bit (Read Access) <b>Holding Registers:</b> 16-bits (Read/Write Access) <b>Input Registers:</b> 16-bits (Read Access)
DISCRETE Address	The starting address for discrete alarm points. All data of the above type will be retrieved starting from this address. Each of the four Modbus data types have an address block from 0–65535 which may overlap the address block of another data type.
DISCRETE Total	The number of discrete alarm points to monitor. Setting this value to 0 will disable the monitoring of this type of alarm point.
ANALOG Data Type	Modbus data type for analog alarm points. See “DISCRETE Data Type” field for data types.
Reg Type	Analog register data type. Determines the valid range of values for the register. This field only applies to Holding Registers and Input Registers. <b>Integer:</b> 16-bit integer, data range — 32,768 to 32,767 <b>Float:</b> 32-bit single precision. Byte order scheme is 1-0-3-2Float <b>Invert:</b> 32-bit single precision. Byte order scheme is 3-2-1-0
ANALOG Address	The starting address for analog alarm points. See “DISCRETE Address” for more information.
ANALOG Total	The starting number of analog alarm points to monitor. See “DISCRETE Total” for more information.
CONTROL Data Type	Modbus data type for control points. See “DISCRETE Data Type” for more information.
CONTROL Address	The starting address for control points. See “DISCRETE Address for more information.
CONTROL Total	The number of analog alarm points to monitor. See “Discrete Total” for more information.

**Analog Provisioning**

Port: 41 Address: 1  
Threshold Mode : RTU (Native Unit Thresholds)

Alg Description	Sig	Unt	MjOvr	MnOvr	MnUdr	MjUdr
1 .....						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						

**Fig. M19.12 - Analog Provision screen.****Step Seven Define Analog Points (Optional)**

1. From the Remote Device Definition screen, press F5 to open the Analog Provision screen, see Section M1-9 for more information..
2. Fill in the Description, Sig, and Unt fields.
3. You may also define analog threshold values, if needed, but you will have to complete the Analog Display Worksheet, which is accessed by pressing F1 in the Analog Provision screen. See Section M1-11 for more information.

**Table M19.J - Fields in the Analog Provision screen**

Field	Description
Port, Address, Site Name	Non-editable fields identifying this Modbus device.
Threshold Mode	Always uses T/MON thresholds.
Point	ID of alarm point (1–16).
Description	Optional description of this alarm point. Note: If analog alarms from this remote will be forwarded as SNMP traps, typing a colon (:) at the beginning of the description will include the analog threshold crossed in the trap.
Sig	Number of digits to display after the decimal point.
Unt	Type of analog unit.
<b>Note:</b> You must complete the Analog Display Worksheet before completing the next four fields. Press F1 to open the Analog Display Worksheet, and follow the instructions given below under “Analog Display Worksheet.”	
MjOvr	Major Over threshold. Enter the threshold value in native units.
MnOvr	Minor Over threshold. Enter the threshold value in native units.
MnUdr	Minor Under threshold. Enter the threshold value in native units.
MjUdr	Major Under threshold. Enter the threshold value in native units.
<b>Note:</b> When these fields are selected, the available range and the value of the input voltage or current will be shown at the bottom of the screen.	

**Step Eight Import/Export Modbus Templates**

You can create device templates or import existing templates into a device, which can greatly speed the provision of your remote devices. Templates provide the ability to save device configurations and import that information into similar device profiles (available for dial-up and LAN devices).

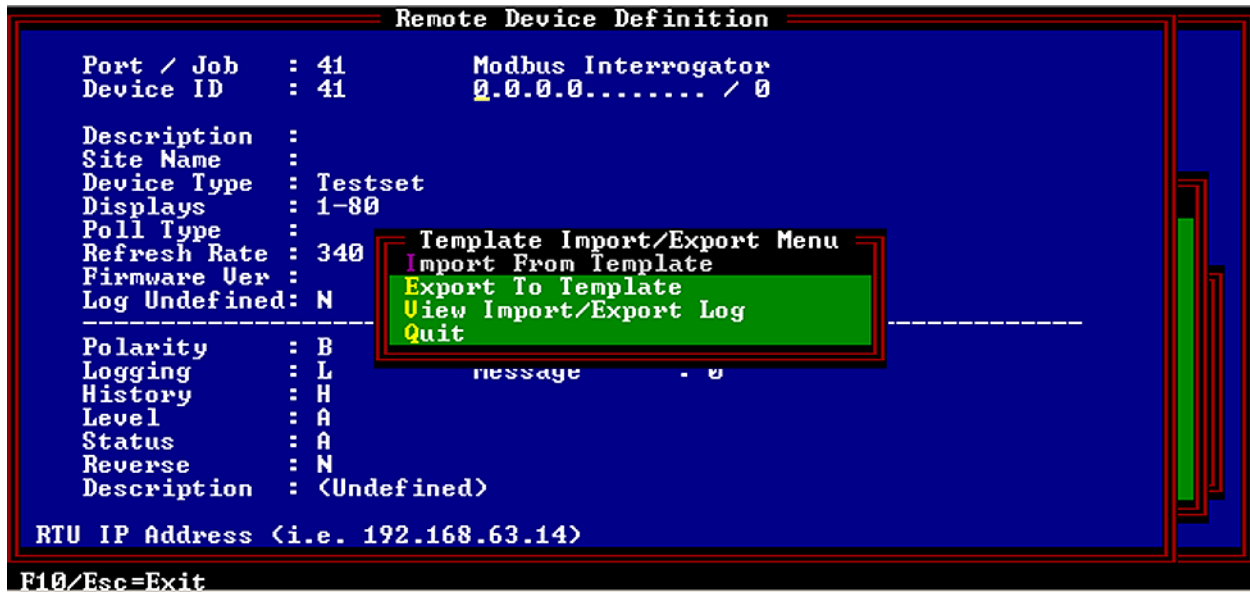


Fig M20.13 - Press Alt-F6 to bring up the Template Import/Export Menu.

Use the following steps to export (save) configuration templates:

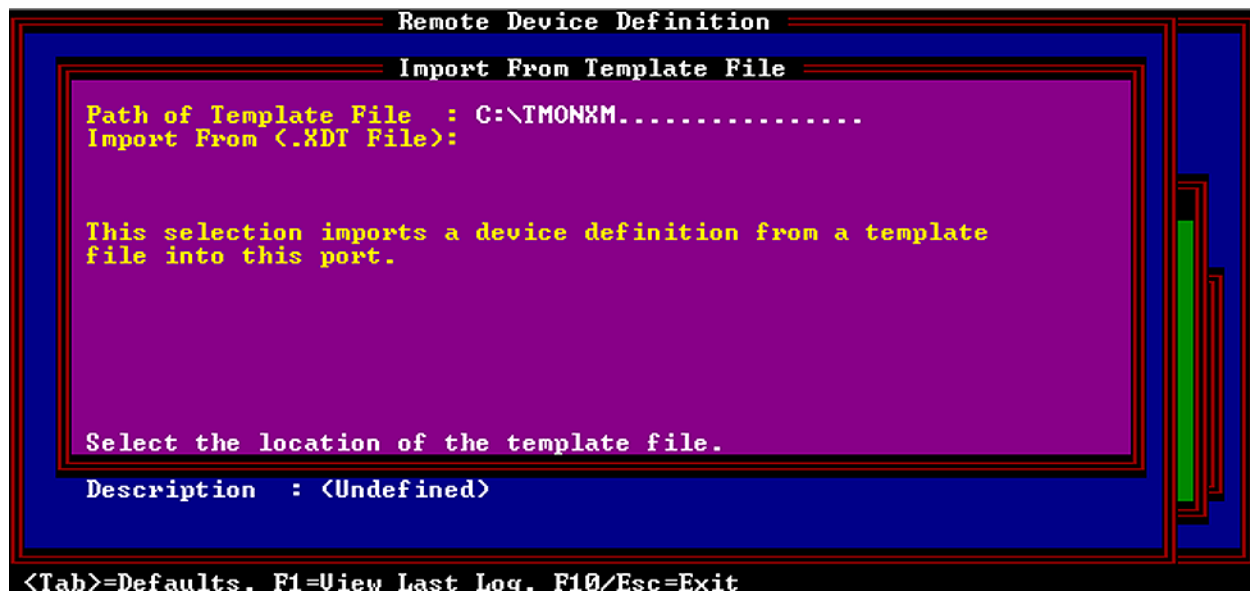
1. Once in the device configuration screen press Alt-F6 to bring up the Template Import/Export Menu.
2. To export the devices' configuration into a template select "Export to Template" and press Enter.
3. Enter the path of the template file and the drive to export to.



Fig M20.14 - Export/save device definition configurations to a template file.

**Use the following steps to import an existing template into a device:**

1. Once in the device configuration screen press Alt-F6 to bring up the Template Import/Export Menu.
2. Select "Import from Template" from the Template Menu and press Enter.
3. Enter the path of the template file and the drive where the file exists.



**Fig M19.15 - Import existing device definition configurations from template file.**



# Software Module 20

## 8 Port Teltrac MUX Interrogator

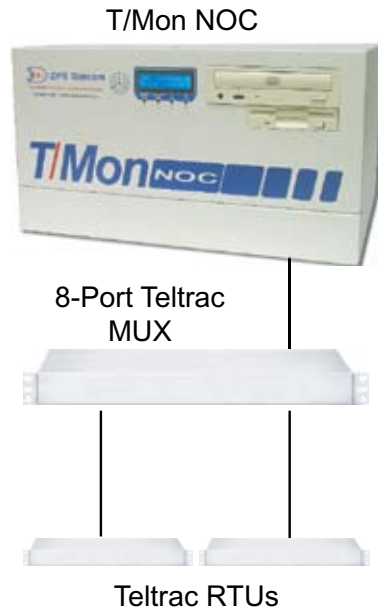


Fig. M20.1 - Typical Teltrac MUX Application

### Overview

The 8-port Teltrac MUX connects up to 8 Teltrac RTUs to a single T/MonXM port.

To prepare the T/Mon or IAM to utilize the Teltrac MUX, a physical port job must be defined for the MUX, and then a virtual port job must be defined for each of the Teltrac MUX ports used.

### Define a Remote Port

1. Select Remote Ports from the Parameters menu. Press F (Find) and enter a serial port number 1-24 — see Figure M20.2 and refer to Table M20.A for field descriptions.
2. In the Port Usage field, press Tab and select “DCP(F) Interrogator.” Refer to Table M20.A for field definitions.

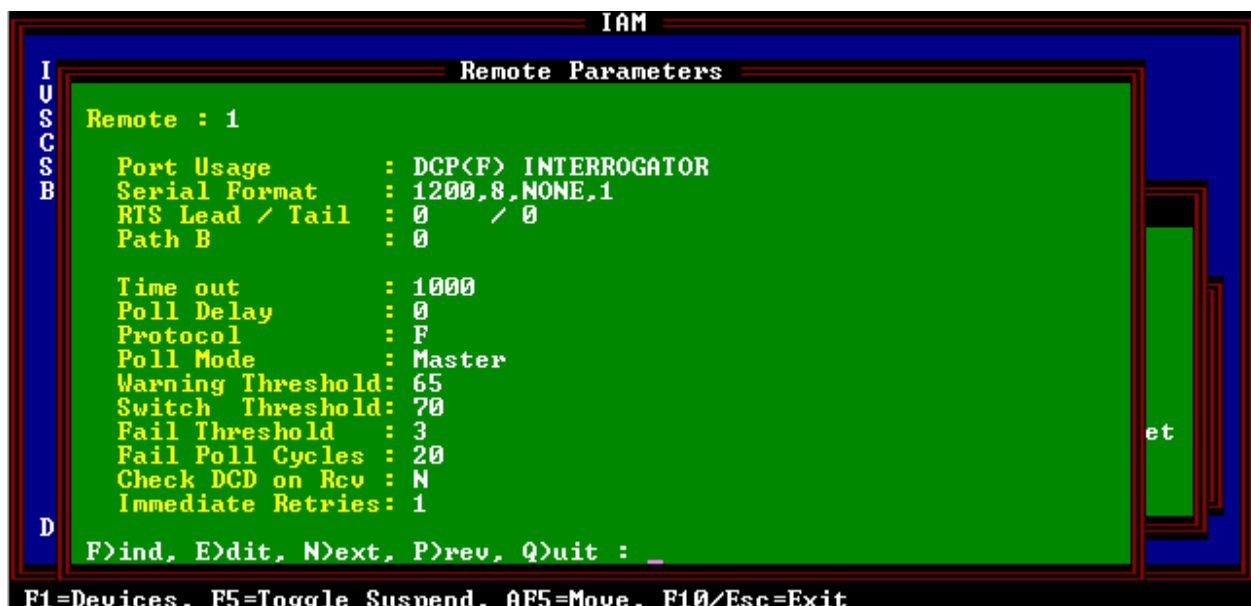


Fig. M20.2 - Define a DCP(F) Interrogator port first

**Table M20.A - Fields available in the Remote Parameters screen for Teltrac Mux usage**

Field	Description
Port Usage	Select a port from 1-24. Valid port types are DCP(F) Interrogator and Halted. Use Halted (default) if no device is connected to the communication port.
Serial Format	Baud rate, word length, parity, and stop bits settings. [1200, 8, NONE, 1]
RTS Lead/Tail	RTS Lead is the time carrier is turned on before data is sent (0-2500 ms). [0] <ul style="list-style-type: none"> <li>Set to 60 for 202 modems. RTS Tail is the time carrier is left on after the last byte is sent (0-2500 ms). [0/0]</li> <li>Set to 40 for 202 modems.</li> <li>Setting the RTS Lead Time and RTS Tail Time both to 2500 will enable a DCP(F) constant carrier.</li> </ul>
Path B	Port for secondary path for ring polling application. [0] <b>Note:</b> For more information about ring polling see section M1-39, "Ring Polling Application."
Time Out	Time the interrogator will wait for a response before failing a poll. Valid entries are 200-9999 milliseconds. [1000]
Poll Delay	The Poll Delay is the time between polls. Valid entries are 0-9999 milliseconds. [0]
DCPF Mode	Enter " <b>F</b> " if you wish to use DCP(F) mode and " <b>N</b> " for DCP mode and " <b>X</b> " for DCP(X). Enter " <b>1</b> " for DCP1 mode. DCP(X) is better error detection. All DPS Telecom RTUs support DCP(F). Newer DPS Telecom RTUs support DCP(X). Use DCP and DCP1 when using third party RTUs. [F]
Poll Mode	These determine the way polling is performed. Valid entries are P)assive only, M)aster only, and C)ombined. Should be "M" if T/MonXM is the is the only device polling the network. [Master] <b>Note:</b> For more information on poll modes, see section M1.
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Valid entries are 5-999 seconds. [65]
Switch Threshold	The Switch Threshold is the seconds of no activity before becoming master. Valid entries are 2-999 seconds. [70] <b>Note:</b> This field is only available when "Combined" is entered in the Poll Mode field.
Fail Threshold	Number of consecutive polls before device failure is declared. [3]
Fail Poll Cycles	The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. Valid entries are 0-255. [20]
Check DCD on Rcv	Y = Enable DCD checking to validate Rcv. N = Disable. [N]
Immediate Retries	Number of retries before proceeding with next address. [1]

**Table M20.B - Function Keys available in the Remote Parameters screen**

Function Key	Description
F1	Devices. Define the DCP(F) devices addresses, alarm displays, and alarm points) that are on the current remote port (see next section).
F5	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
F6	Data Connection (IP/virtual port connections only)
Alt-F5	Allows you to move the port
F10/Esc	Exit

### Remote Device Definition

Press F1 to enter the Remote Device Definition screen. Refer to Figure M20.3 and Table M20.C to complete the available fields on the screen. Save your changes and return to the Remote Parameters screen.

```

Remote Device Definition

Port      : 1          DCP(F) INTERROGATOR
Address   : 2

Description : DCP(F) Port for polling Teltrac Interrog
Site Name  : 8 Port Teltrac Mux Remote Site
Device Type : 8 Port Teltrac Mux.....
Displays   :
Poll Type  :
Refresh Rate :
Firmware Ver :
Log Undefined:
-----
Polarity    :
Logging     :
History     :
Level       :
Status      : A
Reverse     : N
Description : (Undefined)

Press the Tab key to select from the default box.

LIST BOX1 Cursor Keys=Move Highlight Bar. <ENTER>=Select. F10/Esc=Abort

```

Fig. M20.3 - Select the 8 Port Teltrac Mux in the Remote Device Definition

Table M20.C - Fields available in the Remote Device Definition

Field	Description
Port	This port number.
Address	The DCP(F) address that you want to create or edit. Valid DCP(F) addresses range from 1-255. These should match the addresses assigned to the 8 Port Teltrac Mux. (See Software Module 1, DCPF Device Definition for more information.)
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Device Type	Select 8 Port Teltrac Mux — see Figure M20.3.
Displays	Number of displays to be reserved for collection. Enter 1.
Refresh Rate	Number of poll cycles before a refresh cycle occurs.(1-999)
Log Undefined	Select Yes or No to log undefined alarms.

**Note:** Table M20.B continues on following page.

**Table M20.C - Fields available in the Remote Device Definition (continued)**

Field	Description
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A (CR), B (MJ), C(MN) or D(ST) [A]
Status	Alarm(A), Status(S) [A] Defines if T/Mon internal relay will change state.
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which undefined alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

**Note:** When defining a virtual port job, select port 48 or higher, as Jobs 30-47 are reserved for remote access.

#### Define a Virtual Port Job

Press F (Find) or N (Next) and select a virtual port job (48 or higher) for the Teltrac MUX. Select "Teltrac Interrogator" for the Port Usage field. Refer to Figure M20.4 and Table M20.D to complete the remote parameters.

**Fig. M20.4 - Select a job to represent one of the Teltrac Mux ports**

**Table M20.D - Fields in the Remote Parameters screen, Teltrac Mux usage**

Field	Description
Job	Virtual port number where individual Teltrac ports (1-8) from the Teltrac Mux are defined. Must have a Data Connection defined.
Port Usage	Teltrac Interrogator must be selected to define the Teltrac Mux ports.
Description	Up to 40 characters (optional).
Time Out	Time interrogator will wait for a response before failing the poll (200-9999 milliseconds).
Poll Delay	Time between polls in milliseconds (0-9999).
Fail Threshold	Number of polls before device failure is declared (3-20)
Fail Poll Cycles	Polling loop cycles before failed devices are polled (0-255).
Port Fail	Number of times to retry the failed port after the Max modem time is up. (1-9999)
Retry Port Fail	Number of times to retry the failed port after the Max modem time is up. (1-9999)
Max Modem Time	Number of minutes connected via modem before dedicated connection is retried. (1-999)
Dial String	The phone number for the alternate path is entered here.
Modem Init String	Enter the modem initialization string here. Consult your modem's documentation for the appropriate init. string.

**Remote Device Definition (Virtual Port)**

Press F1 to enter the Remote Device Definition screen — see Figure M20.5. Refer to Table M20.E for field descriptions. Save your definition and return to the Remote Parameters.

```

Remote Device Definition

Port / Job      : 60      TELTRAC Interrogator
Device ID      : 1

Description     : .....
Site Name      :

Displays       : 1
Refresh Rate   : 544

Log Undefined: N
-----
Polarity       : B      Address Defaults -----
Logging        : L      Windows           :
History        : H      Message           : 0
Level          : A
Status         : A
Reverse        : N
Description    : <Undefined>

Description (max.40 characters)

Up Arrow=Previous Field, F10/Esc=First Field

```

**Fig. M20.5 - The Remote Device Definition screen**

**Table M20.E - Fields available in the Remote Device Definition**

Field	Description
Port	This port number.
Device ID	Device identification number.
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Displays	Number of displays to be reserved for collection. Enter 1.
Refresh Rate	Number of poll cycles before a refresh cycle occurs.(1-999)
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A, B, C or D [A]
Status	Alarm(A), Status(S) [A]
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which alarms from this site will appear.
Message	ID number of text message associated with alarms from this site.

### Create a Data Connection

1. From the Remote Parameters screen, press F6 to define the Data Connection. This defines the MUX port to be used for this job.
2. From the default box, select one entry from n.1 to n.8 — where n = the defined T/Mon port number and .1 to .8 = the MUX port number. Only the available ports will be listed. Mux ports may be assigned in any order — see Figure M20.6.
3. Save your configuration and press F10 to return to the Remote Parameters screen.
4. Define points for alarm reporting by pressing F1 in the Remote Parameters screen, then F1 in the Remote Device Definition screen. The Point Definition screen will appear — see Section 10 (Point Definition Tutorial) for more information.
5. You can also define Internal Alarms by pressing F3 in the Remote Device Definition screen. The Device Internal Alarm Assignment screen will appear — see Section 14 (Define Internal Alarms) for more information.
6. Repeat steps 4-10 for each Teltrac Mux unit.

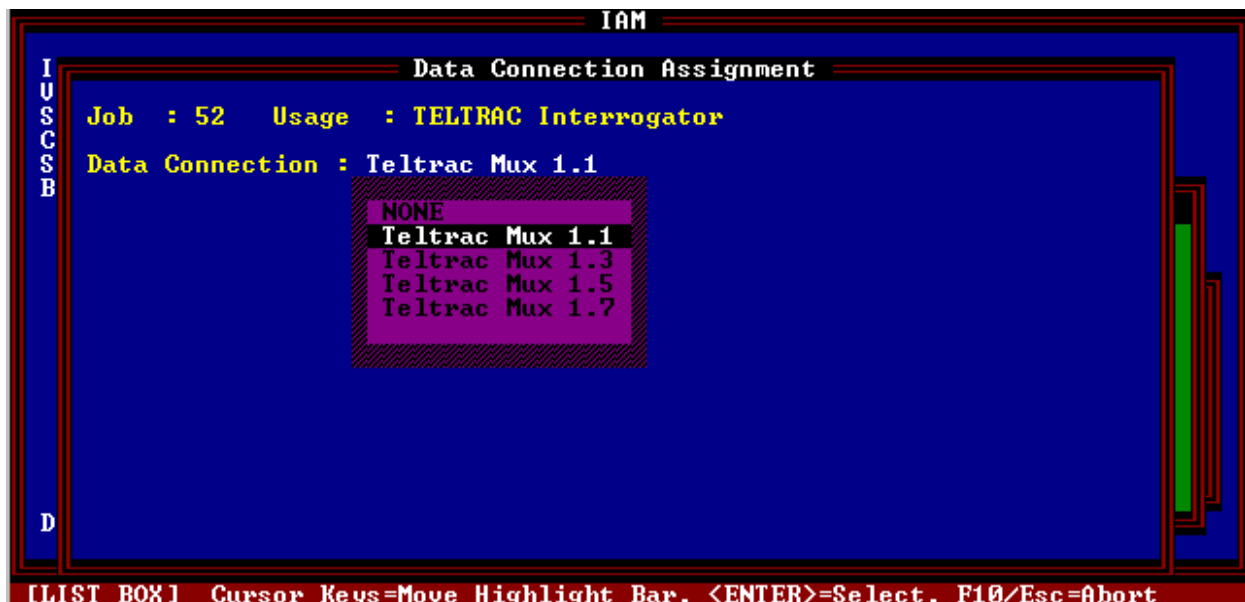


Fig. M20.6 - Define a data connection for each job

**This page intentionally left blank.**



# Software Module 21

## ASCII MUX Interrogators and Responders

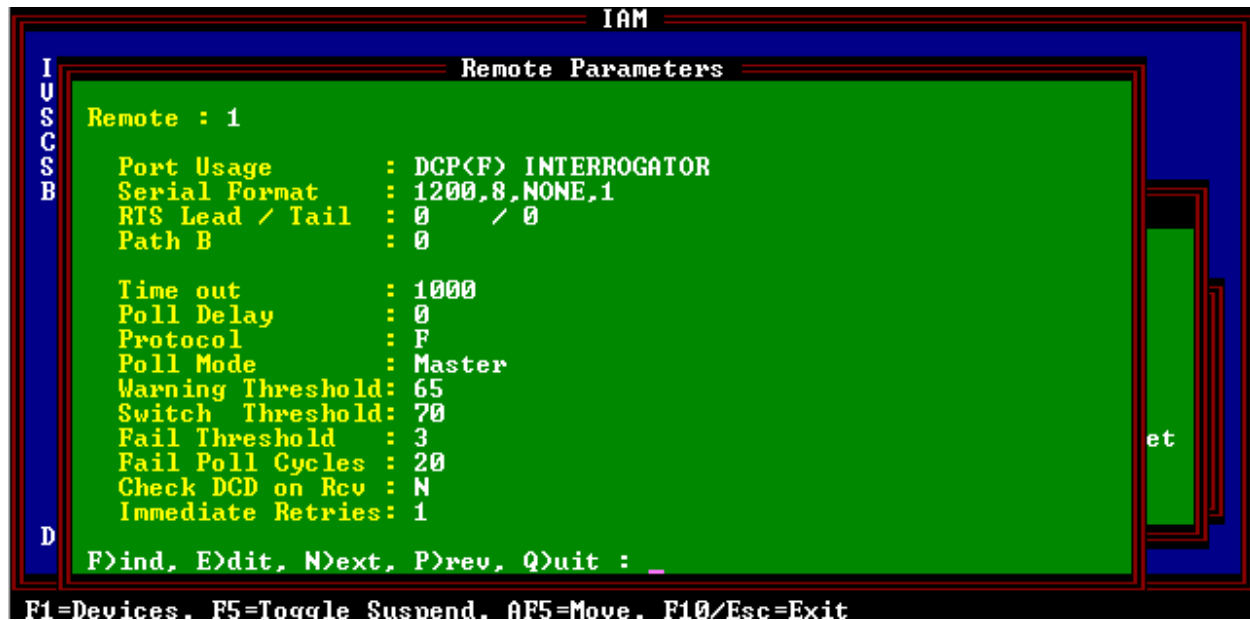


Fig. M21.1 - Example remote port job defined for DCP(F) Interrogator

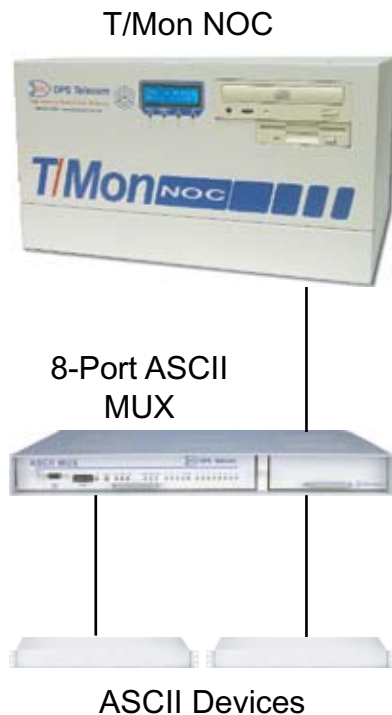


Fig. M21.2 - Typical ASCII MUX Application

**Note:** The ASCII MUX Module must be installed to use ASCII MUX data connection.

The 8-port ASCII MUX connects up to 8 ASCII data sources to a single T/MonXM port. T/MonXM controls the MUX to route data to the correct port. Each channel has a 16K buffer that allows data to be moved between ports at different rates.

To prepare the T/Mon or IAM to utilize the ASCII MUX, a physical DCP(F) Interrogator port must be defined to poll the MUX and a LAN job must be defined for each of the eight MUX ports (or less, if not all ports are currently used).

### Prepare ASCII Rules

Prepare all ASCII rules according to the T/MonXM manual Software Module 6 (for regular ASCII) or Software Module 8 (for Auto-ASCII).

### Define a Remote Port

1. Define a port for the DCP(F) Interrogator to poll the ASCII Mux — refer to Figure M21.1 and Table M21.A to complete available fields.

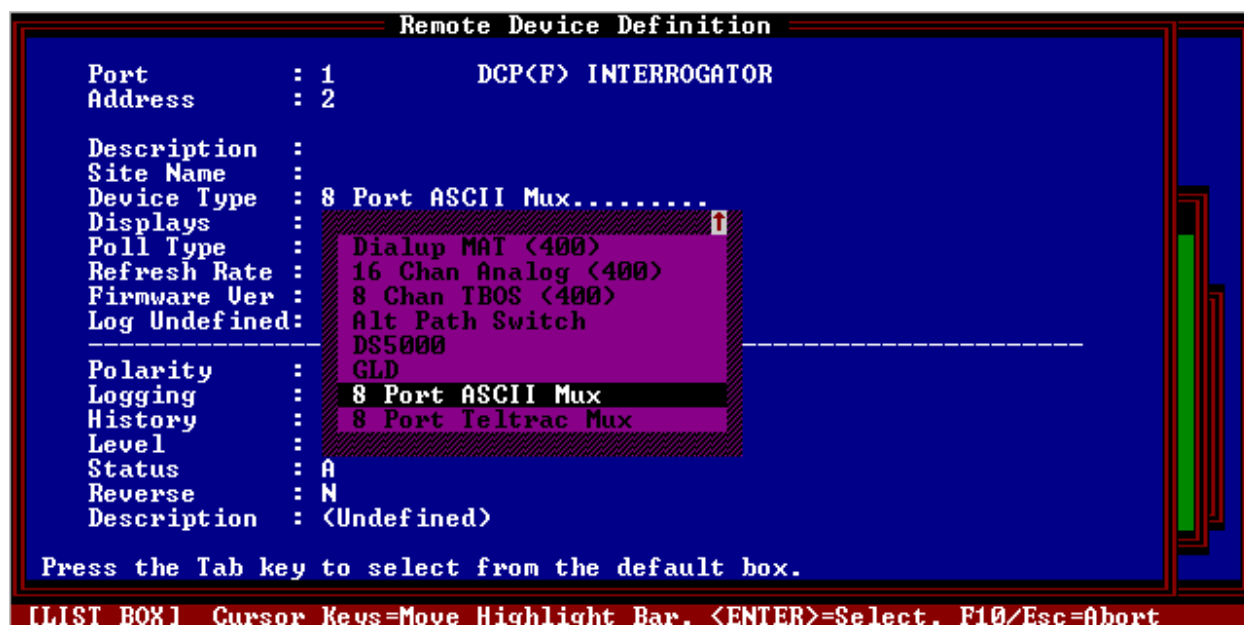
**Table M21.A - Fields in the Remote Parameters screen**

Field	Description
Job	Virtual port number where individual ASCII Mux ports (1-8) from the ASCII Mux are defined. Must have a Data Connection defined.
Port Usage	DCP(F) Interrogator.
Time Out	Time interrogator will wait for a response before failing the poll (200-9999 milliseconds).
Poll Delay	Time between polls in milliseconds (0-9999).
Protocol	Enter "F" if you wish to use DCP(F) mode and "N" for DCP mode and "X" for DCP(X). Enter "1" for DCP1 mode. DCP(X) is better error detection. All DPS Telecom RTUs support DCP(F). Newer DPS Telecom RTUs support DCP(X). Use DCP and DCP1 when using third party RTUs.
Fail Threshold	Number of consecutive polls before device failure is declared. (3-20)
Fail Poll Cycles	The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. Valid entries are 0-255.
Immediate Retries	Number of retries before proceeding with next address. [1]

**Remote Device Definition**

Press F1 to enter the Remote Device Definition screen. Enter the address of the ASCII Mux and press Enter. Press Tab and select "8 Port ASCII MUX" as the Device Type — see Figure M21.3 and refer to Table M21.B to complete available fields.

**Note:** Do not define alarm points for this port and device.

**Fig. M21.3 - Select the ASCII Mux device in the Remote Device Definition screen**

**Table M21.B - Fields in the Remote Device Definition screen**

Field	Description
Port	This port number.
Address	The DCP(F) address that you want to create or edit. Valid DCP(F) addresses range from 1-255. These should match the addresses assigned to the 8 Port Mux. (See Software Module 1, DCP(F) Device Definition for more information.)
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Device Type	Select 8 Port ASCII Mux — see Figure M21.3.
Displays	Number of displays to be reserved for collection. Enter 1.
Refresh Rate	Number of poll cycles before a refresh cycle occurs.(1-999)
Log Undefined	Select Yes or No to log undefined alarms.
<b>Address Defaults</b>	If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm.
Polarity	Bipolar(B) or Uni-polar(U). [B]
Logging	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen.
History	History(H) or No History(N). [H] <b>Note:</b> goes to history.
Level	A (CR), B (MJ), C(MN) or D(ST) [A]
Status	Alarm(A), Status(S) [A] Defines if T/Mon internal relay will change state.
Reverse	Reverse(R) or No Reverse(N) [N]
Description	Default point description. 40 characters (optional)
Windows	Window in Monitor Mode in which undefined alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
Message	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.



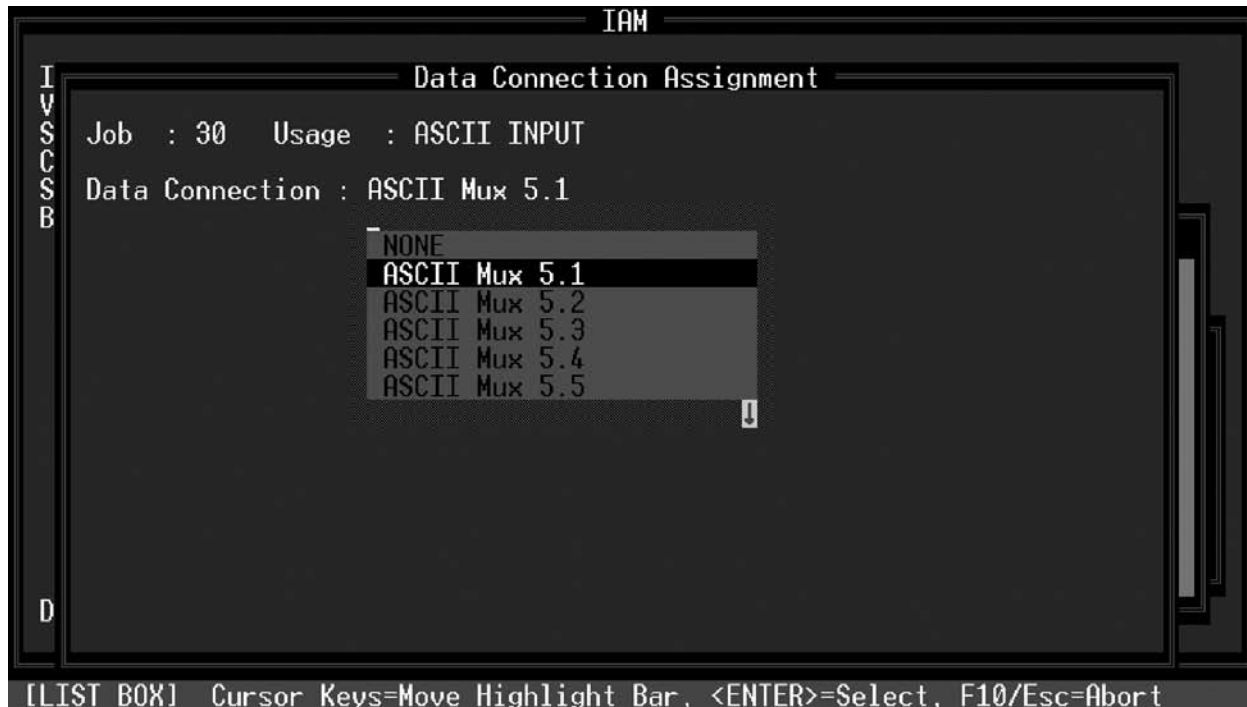
**Fig. M21.4 - Example remote port parameters for ASCII Mux**

#### Define a Virtual Port Job

Press F10 to exit the Remote Device Definition screen. The Remote Port screen will appear. Press N (Next) key to advance to port 48 or higher. This job represents one of the 8 MUX ports. Press E to edit. In the Port Usage field select ASCII Input. Refer to Figure M21.4 and Table M21.C to complete the fields.

**Table M21.C - Fields in the Remote Parameters screen, Job 48 and up**

Field	Description
Port / Job	Phantom port number. Jobs 48 and higher will be available once a device has been defined as "8 Port ASCII MUX."
Port Usage	Select from default box. Default is HALTED. ASCII INTERFACE gives port full alarm and craft interface ability. CRAFT INTERFACE gives port craft the ability to interface only.
Port or Craft Description	Optional 30 Character description.
Full Duplex	Y=Full Duplex. N=Half Duplex. Craft Interface only.
Alarm Alias Port	Number of port whose already defined data base you wish to use for this port. Leave blank for none. If used, enter alias port number, then press F1 and set device rules.
Template Port	To use a pre-defined template, enter the template number here. (801 through 803, leave blank for none.)
Auto Databasing	If Auto Data-basing is being used with the device connected to this MUX port, enter "Y." If regular ASCII is used, enter "N."



**Fig. M21.5 - Select a data connection to designate the MUX port.**

See Software Module 6 for more information about the ASCII and Auto ASCII.

#### Create a Data Connection

1. Press F6 to define the data connection (This defines the MUX port to be used for this job.) Refer to Figure M21.4.
  2. From the default box select one entry from N.1 to N.8, where N= the defined T/MonXM port number and .1 to .8 = the MUX port number. Only the available MUX ports will be listed. Mux ports may be assigned in any order — see Figure M21.5.
  3. Press F10 to return to the Remote Parameters screen. Press F1 to access the Devices screen. Enter information as for regular ASCII (see Software Module 6, “Remote Ports, Dedicated ASCII”) or Auto ASCII (see Software Module 6, “ASCII Input Device Definition”).
  4. Press F1 to access the Point screen. Enter information as for regular ASCII. Point information is not applicable to Auto ASCII — see Software Module 6 for more information.
- When complete, use F10 to return to the Remote Parameters screen. Press N to move to the next job number or press F10 to exit.

**This page intentionally left blank.**

# Software Module 22

## Building Access System

This option is only available if the Building Access System (BAS) software module is installed.

### Building Access System Module

The Building Access System (BAS) is a comprehensive building management system that provides centralized door access control. With the system in place, managers can maintain a database of all access privileges and access granting history. In addition, the BAS eliminates the concern and issues associated with key management (e.g. loss, duplications, and re-keying costs)

The BAS is a profile based access system that assigns each user with a unique user profile that contains information on which Building Access Systems are allowed to be accessed, the door numbers, days of the week access is allowed, a start/stop time, and a beginning and ending date.

### Section Overview

This section is divided into five “How to” sections. See the section that corresponds to your system settings:

Define BAS for NetGuardian

Define BAS for KDA

Define BAU/ECU

Define DTMF Access

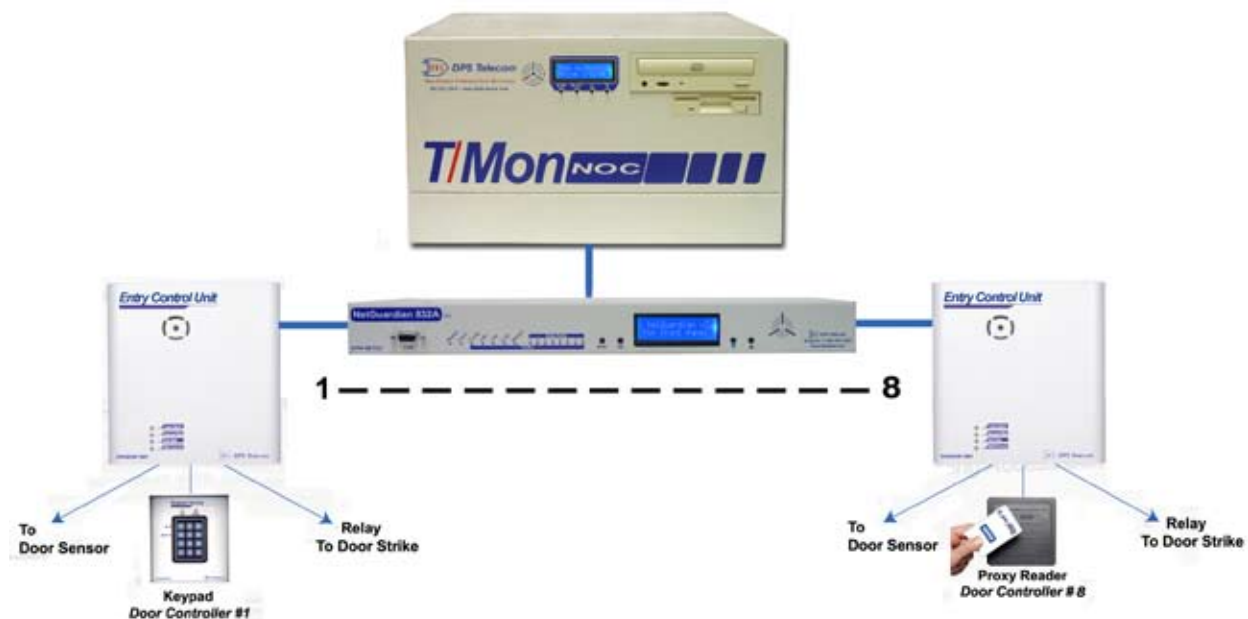


Fig. M22.1 - The BAS can control and regulate up to 16 door entry points.

## BAS for NetGuardian (or BACTL)

The following is an overview for configuring T/MonXM to use the Building Access System for a NetGuardian or BACTL.:

1. Set up a Remote Port.
2. NetGuardian Device Definition
3. Define the Site Definition
4. Define BAS user profiles
5. Example User Profile Using Groups
6. Display Mapping

**BACTL Note:** Although many setup screens and steps refer to “NetGuardian”, this procedure applies to Building Access Controller (BACTL) units as well. Remember to select the appropriate “BACTL” device type, as described in the following procedure.

### Step 1 - Define a Remote Port

Set up a DCP polling port in the Main menu > Parameters > Remote Parameters screen — see Figure M22.2. Create a dedicated port job for polling the BAS over serial connection, or create a virtual port job for polling over a TCP/IP connection. See Software Module 1 (DCPF Interrogator) for more information.

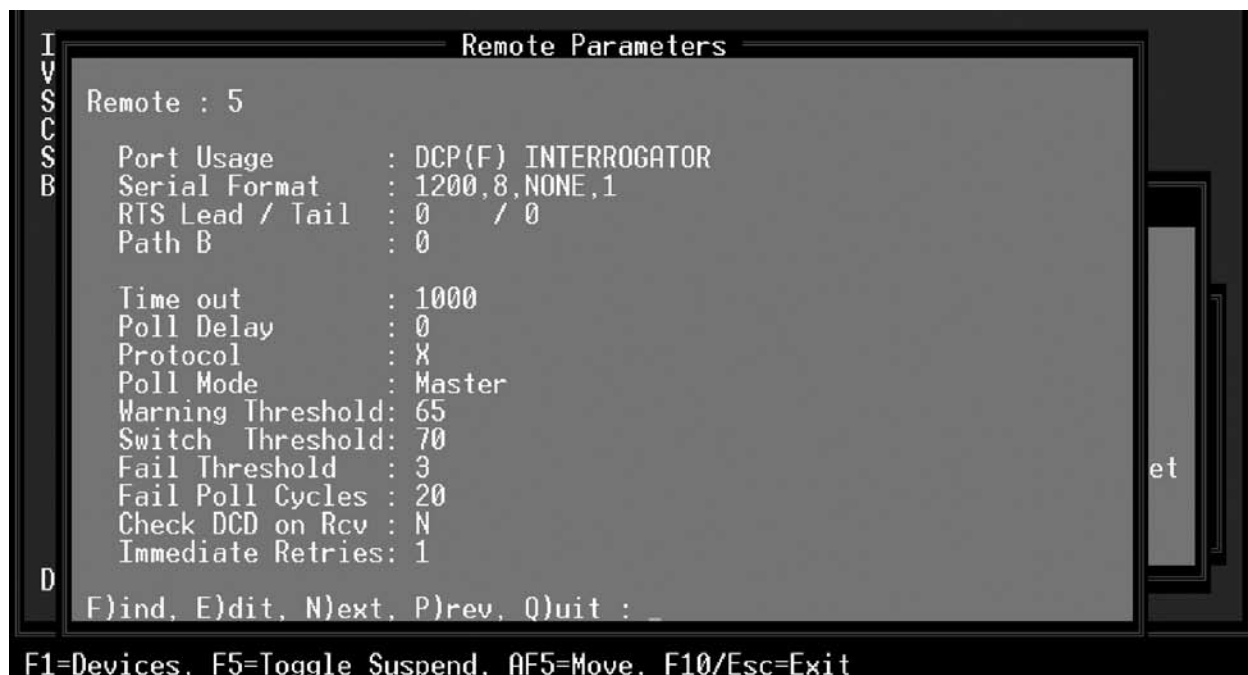


Fig. M22.2 - Example of a defined dedicated port for DCP(F) Interrogators



```

Net Guardian Definition

Site Number      : 5
Description      : NETGUARDIAN
Site Name       : TEST
Password        :
Device Type     : FULL
Base Proxy Port : 3000
Expansion Units  : 1
Expansion Modules: BAC.....

IP Address / Port: 126.10.220.47      2001
Dedicated Port   : 54   Base Addr: 5   Exp
Dialout Port     : 0    Phone:
Polling Type     :
Scheduled Days ---> SUN:   MON:   TUE:   Poll WED:   THU:   FRI:   Test:
Scheduled Hours  :                               (mins)
Scheduled Minute :                               SAT:

Expansion Module

[LIST_BOX] Cursor Keys=Move Highlight Bar, <ENTER>=Select, F10/Esc=Abort
  
```

Fig. M22.3 - NetGuardian Device Definition screen.

**Step 2 - Define the NetGuardian Device**

To define the NetGuardian for BAS, go to the Master menu > Files Maintenance menu > LAN-Based Remotes option. The Net Guardian Definition screen will appear. Fill in the fields with the appropriate information — refer to Tables M22.A. Select BAC (Building Access Controller) in the Expansions Modules list box menu — see Figure M22.3.

**Note:** options will vary according to serial dial-up or TCP/IP mode.

**Table M22.A - Fields in the NetGuardian Device Definition screen**

Field	Description
Site Number	3-digit site number. This number is unique over the entire alarm network. This number is the address field for responders, derived alarms, and labeled controls.
Description	41 character description of the site.
Site Name	15 character site name. This will be stamped on every event from this RTU.
Password	20 character password. (Only needed if T/MonXM will be managing the proxy ports.)
Device Type	Indicates if the NetGuardian is the standard version, the NetGuardian C version, or a BACTL.
Base Proxy Port	Set to 3000 (default) or the same as the Net Guardian.
Expansion Units	Enter the number of NetGuardian expansion units you are using. (Only needed if T/MonXM will be managing the proxy ports.)
Expansion Modules	Select the expansion modules you are using (select BAC).
IP Address / Port	Enter the IP address for the unit. This is the address that T/Mon will use to poll the Net Guardian. Also enter the UDP Port address of the NetGuardian(must match the NetGuardian).

**Note:** Table M22.A continues on following page.

**Table M22.A - Fields in the NetGuardian Device Definition screen**

Field	Description
Dedicated Port	If the NetGuardian reports on a dedicated or Ethernet line (DCP), enter the T/MonXM port number. If the NetGuardian reports only on a dial line, enter 0.
Base Address	The DCP address of the NetGuardian, or of the "BAC1" section of a BACTL32.
Exp. Addr. #1	The DCP address of the NetGuardian's internal BAC (must match the NetGuardian), or - if using a BACTL32 - the "BAC2" DCP address.
Exp. Addr. #2	N/A
Dialout Port	Enter the port number used for dial out, if dialout only or alternate path is used. Enter '0' if dedicated line only (skips out of edit mode).
Phone	Enter the phone number to reach the remote.
Polling Type*	Select Periodic or Schedule from the default box. Periodic polling polls at the interval specified in minutes in the polling interval field. Schedule sets a defined day and time in the week to poll the unit. If periodic is selected, the cursor will skip to the Polling Interval field. If schedule is selected, the cursor will skip to the scheduled days field.
Polling Interval*	Periodic polling only. 0 to 9999 minutes. 0 = never. The cursor will skip out of edit mode after entering a value.
Scheduled Days*	Enter the whole number of each hour (24 hour clock) to place a polling call (0-23, where 0 = midnight). Example: 0, 8-16 polls at midnight and every hour from 8 AM to 4 PM.
Scheduled Minutes*	Enter the whole number of the offset from the hour each call is to be made. (0-59, where 0 = on the hour). Example: 30 polls at half past the hour.

\* Option available for dial-up only.

**Table M22.B - Key commands in the NetGuardian Device Definition screen**

Function Key	Description
F1	Devices. Allows you to view and edit Net Guardian address definition information.
F2	Global Options. Allows you to set the number of Proxy and Craft connections.
F3	Firmware. Copies a Net Guardian firmware file from a floppy disk.
F10/Esc	Exit. Returns you to the previous screen/menu.

### Step 3 - Define Site Definition

From the Master menu, select Files, Building Access, and then Sites/Zones. Enter the appropriate information into the Site Definition fields. See Table M22.C for field names and descriptions.

The Site definition screen allows the user to define a physical relationship in the remote sites between the doors, zones, and sites. In order to save databasing time, managers can also setup groups of doors that can be assigned to a set of users (instead of entering site/zone information for each separate user). Once a user profile is setup (see Step 4 on section M22-7), the user can be assigned to a group of doors instead of assigning doors to a user.

Sites / Zones								
Ref	ID	Description	Win	Type	Port	Dvc	Adr	Dsp Pt Door List
1	002	Site 1 Perimeter	31	BAC	N2		1	1-4
2	003	Site 2 Comp Room	31	BAC	N2		1	5-6
3	004	Site 3 Generator	31	BAC	N2		1	7-8
4	005	Site 4 Storage #1	31	BAC	N2		1	1-2
5	006	Site 5 Storage #5	31	BAC	N2		1	3-4
6		...						
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
Site Number (001-999)								
F1=Goto, F2=INS, F3=Blank, F4=DEL, F8=Save, F9=Help, F10/Esc=Exit								

Fig. M22.4 - Select Building Access and the Site Definition from the Files menu.

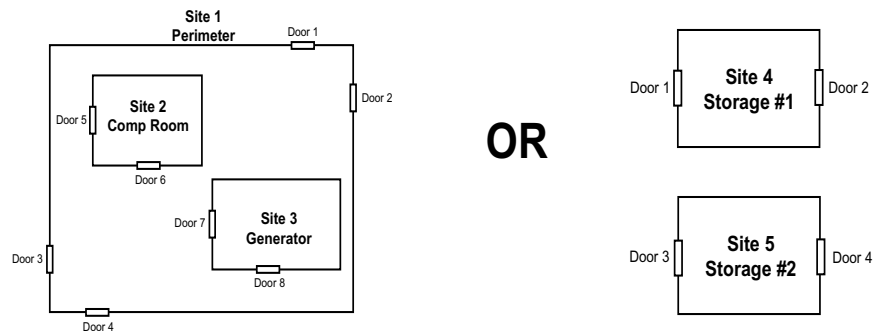
Table M22.C - Fields in the Site Definition screen

Field	Description
Ref	Site definition reference number. This field cannot be edited.
ID	The Site ID is a logical group of one or more doors at a specific physical location. This Site can represent a room within the facility or simply a portion of the facility that only a sub-set of users cleared for the location can access. Users with valid access codes can access any of the doors within that specific Site. The Site ID is a unique 3-digit numeric code used when logging into a site. Valid site numbers are 001-999. You must enter 3 digits — see figure M22.5 for example of site diagrams.

**Note:** Table M22.C continues on following page.

**Table M22.C - Fields in the Site Definition screen continued**

Field	Description
Description	Site description (max. 20 characters).
Win	Window to report the login/logout. Valid windows are 2-90 with standard features.
Type	Manually enter the device type by typing BAC into the field.
Port	Designated port of the NetGuardian with BAC capabilities (N2 for NetGuardian, K2 for KDA).
Dvc	N/A
Adr	Site number of the NetGuardian or KDA with BAC expansion module capabilities.
Dsp	N/A
Pt	N/A
Door List	List of ECU addresses (doors that create sites/zones) polled (door points) (e.g., 1-4, 9-12). Doors can be treated as individual (single) doors, or if, for example, there is a site/zone with multiple doors, it can be provisioned so that it does not make a difference which door a user comes in or out of. The use of sites/zones requires less databasing because users can be assigned to sites/zones rather than having to assign each door to each user. Alternatively, if a site/zone has a specific in or out door, the doors can be treated as individual doors. <b>Note:</b> Use “-” for ranges, or “,” to separate doors.

**Fig. M22.5 - Example of site diagrams****Table M22.D - Key commands available in the Sites/Zones screen**

Function Key	Description
F1	Go to. Allows you to jump to a specific site reference ID by typing in the reference ID number.
F2	Insert. Insert a new line at the current position and moves everything down by one. Note: If the very last entry contains data, a warning will appear to confirm insertion. If there are any blank lines available, use DEL (F4) to delete them. This will make more space to insert.
F3	Blank. Blanks out all the information in the line where the cursor is currently located.
F4	Delete. Deletes entire line at current position. Similar to F3 but will move everything up by one.
F8	Save. Saves the configuration information and returns you to the previous screen.
F9	Help. Brings up the help menu.
F10/Esc	Exit. Returns you to the previous screen/menu.

#### Step 4 - Define BAS User Profiles

Creating user profiles can be a time saving tool that allows you to assign all like users into a single group. It is also easy to maintain, in that if a change is made to a group, it affects all of the users in that group (instead of databasing each user profile individually). The Building Access System also allows managers to define specific user profiles. Here, the information defined in the Site Definition screen will be assigned to users. The user profile will determine which doors are allowed to be accessed, days of the week access is allowed, a start/stop time, and a beginning and ending date.

Based on the Site Definitions, users can be placed into groups as stated above. A type of user can be defined and then users of that type can be assigned to a group. Additionally, there may be groups within a group (up to 14 group layers) and a user profile can have a user name that has access to more than one group.

From the File Maintenance menu, select Building Access and then BAS Profiles.

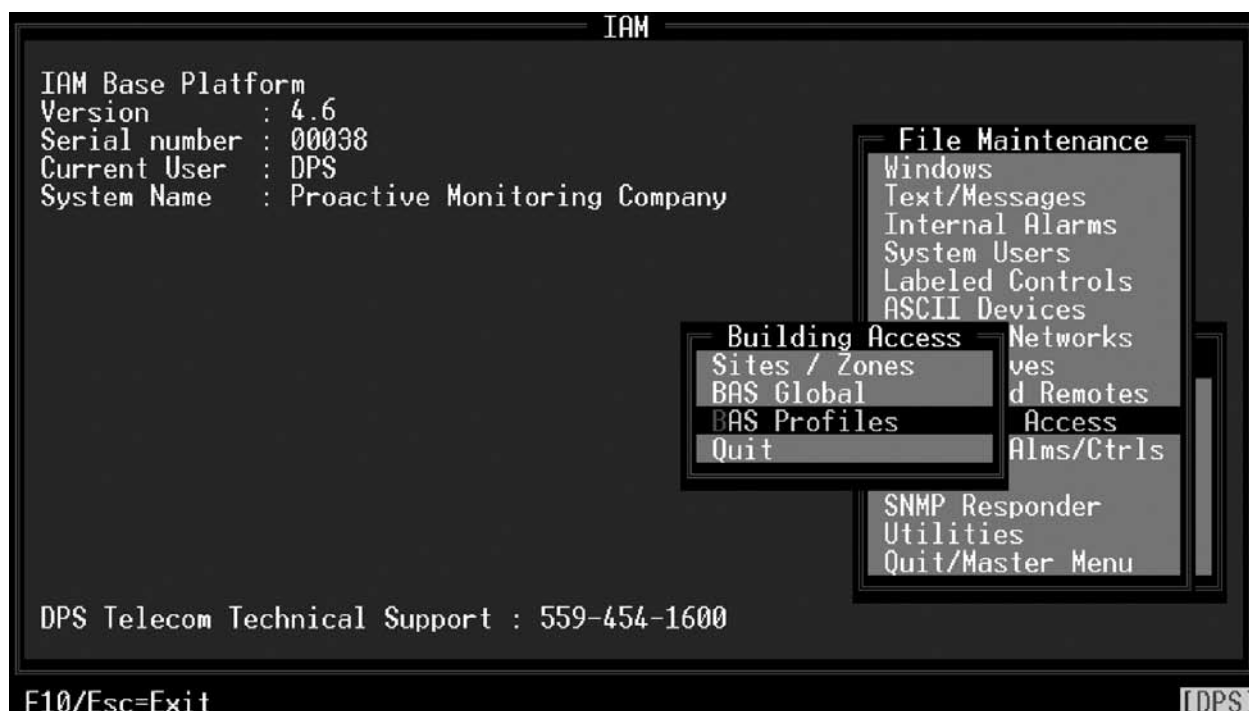


Fig. M22.6 - Select BAS Profiles Master menu > Files Maintenance menu > Building Access

Pressing E)dit allows you to begin entering the information from the first field in the BAS profiles screen. Pressing F)ind engages an alphabetical search function that allows you to find fields by typing the field name. Typing the first few letters of the field name will bring you to that field. To save a profile press F8.

**Note:** After saving a user profile, the information from the previous entry will remain on the screen. To enter a new user profile, type in new information over the existing profile or modify the information to fit the new profile and then save (F8).

```

BAS Profiles
User : Test User      Type : User      Code : 0123456789
Name : Test Name     Title: Test Technician
EMail: DoesNotExist@dpstele.com      Stay Open: Y
Site/Group           From           To           DOW           Time of Day
001                Test                03-21-2007 03-21-2009 SMTWTFS 18:56 23:56

F)ind, E)dit, N)ext, P)rev, D)delete, Q)uit : _

F4=Del Active, F8=Build BAC data, F9=Help, F10/Esc=Exit

```

Fig. M22.7 - Enter the user profile information (group example shown)

Table M22.E - Fields in the BAS Profiles screen

Header Field	Description
User	Abbreviated user/group name (3-10 characters) (case sensitive).
Type	Individual User or Group of users.
Name	Name of user (3-30 characters).
Email	User's email address. <b>Note:</b> Used to notify users of Auto-cycled passwords. (Use Global Options for more information).
Code	Password code to be entered on the keypad for building access (7-14 digits). The code in parentheses represents the old access code. The system is designed to have a roll over period for codes (user definable in BAS Global). However, both the old access code and the new access code remain valid for the period designated in BAS Global. To manually roll the password over, select the Code field and press Enter while holding down the Ctrl key. Users will be notified via email (to the email address indicated on this screen) if their password has rolled over (See NetGuardian manual for information on entering RFID codes).
Title	Describes the users job title/position (max. 30 characters).
Stay-open	Enables user to keep the door open. When a code with this setting is used it will unlock the door and leave it unlocked. This will allow the user to put the ECU in Stay-open mode. Normal users will not be able to lock it once it has been put into Stay-open mode. Only another user /code with Stay-open may lock it again once it has been unlocked.
Detail Field	Description
Site/Group	Describes the site number as defined in the Site Definitions (Step B) or the BAS profile defined as type Group. This controls the sites the user is allowed to access (doors, times, dates, etc.). If a user is being assigned to a group, pressing the down arrow key causes the remaining fields to default to the group settings. However, any information entered into these fields will override the group settings.

**Note:** Table M22.E continues on the following page.

Table M22.E - Fields in the BAS Profiles screen

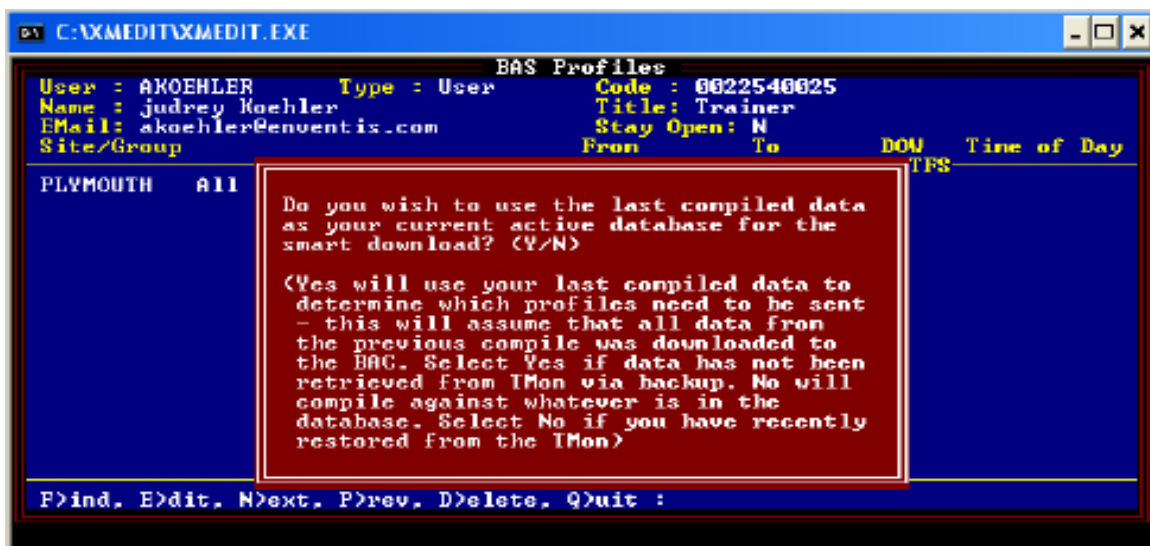
Header Field	Description
From	Indicates the date the user's password code becomes valid (mm/dd/yyyy).
To	Indicates the date the user's password code becomes invalid (mm/dd/yyyy). <b>Note:</b> cannot be longer than ten years.
DOW (SMTWTFS)	Indicates the day(s) of the week the user's password code is valid. Pressing X will automatically populate the space where the cursor is located. You can also use S for Sat/Sun, M for Mon, etc. Pressing the space bar clears the field.
Time of Day	Indicates the beginning and ending time of the day the user's password code is valid (hh:mm on 24 hour clock).

Table M22.F - Function Key Descriptions

Function Key	Description
F4	Deletes the active BAS download data. This is an image of the NetGuardian's BAC data. Deleting this data will force all profiles to be sent to the NetGuardian/KDA.
F8	Build BAC Data. Compiles all profiles and builds data that will be sent to the NetGuardian. All new data will be stored into a new download table that contains all profiles that need to be sent or has already been sent. The current active data will be preserved for the smart download and will be used to determine which profiles have already been sent and which profiles need to be updated or added to the NetGuardian/KDA.
F10/Esc	Exit the BAS Profile window.

**Special note for Xmedit users:** T/Mon builds a database of what it has already sent while in monitor mode. The T/Mon uses this database so both T/Mon and the NetGuardian are in sync while it is still downloading. This database is also used to determine which profiles still need to be sent the next time it compiles the BAS profile data. It will skip the profiles that it knows have already been transferred. This was done so it will only transfer the changes. When compiling BAS profiles on XMedit, it will not have this active database and will think that all of the profiles would still need to be downloaded to the NetGuardian. There are two ways of getting around this:

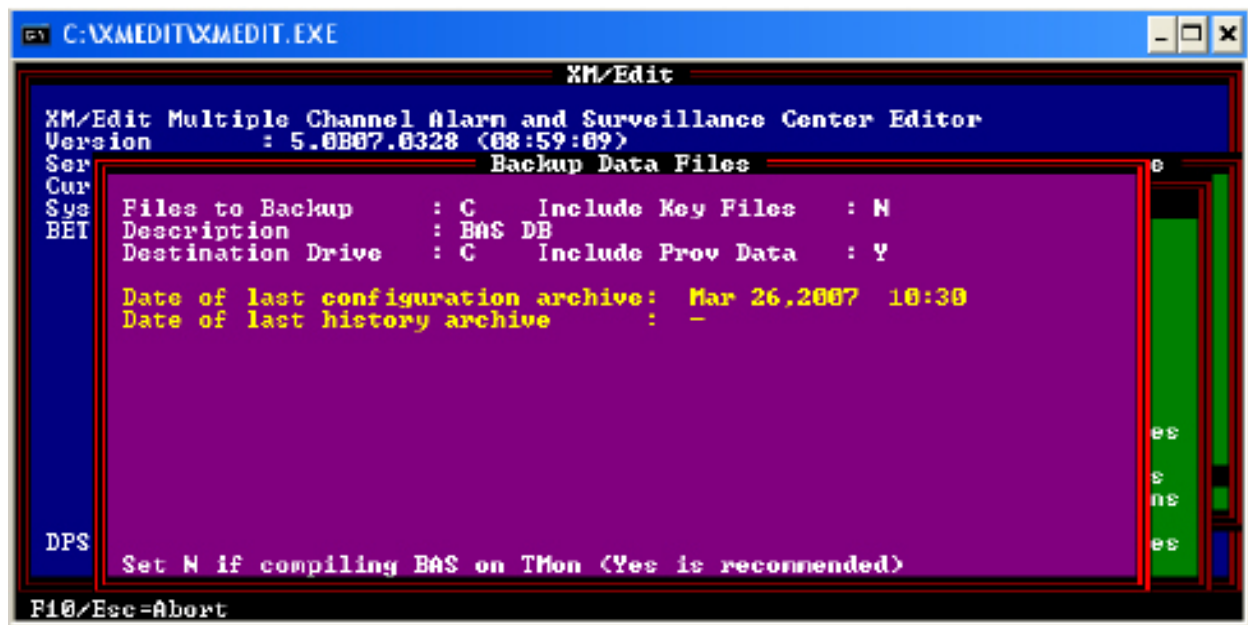
1. Compiling the BAS Profiles in XMedit. This method is recommended because it minimizes the amount of time the T/Mon has to be offline. In the BAS Profiles window (in XMedit), pressing **F8** will give a prompt asking if you wish to use the last compiled data as your current active database for the smart download. Selecting **Yes** will copy the last compiled set of data into the active database. This is the database that gets built in monitor mode and contains which profiles have already been downloaded. It will run through the normal compile process but will use the last compiled data in place of the active database. Compiling on XMedit should only be done when you are ready to do a backup on XMedit and restore on T/Mon.





Selecting **No** will use whatever is already in the database to determine which profiles are new/changed and needs to be downloaded to the BAC. The only cases where you would select no is if you press F4 to clear the active database and want to compile against an empty database. This will force a full download to the BAC. The other case where you would select no is if you had recently did a restore on XMEdit with the newest T/Mon database (this includes the active database after it had already sent everything to the NetGuardian). The data on XMEdit already has an updated active database to compile against so we would not want to use the last compiled data to determine which profiles need to be sent.

Once the data has been compiled on XMEdit, the database can be backed up for transfer to the T/Mon. The backup screen (Files -> Utilities -> Back Up Data Files) should have an extra field that appears only on XMEdit. This field gives the option to "Include Prov Data". We would want to select Yes and include everything since we have already compiled in XMEditRestore on T/Mon should update the database with the compiled BAS data and should be ready to go into monitor.



2. Compiling the BAS profiles in T/Mon. Changes can be made in Xmedit but do not compile on Xmedit. When you do a backup on XMEdit, set "Include Prov Data" to N. This will make sure that when you do a restore on the T/Mon, it will not overwrite the database that contains which profiles have already been downloaded.

Do a restore on T/Mon and go into the BAS Profiles window and press F8 to compile. This will compile against what the T/Mon had already sent to the NetGuardian. This method will allow you compile as many times as you want in case you made any mistakes in the XMEdit database editing. After it has compiled, it should be ready to go back into monitor mode.



### Step 5 - Example User Profile Using Groups

Users may be assigned to groups or groups within groups. For example, if User 1 and User 2 needed full access to Site 1, but only partial access to Site 2, they would be assigned to a group or site designating which doors are allowed to be accessed. In the Sites/Zones screen, a site would be setup (and assigned a description; here - “Test Technicians”) giving full access to Site 1 but only partial access to Site 2. In the BAS Profiles screen, User 1 and User 2 would be assigned to the site/group called “Test Technicians”. Additional users may also be added to the “Test Technicians” site, thus saving database time.

Additionally, users may be assigned to more than one group or site. User 1 in the example above might also be given access to various other sites. This is accomplished by entering all the Sites/Groups that User 1 has access to in User 1’s BAS profile. User 1’s supervisor, however, might be assigned to a group that contains all the access privileges contained in the “Test Technicians” site as well as full access to Site 2 and perhaps other sites.

### Step 6 - ECU Display Mapping

Tables M22.F and M22.G describe the BAS display mapping in T/Mon. Each of the points and descriptions in Table M22.G apply to displays 3-18 (ECUs 1-16) in Table M22.F.

**Table M22.G - N2 Mapping (BAS device)**

Display	Mapping	Display	Mapping	Display	Mapping
1	Internal	7	ECU 5	13	ECU 11
2	Internal	8	ECU 6	14	ECU 12
3	ECU 1	9	ECU 7	15	ECU 13
4	ECU 2	10	ECU 8	16	ECU 14
5	ECU 3	11	ECU 9	17	ECU 15
6	ECU 4	12	ECU 10	18	ECU 16

**Note:** See Table M22.G for specific ECU mapping.

**Table M22.H - ECU Mapping**

Point	Description	Mode
1-8	Unused	N/A
9	Alarm 1 (Door sensor)	Status **
10	Alarm 2	Status **
11	Alarm 3	Status **
12	Door violation alarm (Door opened without code)	Status
13-16	Unused	N/A
17	Door strike active (relay #1)	Status / Control* **
18	Relay #2 active	Status / Control* **
19	Hack lockout (5 invalid passwords have been entered, and BAS will not accept new input) for five minutes.	Status
20	Exit password OK	Status **
21	Propped door active (if door needs to be left open)	Status / Control*
22	Stay-Open Mode (Relay #6)	Status/Control **
23	Unused	N/A
24	Speaker active	Status **
25-61	Unused	N/A
62	ECU is using defaults	Status
63	ECU enabled	Status **
64	ECU polling error (device failure)	Status

\* When using controls from alarm masters, only issue the momentary (MOM) commands.

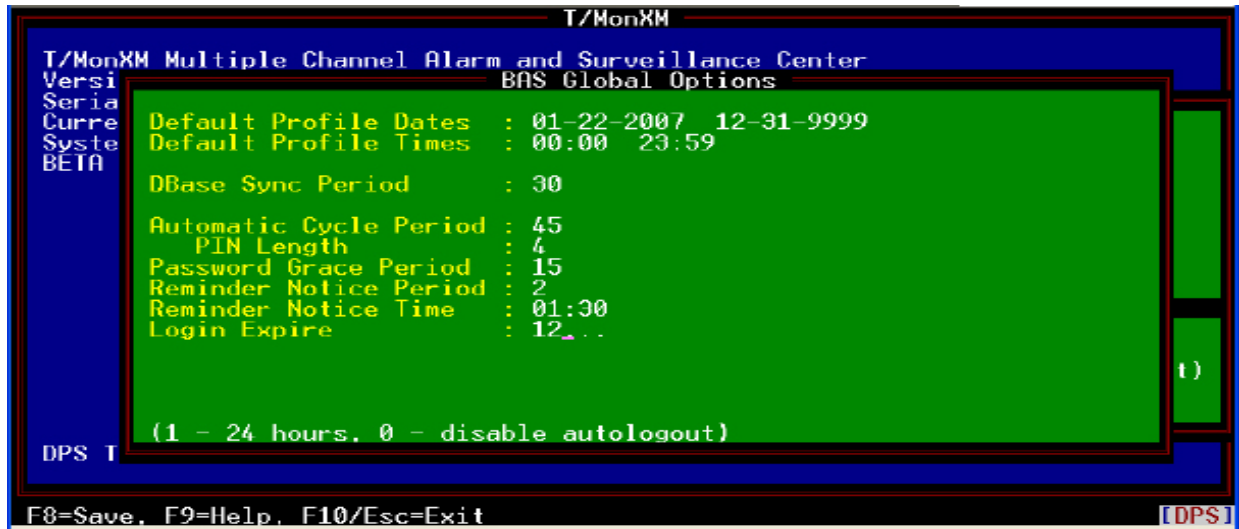
\*\* DPS recommends these alarms be set to “No Log” and “No History” in T/MonXM point setup. T/MonXM uses this data internally for diagnostic purposes.

Note: Please refer to the FAQ section at the end of this document if you have any questions regarding building access.

## BAS Global

To set BAS Global information, select Files, Building Access, and then BAS Global. The information entered here will determine specific criteria applicable to all BAS user profiles.

The table M22.H gives a description of the BAS Global screen fields.



**Fig. M22.8 - The information entered in the BAS Global screen determines specific criteria applicable to all BAS user profiles**

**Table M22.I - Fields in the BAS Global screen**

Field	Description
Default Profile Dates	Determines the default active dates that appear when entering user profiles. (mm/dd/yy)
Default Profile Times	Determines the default active times that appear when entering user profiles. (hh:mm)
DBase Synch Period	Determines the minutes between BAS profile checks (30-10080; 0=none).
Cycle Period	Determines the days between automatic password cycling (4-1096; 0=none). (Note: Should not be used with proximity version of ECU card).
PIN Length	Determines the number of PIN digits that will cycle when the password roll over occurs (1-4).
Password Grace Period	Determines the grace period that old passwords are still valid (0-15 days).
Reminder Notice Period	Determines the number of days between reminder email notices regarding password roll-over (1-5; 0=final only).
Reminder Notice Time	Determines the time of day at which to send notices (hh:mm).
Login Expire	Amount of time before site logins are automatically logged out of the Site Login Window. Enabling this will disable standard logouts when using cards. When a card is used and the user is already logged in, it would normally log the user off of the system. But this will reset the user's entry time instead. (1-24 hours)(0-disable auto logout)

## Site Log In Status

Monitor the status of site access from monitor mode. From the Alarm Summary screen, press Ctrl-F3 to see the Site Login Status screen. All building access devices that are currently logged in will be show, along with identification of the persons logging in and login times.

This screen also allows you to log a user out. This is especially helpful in case a user neglects to logout from a site. You can log-out the site/user that is highlighted by pressing the Alt and F1 keys together. An example of the site login status screen is shown in Figure M22.9.

Site Log In Status						
Site	Dr	Description	Int	Name	Entry Time	Elapsed CN
0	1	[DENIED] INVLD CARD#	UNK	987654321	Jan 21 20:03	00:05 1
0	1	[DENIED] INVLD CARD#	UNK	134	Jan 21 20:05	00:03 2
1	1	[DENIED] INVLD DATE	Te>	Test User2	Jan 21 20:03	00:05 1
1	1	Yale Front Door	Te>	Test User5	Jan 21 20:04	00:04 2
2	2	Madera Office	Te>	Test User1	Jan 21 20:04	00:04 1

Site Log In	
<div style="background-color: green; width: 100px; height: 100px;"></div>	

>	E	I	M	Q	U	V:	D
B	F	J	N	R	W	A:	P
C	G	K	O	S	X	S:	S
D	H	L	P	T		P:X	
STAND	:3	Silenced:	0				
COS	:6	Off Line:	0				
							60305796

Cursor Keys=Move, Alt-F1=Log Out, Alt-F3=Clear All Events, F10/Esc=Exit

Fig. M22.9 - Site Log In Status screen

Table M22.J - Fields in the Site Log-In Status screen

Field Name	Description
Site	Number of the site as defined in the Site Definition screen
Description	Description of site as entered in the Site Definition screen
Int.	Initials of the person logging in, per the System Users screen
Name	Name of person logging in, per the System Users screen
Entry Time	Time log in occurred
Elapsed	Time that has passed since log in (Anything over 12 hours will appear as " ** . ** ")
CN (Count)	The number of times the user logged in before logging out or the number of times the error had occurred before clearing the event. Count for users logged in will only increment to more than 1 if the auto log out feature is enabled.

**Tbl. M22.K - Hot keys available in the site site**

<b>Function Key</b>	<b>Description</b>
Alt-F1	Log Out. This function key allows you to log a user out of a site. The site/user that is highlighted when the Alt F1 keys are pressed together will be logged out and deleted from this screen.
Arrow Keys	Moves up, down, left and right, through the fields
F10/Esc	Exit. Exits Site Log in Status screen

## BAS for KDA

The following is an overview for configuring T/MonXM to use the Building Access System for a KDA:

1. Set up a Remote Port.
2. KDA Shelf Definition
3. Define the Site Definition
4. Define BAS user profiles
5. Example User Profile Using Groups
6. Display Mapping

### Step 1 - Define a Remote Port

Set up a DCP polling port in the Main menu > Parameters > Remote Parameters screen — see Figure M22.2. Create a dedicated port job for polling the BAS over serial connection, or create a virtual port job for polling over a TCP/IP connection. See Software Module 1 (DCPF Interrogator) for more information.

### Step 2 - Define the KDA Shelf

To define the BAS for KDA, go to the Master menu > Files Maintenance menu > KDA Shelves option. The KDA Shelf Definition screen will appear — see Figure M22.10. Fill in the fields with the appropriate information — refer to Table M22.K for field descriptions. Select the BAC (Building Access Controller) under the Expansion list box menu.

**Note:** can only be base unit.

For more information on KDA shelf definition see Software Module 3 (Files Maintenance > KDA Shelves).

**KDA Shelf Definition**

Site Number : 5

Description : KDA

Site Name : TEST

	Host	Expansion
Base	KDA 864	BAC.....
Sat 1	KDA 864	NONE
Sat 2	KDA 864	LR-24
Sat 3	KDA 864	EXP-83

Dedicated Port : 54 Base Addr: 20 Exp

Dialout Port : 0 Phone:

Polling Type :

Scheduled Days ---> SUN: MON: TUE: W

Scheduled Hours :

Scheduled Minute :

LR-24  
8 CHAN ANALOG <B>  
16 CHAN ANALOG  
4 PORT TBOS  
8 PORT TBOS  
8 ALG / 4 TBOS  
BAC  
EXP-832

[LIST BOX] Cursor Keys=Move Highlight Bar, <ENTER>=Select, F10/Esc=Abort

Fig. M22.10 - KDA Shelf Definition screen

**Note:** This section includes instructions for defining the BAC for KDA — for detailed information on defining a KDA unit, see Software Module 3 (Files Maintenance > KDA Shelves).

**Table M22.L - Fields in the KDA Shelf Definition screen**

Field	Description
Site Number	3-Digit site number. This number must be unique over the entire alarm network. It is used to describe this KDA remote, including satellites and expansion cards. This number is the address field for responders, derived alarms and labeled controls. (1-999)
Description	41-Character description of site.
Site Name	15-Character site name. This will be stamped on every event from this RTU.
Base Sat 1 Sat 2 Sat 3	Indicates base or satellite KDA position.
Host	Type of KDA unit. Select KDA-TS from default box (other models will be available in the future).
Expansion	Type of expansion card in host. For Base unit select NONE, LR-24 or 16, or BAC. CHAN ANALOG from default box. For satellite unit select NONE or LR-24 from default box.
Dedicated Port	If the KDA reports on dedicated line (DCPF) enter the T/MonXM port number. (Port must have been previously defined.) If KDA reports only on a dial line enter 0 (skips to Dial Port field).
Base Addr	Enter DCPF address for base unit (1-255). (This is the address that T/Mon will use to poll the KDA.)
Exp Addr #1	Expansion card address #1 (for 16 Chan Analog, or other expansion card in the base unit.)
Exp Addr #2	Expansion card address #2 (for future use to support 2 address exp. cards)
Dial Out Port	Enter port number used for dial, if dial only or alternate path routing is used. Enter "0" if dedicated line only (skips out of edit mode).
Remote Site Phone	Enter Phone Number to reach remote.
Polling Type	Select Periodic or Schedule from the default box. If periodic is selected, the cursor will skip to the Polling Interval field. If Schedule is selected, the cursor will skip to the Scheduled Days field.
Polling Interval	Periodic polling only. 0 to 9999 minutes. (0 = never) (Skips out of edit mode after entering value.)
Test	Enter the number of minutes (0 to 9999) between dial-up integrity tests. This causes T/Mon to check the status of the dial-up link while the primary link is still functional. If T/Mon calls the unit and there is no response from the modem, an alarm condition will occur. The alarm will appear as an internal alarm.
Scheduled Days	Schedule Polling only. For each day of the week enter "Y" to activate polling, enter "N" to deactivate.
Scheduled Hours	Enter the whole number of each hour (24 hour clock) to place a polling call (0 to 23, where 0 = midnight). Example: 0,8-16 polls at midnight and every hour from 8 AM to 4 PM.
Scheduled Minutes	Enter the whole number of the offset from the hour each call is to be made (0-59 where 0 = on the hour). Example: 30 polls at half past the hour.

**Table M22.M - Key commands available in the KDA Shelf Definition screen**

Function Key	Description
F1	Device - Takes you to the Base KDA Shelf Address Definition screen.
F2	Provisioning - Takes you to the Provisioning Target Menu.
F3	Internal Alarms - Brings up a screen for assigning device fail and off-line internal alarms. Follow prompts to specify address, display and point for each device. (Address must be 11 or 12.)
F10/Esc	Exit.

**Step 3 - Define Site Definition**

From the Master menu, select Files, Building Access, and then Sites/Zones. Enter the appropriate information into the Site Definition fields. See Table M22.C for field names and descriptions.

The Site definition screen allows the user to define a physical relationship in the remote sites between the doors, zones, and sites. In order to save databasing time, managers can also setup groups of doors that can be assigned to a set of users (instead of entering site/zone information for each separate user). Once a user profile is setup (see Step 4 on section M22-7), the user can be assigned to a group of doors instead of assigning doors to a user.

Sites / Zones									
Ref	ID	Description	Win	Type	Port	Dvc	Adr	Dsp	Pt Door List
1	002	Site 1 Perimeter	31	BAC	K2		1		1-4
2	003	Site 2 Comp Room	31	BAC	K2		1		5-6
3	004	Site 3 Generator	31	BAC	K2		1		7-8
4	005	Site 4 Storage #1	32	BAC	K2		2		1-2
5	006	Site 5 Storage #2	33	BAC	K2		2		3-4
6									
7									
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
Site Number <001-999>									
F1=Goto, F3=Blank, F8=Save, F9=Help, F10/Esc=Exit									

**Fig. M22.11 - Select Building Access and the Site Definition from the Files menu****Steps 4, 5, and 6**

For more information on defining BAS user profiles and ECU display mapping, see sections M22-7 through M22-9. Also refer to section M22-11 for BAS Global options and M22-12 for Site Login Status information.



## DTMF Access

**Note:** DTMF Building access requires a dedicated port. This port cannot be used for any other devices.

This section is provided to support existing systems using DTMF/ASCII converter, which is not available for new installations.

This function requires the BAU software module. If your T/MonXM is not equipped with this module, this function will not appear on the Parameters menu.

### Overview

This section is a step by step procedure for configuring T/MonXM to use the BAU module for DTMF building access.

1. Configure T/MonXM for DTMF login.
  - A. Define a remote port.
  - B. Define alarm forwarding variables.
  - C. Define options
  - D. Define a personal ID number
  - E. Define a site ID number
2. Log in to the T/MonXM alarm center.
3. Monitor site log in.
4. Log off from the T/MonXM alarm center.

### Step 1 - Configure T/MonXM for DTMF login

The first step in setting up DTMF building access is to configure T/MonXM for DTMF login. To use DTMF login follow the subsequent procedure:

#### Step 1.A. - Define a remote port

1. Selecting Remote Ports from the Parameters menu (press R to select Remote Ports and press Enter) will allow you to select the remote terminals and define the parameters for the remotes.
2. To begin remote port definition, you must first select a port to be defined. Press “F” and enter the port number. You can also use the “P” (previous) and “N” next keys to move up and down the full list of available ports (1-4 standard, up to 24 optional).
3. Press “E” for edit and the cursor will be placed at the Port Usage field. Press the Tab key and select DTMF Log In from the list box by pressing Enter.
4. Enter the appropriate serial format settings — see Figure M22.12 and Table M22.M.

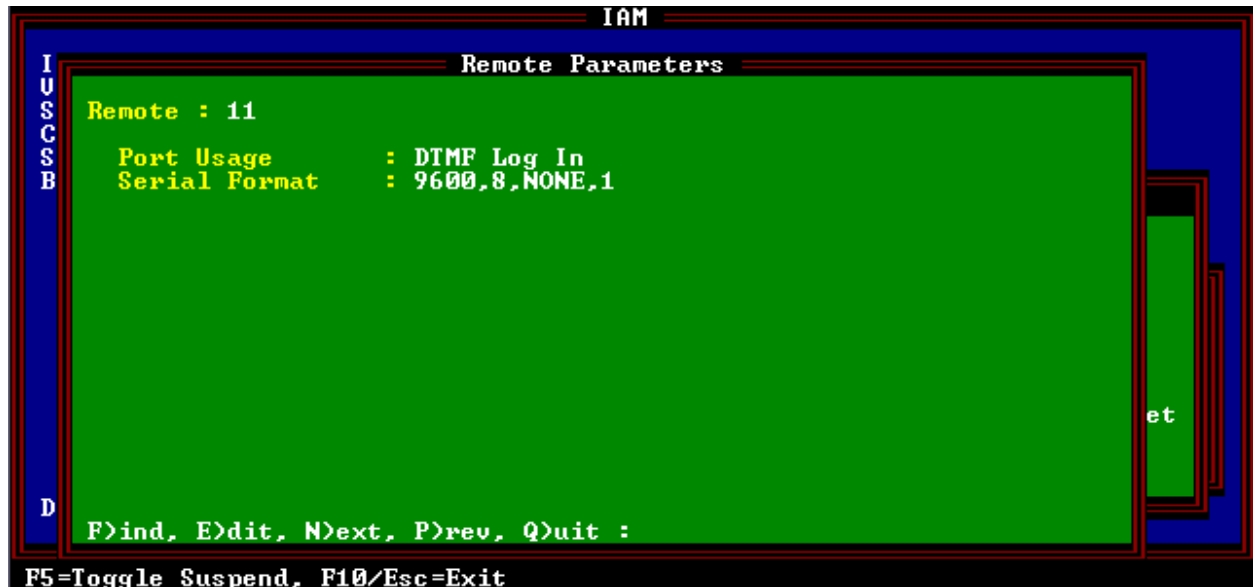


Fig. M22.12 - Remote port defined for DTMF Log In

Tbl. M22.N - Field names and descriptions for the Remote Parameters screen

Field Name	Description
Port Usage	Valid port types are DTMF Log In and Halted. Use Halted if no device is connected to the communication port. [Halted]
Serial Format	Baud rate, data bits, parity, and stop bits.[9600, 8, NONE, 1]

The following table lists the hot keys you can use while in the Remote Parameters screen.

Tbl. M22.O - Hot Keys available in the remote parameters screen

Function Key	Description
F5	Allows you to define but temporarily suspend use of this port. Toggles the suspension state. Available only when cursor is on the prompt line at the bottom of the window.
Up Arrow	Move to the previous field
F8	Save
F9	Help
F10/Esc	Move to the first field or exit without saving (depending on which field the cursor is in)
Tab	List port usages (while cursor is in the Port Usage field)

**Step 1.B. - Define Building Access variables**

Select Building Access from the Parameters menu by pressing “g” to select Building Access and press Enter. Refer to Figure M22.13.

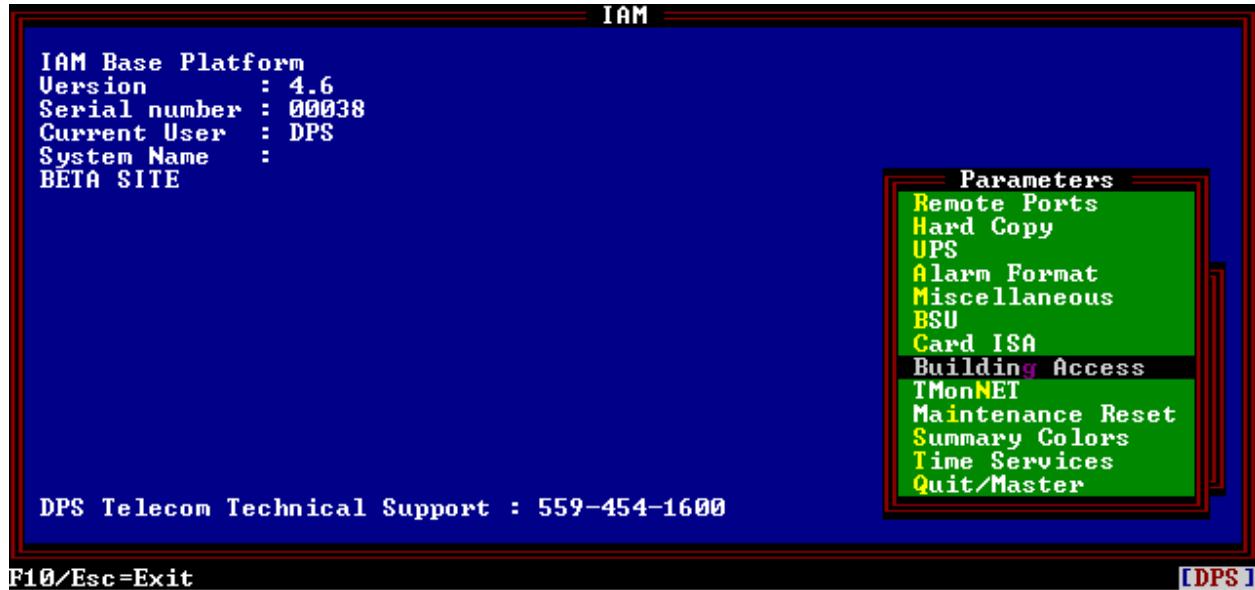


Fig. M22.13 - Select building access from the Parameters menu

A submenu appears listing selections for both DTMF access and BAU access. See Figure M22.14.

Select the General option and press Enter. The Building Access screen, as shown in Figure M22.15, will appear.

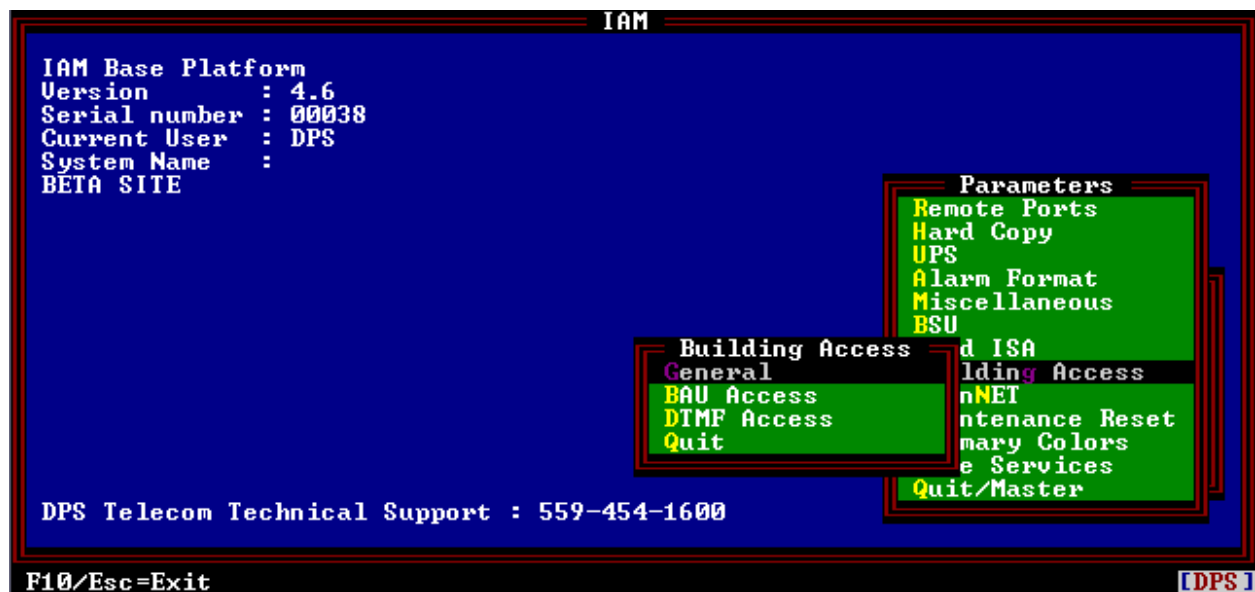


Fig. M22.14 - Select general from the Building Access submenu

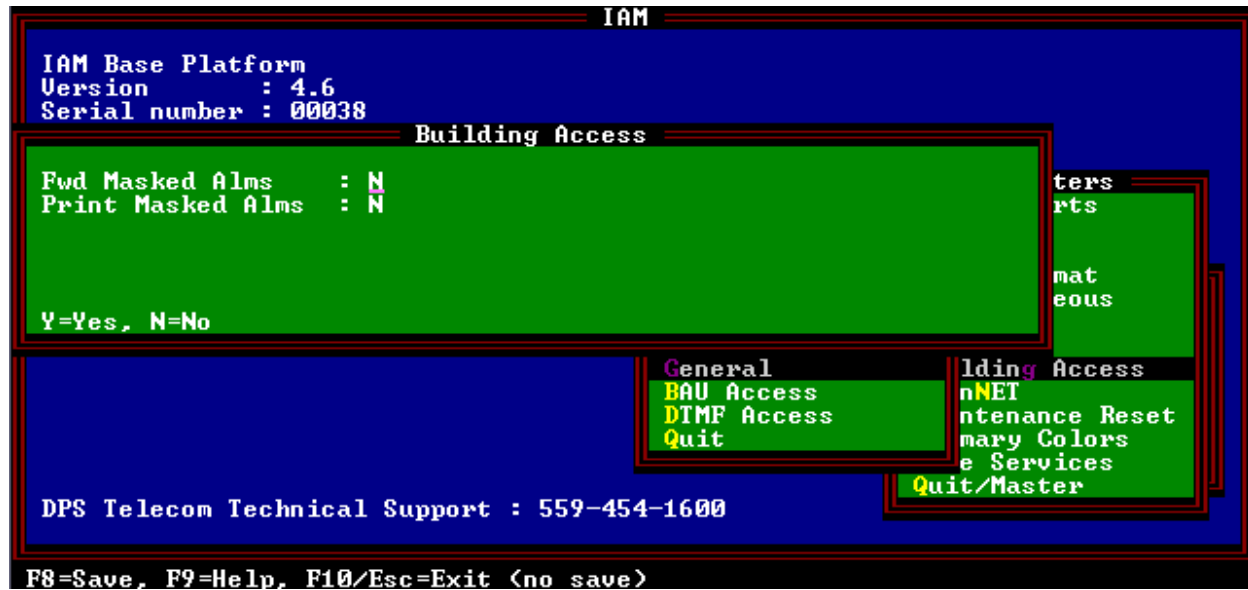


Fig. M22.15 - Define alarm forwarding variables

Building Access alarms are normally masked from the regular alarm display in monitor mode. (Press Ctrl-F3 while in the Alarm Summary screen to display building access status.) These masked alarms can be forwarded via a com port to another monitoring location or can be sent to a printer. Refer to Table M22.O for field definitions.

Tbl. M22.P - Field descriptions for the Building Access window

Field Name	Description
Fwd Masked Alms	Forward masked alarms. This allows you to send masked alarms to a location specified in the Alarm Forwarding Port.
Print Masked Alms	Print masked alarms. This allows you to print your masked alarms.

**Step 1.C. - Define Options**

From the Building Access menu, select DTMF Access and press Enter.

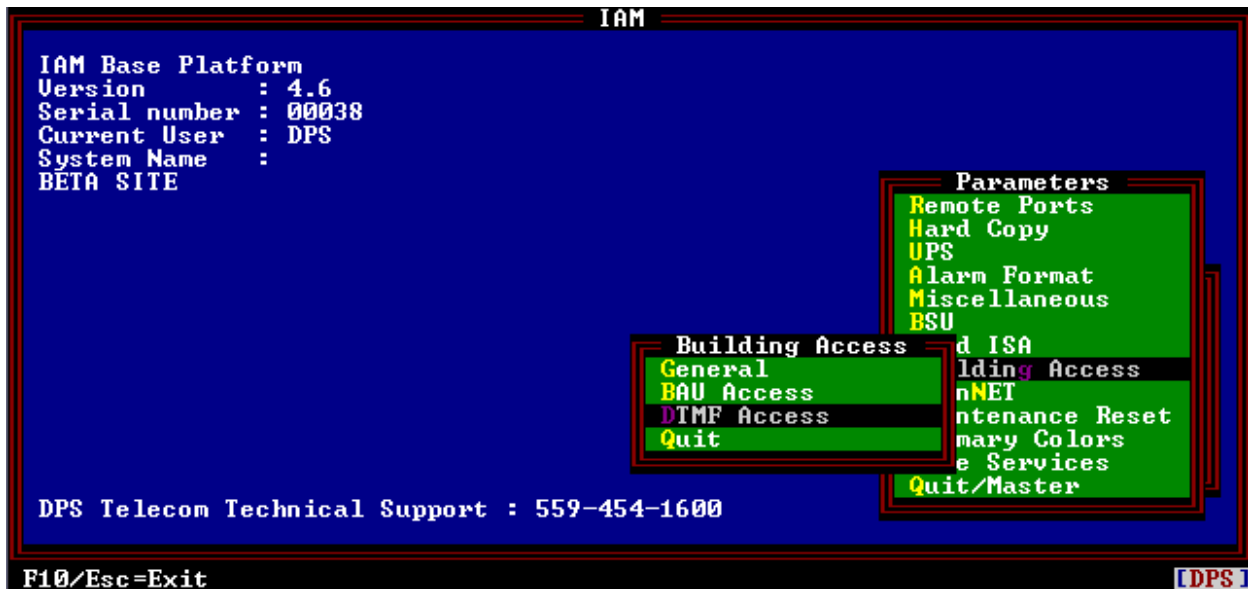


Fig. M22.16 - Highlight DTMF access and press enter

The DTMF Access screen will appear — see Figure M22.17. Refer to Table M22.P for field descriptions. Complete the fields with the appropriate information.

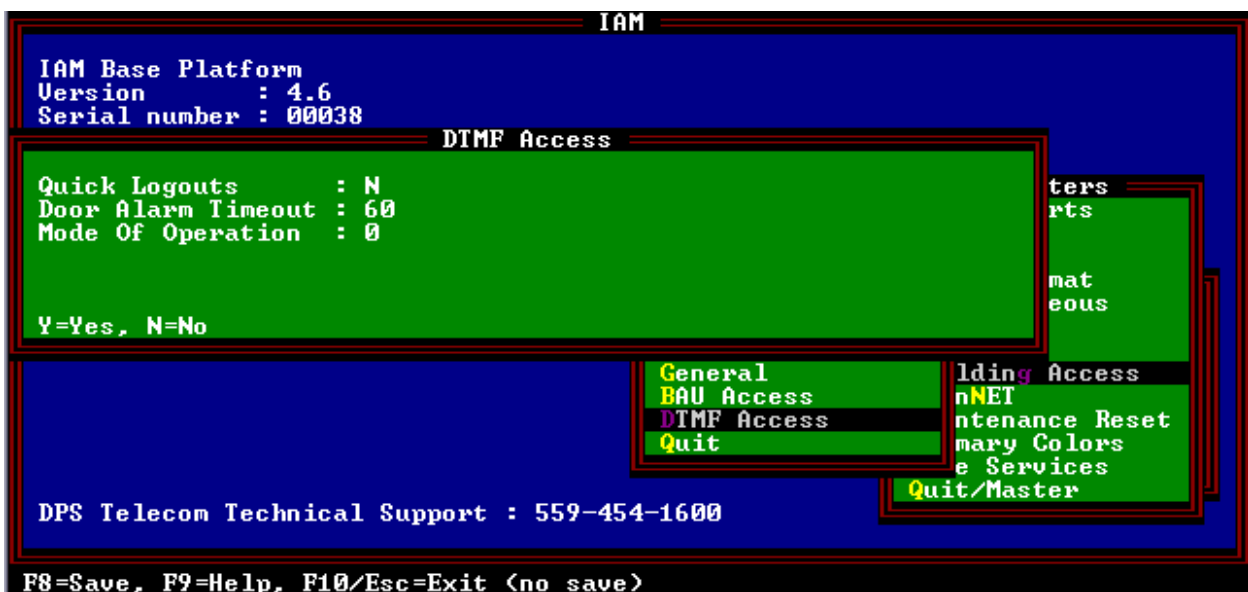


Fig. M22.17 - DTMF access options are set in the DTMF access window

**Tbl. M22.Q - Field names and descriptions for the DTMF access window**

Field Name	Description
Quick Logouts	Selecting "Y" requires only the site ID to be entered. "N" requires site ID and password.
Door Alarm Timeout	Amount of time from door opening until an internal alarm is generated by T/MonXM. You must be logged in before this time expires to prevent an alarm.
Mode of Operation	"0" is standard. Selection "1" is special options only for one user.

**Step 1.D. - Define a personal ID number**

Select the system users option from the File Maintenance menu to define the personal ID number that allows you to log in at a remote site. Then press E)dit from the command menu at the bottom of the screen. Press Enter until you reach the ID number field. Select a 3-digit number to be used for personal ID. Valid ID numbers are 001-899. A blank entry here indicates no site access.

The personal ID number is also displayed on the Monitor Mode Alarm Summary screen on the name of the window assigned to the login site.

**Step 1.E. - Define a site ID number**

Define the site ID number by going to the File Maintenance menu > Building Access sub-menu > Sites/Zone option The Sites/Zone Definition screen will appear — see Figure M22.18. At this screen you can define a 3-digit site ID number and the window that will be used to report the login.

The fields in the Site Definition screen are listed in the following Table M22.Q.

Sites / Zones										
Ref	ID	Description	Win	Type	Port	Dvc	Adr	Dsp	Pt	Door List
1	123	YALE OFFICE	4	BAU	5		2	1		
2	456	MADERA OFFICE	5	BAU	5		3	1		
3	789	NORTH LAB MAIN ENTR	25	DTMF	5		1	1	12	
4	...									
5										
6										
7										
8										
9										
10										
11										
12										
13										
14										
15										
16										
17										
18										
Site Number <001-999>										
F1=Goto, F3=Blank, F8=Save, F9=Help, F10/Esc=Exit										

**Fig. M22.18 - Site definition screen**

**Tbl. M22.R - Field descriptions for the site definition screen**

Field Name	Description
Entry	Site definition reference number. This field cannot be edited.
Site ID	The site ID is a unique 3-digit numeric code used when logging into a site. Valid site numbers are 001-899. You must enter 3 digits.
Win	Window to report the login/logout. Valid windows are 2-29 with standard features. Installation of alarm window modules will allow access to more windows. Each site must be assigned to a unique window. No two sites can share the same window.
BAU Source Data Use	Select "D" for DTMF use (The Port, Addr and Disp fields are used with the BAU).
Description	This is the description that will appear in the alarm that is generated when someone logs in or out of a site.

**Tbl. M22.S - Hot keys available in the site definition screen**

Function Key	Description
F1	Go to. Allows you to jump to a specific site reference ID by typing in the reference ID number.
F2	Insert. Insert a new line at the current position and moves everything down by one. Note: If the very last entry contains data, a warning will appear to confirm insertion. If there are any blank lines available, use DEL (F4) to delete them. This will make more space to insert.
F3	Blank. Blanks out all the information in the line where the cursor is currently located.
F4	Delete. Deletes entire line at current position. Similar to F3 but will move everything up by one.
F8	Save. Saves the configuration information and returns you to the previous screen.
F9	Help. Brings up the help menu.
F10/Esc	Exit. Returns you to the previous screen/menu.

**Step 2 - Login to the T/MonXM alarm center.**

Login to the T/MonXM from a remote site. To login, call the T/MonXM alarm center from any telephone. An automated voice will ask you to enter data. Enter the 3-digit site ID first, followed by your 3-digit Personal DTMF login ID. The automated voice will tell you that the location entry has been accepted. At that point you can hang up the phone.

**Step 3 - Monitor the site login**

To see a remote site login select the Monitor option from the master menu. On the Alarm Summary screen, the window defined for the site's alarm reporting will display three characters of the window name overwritten with the initials of the last person that has logged in. Since logins and logoffs are reported to the window defined for that site's alarm, they can be seen from the COS and Live alarm screens.

**Step 4 - Logoff from the T/MonXM alarm center**

The DTMF logoff procedure is similar to the logon procedure. The exception is that after you enter your site and personal ID numbers you must enter an asterisk. The automated voice will tell you that the location entry withdrawal has been accepted.

A site logoff will remove the personal ID from the Alarm Summary window name defined for that site's alarm reporting.

## Building Access Unit (BAU)

**Note:** The BAU application does not require a dedicated port. It does however, require a port that is defined for either TBOS or DCM protocol. A BAU that is reporting directly to T/MonXM needs to use a TBOS Port. A BAU that is reporting indirectly through a DPS Modular Alarm Transmitter (via a Smart Bypass Card) needs to use a DCM Port.

### Overview

The following is a step-by-step procedure for configuring T/MonXM to use the Building Access Manager module for BAU building access.

1. Configure T/MonXM for network BAU login.
  - A. Define a remote port.
  - B. Define alarm forwarding variables
  - C. Define BAU access parameters
  - D. Define the alarm points
  - E. Define a personal ID number
  - F. Define a site ID number
2. Login to the T/MonXM alarm center.
3. Monitor site login.
4. Logoff from the T/MonXM alarm center.

### Step 1 - Configure T/MonXM for BAU login

The first step in setting up the BAU for building access is to configure T/MonXM for BAU login using the following procedures:

#### Step 1A. - Define a remote port

Selecting remote ports from the Parameters menu (press R to select Remote Ports and press Enter) will allow you to select the remote terminals and define the parameters for the remotes.

If the port for the BAU has already been defined, proceed to B. If not, define the port per the TBOS (see Figure M22.19 and refer to Software Module 9) or DCM Interrogator (see Figure M22.20 and refer to Software Module 8) and then return to B in this section.

#### Step 1B. - Define alarm forwarding variables.

Select building access from the Parameters menu (press G to select Building access and press Enter). Refer to Figure M22.13.

A submenu appears listing selections for both DTMF Access and BAU Access. See Figure M22.14. Highlight General and press Enter.

Building Access alarms are normally masked from the regular alarm display in Monitor Mode. (Press Ctrl-F3 while in the Alarm Summary screen to display BAU status.) These masked alarms can be forwarded via a com port to another monitoring location or can be sent to a printer. Refer to Figure M22.15 and Table M22.N for field definitions.





Fig. M22.19 - Remote port defined for TBOS Interrogator

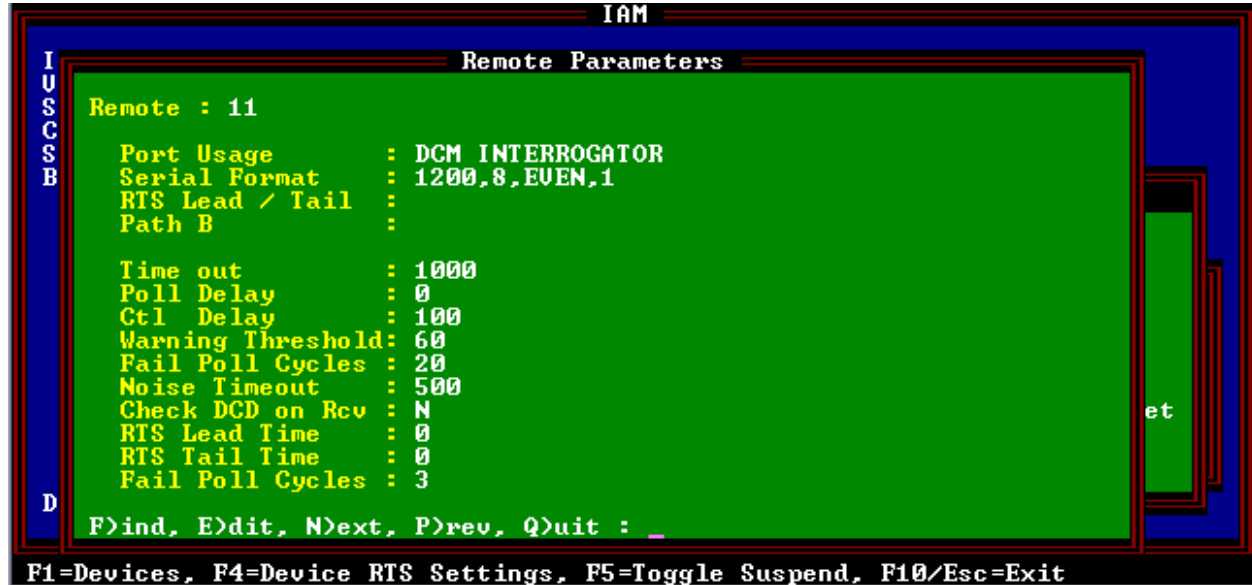


Fig. M22.20 - Remote port defined for DCM Interrogator

**Step 1.C. - Define BAU Access Parameters**

From the Building Access menu, select BAU Access and press Enter.

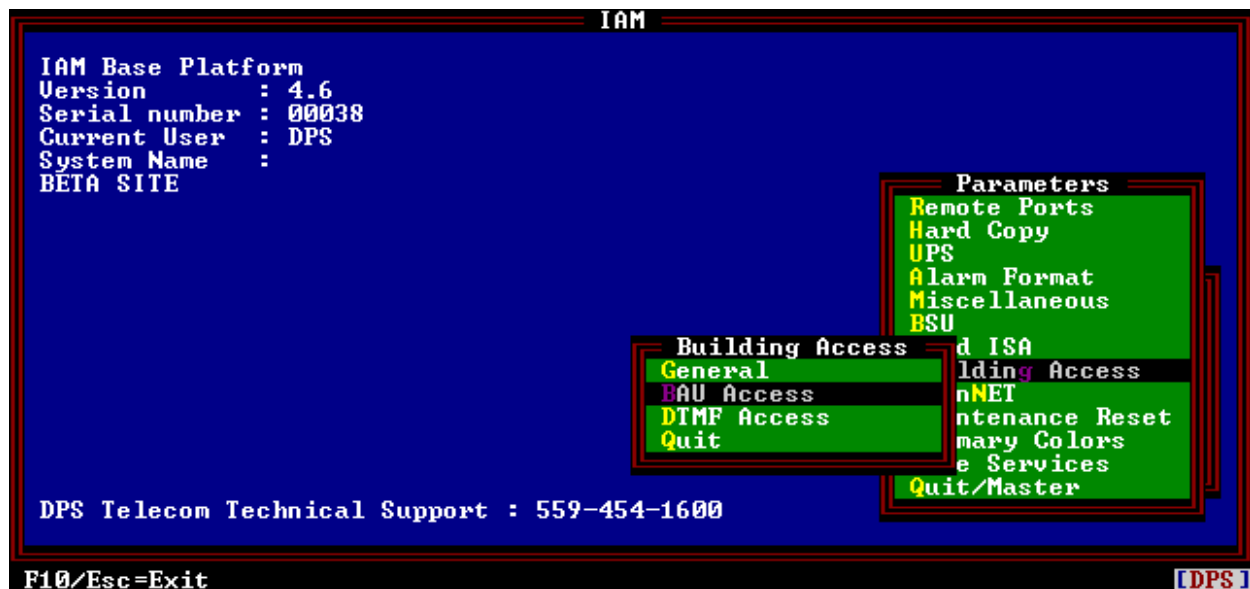


Fig.22.21 - Highlight BAU Access and press Enter

The BAU Access Parameters screen will appear — see Figure M22.22. Refer to Table M22.R for field descriptions. Complete the fields with the appropriate information.

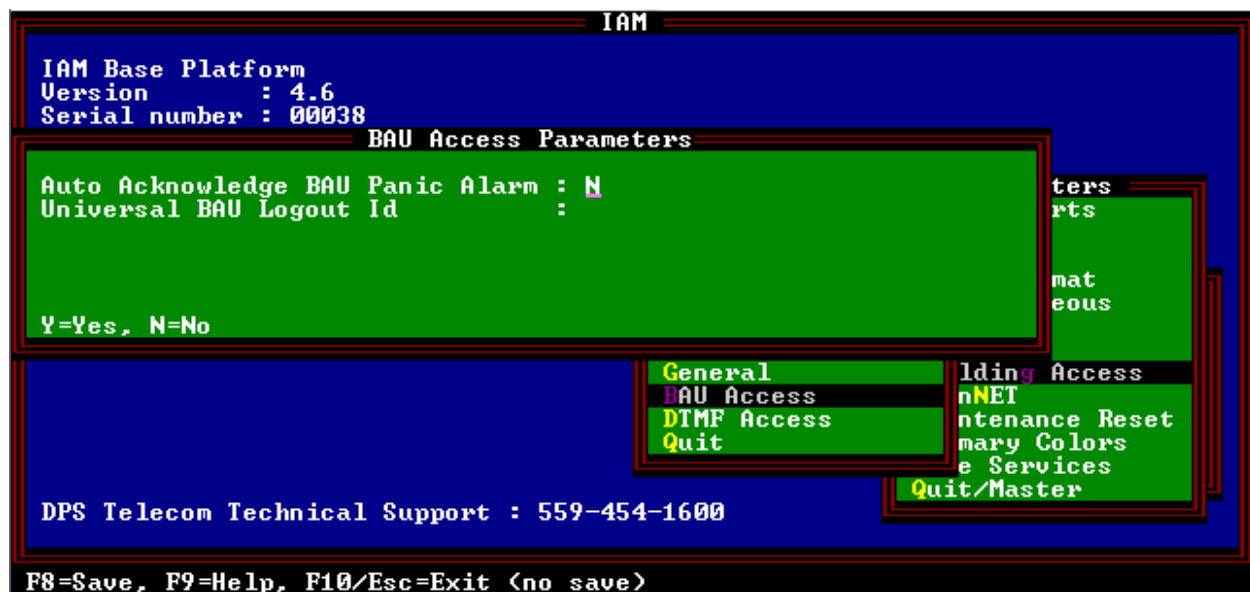


Fig. M22.22 - BAU Access Parameters screen

The BAU Access Parameters allow automatic operation of control point 7 (Clear Panic Alarm Point) as soon as a panic alarm is received. This selection eliminates the need to define control point 7 as either a site control or as a labeled control

The other parameter selection is for a universal logout ID code. It can be used when all logged in persons leave the building at the same time or at the end of a day to be sure all are logged out, incase someone may have left without logging out.

**Tbl. M22.T - Field descriptions in the BAU Parameters screen**

<b>Field</b>	<b>Description</b>
Auto Acknowledge BAU Panic Alm	When set to "Y" a command will automatically be sent to a BAU to acknowledge a panic alarm. When set to "N" the user must send the control manually.
Universal BAU Logout ID	Logout ID that will cause all persons logged into a site to be logged out. Starts re-arming in sequence.

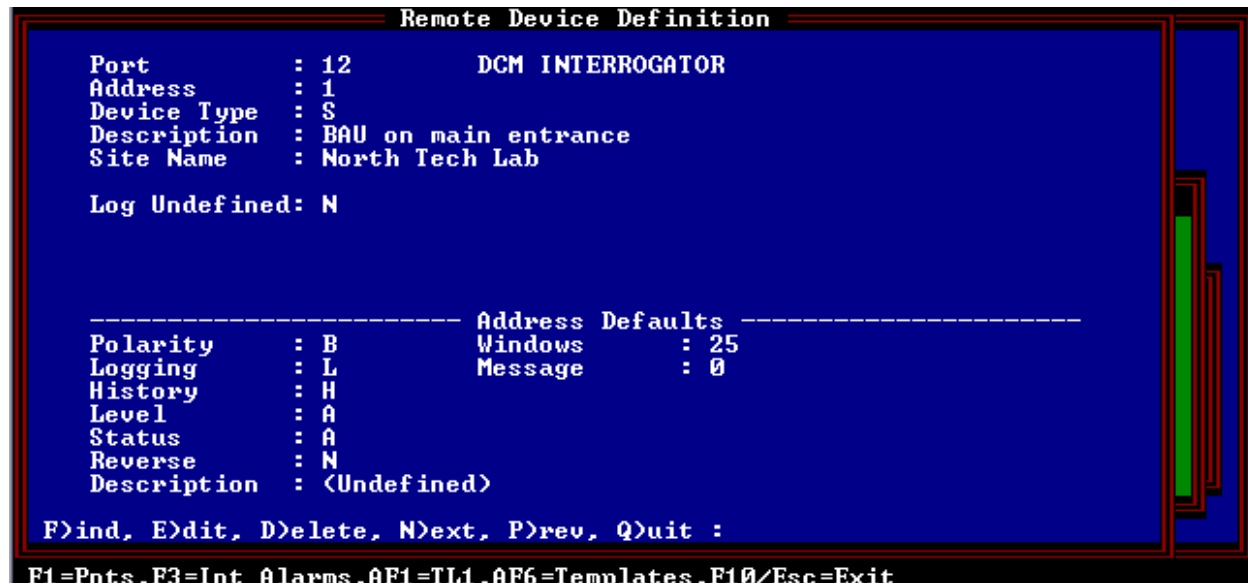


Fig. M22.23 - Remote device definition window

**Step 1.D.- Define the alarm points**

From the Master menu, select Parameters, then select Remote Ports and find the port assigned to BAUs from the Remote Parameters window.

Press F1 to reach the Remote Device Definition window. Find the address of the BAU to be defined and press F1 to reach the Point Definition window. Define the alarm points per instructions in the TBOS or DCM Module sections.

**TBOS Display Interpretation**

The following page describes the 64 alarm points on the TBOS display that are set/cleared by the BAU. The alarm point numbers are defined in T/MonXM under the Point Definition window. Points number are the same in either TBOS or DCM protocol.

**Hint 1:** Enter point 1 and copy to other 48 points.

**Hint 2:** All subsequent BAU definitions can be copied from the first definition.

**Point Definition**

Port : 12    Addr: 1    Disp: 1    Display Desc :

Pt	l	g	t	v	s	s	Description	Fail	Clear
49	B	L	H	A	A	N	Panic Alarm	SET	CLEAR
50	B	L	H	A	A	N	DOOR OPEN	OPEN	CLOSED
51	B	L	H	A	A	N	POWER UP	ALARM	NORM
52	B	L	H	A	A	N	RELAY	OPR	RLS
53	B	L	H	A	A	N	BUILDING OCCUPIED	OCC	UNOCC
54	B	L	H	A	A	N	ILLEGAL ENTRY	ALARM	CLEAR
55	B	L	H	A	A	N	NEED CONFIGURATION	YES	NO
56									

Enter polarity. B = bipolar, U = unipolar

**Message**

F1=GOTO, F2=Desc, F3=Blank, F4=Sect, F5=Range, F6=Read, F8=Save, F9=Help, F10/Esc=Exit

Fig. M22.24 - Point Definition window

Tbl. M22.U - Alarm point interpretations

Alarm Point Number	Interpretations
1-48	Reserved for internal communications. Set as no log and no history
49	Panic alarm
50	Door open alarm
51	Power up alarm
52	Relay status (This is set if relay is operated)
53	Building occupied alarm
54	Illegal entry alarm
55	Need configuration
56	Power loss at BAU or communications failure between BAU and SBC
57-64	Not used. Set as No Log and No History

**TBOS Controls Sent to the BAU**

Shown below is a description of the control points that can be sent to the BAU. Points 7, 9 and 12 are normally user operated. These must be defined as Site Controls, Labeled Controls or as Derived Controls before they can be operated. Control point 6 (clear power-up alarm point) is internally defined as a derived control point operating from alarm point 51. All other control points are for internal T/Mon use. Points number are the same in either TBOS or DCM protocol.

**Tbl. M22.V - BAU control points**

Control Point	Action
1	Valid entry code
2	Invalid entry code
3, 4, 5	Not used
6	Non-specific message ACK
7*	Clear panic alarm point
8	Declare building not empty
9*	Declare building empty
10	Request hardware information
11	Request firmware version
12*	Request serial number
13	Clear power-up alarm point

\*Normally user operated - All others for internal T/Mon use.

An option can be selected to automatically operate control point 7 to clear a panic alarm as soon as it is received by T/MonXM.

**Step 1.E. - Define a Personal ID Number**

Select the System Users option from the File Maintenance menu to define the personal ID number that allows you to log in at a remote site. Then press E)dit from the command menu at the bottom of the screen. Press Enter until you reach the ID number field. Select an 8-digit number to be used for personal ID. Valid ID numbers are 1-89999999. A blank entry here indicates no site access.

Note: A users personal initials (defined at the top of the System Users screen in the "Initials" field) is displayed on the Monitor Mode Alarm Summary screen on the name of the window assigned to the logged-in site.

**Step 1.F. - Define a site ID number**

Select the Building Access option from the File Maintenance menu allows you to access the Site Definition screen. At this screen you can define a 3-digit Site ID number and the window that will be used to report the login. An example of the Site Definition screen is in Figure M22.18.

The fields in the Site Definition screen are listed in Table M22.U.

**Tbl. M22.W - Field names and descriptions for the site definition screen**

Field Name	Description
Entry	Site definition reference number. This field cannot be edited.
Site Id	The Site ID is a unique 3 digit numeric code used when logging into a site. Valid site numbers are 001-899. You must enter 3 digits.
Win	Window to report the Login/Out. Valid windows are 2-30 with standard features. Installation of Alarm Windows modules will allow access to more windows. Each site must be assigned to a unique window. No two sites can share the same window.
BAU Source Data Use	Enter BAU.
BAU source Data Port	Enter the port number for the door alarm. Valid Port numbers are 1-28
BAU source Data Addr	Enter the address of the source data. This field will be skipped over if not needed.
BAU source Data Disp	Enter the display number. Valid display numbers are 1-8. <b>Note:</b> The Port, Address and Display must be unique. You cannot assign another site with the same Port, Address and Display.
Description	This is the description that will appear in the alarm that is generated when someone logs in or out of a site.

**Step 2 - Login to the T/MonXM alarm center (testing)**

The next step is to login to T/MonXM from a remote site. To login, enter your 8-digit personal BAU ID number followed by a “#” pound sign. At that point you are logged in.

**Duress entry login**

A special security login called a Duress Entry Login can be utilized when personnel are forced to login to a site.

To login, using a duress entry login, enter your 8-digit personal BAU ID number prefixed by a “9” and followed by a # sign. For example, a duress login could result in the following sequence: “912345678#”.

**Step 3 - Monitor the site login**

To see a remote site login, select the monitor option from the master menu. On the alarm summary screen, the window defined for that site’s alarm reporting will have the last three characters of the window name overwritten with the personal initials of the last person that has logged in will be displayed. Since logins and logoffs are reported to the window defined for that site’s alarm, they can be

seen from the COS and Live alarm screens.

-or-

Select the site logon screen by pressing Control-F3 from the Alarm Summary screen. This screen shows the name and location of each person who has logged in, what time they entered the building and the elapsed time.

Since logins and logoffs are reported to the window defined for that site's alarm, they can be seen from the COS and Live alarm screens.

#### Step 4 Logoff from the T/Mon alarm center

The next step is to logoff from T/MonXM from a remote site. To logoff, enter your 8-digit personal BAU ID number followed by an "\*" asterisk sign. Then open and close the door. At that point you are logged off.

#### Duress Logout

A special security logout call a Duress Entry Logout can be utilized when personnel are forced to logout of a site. To logout, using a Duress Entry Logout, enter your 8-digit personal BAU ID number prefixed by a "9" and followed by an asterisk. For example, "912345678\*".

Refer to the Building Access Unit (Network Version) operation guide for specific details about operation on the BAU at the remote site.

## Site Report

Selecting reports from the master menu allows you to print a report of the site definitions. An example of a site report is shown in Figure M22.26.

```

Dial Up Sites                                     Page 1
Report generated on 4/15/05 at 4:52pm by DPS
Select Device: KDA Start Site: 1End Site: 100
*****
Device Type           :KDA
Site Name             :1
Description           :DEL MAR HUT (OAK ST)
Remote Site Phone     :222344444
Polling Type          :SCHEDULE
Schedule Days -- SUN: N   MON: Y TUES: Y   WED: Y THU: Y FRI: Y SAT:
N
Schedule Hours       : 5,8,12,15,18,22
Schedule Minute      : 30
Output modem chan    : 7
  
```

**Fig. M22.26 - Site report printout**



## Frequently-Asked Questions (FAQs)

### **Q: What is the difference between Stay-Open mode and Propped Door mode?**

**A:** Stay-Open mode will unlock the door and allow it to be opened and closed without a door violation. It will stay in Stay-Open mode until a stay-open card/code is used to disable Stay-Open mode. The door can also be kept open for as long as needed. In Propped Door mode, the door may only be left open for a certain period of time (15 min.) before a slow beep starts warning the user. This will eventually turn into a door violation in Propped Door mode.

### **Q: How do I enable/disable Stay-Open mode?**

**A:** There are several ways of doing this. One way is to use a stay-open card. This is a card or code that has the stay open setting enabled. When this card/code is used, it will put the unit in stay open mode. Another way to enable stay open mode is to use the T/Mon to send an OPR command to the ECU's point 22 and 17. To disable stay-open mode, send an RLS command to points 22 and 17 or use another stay-open card/code on the card reader/keypad. (see table M22.G – ECU Mapping on control points)

### **Q: How do I send a Propped Door command?**

**A:** The propped door point is set on point 21 (see table M22.G). Define a Labeled Control on the T/Mon that would send a MON command to the ECU on point 21. When in Monitor mode, push Ctrl + F8 to bring up the labeled controls window. Select the control for point 21 and press Enter.

Note: ECU displays start on display 3 on the T/Mon. So ECU 1 on the NG would be display 3 on T/Mon.

### **Q: What is the difference between a site and a zone?**

**A:** A site is defined with only one door. A zone is a site that has multiple doors defined. These are all defined on the T/Mon under Files -> Building Access -> Sites / Zones. A single site number with only 1 door under door list would be considered as a site. A single site number with more than 1 door under the door list would be considered as a zone.

### **Q: What does the Login Expire setting do in the BAS Global Options window?**

**A:** It will automatically log users out of the Site Login Window when in monitor mode. This can be viewed by being in Monitor mode and pressing Ctrl + F3. This window will display all users that have logged in. Usually, when a card is used on a card reader for the first time, it will log them in. Then the second time they use the same card, it will log them out. But when the Login Expire setting is set for anything other than zero, it will not log users out. It will reset their entry time and allow the timer to log them out when it expires.

Login Expire takes values between 1 to 24 hours. This is how long the system will allow users to be logged in before automatically logging them out. If it is set to 1 hour, it automatically log users out if they have been logged in for more than 1 hour. The T/Mon scans this list every 15 minutes for anything that needs to be logged out. When this is set to zero, it will disable auto log outs. Which means that the second card read would log users out.

### **Q: How do I handle the need for extended propped doors?**

**A:** Using the Stay-Open mode would allow the door to stay open for a longer period of time. This is done by sending an OPR command to points 17 and 22 to the ECU (see question about enabling/disabling Stay-Open mode). The door will remain open until it is taken out of Stay-Open mode.

### **Q: How do I “buzz” a person in?**

This can be done remotely from the T/Mon by sending a MON command to point 17 (see table M22.G). This will unlatch the door long enough for the person to open and close it.

**Q:How do I limit access to the Building Access menu?**

One way of doing this would be to set user permissions so they cannot access File Maintenance. This is done by going to the T/Mon's master menu and going to Files -> System Users -> Users and setting File Maintenance to NO. However, this will restrict access to the entire File Maintenance menu. We currently don't have a way to restrict access to each individual submenus.

**Q: When I modify the expansion module setting on the T/Mon's NetGuardian page, it removes the entries under Site / Zones for that address. Why is this?**

**A:**Whenever the expansion module type changes, it deletes everything that use to make reference to it to make sure that data is valid. This includes the site/zone entry. If the site/zone entry had been left intact but the expansion module did not match, it would cause errors when it came to building or using the data.

**This page intentionally left blank.**

# Software Module 23

## Alarm Message Forwarding

The purpose of Alarm Forwarding is to send selected T/MonXM alarm data to another alarm master or master of masters in an easily parsed format.

Alarm message forwarding allows T/MonXM alarm information to be output in ASCII format via T/MonXM's remote access ports. To do this, the user selects a port as the forwarding output port. Then, after assigning the baud, parity, word length and stop bits the user assigns an alarm window to follow in T/MonXM as a forwarding window. All alarms that are assigned to the forwarding window will be displayed in that window. The alarms will also be sent out the selected port in the same format as they appeared on the screen. The last parameter (# of chars to transmit) is the number of characters to transmit per message.

For example: All of the power related alarms from each central office are assigned to window 8. The, window 8 is set to alarm forward to one of the remote ports. This port is tied to a printer in another location. At that time, all of the alarms from Window 8 are output to the printer. These alarms and all other alarms are only seen at the main workstation.

### Basic Operation and Setup

Installation of the optional alarm message forwarding software module is required to define or access a port for the Alarm Forward option. Refer Section 2 - Software Installation for installation procedures.

When the software module is installed, selecting Remote Ports from the Parameters menu will allow you to select and define the alarm forward port and parameters.

An example of the Remote Parameters screen defined for Alarm Forward is on the next page.



Fig. M23.1 - Example alarm forwarding text

**Note:** Format will follow alarm format seen in COS and Standing screens.

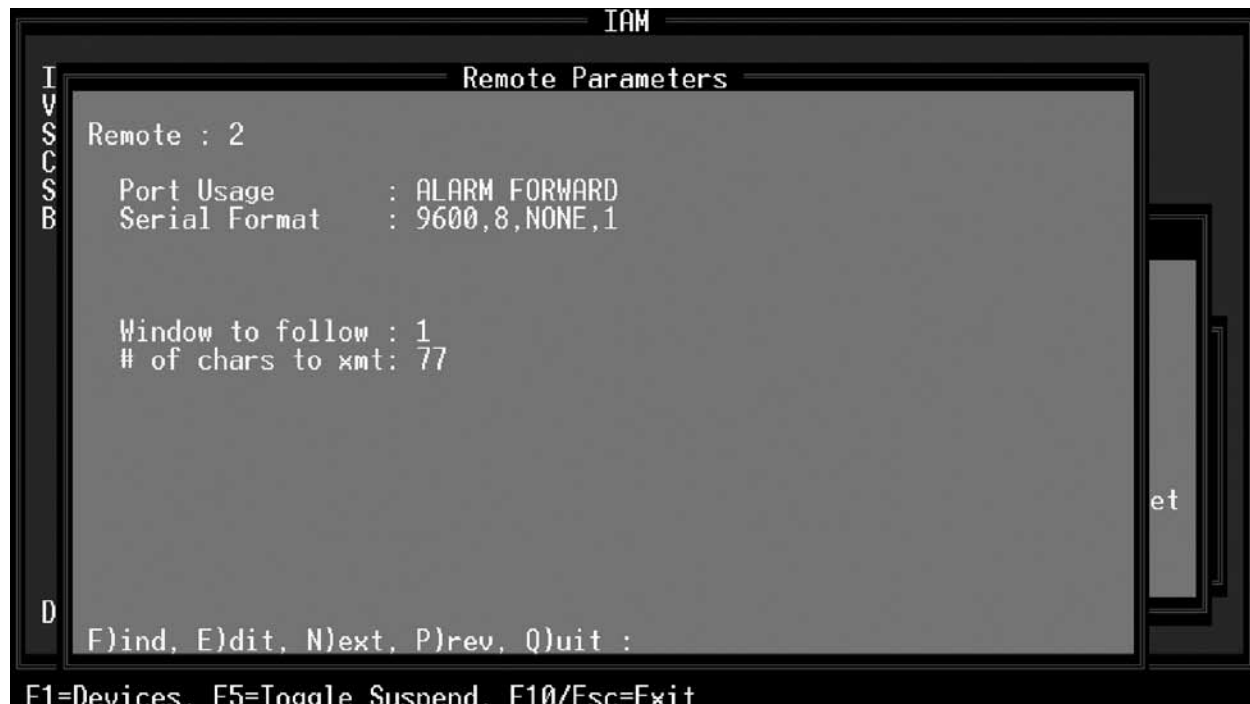


Fig. M23.2 - Remote Parameters screen defined for Alarm Forward

## Alarm Forward Parameters

**Note:** Alarm Forwarding can be assigned only to Intelligent Controller Card Ports (Ports 1-20).

### Port Usage

Enter Alarm Forward in the port usage field. Use Halted (default) to disable the port.

**Note:** The fields on the Remote Parameters screen vary according to port usage.

### Serial Format

Baud rate, word length, parity, and stop bits settings. Default values are 9600 baud, 8 bits, none, and 1.

### Window to Follow

Standard features allow 90 windows plus the All Alarms window. When you install the optional alarm window software modules, you will be able to access additional windows. Default value is Window 1 (All Alarms).

**Note:** You can assign windows to Alarm Message Forwarding without having security access to those windows.

### Number of Characters to Transmit

The valid range of characters to transmit per message is 10-200. Default value is 77.

# Software Module 24

## T/Mon SQL

The T/Mon SQL job is designed to store history events in a SQL database. Once in the SQL database they can be queried from any number of outside sources. The process of querying the SQL database will be left up to the user, but a data-dictionary is provided in this section. Storing history events in SQL database will make the T/Mon history events widely available. In order to accomplish this the T/Mon must forward it's history events via TCP to the T/Mon SQL Agent which will insert them into the SQL database. The T/Mon SQL Agent is used to manage the SQL database.

### Setup Overview

The configuration process consists of two parts:

- I. Configure the T/Mon SQL Agent  
and
- II. Defining a T/Mon SQL job

## I. Configure T/Mon SQL Agent

**Note:** MyODBC is required to connect to the user MySQL server. The MyODBC installer is included in the download package. DPS recommends that you use the MyODBC driver shipped with your T/Mon SQL software module. It has been tested and proven to be reliable. We have discovered that version 3.52 of the MyODBC driver does not work well with Microsoft Access.

The TMon SQL Agent receives history events from either multiple T/Mons or a single T/Mon and stores them into a MySQL database.

The following setup must be performed to configure the agent to communicate to a T/Mon.

1. Start the agent.
2. Click on the T/Mon Instance(s) menu and create a T/Mon Instance — see Figure M24.1.

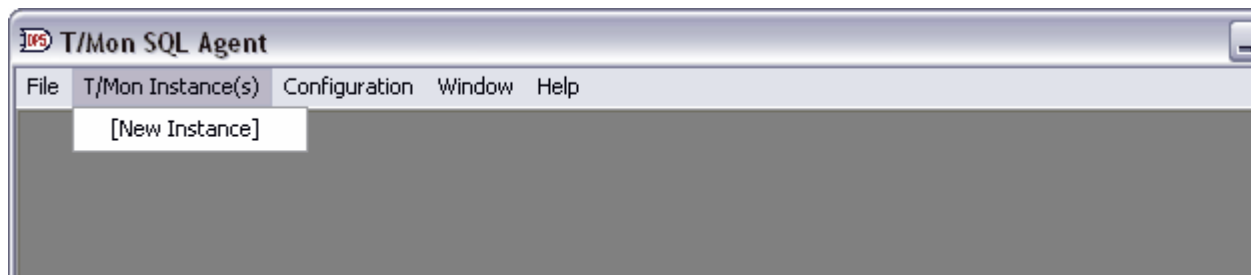


Fig. M24.1 - Click on the T/Mon Instance(s) menu and create a T/Mon Instance

The image shows a 'T/Mon Connection' dialog box. It is divided into two main sections: 'T/Mon Setup' and 'Database Connection Values'. In the 'T/Mon Setup' section, there are two text input fields: 'T/Mon Name:' which is empty, and 'T/Mon Port:' which contains the value '3000'. In the 'Database Connection Values' section, there are five fields: 'DSN:' is a dropdown menu currently showing '(None)'; 'UID:' is an empty text field; 'Password:' is an empty text field; 'Database:' is an empty text field; 'Driver:' is a dropdown menu; and 'Server:' is an empty text field. At the bottom of the dialog, there are four buttons: 'Reset Counters', 'Restart', 'OK', and 'Cancel'.

**Fig. M24.2 - T/Mon Instance configuration settings**

3. Configure the instance — see Figure M24.2.

There are two parts to configuring an instance:

A. The connection with the T/Mon. (The T/Mon connects to the agent)

- T/Mon name is a way for the user to identify what tmon will connect to that instance.
- T/Mon Port is what port the T/Mon will connect to.

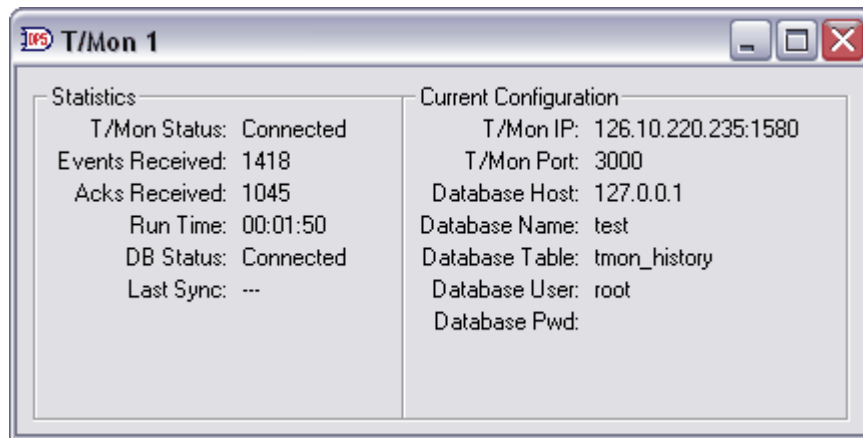
B. The connection to the database. The user can either use a preconfigured DSN or enter the connection info in manually. (They cannot do both)

- DSN is a preconfigured connection setup in windows.
- UID is the username used to connect the database.
- Password is the password used to connect to the database.
- Database is the name of the database that already exists on the database server that they will be connected to. (The connection will not work unless the database exists on the database server.
- Driver is the ODBC driver used to communicate to the database server. (This must be installed ahead of time)
- Server is the hostname or IP of the database server.

Click OK.

**NOTE:** See the following link for more information on how to setup a DSN connection: <http://dev.mysql.com/doc/mysql/en/dsn-on-windows.html>.

4. A T/Mon Instance will look like the following:



**Fig. M24.3 - T/Mon Instance configuration settings**

Repeat steps 2-3 to add another instance. Each T/Mon will need its own instance.

5. Save your configuration by pushing Ctrl-S or by selecting File -> Save, then choose the filename and location where you want to save the file. (The filetype is a .dat file)

### Changing Instances

Changing a instances configuration can be done by either selecting the instance window or by checking that instance in the T/Mon Instance(s) menu, then selecting Configuration > T/Mon Configuration.

### Reset Counter

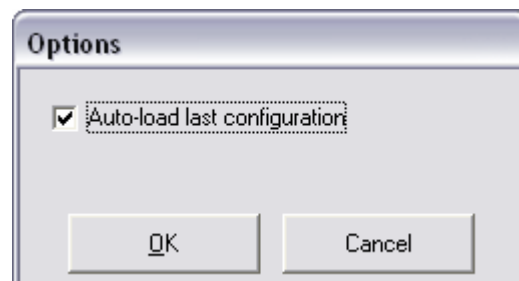
Reset Counter will reset the Events Received & Acks Received count.

### Restarting

Restart will restart a failed connection to the database server.

## I.A Application Options

To change application options, click the Configurations menu and select Options. In the Application Options box, check the box if you want to load the last configuration saved. This will be useful if the computer that is running the agent on reboots, and you have the SQLAGENT.exe in your windows startup. The agent will then start up and load your last configuration automatically.



**Fig. M24.4 - Check the box if you want to load the last configuration saved at startup**



### Creating New Configuration Files

Create a new configuration by selecting File > New and then create the configuration.

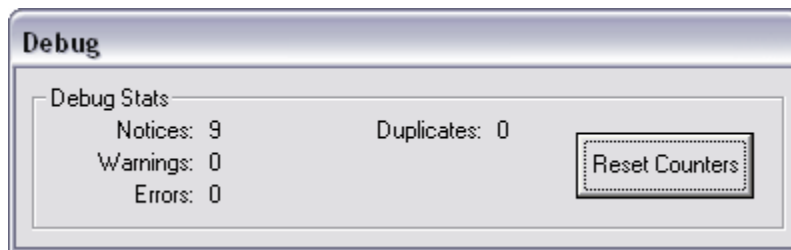
### Hide the Application Window

Hide application in the Windows System Tray by selecting Window > Hide to System Tray or push Ctrl-H.

## I.B Debug Mode

You can show the full program by right-clicking the DPS logo and selecting Show Full Program.

Debug mode has two parts: the Debug Stats as well as a TCP Socket Connection that allows the users in real-time to see the debug as it occurs.



**Fig. M24.5 - The Debug Status screen**

A debug.log file is created in the install directory for reference.

- Notices are normal status indications.
- Warnings are typically like duplicate port issues.
- Errors are when the agent can't talk to the database or there are fatal errors that will stop the program.
- Duplicates are when it tries to enter a record that already exists.

**Debug port:** A single user can make a TCP connection to the debug port 2002. Refer to Figure M24.6.

**Note:** If you receive any of the above error messages contact DPS Tech Support.

### Debug Reset Counter

Reset Counter will reset the Debug Stats count.

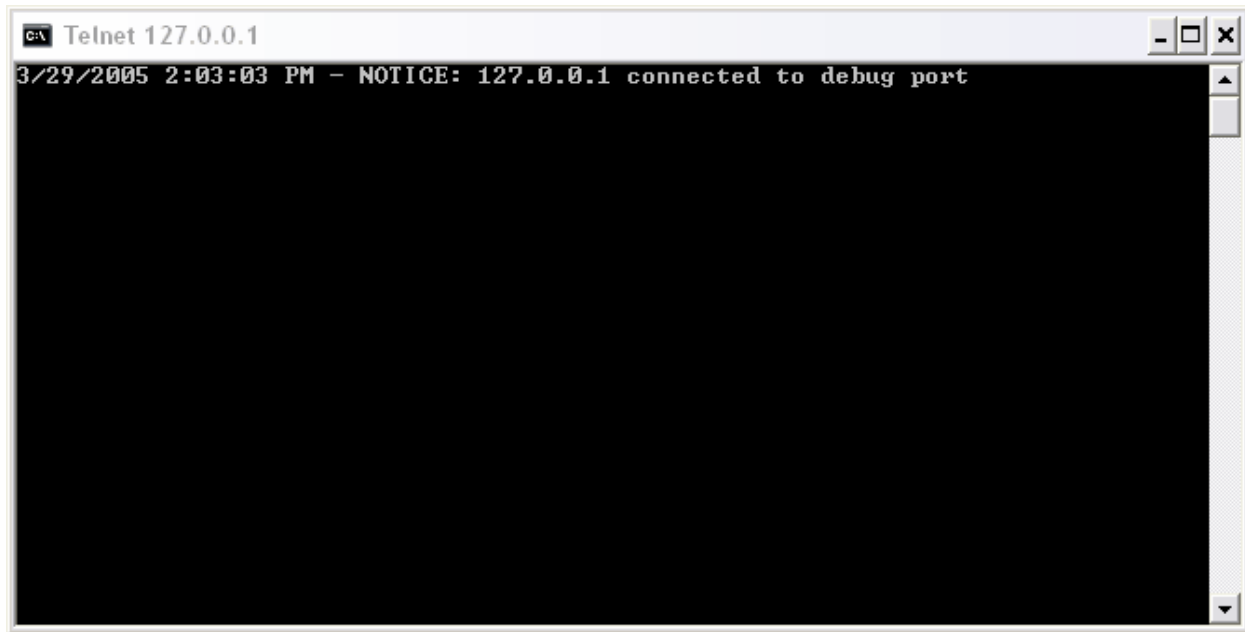


Fig. M24.6 - The TCP Socket Connection screen

## Data Dictionary

Table M24.A - (Tmon\_history) Data Dictionary field descriptions

Field Name	Field Type	Description	ArrowNull	Key	Default
IPAddr	varchar(15)	IP Address of the TMon.		PRI	
IPPort	smallint(6)	IP Port of the TMon.		PRI	0
EventDateTime	datetime	The date and time which the TMon received the event.		PRI	0000-00-00 00:00:00
Port	smallint(6)	The port which the TMon received the event on.			0
Address	smallint(6)	The address which the TMon received the event on.			0
Display	smallint(6)	The display which the TMon received the event on.			0
Point	smallint(6)	The point which the TMon received the event on			0
EventCounter	tinyint(4) unsigned	Forms a unique identifier when used in conjunction with the EventDateTime.		PRI	0
AckDateTime	datetime	The date and time which the event was acknowledged. This field is only relevant if the "Initials" field is not blank.	YES		

**Note:** Table M24.A continues on following page.

**Table M24.A - Data Dictionary field descriptions continued**

Field Name	Field Type	Description	ArrowNull	Key	Default
Initials	varchar(10)	The initials of the user that acknowledged the alarm.	YES		
AlarmState	char(1)	The state of the event. • 'S'=Silenced • 'C'=Cleared • 'F'=Set	YES	MUL	
AlarmLevel	char(1)	The severity level of the event. • 'A'=Critical • 'B'=Major • 'C'=Minor • 'D'=Status	YES		
SubDevice	char(3)	Name of the subdevice which reported the event.	YES		
SiteName	varchar(40)	Name of the site which reported the event.	YES		
PointName	varchar(40)	Name of the point which corresponds to the event.	YES		
AuxPointName	varchar(40)	Auxiliary name of the point which corresponds to the event.	YES		
AlarmStatus	varchar(8)	Description of the current status of the event.	YES		
DispDesc	varchar(40)	Name of the display which the TMon received the event on.	YES		
	datetime	The date and time which the device that reported the event to the TMon received the event.	YES		
TStamp	timestamp	Current timestamp used by Microsoft Access.	YES		CURRENT_TIMESTAMP

**Table M24.B - Data Dictionary key names and field names**

Key Name	Field Name	Collation	Cardinality
PRIMARY	IPAddr	A	
PRIMARY	IPPort	A	
PRIMARY	EventDateTime	A	
PRIMARY	EventCounter	A	7776
INDEX ack	Initials	A	
INDEX ack	AckDateTime	A	
INDEX ack	EventDateTime	A	

**Table M24.C - (file\_list) List of dat files that can be transferred to the SQL database.**  
**Used to determine if the file has changed and needs to be retrieved.**

Field Name	Field Type	Description	ArrowNul 1	Key	Default
IP Addr	Varchar(13)	IP address of T/Mon where packet came from		YES	
FileName	Varchar(15)	Name of T/Mon DAT file		YES	
TimeStamp	Varchar(30)	Timestamp of T/Mon DAT file			
CRC	Varchar(30)	CRC of received DAT file			0

**Table M24.D - (tmon\_history\_windows)**

This table contains the windows associated with each alarm point from the tmon\_history table.

Field Name	Field Type	Description	ArrowNull	Key	Default
IP Addr	Varchar(15)	IP Address of T/Mon where packet came from		YES	
IPPort	Smallint(6)	Port of the SQL connection on T/Mon		YES	0
EventDateTime	Datetime	The date and time which the T/Mon received the event		YES	0000-00-00 00:00:00
EventCounter	Double(4)	Forms a unique identifier when used in conjunction with the EventDateTime		YES	0
WindIDX	Smallint(6)	Windows index. This ranges from 1 to 8. Each alarm point on T/Mon can be associated with up to 8 windows.		YES	0
Window	Smallint(6)	Windows value. This is the window that an associated alarm would report to.			0

**Table M24.E - (DAT\_EMWIN)**

This table contains data from EMWIN.DAT on T/Mon

Field Name	Field Type	Description	ArrowNull	Key	Default
WinIdx	Smallint(6)	Tmon window index		YES	0
WinName	Varchar(15)	Window name	YES		
WinDesc	Varchar(41)	Window description	YES		

## II. Configure Settings for the T/Mon SQL Agent

Navigate to the Parameters > TMonNET > TMon SQL sub-menu. Here you will configure the settings necessary to communicate with the TMon SQL Agent.

The IP Address must be set to that of the system hosting the TMon SQL Agent and the Port must be the listening port of the TMon SQL Agent. The listening port can be configured in the TMon SQL Agent application. Make sure that the port selected is unused on the TMon SQL Agent since there can only be one TMon connected per Port.

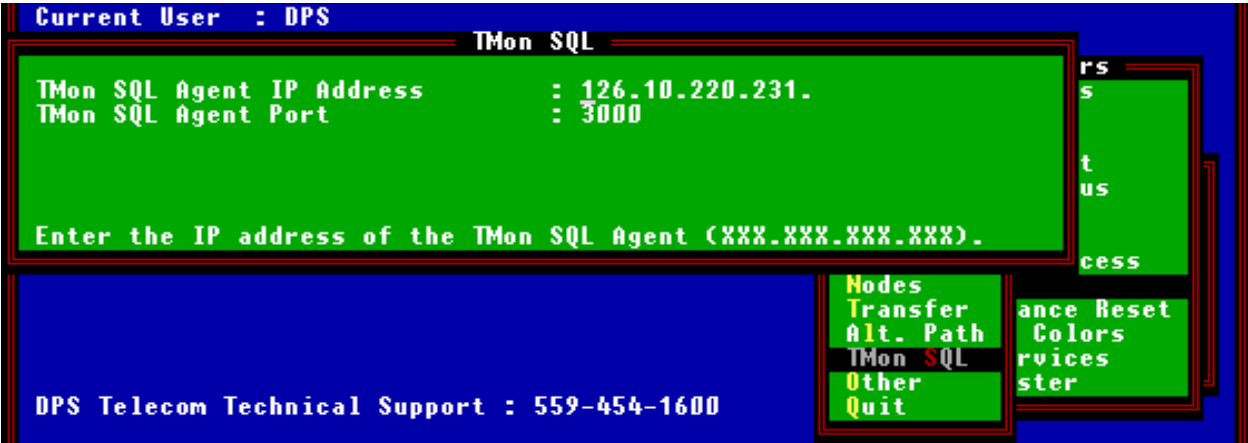


Fig. M24.1 - Configure settings for communicating with the TMon SQL Agent in the Parameters > TMonNet > TMon SQL sub-menu options

### II.A Remote Parameters Settings

Setup the TMon SQL job in the Remote Parameters menu. The job must be run on one of the virtual ports (30+). Use the default “Time out” value.

Refer to Table M24.C for field definitions and Table M24.D for function keys descriptions.

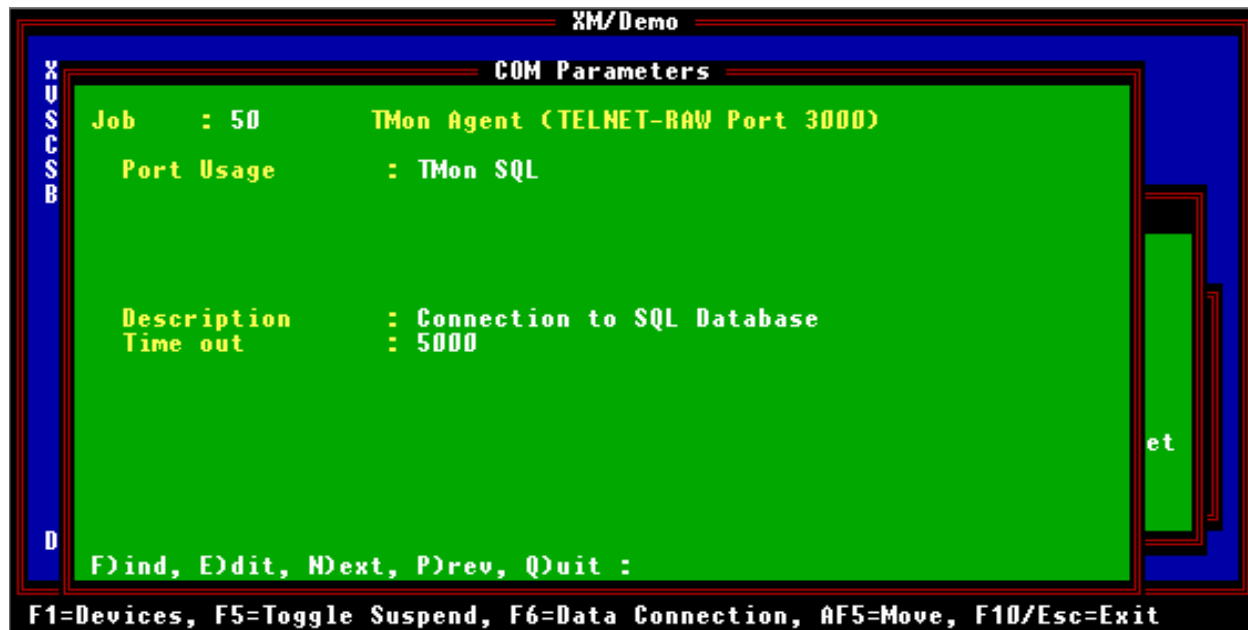


Fig. M24.7 - Configure settings for communicating with the TMon SQL Agent in the Parameters > TMonNet > TMon SQL sub-menu options

Table M24.F - Remote Parameters screen defined for T/Mon SQL Agent

Field	Description
Port Usage	TMon SQL
Description	Optional. Enter a description for this port job. [blank]
Time Out	Time the T/Mon will wait for a response before failing a poll. Valid entries are 200-9999 milliseconds. Use default time out of 5000.

Table M24.G - Key commands available in the Remote Parameters Screen

Function Key	Description
F1	Devices. Define the T/Mon SQL Agent address, alarm displays, and alarm points that are on the current remote port.
F5	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
F6	Data Connection (IP/virtual port connections only)
Alt-F5	Allows you to move the port.
F10/Esc	Exit.

## II.B Setup a Data Connection

Setup a TELNET-RAW data-connection in the Ethernet TCP Port Definition screen by pressing F6 (Data Connection) from the Remote Parameters screen.

The IP Address is irrelevant since the IP address for the TMon SQL Agent is defined under the Parameters > TMonNET > TMon SQL menu — see section M24-1. Set the IP Address to 127.0.0.1 and the TCP Port to 1.

Ethernet TCP Port Definition				
Entry	Type	IP Address	TCP Port	Description
1	TELNET-RAW	127.0.0.1	1	TMon SQL Agent
2				
3				

Fig. M24.8 - Set the IP Address to 127.0.0.1 and the TCP Port to 1

## II.C Define the Remote Device

Define the TMon SQL Agent remote device on address 1. Use the default “Description”, “Site Name” and “Displays” values. See Tables M24.E for field descriptions.

Remote Device Definition	
Port / Job	: 50 TMon SQL
Device ID	: 1
Description	: TMon SQL Agent
Site Name	: TMon SQL Agent
Displays	: 1
F1=Find, E)dit, D)delete, N)ext, P)rev, Q)uit :	
F1=Pnts, AF1=TL1, AF6=Templates, F10/Esc=Exit	

Fig. M24.9 - Remote Device Definition screen defined for TMon SQL Agent

Table M24.H Remote Device Definition screen defined for T/Mon SQL Agent

Field	Description
Port	This port number.
Address	Address of this T/Mon SQL Agent. Use Address 1.
Description	Optional device description.
Site Name	Optional site name. This name will identify the site in Monitor Mode and will be stamped on all events from this RTU.
Displays	Number of displays to be reserved for collection. The default setting is 1, which should never be changed.



## II.D Internal Alarms

The following housekeeping alarms (aka internal alarms) are available for the T/Mon SQL Agent (address 1):

**Cannot communicate with T/Mon SQL Agent:** This alarm is set when the T/Mon SQL Agent fails to respond to the T/Mon's keep-alive request or the TMon is unable to establish a TCP network connection with the T/Mon SQL Agent. This alarm clears when the T/Mon SQL Agent successfully responds to the T/Mon's keep-alive request.

**Cannot connect TCP with T/Mon SQL Agent:** This alarm is set when the TMon is unable to establish a TCP network connection with the T/Mon SQL Agent. This alarm clears when the TMon is able to establish a TCP network connection with the T/Mon SQL Agent.

**Excessive Errors - See Performance/Stats:** This alarm is set when the TMon receives an excessive amount of error messages. The purpose of this alarm is to prompt the user to look at the Performance/Stats Window. This alarm clears when the Performance/Stats are reset (Alt-F2) or the TMon is re-initialized.

**SQL Sever Failed - see T/Mon SQL Agent:** This alarm is set when the T/Mon SQL Agent loses communication with the SQL Server. If this happens you should check if the SQL Server is still running. This alarm clears when the T/Mon SQL Agent restores communication with the server.

## II.F Performance/Stats in Monitor Mode

The following performance statistics are displayed in the Performance/Stats Window from Monitor Mode:

<b>Sync Tot:</b>	Total number of history synchronization attempts.
<b>Sync Ok:</b>	Total number of successfully completed history synchronizations.
<b>Hst Evt Tot:</b>	Total number of history events sent.
<b>Hst Evt Ok:</b>	Total number of successfully completed history events.
<b>Time Out:</b>	Received a partial message.
<b>No Response:</b>	Receive no message.
<b>New CMD Err:</b>	Received an unknown command.
<b>Msg Err:</b>	Received an invalid message.
<b>Noise Chars:</b>	Invalid/unexpected characters.
<b>Comm Err:</b>	Failed attempt to communicate with T/Mon SQL Agent (Keep-Alive or TCP connection).

# Software Module 25

## T/Mon Hard Drive Mirroring

The T/Mon NOC has two hard drives for primary-secondary hard drive mirroring, which provides a back-up in case of hard drive failure. The data written to the primary hard drive is mirrored to the secondary hard drive at user definable intervals.

DPS predefines the hard drive mirroring job on remote port 500 before shipment. Using the default configuration is recommended, but the settings can be changed if necessary — see Table M25.A for field definitions.



**M25.1 - Remote parameters defined for Hard Drive Mirroring**

**Table M25.A - Fields in the Remote Parameters screen**

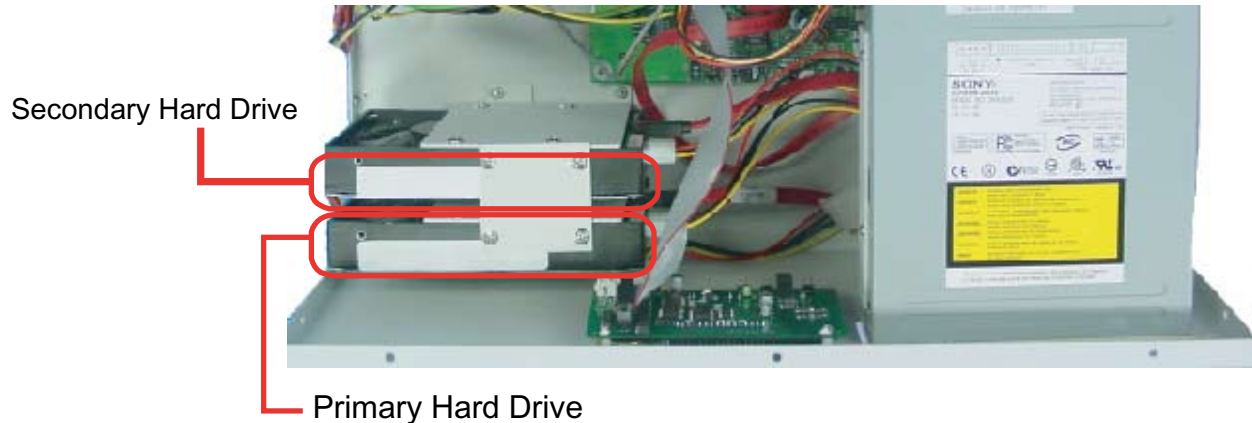
Field	Description
Port Usage	Press the tab key. A list box menu will appear. Use the Up and Down Arrow keys to highlight and select Hard Drive Mirroring.
Target Drive	The drive letter of the secondary hard drive (e.g "D"), which will store the backup mirror image of the primary hard drive ("C:" drive).
Block Size	Size of the data block to copy from the primary hard drive to the secondary hard drive per pass.
Block Count	Number of data blocks to copy from the primary hard drive to the secondary hard drive per pass.
Daily Frequency	Number of times to mirror the primary hard drive to the secondary hard drive per day.

If your primary hard drive fails, your T/Mon NOC system will automatically be restored from the secondary drive, with minimal data loss and downtime.

If your hard drive fails, the T/Mon NOC will reboot, and an internal alarm in Monitor Mode will notify you of the hard drive failure.

If this happens, call DPS Telecom Technical Support at (559) 454-1600 to order a replacement drive.

To set up your replacement drive, follow the instructions in the “Hard Drive Recovery Program” section below.



**Fig. M25.2 - A portion of the interior of the T/Mon NOC, showing the primary and secondary hard drives**

## Hard Drive Recovery Program

In most cases, replacing a failed hard drive is purely plug-and-play. All you have to do is install the new hard drive and the W/Shell Hard Drive Recovery Program will automatically set it up for you

To install a new hard drive:

1. Power down the T/Mon NOC by removing all fuses or power cables.
2. Open the T/Mon NOC case and install the new hard drive, following the instructions that shipped with the new drive.
3. Reconnect the T/Mon NOC to its power and network connections and power up the unit.

The Hard Drive Recovery program will automatically start and begin setting up the new disk. The disk set-up status will be displayed on the T/Mon NOC LCD display (see section M25-3, “Hard Drive Recovery Status Messages”) and on screen on the T/AccessMW console. (See Figure M25.3) This is for your information only — no user action is required to successfully set up your new hard disk.

However, under certain abnormal conditions, you may need to provide the Hard Drive Recovery Program with additional information — see section M25-3 (Abnormal Hard Drive Recovery).



Fig. M25.3 - W/Shell Hard Drive Recovery Program

## Hard Drive Recovery Status Messages

The Hard Drive Recovery status messages will appear in the LCD screen when the W/Shell Hard Drive Recovery Program is rebuilding a disk drive. Hard Drive Recovery status messages are described in Table M25.B.

Table M25.B - Hard Drive Recovery status messages

Field	Description
Rebuilding PRI File #...	Hard Drive Recovery Program is rebuilding primary drive "File #" line shows current file being rebuilt.
Rebuilding SEC File#...	Hard Drive Recovery Program is rebuilding secondary drive "File #" line shows current file being rebuilt.

## Abnormal Hard Drive Recovery

On rare occasions, the Hard Drive Recovery Program may not be able to determine which drive is the primary. If that happens, the program will prompt you to provide information to resolve the problem.

If the Hard Drive Recovery Program prompts you for information, please feel free to call DPS Technical Support at **(559) 454-1600** for help in resolving the problem. Alternatively, you can correct the problem yourself by following the on-screen instructions and prompts.

### READ THE ON-SCREEN INSTRUCTIONS CAREFULLY AND FOLLOW THEM.

If the Hard Drive Recovery Program cannot determine which hard drive is the primary, it will first ask you to check if the hard drive cables are reversed. If you answer yes, the program will prompt you to power down the T/Mon NOC, swap the hard drive cables, and restart the T/Mon NOC — see Figure M25.4.

If the hard drive cables are correctly connected, the Hard Drive Recovery Program will ask you which hard drive has the most current data. Check in the disk information window of the Hard Drive Recovery screen (see Figure M25.4), where disk information, including the date of the History File, is displayed. This information will help you decide which is the most current disk.

```

Harddrive Recovery

C Drive Volume Label: SEC          D Drive Volume Label: PRI
KB Used      : 376320             KB Used      : 376384
KB Free      : 1711808           KB Free      : 1711744
History File Date : Aug 10,2004   History File Date : Aug 9,2004

Restoring      :
File #         :

Activity
Your harddrives appear to be in an invalid configuration.
Follow the instructions below to resolve this issue.
Please review the KB Used and History File Date to determine which
drive contains the most current data. To postpone this recovery and
return to single drive operation (without Mirroring), power down now
and remove the drive you just installed.
Please contact DPS Telecom (559) 454-1600 for technical support.

Are the harddrive cables reversed (Y/N)? n

Which drive contains the must current data (C/D)? d
Warning: All data on drive C will be lost, continue (Y/N)?

```

**Fig. M25.4** - The Hard Drive Recovery Program may prompt you to check the hard drive cables or select the drive with the latest data

# Software Module 26

## ASCII Query Language

This option is only available if the ASCII Query Language (AQL) software module is installed.

### ASCII Query Language Module

The ASCII Query Language (AQL) Module provides a generic way for users and computers to access T/Mon data, control aspects of T/Mon, and retrieve real-time alarm data.

AQL is also an easy way for network operators to integrate their T/Mon with their own proprietary collection system and query T/Mon for its various data sets.

## AQL- ASCII Query Language

### AQL Job Setup

The AQL job allows users to remotely view and retrieve alarm data for specific windows.

To set up an AQL job, select Parameters from the main master menu. Then select Remote Ports and find an available job/port.

Press 'E' to edit the empty job/port and hit 'TAB'. This will select a job type from the list. Select 'ASCII Query Language' and press enter.

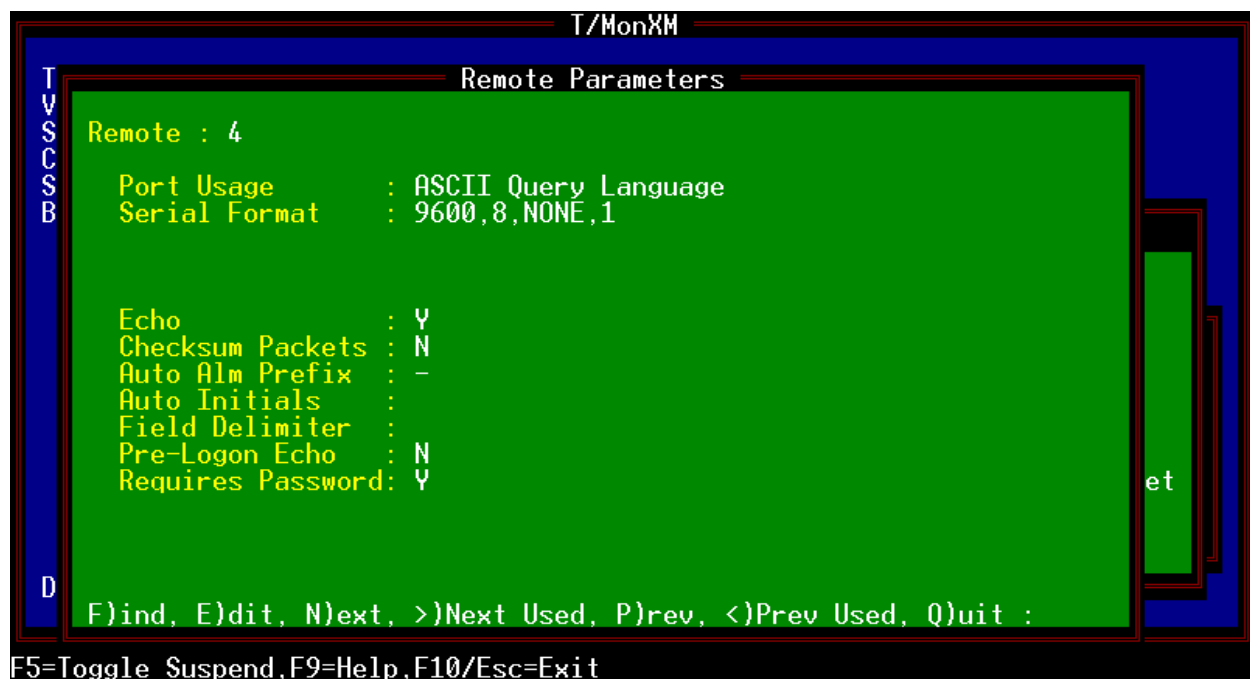


Fig. M26-1 - ASCII Query Language job screen

**Table M22.A - Remote Parameters screen field descriptions**

Field	Description
<b>Port Usage</b>	Type of job for this port. Should be ASCII Query Language
<b>Serial Format</b>	Baud rate, word length, parity, and stop bits settings [1200, 8, NONE, 1] Note: This field only appears for Ports 1 to 24. Anything above will require a data connection.
<b>Echo</b>	If this is set to Y, everything that the user types in will be displayed back onto the screen. If this is set to N, the user may type and the AQL job will accept the input, but it will not display what the user is typing. All messages from the AQL job will be echoed to the screen regardless of what this option is set to. If a computer is connecting to it, you don't want ECHO turned on as the computer knows what is being sent. If a user is connecting, turn ECHO on so the user can receive feedback on what is being sent.
<b>Checksum Packets</b>	This will calculate and send the checksum of each packet to make sure that each packet comes through ok. This should be set to Y when the AQL job is communicating directly with another computer. N if the other end is a standard user.
<b>Auto Alm Prefix</b>	This gets appended to the beginning of each alarm message.
<b>Auto Initials</b>	Initials of user that will be used to automatically log on to the port. If field is blank, then it is disabled. User will need to type a logon command to log in.
<b>Field Delimiter</b>	Each field in the alarm messages will be separated by this character.
<b>Pre-Logon Echo</b>	If this is enabled, it will echo user inputted characters back on the screen before anyone is logged on. After logon "Echo" field takes precedence. This can be used to prevent the user password from being echoed back to the screen as it is being typed. Setting this to Y will make it easier to use, but setting it to N will have better security.
<b>Requires Password</b>	If this is set to Y, AQL will require a password when logging on. The logon command would require an extra field for the password so it would follow this format: LOGON USERID PASSWORD; We recommend disabling Pre-Logon Echo when using this so the userID and password are not being displayed as they are being entered.

Function Key	Description
<b>F1</b>	Devices. Define the DCP device addresses, alarm displays, and alarm points that are on the current remote port.
<b>F5</b>	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
<b>F6</b>	Data Connection (IP/virtual port connections only)
<b>F9</b>	Help.
<b>Alt-F5</b>	Allows you to move the port.



## Security

The AQL has security to prevent unauthorized access similar to the security that is present in T/MonXM. The AQL user must log on before he can access the system. Once logged on, the user can only access those functions that a user has been given clearance for.

## Packet Structures

AQL treats every line of ASCII as a packet. Therefore each command request is a single packet, and responses may consist of multiple packets. There are two types of packet formats. The first format has an ASCII message integrity mechanism for use with AUTOMATED MANAGERS (COMPUTERS) to verify successful transmission of information. The second is designed for human interface.

### Checksum Packets (For Computers)

Checksum packets are packets that use data integrity checks, to prevent invalid information from being passed between the computers. This packet structure should not be used by people since it is impractical to manually calculate the checksums.

#### Overview:

If the MANAGER receives a <PKT ERR> in response to a query, it means that T/Mon received a message that did not pass the integrity check. If the MANAGER receives a message that contains a message which does not pass its integrity check, it means that T/Mon received the command but the response was damaged during transmission. In either of the above cases, or if no response is received, then the MANAGER should re-submit the request.

*Packet format with error detection:*

DATA-PACKET \*HH CR {LF}

*“For people” format:*

DATA PACKET; CR {LF}

Where:

DATA-PACKET- a line of ASCII text

\* : Helps frame messages in conjunction with HH and CR.

It also identifies the data as a secured packet.

HH: Two hex characters ‘0-F’, that together represent a single byte of CHKSUM info. i.e. ‘4B’

CR: Hard terminator for end of line.

LF: Option line feed character that may be turned on.

## Command Syntax Summary:

To facilitate testing, the following commands are shown in “people format” (or non-secured form)

ANALOG PORT **number** ADD **number** CHAN **number**;

AUTO ALARM [ON/OFF];

COS WIN {#} **identifier**;

CTRL GRP **Group-number** ENT **Entry-number**;

CTRL SITE **Site-number** GRP **Group-number** ENT **Entry-number**;

DEV [ONLINE/OFFLINE/STATUS] PORT **number** ADD **number**  
           {devtype};

HELP;

LF [ON/OFF];

LIVE WIN {#} **identifier**;

LOGON **initials** {password};

LOGOFF;

STATS PORT **number** ADD **number**; (address is optional)

STATS RESET PORT **number**;

### Standard success message:

Command-Accepted

### Standard Error Responses and their meanings:

PKT-ERR- Bad chksum or missing ‘;’ or ‘\*’.

CMD-ERR- Invalid command syntax.

RANGE-ERR- Parameter out of range.

SEC-ERR- User does not have adequate security privileges to perform command.

LOG-ERR- User is not logged on

PORT-ERR NO STATS- Returned on STATS command when specified port does not have ability to display stats

*The previous generic error messages may be sent in response to any invalid command line. Individual commands may generate more specific error messages. These messages are listed under each command in the following tables.*

ADDR-ERR NO STATS- Returned on STATS command when specified address does not have stats to display

## **Syntax Notes**

**Brackets:** Options surrounded by brackets “[ ]” indicate that one and only one of the items within the brackets may be included in the commands.

**Braces:** Options surrounded by braces “ { }” indicate that at most one item may be included in the command. Items within braces may or may not need to be physically present.

**Bold:** User specified parameters

## **General Notes**

All commands with the exception of the **LOGON** command require that you be logged on first.

Command	Description	
<b>ACK EVENT</b>	Summary	Acknowledges the alarm associated with the event number
	Syntax	ACKEVENT <b>number</b> ;
	Output:	ACKEVENT 4034; COMMAND-ACCEPTED;
	Functionality	This command is designed to provide acknowledgement of any alarms associated with a specific event number

Command	Description	
<b>ANALOG</b>	Summary	Displays analog values
	Syntax	ANALOG PORT <b>number1</b> ADD <b>number 2</b> {CHAN <b>number 3</b> };
	Where:	Number 1- The port number whose analogs are to be displayed Number 2- The address that contains the analogs that are to be displayed. Number 3- The channel number whose analog value is to be displayed. If this parameter is not entered, then all values for that address will be displayed.
	<b>Example</b>	
	Input	ANALOG PORT 2 ADD 3 CHAN 4; ANALOG PORT 2 ADD 3;
	Responses	The response will include the analog description that was entered into T/MonXM.  PORT 2 ADD 5 CHAN 5 <BATTERY ROOM>=-47.2  <i>Error Responses:</i> Non-Analog Device LOG-ERR
	Functionality	This command only works on analog devices that T/MonXM directly polls. It will not work with analog data that is indirectly transported over standard protocols.

Command	Description	
<b>AUTO ALARM</b>	Summary	Enables/Disables automatic alarm reporting.
	Syntax	Auto Alarm [ON/OFF];
	Where:	<p>ON- Used if you want alarms to be spontaneously reported as they occur and clear. The alarm output will be similar in format to that of the alarm forwarding module. ON is the AQL default.</p> <p>OFF- Turns off the spontaneous alarm reporting feature. Once disabled, alarms will neither be reported, or queued for reporting. This mode is typically used prior to issuing manual requests, in order to keep the output from both sources separated.</p>
	<b>Example</b>	
	Input	AUTO ALARM ON; AUTO ALARM OFF;
	Responses	Command-Accepted LOG-ERR

Command	Description	
<b>COS WIN</b>	Summary	Reports all alarms that have not been acknowledged for a specified window
	Syntax	SCOS WIN {#} <b>identifier</b> ;
	Where:	<p># is used if the identifier is a physical window number. Valid window numbers are in the range of 1-720. The “#” should be omitted if the identifier is the window name.</p> <p>Identifier is the window identifier that may be either the physical number, or the 14 character alarm window name.</p>
	<b>Example</b>	
	Input	COS WIN #2; COS WIN MAJOR;
	Output	<pre> START REPORT;   2/15 11:21 ALM   ng 183           ng point 1 NG.999. 1. 1 CR ACK:           1073742175 TS: ;   2/15 11:31 ALM   analog test     ng point 1 NG. 1. 1. 1 CR ACK:           3263      TS: ;   2/15 11:31 TAG   ng 183           ng point 1 NG.999. 1. 1 CR ACK:           3334      TS: ;   2/15 11:32 ALM   ng 183           ng point 1 NG.999. 1. 1 CR ACK:           3335      TS:   2/15 12:14 CLR   ng 183           ng point 1 NG.999. 1. 1 CR ACK:           3627      TS:   2/15 12:14 ALM   ng 183           ng point 1 NG.999. 1. 1 CR ACK:           1073742223 TS: ;   2/15 12:14 ALM   ng 183           ng point 2 NG.999. 1. 2 CR ACK:           3628      TS: Jan 29 14:35:10.00 ; REPORT COMPLETE; </pre>
	Functionality	Displays all the unacknowledged alarms for the selected window. The actual alarm state ie. Fail/Normal has no bearing on which alarms are displayed. The output format of this command will consist of a single alarm per line. The format and content of this alarm line will be determined by the standard “Alarm Format” and therefore can be customized.

Command	Description	
<b>CTRL GRP</b>	Summary	Issues a labeled control
	Syntax	CTRL GRP <b>Group-number</b> ENT <b>Entry-number</b> ;
	Where:	<p>Group-number is the control group number of the security/ logical group that you wish to control. The maximum number of control groups is 40.</p> <p>Entry number is the number, that specifies which control in the selected group that will be executed. The maximum number of controls that can be in a group is 200. Neither field permits a symbolic reference to a control entry since the description fields are sufficiently long as to make an exact match on the ASCII master impractical.</p> <p>Note:  <i>Controls will only be forwarded if there is a specific group/ Entry number defined in the T/MonXM database.</i></p>
	<b>Example</b>	
	Input	CTRL GRP 5 ENT 7;
	Responses	Command-Accepted Range-ERR Grp-Number-Undefined Entry-Number-Undefined LOG-ERR
	Functionality	<p>This command allows the ASCII master to issue the same controls that a T/Mon user would issue from labeled controls. This command is fully integrated into the security system. If the logged on user does not have specific access to a control group then he may not issue any controls within the group. Also keep in mind that a single control command could actually activate multiple points if T/Mon was provisioned to do so.</p>

Command	Description	
<b>DEV ONLINE</b>  <b>DEV OFFLINE</b>  <b>DEV STATUS</b>	Summary	Places the selected address on or offline, or shows current status
	Syntax	DEV [ONLINE/OFFLINE/STATUS] PORT <b>number</b> {ADD <b>number</b> {devtype}};
	Where:	<p>ONLINE/OFFLINE/STATUS- Determines the action that will be done to the specified device.</p> <p>           ONLINE - Places the device in the polling list            OFFLINE - Removes the device from the polling list            STATUS - Shows the current device status         </p> <p>Status may be:</p> <p>           ONLINE - Normal            OFFLINE - Removed from service            FAILED - Device not answering         </p> <p>Note: Offline devices have a higher precedence than failed devices.</p> <p>Port number is the physical T/Mon port that contains the address that you wish to operate on. Typically this will be in the range of 1 through 24.</p> <p>Address number is the addresss that you wish to inspect or modify. The actual address range permissible will vary depending on the protocol that has been assigned to the port. If address is not specified, then all addresses on the port will be operated on.</p> <p>Device type is only required under special circumstances where an individual address does not uniquely identify a device. Such is the case with DCM where device types MAT, CPM or VDM may occupy the same address space.</p>
	Example	
	Input	DEV ONLINE PORT 7 ADD 450; DEV OFFLINE PORT 3 ADD 23 MAT; DEV STATUS PORT 4 ADD 3;
	Output	DEV OFFLINE PORT 3; PORT 3 ADD 1 OFFLINE; PORT 3 ADD 2 OFFLINE; PORT 3 ADD 3 OFFLINE; PORT 3 ADD 4 OFFLINE; PORT 3 ADD 5 OFFLINE;
	Responses	PORT 4 ADD 3 ONLINE PORT 4 ADD 7 FAILED LOG-ERR



Command	Description	
<b>HELP</b>	Summary	Displays all commands and their syntax
	Syntax	HELP;
	Output:	<p>T/MonXM Version : 5.0B07.0214 (12:03:40) ASCII Query Language Port #4;  ; Available Commands;;  ; ANALOG PORT number ADD number {CHAN number}; Reports analog values.;  AUTO ALARM [ON/OFF] Toggles reporting of spontaneous alarms; as they occur.;  COS WIN {#} identifier Generates a report of COS alarms that are; currently present in the specified window.;  DEV {ONLINE/OFFLINE/STATUS} PORT number {ADD number {devtype}}; Take addresses on/offline or report status.;  LF [ON/OFF] Toggles automatic generation of a line feed; after each carriage return.;  LIVE WIN {#} identifier Generates a report of LIVE alarms that are; currently present in the specified window.;  LOGON initials Logs a user onto the AQL port.;  LOGOFF Logs the current user off of the AQL port.;  ACKEVENT number Acknowledges the alarm associated with the; event number.;  TAG alarm_id Tags the specified alarm. The format of; alarm_id is: port addr.disp.pnt;  UNTAG alarm_id Untags the specified alarm. The format of; alarm_id is: port addr.disp.pnt;  CTRL GRP number ENT number Sends labeled controls.;  CTRL SITE number GRP number ENT number Sends site controls.;  ;</p>
	Functionality	This command is designed to provide online assistance for people using the query language. Help will display the syntax of all valid commands. The format of this help will be very similar to the "Command Syntax Summary" portion of this specification.

Command	Description	
<b>LF</b>	Summary	Enables/Disables line feeds
	Syntax	LF [ON/OFF];
	Where:	ON - Line feeds will be present after carriage returns OFF - Line feeds will be suppressed
	<b>Example</b>	
	Input	LF ON; LF OFF;
	Responses	Command-Accepted LOG-ERR
	Functionality	This command allows the user of AQL to control line feed usage to suit his particular requirements. AQL normal default line termination state is LF ON.

Command	Description	
<b>LIVE WIN</b>	Summary	Reports standing alarms for the specified window
	Syntax	LIVE WIN {#} <b>identifier</b> ;
	Where:	<p># is used if the identifier is a physical window number. Valid window numbers are in the range of 1-720. The “#” should be omitted if the identifier is the window name.</p> <p>Identifier is the window identifier that may be either the physical number, or the 14 character alarm window name</p>
	<b>Example</b>	
	Input	LIVE WIN #4; LIVE WIN MAJOR;
	Output	<pre> START REPORT;   2/15 11:21 ALM           Alternate Path Active [1] IA. 13. 1. 1 CR ACK:      1073742166 TS:           ;   2/15 11:21 ALM           DATABASE NEEDS TO BE BACKED UP IA. 0. 1.58 CR ACK:       1073742169 TS:           ;   2/15 11:21 ALM           GOING ACTIVE [252] IA. 0. 1. 1 CR ACK:       1073742171 TS:           ;   2/15 11:21 ALM           GOING ACTIVE [495] IA. 0. 1. 1 CR ACK:       1073742172 TS:           ;   2/15 11:21 ALM           GOING ACTIVE [3] IA. 0. 1. 1 CR ACK:       1073742173 TS:           ;   2/15 11:21 ALM   ng 183   ng point 1 IA. 11. 1. 3 CR ACK:      1073742183 TS:           ;   2/15 11:21 ALM   s4      I can change this 3.4 IA. 11. 1. 4 CR ACK:      1073742185 TS:           ;   2/15 11:21 ALM   s5      DEVICE FAILURE FOR ADDRESS 3.5 IA. 11. 1. 5 CR ACK:      1073742187 TS:           ; REPORT COMPLETE; </pre>
	Functionality	Displays all the standing alarms for the selected window. A standing alarm is an alarm that is currently in a failed state. The fact that the alarm may or may not have been acknowledged has no effect on this command. The actual output format of this command will consists of a single alarm per line. The format and content of this alarm line will be determined by the standard “Alarm Format” and therefore can be customized.
	Errors	Invalid-Window-Number Window-Name-Not-Found SEC-ERR LOG-ERR

Command	Description	
LOGON	Summary	Allows user to gain access to AQL
	Syntax	LOGON <b>initials</b> ;
	Where:	Initials- The T/Mon user id that has been defined in the system users screen. These initials will determine the extent to which the user can view and affect T/MonXM.  Password- The password that is associated with the users initials
	<b>Example</b>	
	Input	LOGON FBG;
	Output	FBG LOGGED ON : Feb 15,2007 13:31:24;
	Responses	Command-Accepted Invalid-Logon
	Functionality	This command logs users onto the AQL. Until a user is logged on, no AQL commands with the exception of LOGON may be performed

Command	Description	
LOGOFF	Summary	Allows user to log off of the current AQL port
	Syntax	LOGOFF <b>initials</b> ;
	Where:	Initials- The T/Mon user ID that has been defined in the system users screen. These initials will determine the extent to which the user can view and affect T/MonXM.
	<b>Example</b>	
	Input	LOGOFF FBG;
	Output	FBG LOGGED OFF : Feb 15,2007 14:12:44;
	Functionality	This command logs users off of the AQL. Once a user is logged off, no AQL commands with the exception of LOGON may be performed

Command	Description	
<b>STATS</b>	Summary	Reports site statistics for the specified port and address
	Syntax	STATS PORT port_num {ADD addr_num}
	Where:	Port_num – The port that the T/Mon will generate the report on. (RTU Dedicate Interrogator ports only)Addr_num – The address that the T/Mon will generate the report on. (Address is optional, if address is not specified, the report will generate all addresses for a given port. If the address is specified, it will only report one address.)
	<b>Example</b>	
	Input	STATS PORT 50 ADD 1;
	Responses	START REPORT; Address Device Site Name Polls Good Bad Status; 1 STD 8828 8825 0 ACTIVE ; REPORT COMPLETE;
	Functionality	Displays the Site Statistics of a port. This is the same info that is displayed on the console in monitor mode and pressing Shift + F6

Command	Description	
<b>STATS RESET</b>	Summary	Resets the site statistics for the specified port.
	Syntax	STATS RESET PORT port_num
	Where:	Port_num – The port on the T/Mon that the stats will be cleared for. (RTU Dedicate Interrogator ports only)
	<b>Example</b>	
	Input	STATS RESET PORT 50;
	Responses	START REPORT; Address Device Site Name Polls Good Bad Status; 1 STD 0 0 0 ACTIVE ; REPORT COMPLETE;
	Functionality	Resets the stats for a port and displays a report. This functions the same as pressing F1 while on the Site Statistics window on the T/Mon console.

Command	Description	
<b>TAG</b>	Summary	Tags the specified alarm
	Syntax	TAG <b>alarm_id</b> port addr.disp.pnt;
	Where:	Number- The T/Mon XM port # that you wish to get statistics on
	<b>Example</b>	
	Input	TAG 3 2.4.5.6
	Responses	Ack-Port-Error Tag-Port-Error LOG-ERR
	Functionality	Provides the AQL user with a way of tagging specified alarms

Command	Description	
<b>UNTAG</b>	Summary	Untags the specified alarm
	Syntax	UNTAG <b>alarm_id</b> port addr.disp.pnt;
	Where:	Number- The T/Mon XM port # that you wish to get statistics on
	<b>Example</b>	
	Input	UNTAG 3 2.4.5.6
	Responses	Ack-Port-Error Tag-Port-Error LOG-ERR
	Functionality	Provides the AQL user with a way of untagging specified alarms

# Software Module 27

## TAP Interrogator

### **The TAP Interrogator Software Module**

The TAP Interrogator Software Module allows the T/Mon to receive alpha pages and forward them to an ASCII port. Pages are collected by receiving calls via phone line. The T/Mon internal modem accepts calls and sends the received data to an ASCII job to be processed.

## TAP Interrogator

### Fields in Remote Parameter screen:

#### Port Usage-TAP Interrogator

**Serial Format-** Baud rate, parity word length, and stop bits settings that T/MonXM will use to communicate with the equipment.

**Modem Setup String-** 30-character configuration string. This field defaults to the correct string for standard DPS devices. If you are using a non-standard modem, consult Appendix I (Quick Reference Tables) or the modem manufacturer's instructions for details.

**ASCII Port-** The TAP Interrogator will forward received messages to this ASCII port. This ASCII port must not have a data connection.

**TimeOut-** This how long the job will wait between receiving characters before dropping the connection

#### *Key commands available in the Remote Parameter screen:*

Command	Function
Up Arrow	Moves to Previous Field
F5	Toggle Suspension
Alt+F5	Moves the job to another port
F9	Help screen on TAP Interrogator edit screen

**Note:**TAP Interrogator is only allowed for ports 1-24

### TAP Interrogator

Several TAP Interrogators can be set up, as long as there is enough hardware to support them. TAP Interrogators can only be set up on ports 1 to 24.

The TAP Interrogator Software Module is required to enable this job. An ASCII job is also required to process the data. Setting up the ASCII job for receiving TAP pages is the same as setting up an ordinary ASCII job, except that it will not have a data connection. **<No Data Connection>** will flash at the top of the screen when trying to edit the ASCII job. Normally, this would give an error when trying to initialize, but it will be allowed if a TAP Job is set to use the ASCII job. Conversely, you will receive an error if the TAP Interrogator job points to an ASCII job that has a defined data connection.



To prepare the T/Mon to utilize the TAP Interrogator, perform the following steps:

1. Navigate to Parameters->Card PCI and define your modem port.

PCI Card Definition					
Port	Type	Port	Type	Port	Type
1	212/33.6 Mdm	9	None	17	None
2	None	10	None	18	None
3	None	11	None	19	None
4	212/33.6 Mdm	12	None	20	None
5	None	13	None	21	None
6	None	14	None	22	None
7	None	15	None	23	None
8	None	16	None	24	None

Select docking pad interface

DPS Telecom Technical Support : 559-454-1600

Quit/Master

F8=Save, F9=Help, F10/Esc=Exit

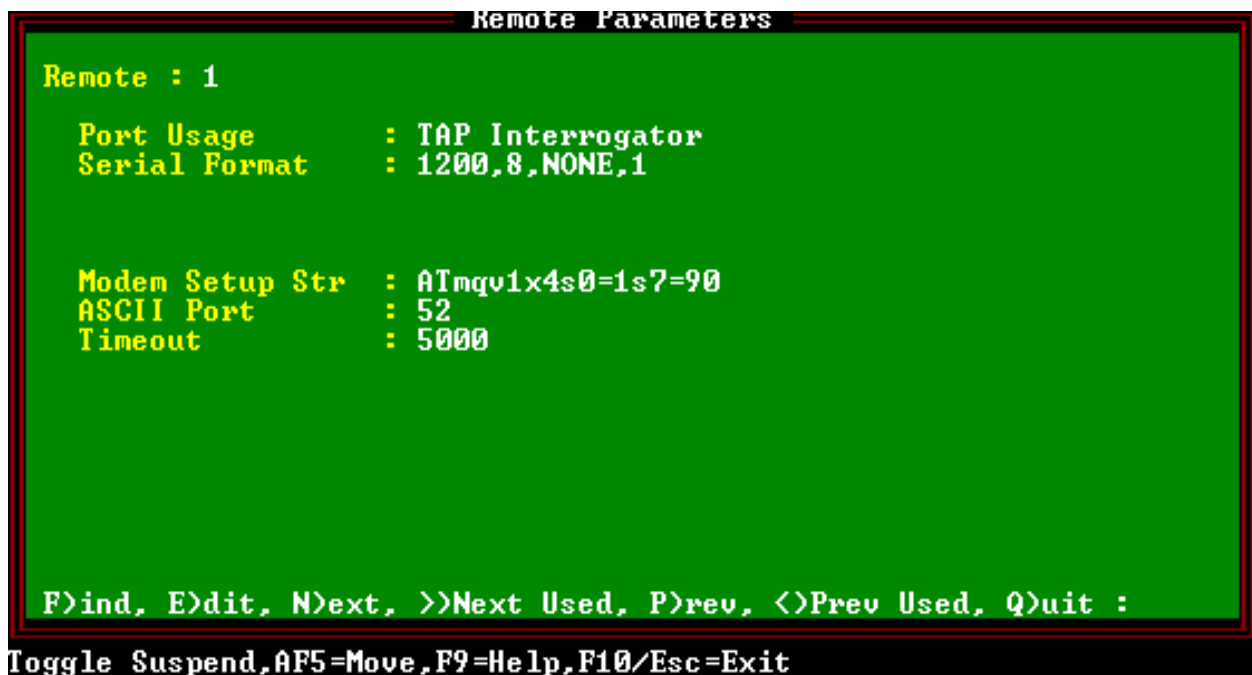
2. Navigate to Parameters->Remote Ports. If you do not already have an ASCII job defined, find an available port and define an ASCII job.

3. Press F6 to set the Data Connection. Press TAB and select NONE from the list. The data connection must be NONE for the TAP Interrogator to forward messages.

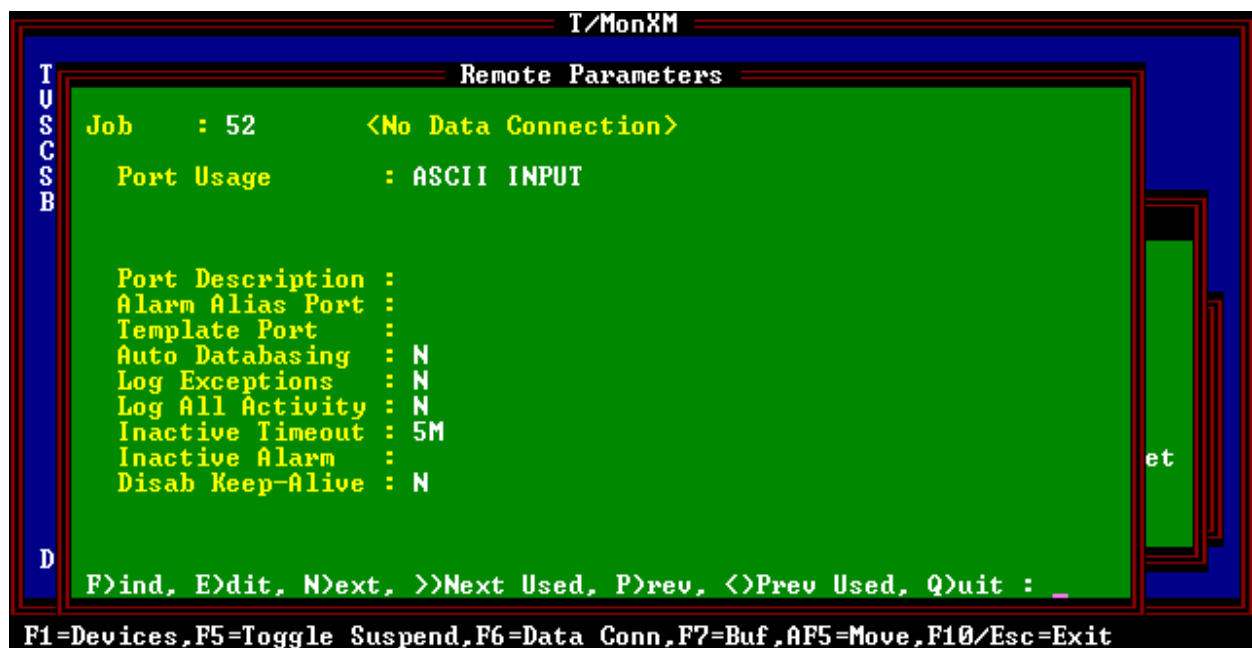
T/MonXM	
Remote Parameters	
Job	: 52 <No Data Connection>
Port Usage	: ASCII INPUT
Port Description : Alarm Alias Port : Template Port : Auto Databasing : N Log Exceptions : N Log All Activity : N Inactive Timeout : 5M Inactive Alarm : Disab Keep-Alive : N	
F>ind, E>dit, N>ext, >>Next Used, P>rev, <<Prev Used, Q>uit : _	

F1=Devices, F5=Toggle Suspend, F6=Data Conn, F7=Buf, AF5=Move, F10/Esc=Exit

4. Go back to Parameters/Remote Ports. Navigate to an available port between 1 and 24 and define a TAP Interrogator job.



5. Set the ASCII Port to the ASCII job that was just defined.
6. Navigate back to the assigned ASCII job and make sure it says TAP Job [port number] instead of <No Data Connection>



*The fields on the TAP Interrogator edit screen are as follows:*

**Modem Setup String-** This gets sent to the modem to prepare it for connection. ATSO=1 sets it to auto answer on the first ring.

**ASCII Port-** The TAP Interrogator will forward received messages to this ASCII port.

**TimeOut-** This is how long the job will wait between receiving characters before dropping the connection.

# Software Module 28

## DNP3 Interrogator

### The DNP3 Interrogator Software Module

Interrogators allow data to be brought into the system. When you use Interrogators, you specify the display list of the items you want to have polled. You can show alarm points on the normal T/MonXM screens under COS windows and Live alarms. The DNP3 Interrogator software module must be installed before you can access the DNP3 Interrogator. Refer to Section 2 (Software Installation) for installation procedures.

## DNP3 Interrogator

To define a remote port for communication to DNP3 equipment, select Remote Ports from the Parameters menu and then select DNP3 Interrogator at the Port Usage field.

**Table M28.A - Remote Parameters screen field descriptions**

Field	Descriptions
<b>Port Usage</b>	Select a port from 1-24. Valid port types are DNP3 Interrogator and Halted. Use Halted (default) if no device is connected to the communication port. [DNP3 INTERROGATOR]
<b>Serial Format</b>	This contains information on Baud rate, data bits, parity and stop bits. [1200,8,NONE,1]
<b>RTS Lead/Fail</b>	RTS on and off time (0-2500 msec) <b>Note:</b> Set Lead to 60 and Tail to 40 for 202 modems. Setting both to 2500 will create a constant carrier. Setting both to 2490 will create a manual carrier.
<b>Description</b>	Description for this job.
<b>DNP Address</b>	DNP address of the T/Mon unit as the DNP Master station. This is used to verify if responses are meant for us before processing.
<b>Time Out</b>	Time the interrogator will wait for a response before failing a poll. Valid entries are 200-9999 milliseconds. [1000]
<b>Poll Delay</b>	The Poll Delay is the time between polls. Valid entries are 0-9999
<b>Fail Threshold</b>	Number of consecutive polls before device failure is declared. [3]
<b>Fail Poll Cycles</b>	The Fail Poll Cycles are the polling loop cycles allowed before failed devices are polled. Valid entries are 0-255. [20]



Fig. M28.1 - Defined Remote Parameters Definition screen

Once you have finished entering in the parameters for the DNP3 remote port, the function keys shown below will become available.

Press F1 (Devices) to define the DNP3 equipment addresses and displays that you wish to monitor on the remote port.

**\*Note:** Setting the RTS Lead Time and RTS Tail Time both to 2500 will enable a DNP3 constant carrier.

## DNP3 Device Definition

Pressing F1 (Devices) from a Remote Parameters screen that is defined for communicating to a DNP3 device will bring you to the Remote Device Definition screen. The purpose of the Remote Device Definition screen is to create the alarm equipment polling list from which T/MonXM will use to gather its information.

The addresses of each DNP3 device that is to be monitored or polled within the alarm system must be entered from here. Each Address Definition represents one device.

An Address Definition consist of a DNP3 device address, a user-definable name, device type and displays to monitored.

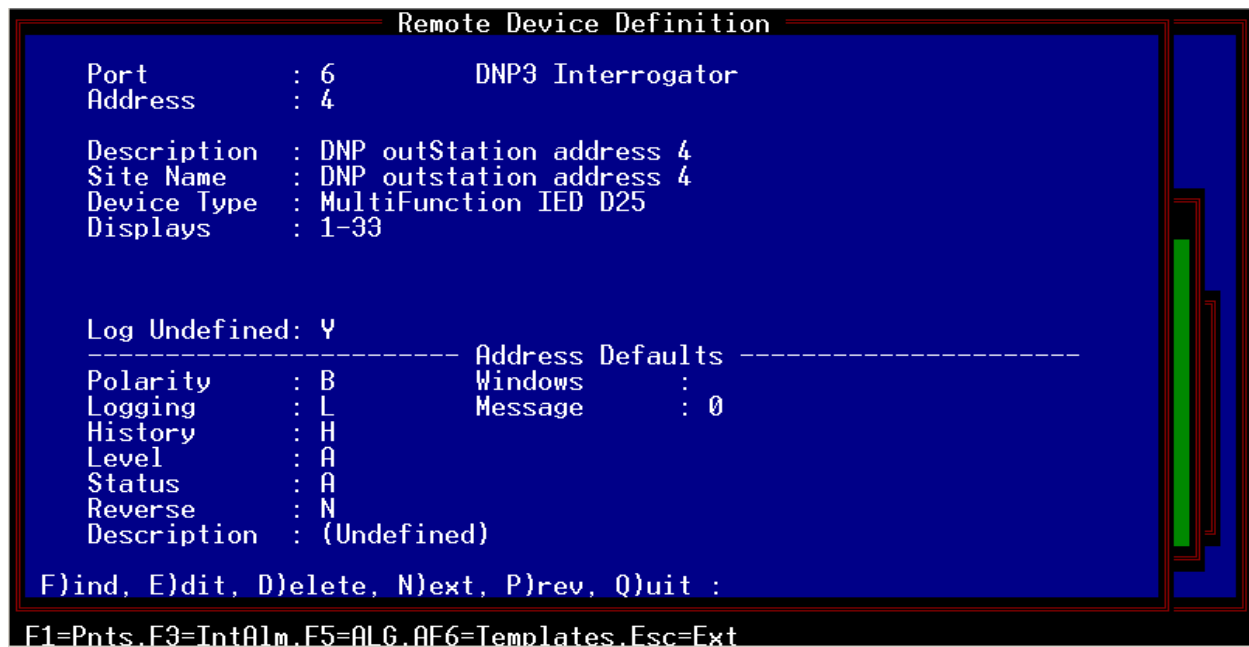


Fig. M28.2 - Defined Remote Device Definition screen

## Defining an Address

First enter the DNP3 address number you wish to define or edit. This must match the DNP outstation address of the device that you wish to poll. At this point, T/MonXM will check the system for the address entered to see if it exists. If the address is found, any previously defined information for that address will then be displayed on the screen and an option line will be displayed at the bottom of the screen.

If the address isn't found, T/MonXM will ask if you want to add it to the system:

*"This item is not in the database. Would you like to add it (Y/N)?"*

Once added, you may then go down, line by line, making changes as needed. After the last field has been entered, the cursor will go to the "Find, Edit, Delete, Next, Prev, Quit:" prompt to get ready for another definition.

**Caution!** Deleting a unwanted Address Definition will not delete the points that were defined for that address. Therefore, you should first delete all the points contained in a DNP3 address before deleting the DNP3 address. The delete function was implemented this way in order to protect the user from the deletion of a large point database because of the accidental erasure of the wrong DNP3 address.

**Table M28.A - Remote Parameters screen field descriptions**

<b>Field</b>	<b>Description</b>
<b>Port</b>	The Port number used by the remote device.
<b>Address</b>	The DNP outstation address that you want to create or edit. Valid DNP outstation addresses range from 1-255. These should match the addresses assigned to the DNP devices.
<b>Description</b>	The description of the use of the address. A maximum of 50 Alphanumeric characters can be used.
<b>Site Name</b>	This field allows you to assign a name to all alarm information that is gathered under the DNP address. A maximum of 50 Alphanumeric characters can be used.
<b>Device Type</b>	Enter the device type that you wish to define for the current address definition
<b>Displays</b>	The alarm displays of the DNP device addresss that are to be monitored. Valid alarm displays range from 1-140. Sample display range inputs: 5,7,20,30 or 5.12, 30-45, 8 These will be automatically be filled in depending on the device type.
<b>Log Undefined</b>	These will automatically be filled in depending on the device type. Enter Y=Yes, N=No.

## Address Default

If an alarm point is reported from the RTU that does not have a definition in T/MonXM, it will use the following parameters to display the alarm:

**Table M28.B - Address Default field descriptions**

Parameter	Description
<b>Polarity</b>	Bipolar(B) or Uni-polar(U). [B]
<b>Logging</b>	Log(L) or No Log(N) [L] <b>Note:</b> goes to screen
<b>History</b>	History(H) or No History(N) [H] <b>Note:</b> goes to history
<b>Level</b>	A(CR), B(MJ), C(MN), or D(ST) [A]
<b>Status</b>	Alarm(A), Status(S) [A] Defines if T/Mon internal relay will change state.
<b>Reverse</b>	Reverse(R) or No Reverse(N) [N]
<b>Description</b>	Default point description. 40 characters (optional)
<b>Windows</b>	Window in Monitor Mode in which undefined alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
<b>Message</b>	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.



**Table M28.C - DNP3 Interrogator Display Map for Device Type D25**

<b>Display</b>	<b>Description</b>
<b>1</b>	Digital Input 1-64
<b>2</b>	Digital Input 64-96
<b>3</b>	DC Analog Channel 1
<b>4</b>	DC Analog Channel 2
<b>5</b>	DC Analog Channel 3
<b>6</b>	DC Analog Channel 4
<b>7</b>	DC Analog Channel 5
<b>8</b>	DC Analog Channel 6
<b>9</b>	DC Analog Channel 7
<b>10</b>	DC Analog Channel 8
<b>11</b>	DC Analog Channel 9
<b>12</b>	DC Analog Channel 10
<b>13</b>	DC Analog Channel 11
<b>14</b>	DC Analog Channel 12
<b>15</b>	DC Analog Channel 13
<b>16</b>	DC Analog Channel 14
<b>17</b>	DC Analog Channel 15
<b>18</b>	DC Analog Channel 16
<b>19</b>	AC Analog Channel 1
<b>20</b>	AC Analog Channel 2
<b>21</b>	AC Analog Channel 3
<b>22</b>	AC Analog Channel 4
<b>23</b>	AC Analog Channel 5
<b>24</b>	AC Analog Channel 6
<b>25</b>	AC Analog Channel 7
<b>26</b>	AC Analog Channel 8
<b>27</b>	AC Analog Channel 9
<b>28</b>	AC Analog Channel 10
<b>29</b>	AC Analog Channel 11
<b>30</b>	AC Analog Channel 12
<b>31</b>	AC Analog Channel 13
<b>32</b>	AC Analog Channel 14
<b>33</b>	AC Analog Channel 15

## Point Definition (F1)

**Note:** For Point Definition Field descriptions refer to Section 10.

This option allows the user to assign attributes and English descriptions to individual alarm points within the selected displays of the DNP device. Defining alarm point definitions are done on a display-by-display basis. Note that you must have defined the displays previously in the Address Definition section.

1. Entering F1 (Points) from the Remote Device Definition screen will bring you to the Point Definition screen.
2. If no display was previously entered, the cursor will be at the display number from which the DCP(F) stores the alarm point information.
3. After <Enter> has been pressed at the Display field, the database management system checks to see if any points in that display have been defined previously. If none are found, then the cursor immediately moves into the point editing area.
4. If points in the display have been defined before, then the Standard Key Entry prompt, appears at the bottom of the window. To edit the points, press 'E' to select the Edit option.
5. When the cursor is in the point editing area, the Message window displays the message associated with the point that is currently being edited.
6. The Up Arrow, Down Arrow, PgUp, PgDn, Home and End keys are used to select a point for editing. Note that these keys are only active when the cursor is at the Pol (polarity) field.

Point Definition

Port : 6 Addr: 4 Disp: 1 Display Desc :

Pt	Pol	L	H	A	S	R	Description	Fail	Clear
1	B	L	H	A	A	N	Open Door	Open	Closed
2	B	L	H	A	A	N	High Temp	Hi	Norm
3	B	L	H	A	A	N	Low Temp	Lo	Norm
4	B	L	H	A	A	N	Beacon	Out	Norm
5	B	L	H	A	A	N	East Radio	Fail	Norm
6	B	L	H	A	A	N	West Radio	Fail	Norm
7	B	L	H	A	A	N	Primary Switch	Fail	Norm
8	B	L	H	A	A	N	Secondary Switch	Fail	Norm

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit :

Message

F10/Esc=Exit

Fig. M28.3 - Point Definition screen

## Analog Point Definition (F5)

1. From the Remote Device Definition screen, press F5 to open the Analog Provision screen.
2. Fill in the Description, Sig (Significant digits), and Unt (Units ) fields.

The screenshot shows the 'Analog Provisioning' screen. At the top, it displays 'Port: 6' and 'Address: 4'. Below this, it says 'Local Thresholds: Yes' and '(Native Unit Thresholds)'. The main part of the screen is a table with columns: 'Alg Description', 'Sig', 'Unt', 'Mj0vr', 'Mn0vr', 'MnUdr', and 'MjUdr'. The table lists four points: '1 Battery A', '2 Battery B', '3 Tower Lt Curr', and '4 Loop Current'. Below the table, there are lines for entering a description, starting with a colon to include threshold crossed in SNMP Trap. At the bottom, a legend explains function keys: F1=Define Scale, F2=Toggle Threshold Mode, F8=Save, F9=Help, F10/Esc=Exit.

Alg	Description	Sig	Unt	Mj0vr	Mn0vr	MnUdr	MjUdr
1	Battery A	2	vdc	4.000	3.500	1.000	0.500
2	Battery B	2	VDC	4.000	3.500	1.000	0.500
3	Tower Lt Curr	2	mA	3.000	2.500	0.500	0.300
4	Loop Current	2	mA	4.300	4.000	0.200	0.100
5	.....						
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							

Enter description (begin with ":" to include threshold crossed in SNMP Trap)

F1=Define Scale, F2=Toggle Threshold Mode, F8=Save, F9=Help, F10/Esc=Exit

Fig. M28.4 - Analog Provisioning screen

**Table M28.D - Analog Point Definition screen field descriptions**

<b>Field</b>	<b>Description</b>
<b>Alg</b>	Point number (fixed field)
<b>Description</b>	Enter the point description. Can be up to 14 characters.
<b>Sig</b>	Significant digits. Enter the number of digits to display after the decimal.
<b>Unt</b>	Enter the Units label, e.g., VDC, VAC F, C, psi, mA, etc.
<b>F1-Define Scale</b>	Calculates offset and scale values for each analog point. This should be done before entering Threshold values. See description below. Press F6 to set scale and offset value to unity..
<b>MjOvr</b>	Major over threshold. Enter the threshold value in native units. Note: The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
<b>MnOvr</b>	Minor over threshold. Enter the threshold value in native units. Note: The bottom line in the window will show the available range in native units and the value of the input voltage or current (in mA).
<b>MnUdr</b>	Window in Monitor Mode in which undefined alarms from this site will appear. Enter the default windows. Valid windows are 2-30 with standard features. More windows are available with the Alarm Windows software modules installed. Eight (8) windows maximum can be assigned.
<b>MjUdr</b>	Enter the message number. Enter "0" for no message. The maximum messages available are limited by the number of messages in the message file.

## Analog Display Worksheet

**Note:** This operation is optional for users who want to change the analog reference scale so that the displayed analog values correspond to real world values.

To define your analog reference scale, press F1 from the Analog Provisioning screen. The Analog Display Worksheet screen is used to convert the analog voltage and current readings into meaningful measurements and units. The analog inputs actually only measure either voltage or current. The values must be converted to their actual units by determining the scale and offset for each input. By entering in a few simple values, T/Mon will make the conversion calculations automatically. Each field and its function are described below.

### Analog input type - Volts or Current (V/C)

This field is where the type of electrical input to the analog channel is selected. This is either V or C for voltage or current. Determine this by the type of sensor or input device used for each input.

### Voltage/Current value 1

This is the lowest/minimum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

Port: 6 Address: 4  
Local Thresholds: Yes (Native Unit Thresholds)

Algo Analog Display Worksheet

Editing Analog Channel 1 Battery A

1 Enter a pair of analog values and corresponding display units.  
2 The Display Scale and Display Offset used to convert voltage  
3 (or current) into display units is calculated automatically.  
4

5 Analog input type - Volts or Current (V/C) : V  
6

7 Voltage value 1: 0.00000 Unit value 1 : 0.00000 vdc  
8 Voltage value 2: 79.9000 Unit value 2 : 79.9000 vdc  
9

10 Calc Scale : 1.00000 Calc Offset: 0.00000  
11  
12  
13

14 Enter analog input type: V for Volts, C for Current  
15  
16

Enter description (begin with ":" to include threshold crossed in SNMP Trap)

Up Arrow=Previous Field, F6=VDC, F8=Save, F10/Esc=First Field [DPS]

Fig. M28.5 - Analog Display Worksheet screen

**Unit value 1**

This is the lowest/minimum measurement in the native units of the analog input (degrees, % relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the minimum range here.

**Voltage/Current value 2**

This is the highest/maximum voltage or current measurement in the range of the analog input. It is the actual voltage or current being input in to the analog channel. The minimum (value 1) and maximum (value 2) values must be entered in for conversion calculations.

**Unit value 2**

This is the highest/maximum measurement in the native units of the analog input (degrees, % relative humidity, psi, etc.). The input device manual should specify its minimum and maximum range of measurement. Enter the maximum range here.

After entering the minimum and maximum ranges in both actual voltage or current values and native units, the calc scale and calc offset will automatically be calculated. After exiting the worksheet, key through the remaining entries for that input to make the changes effective.

## Device Failures/ Offlines (F3)

Entering F3 (Int Alarms) from the Remote Device Definition screen for defined DNP3 Interrogators will bring you to the Device Internal Alarm Assignment screen. Refer to Section 14 for more information on Internal Alarms.

Device Internal Alarm Assignment				
Port : 6				
Address	Dev	Description	Fail	Offline
4	DNPI	DNP outStation address 4	11.1.1..	11.1.2
Enter internal point (addr.disp.pnt) (blank=none) (address range: 0-14)				
F8=Save. F10/Esc=Exit				

Fig. M28.6- Device Internal Alarm Assignment screen

## Address Statistics (Monitor Mode)

Pressing Shift F6 (Address Statistics) from the Monitor Mode Alarm Summary screen brings up the Site Statistics screen. An example of the Site Statistics screen is illustrated below:

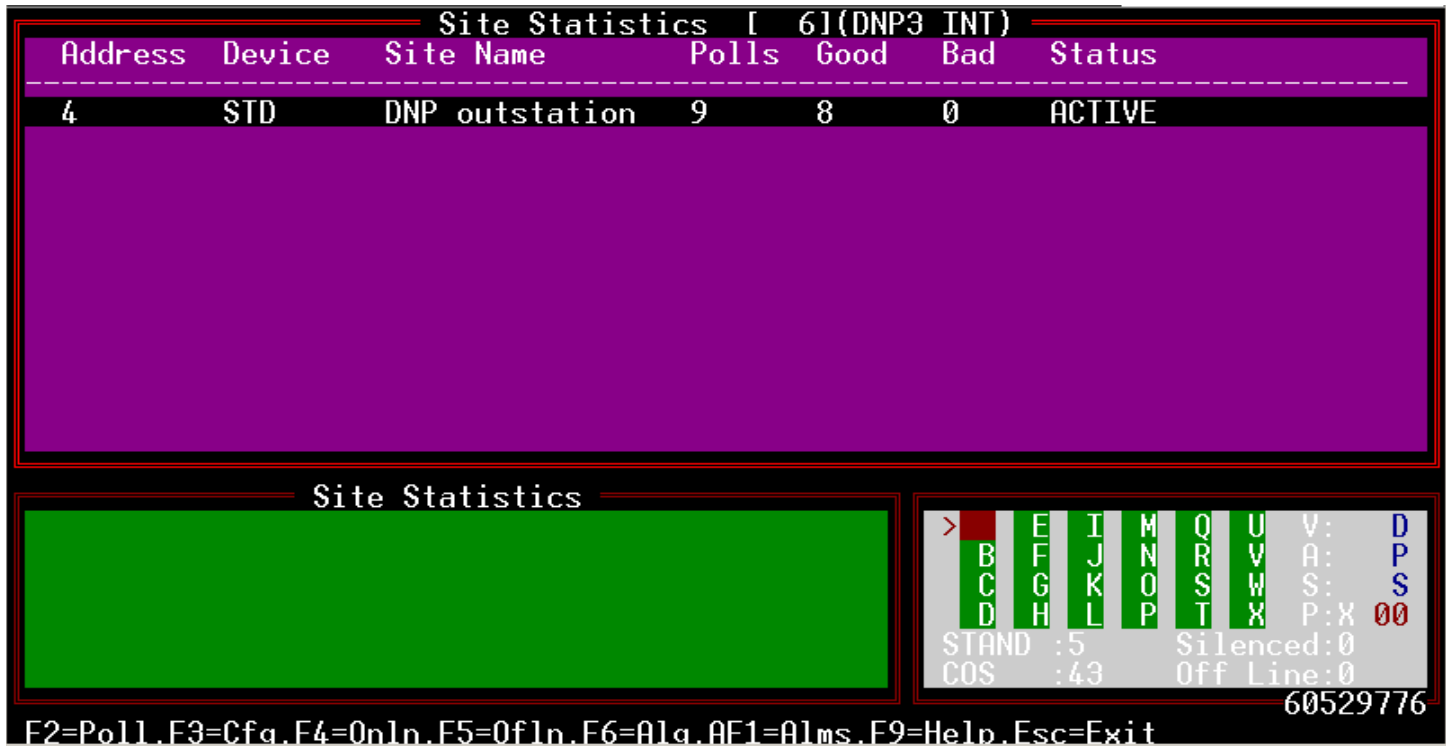


Fig. M28.7- Site Statistics screen

Table M28.E - Key commands available in the Site Statistics screen

Function Key	Description
F1	Init Stats. This resets the counts back to zero to start fresh.
F2	Force poll to remote.
F4	Put unit online.
F5	Take unit offline.
F6	View analogs.
F10/Esc	Exit. Exits from this portion of the program.

**Table M28.F- Fields in the Site Statistics screen**

Field	Description	
Address	The device address that is assigned to that port.	
DCM Interrogator Devices	MAT	MAT (400)
	CPM	Critical Point Module
	VDM	Dantel™ Card
	SBP	Smart Bypass Card
DCP(F) Interrogator Devices	STD (DCPF)	Standard JACE-5XX (Modbus device) Testset
	NET	Network slaves that are on the system
	DPM	Discrete Point Module
	BVM	Battery Voltage Monitor Card
	PWS	Protection Switch
	DAS	TBOS/ASCII Expansion
	A08	8 Channel Analog (Exp)
8 Channel Analog (B) (Exp)	KDA	KDA Timestamp Base
KDA 832-T8	A16	16 Channel Analog (Exp)
16 Channel Analog (400)	A8T	8 Analog/4 TBOS
	T08	8 Channel TBOS (400)
	NG	NetGuardian
	NGC	NetGuardian C
	216	NetGuardian 216
	NW	NetWatchman
	GLD	General LED Display
	BAC	Building Access Controller
	APS	Alt Path Switch
	D5K	DS5000
	UNK	All other devices not listed
Site Name	This is the site name that was assigned to the device.	
Polls	This is a continuous count of the polls that have been sent out to the site	
Ok	This is the number of OK responses to the polls.	
Fail	This is the number of Failed responses to the polls.	
Status	Indicates whether or not the device is actively being monitored and is a good device that is answering. An OFFLINE statement occurs if the device is manually taken offline. A FAILED statement occurs if the device failed to answer in 3 consecutive polls.	



## View Analogs

To read analog values from the DNP remote equipped with an Analog Expansion Card press Shift-F6 while in the main monitor screen. The Site Statistics screen will be displayed. Select the address/ device / site name for the desired remote.

Press F6 to see the View Analogs screen. The Page Index Window will indicate if any new alarms are received. If there are more than 16 analogs defined, press N to view the next set of analogs. P will view the previous set of analogs for a given address.

Points in alarm will display the severity (alarm level) color behind the point value, plus an arrow pointing up for over threshold alarms and an arrow pointing down for under threshold alarms.

**View D25 Analogs**

Port : 6 Address : 4 Site Name : od 0 Haç9σ0ç9JL♥

Channel	Description	Value	Channel	Description	Value
CH 1	Battery A	DISABLED	CH 9		DISABLED
CH 2	Battery B	DISABLED	CH 10		DISABLED
CH 3	Tower Lt Curr	DISABLED	CH 11		DISABLED
CH 4	Loop Current	DISABLED	CH 12		DISABLED
CH 5		DISABLED	CH 13		DISABLED
CH 6		DISABLED	CH 14		DISABLED
CH 7		DISABLED	CH 15		DISABLED
CH 8		DISABLED	CH 16		DISABLED

**D25 Analogs**

N=Next, F10/Esc=Exit

> B C D E F G H I J K L M N O P Q R S T U V W X V: D P S  
 STAND :5 Silenced:0  
 COS :43 Off Line:0  
 60530448

Fig. M28.7 - View analogs screen shows each channel and its description

# Software Module 29

## ASCII Gateway

The T/Mon ASCII Gateway feature is designed to extend the number of TCP/UDP connections that are used up for ASCII jobs. This is done by establishing a connection between the T/Mon and the T/Mon ASCII Gateway Agent on a windows machine. Data from the ASCII devices will go through the T/Mon ASCII Gateway Agent which will get forwarded to the T/Mon through a single TCP/UDP port. This allows the T/Mon ASCII Gateway Agent to monitor several ASCII devices that will only use a single port on the T/Mon.

### Setup Overview

The configuration process consists of several parts:

- I. Define the ASCII gateway connection to T/Mon
- II. Define the ASCII gateway subconnections
- III. Modify/Create ASCII input jobs that will use these connections
- IV. Configure the T/Mon ASCII Gateway Agent

### I. Define the ASCII Gateway Connection on T/Mon

#### Define the IP Mux connection:

1. From the Master Main menu, go to **Parameters | Remote Ports**. Find Job **28** and press **F1**.
2. Find a blank line and press tab to define a new data connection. There should be 2 options at the bottom for **IPMux-TCP** and **IPMux-UDP**.
  - IPMux-TCP will establish a TCP connection to the T/Mon ASCII Gateway Agent.
  - IPMux-UDP will establish a UDP connection to the T/Mon ASCII Gateway Agent.

Ethernet TCP Port Definition					
Ent	Type	IP/Hostname	TCP Port	Description	Job
1	IPMux-TCP		6000	IP mux windows 1	0
2	IPMux-TCP				0
3	IPMux-TCP				0
4	UDP			TELNET (ASCII,CRAFT: if TELNET negotiation required)	250
5	UDP			UDP (DPS RTU,SNMP TRAP Processing,SNMP Agent)	251
6	UDP			ICMP (PING)	252
7	IPMux-TCP			IPMux-TCP (IP MUX APP)	0
8	IPMux-UDP			IPMux-UDP (IP MUX APP)	131
9	IPMux-TCP		6004	ip mux windows 5	0
10	TELNET-RAW	126.10.220.231	9000	craft filler 1	51
11	TELNET-RAW	126.10.220.231	9001	craft filler 2	62
12	TELNET-RAW	126.10.220.231	9002	craft filler 3	72
13	TELNET-RAW	126.10.220.231	9003	craft filler 4	83
14	TELNET-RAW	126.10.220.231	9004	craft filler 5	86
15	TELNET-RAW	126.10.220.231	9005	craft filler 6	87
16	TELNET-RAW	126.10.220.231	9006	craft filler 7	88
17	TELNET-RAW	126.10.220.231	9007	craft filler 8	89
Target: 126.10.220.231					
[LIST BOX] Cursor Keys=Move Highlight Bar, <ENTER>=Select, F10/Esc=Abort					

3. Select the desired connection type (IPMux-TCP or IPMux-UDP) and press enter.
4. Enter the desired port that will be used for the ASCII Gateway Agent.
5. Enter a description for the connection and enter again to save it.

### Internal Alarms

The following internal alarms are available for an IPMUX\_TCP/IPMUX\_UDP connection:

**ASCII GATEWAY DISCONNECTED-** This can be defined by pressing F2 on the “Ethernet TCP Port Definition” window. This will set when a keep-alive from the ASCII Gateway Agent has not been received for 15 seconds.

Data Connection Internal Alarm Assignment			
Job : 0			
Ent	Type	Description	Disconnected
1	IPMUX-TCP	IP mux windows 1	12.1.6..

Enter internal point (addr.disp.pnt) (blank=none) (address range: 0-14)

F8=Save, F10/Esc=Exit

## II. Define the ASCII Gateway Subconnections

These are the connections that the T/Mon ASCII Gateway will be monitoring

1. While in the Ethernet TCP Port Definition screen, highlight the IPMux entry and press **F4**
2. These should be defined the same way that you would define a connection for an ASCII job. The following types are allowed [UDP, TELNET, TELNET-RAW]
3. Press **F8** to save

IP Mux Port Definition					
Subtable for:					
1	IPMux-TCP		6000	IP mux windows 1	0
Ent	Type	IP/Hostname	TCP Port	Description	Job
1	UDP.....		7200	ascii dev 101	101
2					
3	TELNET-RAW	126.10.241.200	7201	ascii dev 102	102
4	TELNET-RAW	126.10.241.200	7202	ascii dev 103	103
5					
6	UDP		7203	ascii dev 104	104
7	TELNET-RAW	126.10.241.201	7204	ascii dev 105	105
8	TELNET-RAW	126.10.241.201	7205	ascii dev 106	106
9					
10					
11					
12					
Tab=Defaults, F3=BLANK, F8=Save, F10/Esc=Exit					

## III. Modify/Create ASCII Input Jobs That Will Use These Connections

1. Create an ASCII INPUT job and press **F6** for Data Conn.
2. The connections that were created in Step 2 should now be available for use
3. These connections will have **IPMUX:** added to their descriptions

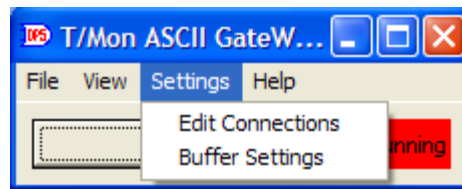
## IV. Configure the T/Mon ASCII Gateway Agent

Run the ASCII Gateway install file. This should create a shortcut to the desktop called "T/Mon ASCII Gateway Agent"

This software will receive data from the ASCII devices and forward it to the T/Mon.

The following setup must be performed to configure the agent to communicate to a T/Mon:

1. Start the agent
2. Click on **Settings** | **Edit Connections**



3. Start with the first line and a description for the connection. Enter Primary T/Mon's IP address under the **Primary IP Addr** field and port under the **Port** field. The secondary T/Mon settings are only necessary when TmonNet is being used. The connection type should reflect the setting on T/Mon. These are the settings that were defined in Step 1.

	Description	Primary IP Addr	Port	Secondary IP Addr	Port	Connection Type
1		255.255.255.255	0	255.255.255.255	0	TCP
2		255.255.255.255	0	255.255.255.255	0	TCP
3		255.255.255.255	0	255.255.255.255	0	TCP
4		255.255.255.255	0	255.255.255.255	0	TCP
5		255.255.255.255	0	255.255.255.255	0	TCP

4. Click on **Save**
5. Start the agent by clicking on the **Start** button
6. You may view the connection status by clicking on the **View** menu item and **Stats**

When the agent connects to the T/Mon, it will retrieve the information for which ASCII devices it should be watching. All databasing other than the IP/Port of the Primary/Secondary T/Mon will be done on the T/Mon itself.

The **Start** button will start the actual process.

# Software Module 30

## Modbus Responder

The Modbus Responder software module enables T/MonXM to forward any alarm to a Modbus Interrogator. The Modbus Responder software module fully supports the following features: discrete inputs, analog inputs and control relays. All Modbus protocols are supported. (ASCII, RTU, and TCP).

### Part One

#### Install or Upgrade the Software

Under normal circumstances installation will only need to be done for software updates or newly ordered modules. The original disks have been supplied with the T/Mon for archival or emergency recovery procedures. See Section 2 of the T/MonXM user manual for further instructions on upgrading or installing software.

### Part Two

#### Configure the Modbus Responder

##### Step One

##### Define the Remote Port

1. From the Master menu, select Parameters > Remote Ports.
2. Using the F)ind, P)revious, or N)ext commands, navigate to an unused port/job.
3. In the 'Port Usage' field, select "Modbus Responder".



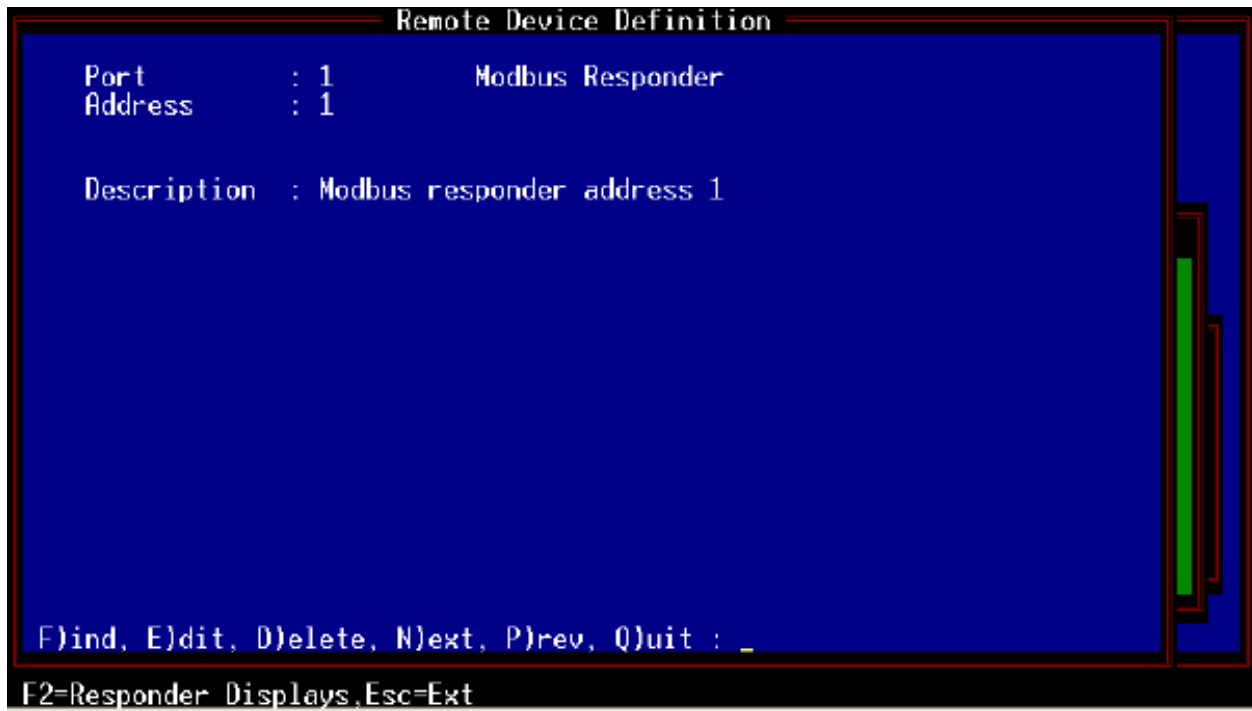
Fig. M30.1 - Using the Remote parameters menu to setup Modbus Responder

**Table M30.A - Fields in the Modbus Responder Remote Parameters screen**

Field	Description
Port Usage	Modbus Responder
Serial Format	Baud rate / word length / parity / stop bits. Used to communicate with equipment. This field does not apply to virtual ports that is connected over LAN.
RTS Lead / Tail	RTS Lead is the time carrier is turned on before data is sent (0-2500ms). (Set to 60 for 202 modems.) RTS Tail is the time carrier is left on after the last byte is sent (0-2500 ms). (Set to 40 for 202 modems.) Note: Setting the RTS Lead Time and RTS Tail Time both to 2500 will enable a constant carrier.
Time Out	Time out in milliseconds (20-9999).
Protocol	Protocol Mode <R=RTU Mode or A=ASCII Mode> Selecting a virtual port will automatically activate TCP.
Native Protocol	Dedicated for serial connections (RTU or ASCII mode). Or TCP for TCP protocol. If the interrogator is going over a TCP proxy where the protocol should be serial RTU or ASCII, set Native Protocol to Dedicated and modify the Protocol. Otherwise, TCP connections should always have this set to TCP.
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Valid entries are 5-999 seconds.
Check DCD on Rcv	Y = Enable DCD checking to validate Rcv. N = Disable. [N]

**Step Two     Define Mobus Responder Remote Device**

Pressing F1 (Devices) at the Remote Parameters screen for defined Modbus Responders will bring you to the Remote Device Definition screen.



**Fig. M30.2 - Remote Device Definition screen for Modbus Responder**

**Table M30.B - Fields in the Modbus Responder Remote Device Definition screen**

Field	Description
Port/Job	The port number and description used by the Responder you have defined. This is not editable.
Address	The Modbus address that this job will be responding to. Valid values are 1 to 255.
Description	The description of the device.



**Step Three     Define Modbus Responder**

Entering F2 (Responder Displays) from the Remote Device

Definition screen will bring you to the Responder Definition screen.

Remote Device Definition				
Port	:	1	Modbus Responder	
Address	:	1		
Responder Definition				
Display	PORT	DEVICE	Interrogator ADDR	DISPLAY
1....	3		1	1
2	3		1	2
3	3		1	3
4	3		1	4
62	NG		100	7
63	NG		100	8
64	NG		100	9

Enter Responding Display Number (1-64)

F3=BLANK, F8=Save, F10/Esc=Exit

**Fig. M30.3 - Responder Definition screen**

**Table M30.C - Fields in the Modbus Responder Definition Screen**

Field	Description
Display	Enter the Responding Display Number. Valid entries are 1-64.
Port	Enter the Port Number. Valid entries are 1-500, IA, RP, K1, K2, NG, N2.
Device	This field is an address modifier for applicable protocols such as DCM.
Addr	Enter the Address Number. Valid entries are 1-255. Note: Enter Address Number 11-12, when IA (User Internal is selected on the Port field).
Display	Enter Display Number. Valid entries are 1-64.

**Mapping for modbus function code 0x02 (Read Discrete Inputs) :**

Each point is assigned to its own address. Address 0 will return the status of Modbus responder display 1 point 1. Address 2 will return the status of Modbus responder display 1 point 3.

To determine the Discrete Input Address use the following equation:

$$\text{Discrete Input Address} = ((\text{Display} - 1) \times 64) + (\text{Point} - 1)$$

Valid addresses are 0 to 4095.

**Table M30.D - Modbus-to-T/Mon Alarm Point Numbering**

Discrete Input Address	Tmon Display	Tmon Point
0	1	1
1	1	2
2	1	3
63	1	64
64	2	1
4095	64	64

**Mapping for modbus function code 0x04 (Read Input Registers):**

A single register contains the status for a group of 16 points. This can be used to retrieve a group of discrete inputs but is mainly used to retrieve the value of an analog channel.

Points are mapped so register 0 has display 1 and points 1-16. Register 2 will map display 1 and points 17-32.

Use the following equation to determine the Read Input Register address for a given display and point:

$$\text{Read Input Register Address} = ((\text{display} - 1) \times 4) + ((\text{Point} - 1) / 16)$$

Use the integer value only. Do not include the decimal value.

**Table M30.D - Modbus-to-T/Mon Register Alarm Point Numbering**

Input Register Address	Tmon Display	Tmon Point
0	1	1-16
1	1	17-32
2	1	33-48
3	1	49-64
4	2	1-16
8	3	1-16
12	4	1-16
252	64	1-16
255	64	49-64

### Assigning Analog Channels

In order to forward Analog values, set the Responder Definition to the device's analog channel. (NG analog channel 1 is display 3).

Use the Read Input Register function to read points from the analog display (see below for which points to read). Use the equation listed above for the address. This will return the raw analog value.

#### **Guidelines for interpreting the raw analog data for display.**

- Analog values are in groups of two bytes. The raw analog value will need to swap the high byte with the low byte before processing.
- The analog configuration data can be retrieved by reading points 1 to 16. Use the Read Input Register function with the address for point 1. The register will have the following bitmap:
  - bit 1-8 : Reserved
  - bit 9-10 : Range (0-3 to select voltage resolution)
  - bit 11 : Polarity (1=Negative, 0=Positive)
  - bit 12 : Status (1=Enabled, 0=Disabled)
- If the analog channel belongs to a NetGuardian216 or a NetMediatorT2S device, the raw analog value can be read from points 41 to 56. Make sure to also read points 1 to 16 for the polarity configuration. The raw analog value will be BCD encoded. (0x0742 will be converted to 742 in decimal). Take this value and divide by 100. The final value should be 7.42. Range is not used in this case. The polarity from the configuration byte will apply.
- If the analog channel belongs to anything other than a NetGuardian216 or a NetMediatorT2S, the raw analog value can be read from points 17 to 32. Points 1 to 16 is needed for the Range and Polarity values.
- If the high bit is set, mask the raw value with 0x3FFF. This will return the display value. Mask with 0x4000 to determine the polarity. If 0x4000 is set, it is negative. If clear, it is positive.
- If the high bit is clear, use the table below to determine the voltage resolution and multiple this with the raw analog value to get the display value. The raw value is in hex. Use the Polarity settings for polarity.
- Reading of Point 33 will result in a scaled analog value between -29,999 and 29,999. The value read here will be a signed 16-bit integer. This will return a processed value with range and the polarity bit taken into account.

**Table M30.F - Voltage Resolutions**

Device	Range Value	Voltage Resolution
8 Analog Expansion (A08)	0	0.00151147
	1	0.00385374
	2	0.00811031
	3	0.01832803
Badger 481	n/a	0.001244037
Larse/Badger 1200/1400	n/a	0.000490190
DS5000	n/a	0.010000000
DNP3 D25	n/a	0.002442598
Modbus Interrogator	n/a	0.010000000
Default	0	0.001510967
	1	0.003850723
	2	0.008097302
	3	0.01826261

**Mapping for modbus function code 0x05 (Write single coil):**

Addresses passed by the write single coil function will allow labeled controls to be executed. The upper byte of the address will contain the Labeled controls Category number. The lower byte of the address will contain the Labeled controls Entry number to be executed.

The address can be calculated by using the following equation:

$$\text{Write Single Coil address} = (\text{Category} \times 256) + \text{Entry Number}$$

**Note:** A command to set the coil on will only execute the labeled control if the labeled control is an ONR command. A command to clear a coil will also only execute if the labeled control command is also ONR. Otherwise, it will return an ILLEGAL DATA VALUE error.

**Mapping for modbus function code 0x01 (Read Coil Status):**

The last processed command from the Write Single coil function can be retrieved by using the read coil status function. The addressing is the same as Write Single Coil and will return the value of the associated labeled control. All labeled controls with the same channel / id / unit / point will return the same value.

**Note:** DPS recommends creation of labeled control entries for individual control points when using the Read/Write coil functions. Do not group points in the same entry. Also create an ONR and a RLS entry for the same points. By default, ONR will behave identically to OPR, but it may be overridden by responders to be either OPR or RLS.

**This page intentionally left blank.**

# Software Module 31

## DNP3 Responder

### DNP3 Responder

The DNP3 Responder software module must be installed before you can access the DNP3 Responder. Refer to Section 2 - Software Installation for installation procedures.

To define a remote port for communication to DNP3 equipment, select Remote Ports from the Parameters menu and then select DNP3 Responder at the Port Usage field.

An example of the Remote Parameters screen defined for DNP3 Responders is illustrated in Figure M31.1. Refer to Table M31.A for field descriptions.

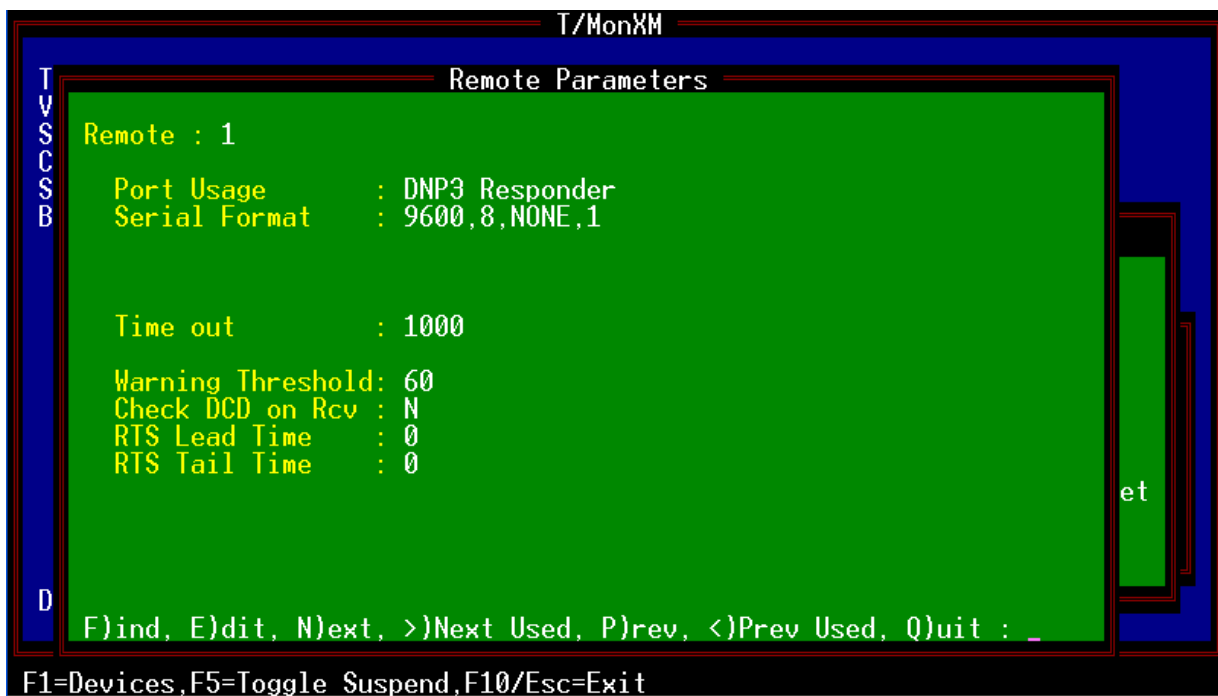


Fig. M31.1 - Remote Parameters screen defined for DNP3 Responder

Table M31.A - Fields in the Responder Definition screen

Field	Description
Port Usage	Valid port types are DNP3 Responder and Halted. Use Halted (default) if no device is connected to the communication port.
Serial Format	Baud rate, word length, parity, and stop bits settings. [1200, 8, NONE, 1]
Time Out	Time the interrogator will wait for a response before failing a poll. Acceptable values are 200-9999 milliseconds. [1000]
Warning Threshold	The Warning Threshold is the seconds of no activity before a warning is issued. Acceptable values are 5-999 seconds. [60]
Check DCD on RCV	Y = Enable DCD checking to validate RCV. N = Disable. [N]
RTS Lead Time	RTS on time (0-2500msec). [0] <b>Note:</b> Set to 60 for 202 modems.
RTS Tail Time	RTS on time (0-2500msec). [0] <b>Note:</b> Set to 10 for 202 modems.

## Remote Device Definition

Pressing F1 (Devices) at the Remote Parameters screen for defined DNP3 Responder will bring you to the Remote Device Definition screen.

An example of the Remote Device Definition screen is illustrated in Figure M31.2.

Remote Device Definition

Port : 1 DNP3 Responder

Address : 1

Description :

F)ind, E)dit, D)elele, N)ext, P)rev, Q)uit :

F2=Responder Displays, Esc=Ext

Fig. M31.2 - Remote Device Definition screen

Table M31.B - Fields in the Remote Device Definition screen

Field	Description
Port	Enter the Port. Valid entries are 1-500.
Address	Enter the DNP3 Address of the device. Valid entries are 1-999
Description	Enter the Description of the device.

Remote Device Definition				
Port	:	1	DNP3 Responder	
Address	:	1		
Responder Definition				
Display	-----Interrogator-----			
	PORT	DEVICE	ADDR	DISPLAY
1....	NG		100	1
2	NG		100	2
3	NG		100	3
4	NG		100	1
Enter Responding Display Number (1-64)				
F3=BLANK, F8=Save, F10/Esc=Exit				

Fig. M31.3 - Responder Definition screen

## Responder Definition

Entering F2 (Responder Displays) from the Remote Device Definition screen will bring you to the Responder Definition screen. See Figure M31.3.

Table M31.C - Fields in the Responder Definition screen

Field	Description
Display	Enter the Responding Display Number. Valid entries are 1-64.
Port	Enter the Port Number. Valid entries are Port 1-500, IA (User Internal), LC (Local Control), RP (Modem), K1, K2, NG, and N2.
Device	This field is an address modifier for applicable protocols such as DCM, ASCII, DCP.
Addr	Enter Address Number. Valid entries are 1-255. <b>Note:</b> Enter Address Number 11-12, when IA (User Internal) is selected on the port field.
Display	Enter Display Number. Valid entries for this field are relative to the device defined on the Port field

Table M31.D - Key commands available in the Responder Definition screen

Function Key	Description
F3	Blank. Deletes the current entry.
F8	Save. Saves the Network Node Definition database.
F10/Esc	Exit. Exits without saving any changes that may have been made.



---

## DNP3 Databasing Notes

Discrete alarms and analogs need to be databased under different addresses. An address should be polled as discrete alarms or analogs, but not both.

A reversed status on the T/Mon point definition is not checked by the DNP3 responder. If a point is set as reverse, the responder will report the pre-processed data.

Responsiveness of analog values will depend on how often T/Mon polls for analogs from the associated device. This is usually controlled by the refresh rate, or by sending FUDR requests on the Interrogator job. (Set to always poll with FUDR to get the most up-to-date data.)

# Software Module 32

## DPS Site Dialer

### Site Dialer

The DPS Site Dialer is a device that allows you to send voice notification for points databased in T/Mon. You can assign voice notifications for a few specific alarm points or all the points at a site.

The following steps for configuring the Site Dialer for T/Mon assume you already have the following configured in your T/Mon LNX:

Pager Job

Ethernet Job

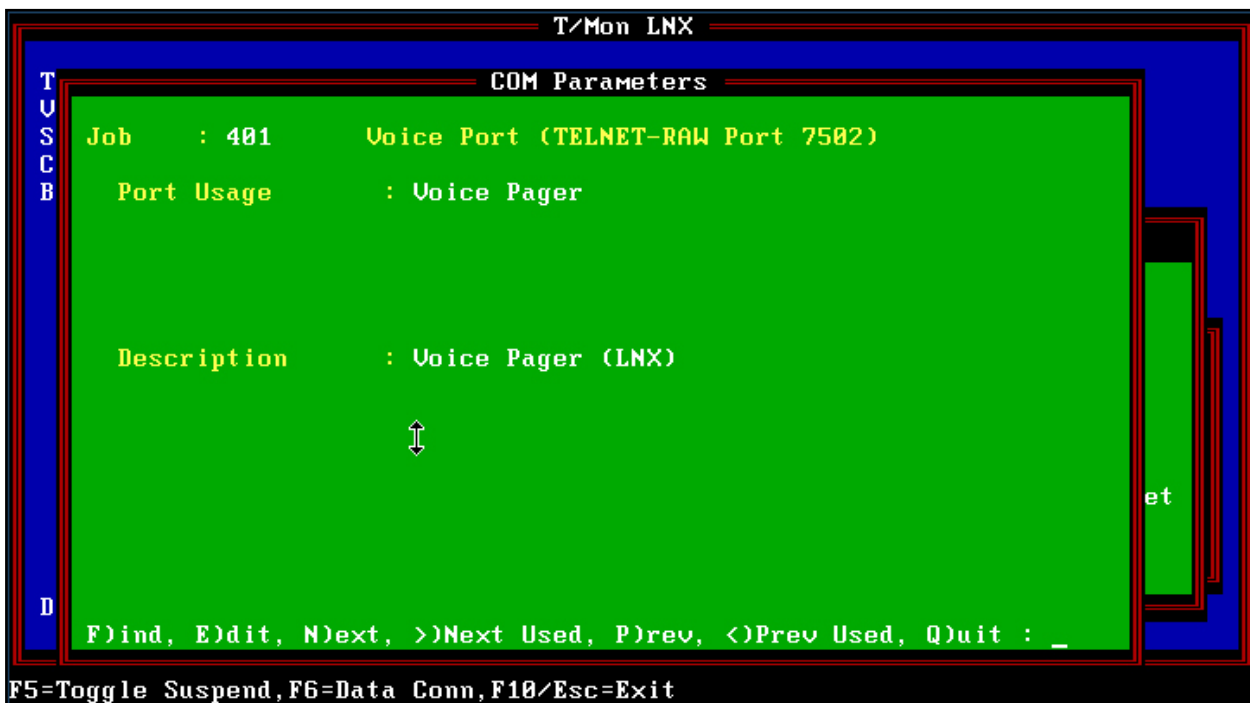
For help, configuring the pager and ethernet jobs, see section three of this manual.

### Step 1: Setup the Voice Pager Job

The Voice Pager Job is the job that “talks” to T/Mon. It is essential for the Site Dialer function.

To Configure the Voice Pager Job:

1. Go to the Remote Parameters screen (accessed from Main menu > Parameters > Remote Ports).
2. press F)ind to locate the next available job above 47.
3. Press E)dit.
4. Press Tab and select Voice Pager from the submenu.
5. Press Enter.
6. Enter a description (optional) and press Enter.



7. Press F6 to go to the Data Connection Assignment screen.
  - a. Press F1 to begin creating the assignment
  - b. Type: TELNET-RAW
  - c. IP / Host Name: Enter 127.0.0.1 (This is the default local host name.)
  - d. TCP Port: 7502. (This is the default port.)
  - e. Description: Enter a description here, such as 'Site Dialer LNX'.
  - f. Hit F8 to Save. You'll now be back on the Data Connection Assignment screen.
7. Tab over to the new data connection you've just created and press Enter.

## Step 2:

### Setup the Voice Site Dialer RTU Job

1. On the Remote Parameters screen, press F)ind to locate the next available job.
2. Press Tab to select Site Dialer from the submenu, then press Enter. (This is the job that "talks" to the Site Dialer RTU.)
3. Description is optional. Press Enter to select all the defaults for Time Out, Poll Delay, Fail Threshold, Fail Poll Cycles, and Immediate Retries.
4. Press F6 to go to the Data Connection Assignment screen.

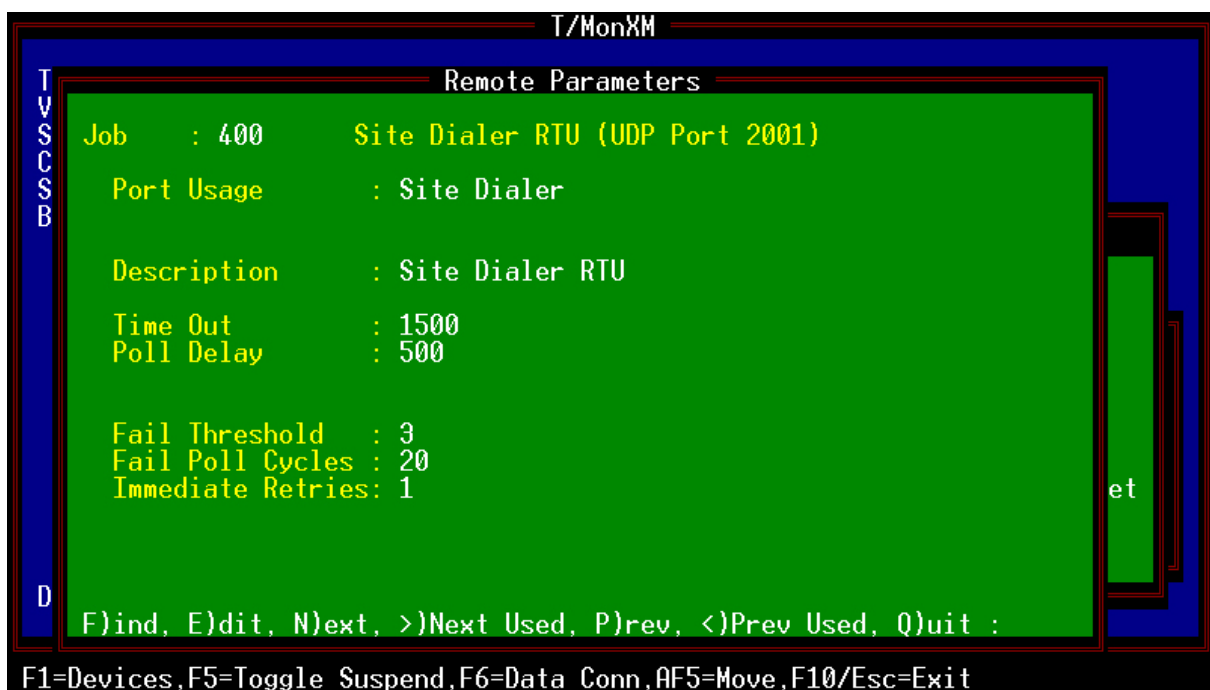


Fig. M32.2 - Remote Parameters screen defined for Site Dialer

5. Press F1 to begin creating the assignment.
  - h. Type: UDP (DPS RTU, SNMP Trap Processing, SNMP Agent)
  - i. TCP Port: 2001
  - j. Description: Enter a description here, such as "Site Dialer RTU".
  - k. Hit F8 to Save. You'll now be back on the Data Connection Assignment screen.
6. Tab over to the new data connection you've just created and press Enter.

### Step 3:

## Assign the Site Dialer Device

1. On the Remote Parameters screen for the Site Dialer Job, press F1 to create the device.
2. Enter the Device ID. The default is 1, unless you've changed it in the RTU. (This is the DCP address of the RTU.)
3. At the bottom of the screen, you'll see the message: "This item is not in the database. Would you like to add it (Y/N)?" Press Y)es.
4. Enter in the IP address and port (default is 2001) of the Site Dialer RTU.
5. Description and Site Name are optional.
6. For Device Type, select Site Dialer. (This is the only option.)
7. Press Enter to select all the defaults for Displays, Poll Type and Refresh Rate.
8. Press Enter to select all the defaults under Address Defaults.

```

Remote Device Definition
-----
Port / Job   : 400      Site Dialer
Device ID    : 1        192.168.1.1    / 2001

Description  : Site Dialer RTU
Site Name    : Fresno
Device Type  : Site Dialer
Displays     : 1-9
Poll Type    : U
Refresh Rate : 291

Log Undefined: N
-----
Polarity      : B      Address Defaults -----
Logging       : L      Status           : A
History       : H      Reverse          : N
Level         : A      Windows          : 
Description   : (Undefined) Message      : 0

F)ind, E)dit, D)delete, N)ext, P)rev, Q)uit : _

F1=Pts, F3=IntAlm, F5=ALG Prov, AF1=TL1, AF6=Templates, Esc=Ext
  
```

Fig. M32.3 - Device Definition Screen Defined for the Site Dialer

## Step 4:

### Assign Pager Carriers

1. Return to the Master menu and choose Files.
2. Select Pager > Pager Carriers. This is where you add your operators, who get called when an alarm comes in.
3. Enter in the Int (Initials) and Name for your operators.
4. For Type, select V for Voice.
5. For Pager/Phone, enter the phone number to call.
6. The ID/Delay field should be filled in for added security. This is the ID you'll press on your phone to acknowledge an alarm. Example: If your ID is 123, you'll press 123# to ack an alarm from your phone. If you did not enter in an ID, you'll simply press # to ack.
7. Finish entering in all your operators and press F8 to Save.

## Step 4:

### Assign Pager Carriers

1. From the Pager sub-menu, select Voice Format.
2. Define what T/Mon fields you;d like to include the spoken phrase.

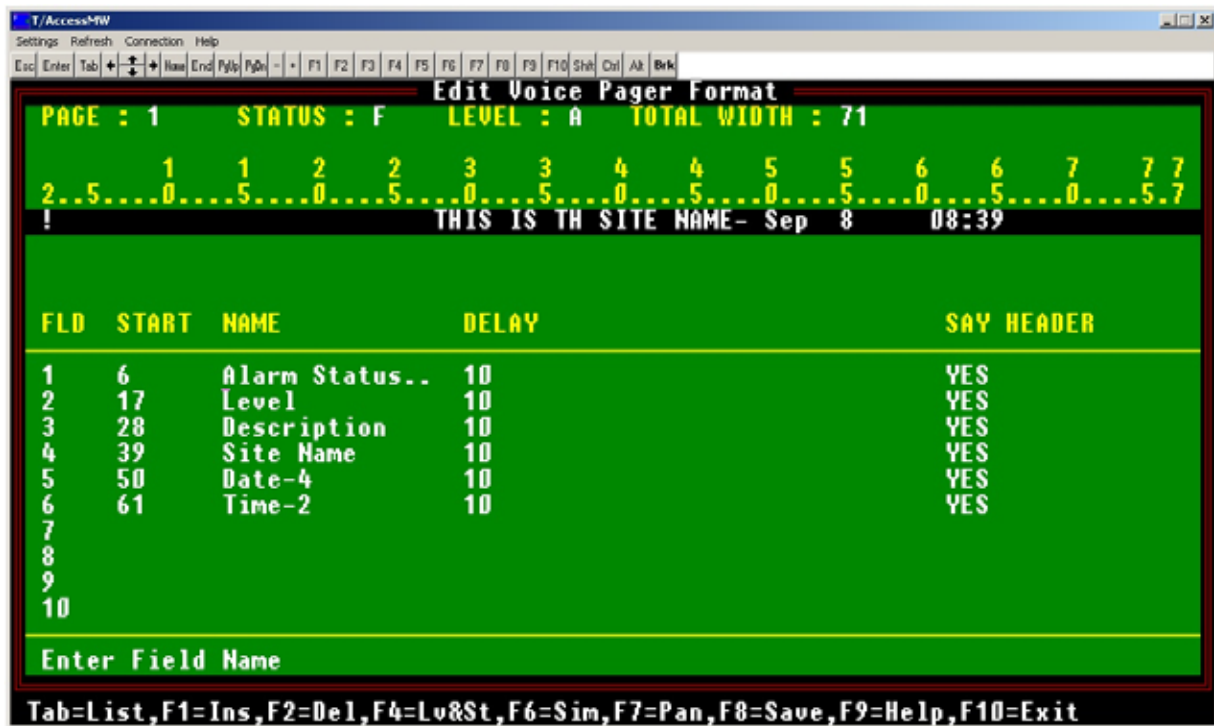


Fig. M32-4 Edit Voice Pager Format Screen

# Appendix A

## ASCII Tutorial

---

### Introduction: How To Use This Tutorial

This tutorial expands upon the ASCII Reference sections, Software Module 6 for basic ASCII processing and the extensions provided by ASCII auto-databasing. It provides a number of practical examples to illustrate the methods described in those sections. Before starting the tutorial, we suggest that you:

1. Scan through Basic Concepts and ASCII Terms in Software Module 6, pages M6-3 – M6-5, to get a general idea of how ASCII processing works, without at this point trying to understand it all.
2. Scan through the Language Reference tables on pages M6-13 – M6-24 to get a general idea of how databasing is done and what the various commands do.
3. Scan through the debugger section beginning on page M6-38 to get a general idea of what it can do.
4. Review the Alarm Processing section on page M6-44 for the method you will be using, Dialup or Direct Connect. If you will be using auto-databasing, review sections M6-67 to M6-82 as well.

Then, after you have gained a general picture of ASCII processing, go through this tutorial in detail, working the examples and relating them to the preceding reference materials.

The tutorial makes use of sample input messages which are available for use with the debugger in file ALDEMO.REP. This file is included with ASCII module distribution disks.

**Note:** Use the ASCII worksheet on section A-28 as a reference guide. See section A-29 for special rules questions and examples. Refer to section A-33 for an illustration of an ASCII databasing map.

## Overview: ASCII Messages

Some devices present alarm information in the form of ordinary text-based messages. Some examples:

```
Low Oil Pressure
Out Of Paper
Paper Jam
No Dial Tone
```

```
***ALARM CELL 47 DOOR OPEN
***CLEAR CELL 47 DOOR OPEN
```

```
**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILED
    STATE: OFF NORMAL
    DEVICE - TTY0
07/23/00 14 #855650
```

← *Sets an alarm*

```
**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILED
    STATE: NORMAL
07/23/00 14 #855650
```

← *Clears same alarm*

```
STATUS REPORT CELL 47
DOOR                OPEN
TOWER LIGHT         ON
GENERATOR            OFF
TEMPERATURE          NORMAL
GATE                 LOCKED
```

← *Data arranged in columns*

```
FRESNO 99-08-17 09:38:40
** 344 REPT ALM T1
    "RECTIFIER:CR,DOWN,SA,, ,NEND,NA"
```

← *TL1, a common ASCII format*

The purpose of ASCII processing is to receive incoming ASCII text, interpret what it says, and generate alarm information as appropriate. To the user, alarms triggered by ASCII input look just like any other alarm. It doesn't matter how an alarm is reported - they all end up being presented in the same common T/Mon format.

Due to the free-form nature of ASCII text, messages can say almost anything and be arranged in almost any arbitrary pattern. You usually don't have any control over this and have to accept them as is. This greatly complicates the databasing of ASCII alarms, since T/Mon essentially has to be trained to recognize and respond to particular patterns and phrases in ordinary text. This is second nature to most people, but not so easy for a computer. The following pages explain how it does it.

## Overview: How the ASCII Processor (Message Processing) Works

ASCII Processing has two major parts: Message Processing and Alarm Processing. This page describes Message Processing, which is set up under Files - ASCII Devices.


When the system is in use, ASCII text comes streaming in an ASCII port. Some of it may contain alarm information, some may have nothing to do with alarms at all.

Using Pattern Recognition Rules, the ASCII Processor detects potentially significant alarm messages and notes where they begin and end.

There are three key pieces of information you must get from any ASCII message:

- 1) The site name, which identifies the message source,
- 2) The unique point identifier, which uniquely identifies that alarm, and
- 3) The alarm state, which indicates it failing or what indicates it clearing.

```
login: dpsuser3
Passing on SIGTERM to 222666
TECH ENTERING SITE
TIME CHECK 1453
HI TOM
**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILED
    STATE: OFF NORMAL
    DEVICE - TTY0
07/23/00 14 #855650
BYE TOM
TECH LEAVING SITE
CRC error 1297 - retransmitting
```



```
**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILED
    STATE: OFF NORMAL
    DEVICE - TTY0
07/23/00 14 #855650
```

Using Extraction Rules, the ASCII Processor locates significant parts of the message and copies them into slots, which are pigeonholes for temporarily holding ASCII text. Slots 1-9 are used for action information, slots 10-14 for sites.

In this example, following the rules it has been given for this device, the ASCII Processor copies the cell number (75), the scan point (2) and offset (1), and the alarm state (OFF) into slots noted below.

Action Slot Number :	1	2	3	4	5	6	7	8	9
Action Slot Contents:	<b>75</b>	<b>2</b>		<b>1</b>				<b>OFF</b>	

The rules also tell it to add colons in certain slots to act as separators between other slots:

Action Slot Number :	1	2	3	4	5	6	7	8	9
Action Slot Contents:	<b>75</b>	:	<b>2</b>	:	<b>1</b>		:	<b>OFF</b>	

The Site Slots have only one entry, the cell number (75):

Site Slot Number :	10	11	12	13	14
Site Slot Contents:	<b>75</b>				

Finally, the ASCII Processor squeezes the slot contents together into continuous strings of characters called keys. Any empty slots are omitted:

Action Key:	<b>75:2:1:OFF</b>
Site Key:	<b>75</b>

*Note that these keys uniquely identify exactly what happened, and where it happened, in highly compressed form. They are the end product of message processing, and will be passed on to the alarm processor to actually generate an alarm.*



## Overview: How the ASCII Processor (the Alarm Processor) Works

This page describes the second part of ASCII Processing, the Alarm Processor, which receives ASCII keys from the Message Processor and acts upon them to generate alarms.

In T/Mon, ASCII Alarm Points are set up exactly like any other alarm, using the standard T/Mon point editing screens.

In addition, each ASCII alarm point is databased with two action strings, one to set the alarm and another to clear it. When an action key is received from the Message Processor, the Alarm Processor searches for a matching action string and takes appropriate action if it is found. It is this match of action keys to action strings that links an incoming ASCII message to an actual alarm.

In our example, if Action Key 75:2:1:OFF has been generated by the Message Processor, and the following has been entered for action keys on the port receiving the message, then alarm 2 will be set.

ASCII Alarm Database Entries: Key generated by Message Processor:

PNT	Type	Action String	Action Key
1	SET	75:1:2:OFF	75:2:1:OFF
	CLEAR	75:1:2:NORMAL	
2	SET	75:2:1:OFF	75:2:1:OFF
	CLEAR	75:2:1:NORMAL	
3	SET	75:3:0:OFF	75:2:1:OFF
	CLEAR	75:3:0:NORMAL	
4	SET	75:5:2:OFF	75:2:1:OFF
	CLEAR	75:5:2:NORMAL	
5	SET	221:1:2:OFF	75:2:1:OFF
	CLEAR	221:1:2:NORMAL	
6	SET	221:3:0:OFF	75:2:1:OFF
	CLEAR	221:3:0:NORMAL	
7	SET	221:5:2:OFF	75:2:1:OFF
	CLEAR	221:5:2:NORMAL	
...	...	...	...

The Action String table shown above can be entered into the database three different ways:

- Manually, under a specific port, address, and display. The site key is not significant in this case.
- As a template, which is useful if a number of different sites are identically equipped and report alarm information the same way, differing only in a site identification that can be extracted from an incoming message. In this case, Action Strings are filled out only for a generic template site that represents them all. Site strings are then filled out manually under the appropriate port to route alarms from different sites to specific addresses.
- Automatically, available only if the ASCII auto-databasing module is installed. You do not have to enter alarm information at all; instead, the system derives it from incoming messages. If a particular alarm has not yet been entered in the database it is added automatically. Over time, the database populates itself. Site strings must be filled out manually under the appropriate port to route alarms from different sites to specific addresses.

## Recognizing Patterns In Messages

In the simplest possible case, we could be receiving simple, unique, one-line messages for a limited number of possible alarms. In such a case, we could simply make our **pattern recognition rules** recognize the entire message, have our **extraction rules** build an action key out of the entire message, and set up **action strings** for each possible alarm. We would need a set of rules for each possible alarm.

**Example:** *if we have a printer that can send messages such as OUT OF PAPER to a T/Mon ASCII port, we could set up a pattern recognition rule to recognize the input line OUT OF PAPER, set up an extraction rule to create an action key OUT OF PAPER, and set up an action string OUT OF PAPER for a particular alarm on that port.*

Things usually aren't this simple. In the next example, we are receiving messages that identify a particular piece of equipment and a particular fault condition:

```
PRINTER 3    PAPER JAM
PRINTER 12   TONER LOW
PRINTER 3    PAPER JAM   CLEARED
```

In this case, we have a pattern — things that stay the same for all messages of this type. Some things we might note about this pattern are:

- All the messages are just one line long
- They all start with the word PRINTER
- That word is always followed by a number containing one or more digits
- There is a condition that follows after a few spaces;
- The conditions all seem to line up in a vertical column.

We could detect this pattern by setting up a **pattern recognition rule** that would look for lines starting with the word PRINTER followed by a space and then a number. If it passes this pattern recognition test, we could invoke an **extraction rule** that would create an action key consisting of just the number and the condition. Since these are in predictable locations in the message, we could use just one pattern recognition rule and one extraction rule to cover all messages of this type

On the alarm processing side, we would still have to enter individual **action strings** for all possible alarms that we are interested in. If the Auto Databasing ASCII software module is available, it can automate this process and greatly reduce the work required to set up an ASCII processing system.

- The next example shows several multi-line messages that have a common pattern:

```
**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILED
    STATE: OFF NORMAL
    DEVICE - TTY0
07/23/00 14 #855650

**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILURE
    STATE: NORMAL
07/23/00 14 #855653

* 56 REPT:CELL 221 ALARM SCANNING
    SCAN POINT:OFFSET 5, BIT 2
    ALARM: DOOR ALARM
    STATE: OFF NORMAL
07/23/00 56 #855638
```

We might guess that messages of this type have the following patterns in common:

- The first line starts with an asterisk
- (sometimes more than one, possibly indicating severity)
- The first line contains REPT:CELL, ALARM, and SCANNING
- The first line also contains a number that could identify a particular location
- The second line contains SCAN and POINT, and some numbers identifying a particular alarm
- The third line contains ALARM and a description of the alarm in plain text
- The fourth line contains STATE and NORMAL
- The fourth line also seems to contain OFF if this is an alarm, but not if it is a clear
- One or two lines follow, ending with a date

- The final example shows two messages in TL1 format, a very common type of ASCII report:

```
RGXT11M 07-23-00 18:30:33
M 305 COMPLD
"DOM133,EQPT:CR,DOWN,SA,, ,NEND,NA"

RGXT11M 07-23-00 18:39:33
M 12 COMPLD
"XRB122,,,,,,NEND,NA"
"TON17,EQPT:MJ,,,,,, "
```

Although these messages show some obvious patterns, it would be difficult to decipher what they actually mean or determine what parts to extract unless you had access to a TL1 manual.

- Conclusion: In simple cases, you can usually figure patterns out by looking at a few typical messages. For more complex cases such as those shown on this page, you may have to have a technical description available in order to make much sense of the message format and contents.

---

## Lines, Columns, Fields and Separators

In a typical ASCII message, there are some obvious structural elements:

```

**14 REPT:CELL 75 ALARM SCANNING
    SCAN POINT:OFFSET 2, BIT 1
    ALARM: POWER CABINET AC FAILED
    STATE: OFF NORMAL
    DEVICE - TTY0
07/23/00 14 #855650

```

- This message contains six **lines**. Although you can't see it, the incoming ASCII message actually contains a special character (usually a *line feed*) to mark the end of each line. In setting up ASCII rules, you will need to specify the line terminator character used by each ASCII device.
- Some information appears in particular **columns** - for example, the first line begins with an asterisk in column one, and the alarm description begins on line 3 column 13. It may be useful to locate certain parts by column, particularly if the incoming message is arranged in column form.
- The message contains a number of words, phrases, numbers, dates, and punctuation symbols. Although we don't often think of it this way, an ordinary written word is distinguished by what surrounds it, usually spaces. A sentence ends with a period. A quotation is enclosed by quotation marks. A paragraph starts on a new line and is often indented. Messages also include invisible control characters such as tabs, carriage returns, and line feeds. These all represent different ways to mark special parts of the text so they can be recognized and given an appropriate interpretation.

In ASCII processing, a portion of text that can be distinguished from what surrounds it is called a **field**. For instance, the 75 in the first line of the message above is a field identifying a particular alarm location. POWER CABINET AC FAILED is a field describing the alarm itself.

How can we pick out a field? By using **field separators**, which are individual ASCII characters such as spaces, commas, periods, line feeds, and so forth. The ASCII processor recognizes two kinds of separators, **soft field separators** and **hard field separators**. The difference between them is:

- Commands that act on fields have two forms: one will end the field on any separator, hard or soft; the other only on a hard separator. For example, if spaces are soft separators and commas hard, and we have the following text:

OFFSET 2, BIT 1

then the ASCII processor command \K1 (which puts the current field in Slot 1) would extract the field OFFSET (stopping at the space), but the hard-field form \KH1 would extract the field as OFFSET 2 (stopping only at the comma).

- Multiple soft separators in succession are treated as a single separator, but multiple hard separators each mark a different field. For example, if spaces are soft separators and commas hard, and we have the following pair of input lines:

OFFSET 2 BIT 1  
OFFSET 2,,,BIT 1

then, if we are using the any separator form of a command, the word BIT would be the third field in the top line but the sixth field in the bottom line (fields 3 to 5 would be empty, but would still count as fields).

---

## Example 1: Using Separators

This example works with the following input text:

```
Separator Demo   ,Commas,,, End Demo<0D><0A>
```

(The word Separator starts in column 1, there are three spaces following Demo, then a comma, the word Commas, three more commas and a space before End Demo. The line ends with the standard Carriage Return - Line Feed sequence, hex <0D><0A>)

From the Master Menu, select Files - ASCII Devices - ASCII Rules.

Select F)ind, enter ASCII DEVICE = SEPS, Rule # = 0, then enter the following header rule.

You can enter the the space by hitting the space bar, then Enter. For the hex characters 0D and 0A be sure you use zeros, not the letter O. Notice that the screen display for these characters changes to a more human-readable form after they have been entered.

```
Description      :  Separator Demonstration
Soft Separators   :  Space 0D
Hard Separators   :
Line Terminator   :  0A
```

Hit Enter to accept defaults for all other entries on this screen, then select F)ind, accept SEPS as the ASCII Device, then enter the following:

```
Rule              : 10
Descr             : Separator Demonstration
Pattern Recognition 1 : \MSEPARATOR\F1\F1\F1\F1
Action Extraction 1  : \K1\F1\K2\F1\K3\F1\K4\F1\K5
```

Hit Enter to accept defaults for all other entries on this screen, then select F4 = Debug.

On the debug screen, hit F2 to select input text, then F2 again to select the file ALDEMO.REP.

Locate the text under EXAMPLE 1 (should be just one line starting **Separator Demo**), use F4 to toggle marking, then Enter to accept.

On the debug screen, note the following:

- Input text has been converted to all upper-case. The ASCII processor always converts inputs to upper-case and is consequently not case-sensitive.
- Soft Separators are in green. Spaces used as soft separators show as a green squares or stripes.
- Line Terminator is in red.

Repeatedly hit C to step by individual command, noting the position of the pointer in the upper window (a single highlighted character) and the highlighted command in the lower window (this is the next command to be executed, before it executes).

In this example, the pattern recognition commands simply step through the fields one at time and the extraction commands put the first 5 fields it finds in the Action Key. When all commands have executed, select F4 to view the resultant keys.

Escape out of the debugger, use P)rev to get back to rule 0 (header rule) for SEPS, and **delete the carriage return** from the list of **soft field separators**. Leave all other entries the same and save the page. Use N)ext to get back to Rule 10 and select F2 to start the debugger (notice that the debugger can only start from a numbered rule). Repeatedly hit C to step by individual command. Note the difference in the results.

The primary effect is that <0D> gets appended to the end of the Action Key, which *will not* match an Action String that does not also contain it. You can't enter a carriage return character when you are editing Action Strings, so you won't get any alarms. The lesson is: **always include 0D as a soft separator when you are dealing with ASCII lines terminated by a carriage return-line feed sequence**, which will be the case most of the time.

Escape out of the debugger, return to the header rule, and enter 0A as a soft field separator and 0D as the line terminator character (this is backwards from their usual usage). Then get back into the debugger and observe the results.

The primary effect is that lines after the first line don't begin where you expect them to - they have a 0A in front. This might not have an adverse effect with some rules, but could disable others.

Escape out of the debugger, return to the header rule, and restore 0D as a soft field separator and 0A as the line terminator. Then define a hard field separator as a comma. Then get back into the debugger and observe the results.

Notice that hard-field separators are shown in yellow in the upper window. There is a profound effect on what the processor considers to be a field.

Escape out of the debugger and change all of the extraction rules to their **hard-field** forms:

Action Extraction    1    : \KH1\FH1\KH2\FH1\KH3\FH1\KH4\FH1\KH5

Get back into the debugger and step through all commands, noting the differences.

## Example 2: A Typical Multi-line Input Message

This example works with the following input text: (all lines start in column 1 and end with the standard Carriage Return - Line Feed sequence)

Example of alarm occurring:

```
02/21/01 09:04:10 #25623

** 04 REPT:CELL 14 ALARM SCANNING
SCAN POINT: 27
ALARM: CELL SITE INTRUSION
STATE: ALARM
```

Example of alarm clearing:

```
02/21/01 09:04:10 #25674

** 04 REPT:CELL 14 ALARM SCANNING
SCAN POINT: 27
ALARM: CELL SITE INTRUSION
STATE: NORMAL
```

You need to know something about what these messages mean, how to recognize them as a whole, and how to locate the fields within them that uniquely identify a particular alarm and its state. You can find this out by looking at a number of sample messages and puzzling out the answers, or by looking at documentation if you are fortunate enough to have it. In this case, we'll just tell you:

- The top line is a date/time stamp plus message number, not useful for identifying a particular alarm but could help the system recognize that a message in this format is coming in.
- **\*\*** indicates severity - one asterisk is minor, two major, three critical.
- **04 REPT:CELL** is a message type identifier that appears on all messages in this format.
- **14** is the site identifier and will be different for alarms coming from different sites. This could be significant in uniquely identifying an alarm if we are working with different sites. We will assume in this example that it is.
- **ALARM SCANNING** and **SCAN POINT**: appears in all alarm messages in this format, could help identify the format but otherwise doesn't tell us anything.
- **27** is very useful, tells us uniquely what specific alarm is involved.
- **ALARM**: is just a heading, appears in all alarm message in this format.
- **CELL SITE INTRUSION** says in plain English what point 27 is but doesn't tell us anything new. For interpretation by the computer it is better to work with the most compact symbology we can find rather than longer human-oriented text like this, so we will use the 27.
- **STATE**: is just another heading, but the word following it is the only thing in the message that tells us what this particular point is doing.

For purposes of setting or clearing an alarm, it appears that this message can be reduced to:

- The numeric cell identifier contained in the field following **REPT:CELL**
- The numeric alarm identifier contained in the field following **SCAN POINT**:
- The state expressed in the field following **STATE**:

## Pattern Recognition

The first thing we need to do is recognize when a message in this pattern is coming in, bearing in mind that it could be embedded in streams of text containing all kinds of other messages and random traffic. There are usually many different ways to do this; the important thing is to check enough of the fixed parts of the message to be reasonably sure that we are looking at a message of this type while filtering everything else out. We also need to accept all of the lines in the pattern recognition phase that we will be using later in extraction, because in general the extraction processor only works with lines captured between the beginning and end of pattern recognition.

A possible set of pattern recognition command lines follows:

1. `\M\M\M:\M:` Looks for a line containing two forward slashes and two colons, passes if those characters are found anywhere in the line in that order. This command line would accept the time stamp line at the top of the message.
2. `\M~BL` Match Blank Line, accepts and skips over blank line following time stamp.
3. `\MREPT:CELL` Passes if the string REPT:CELL is found in the third line
4. `\MSCAN` Passes if the word SCAN is found in the fourth line
5. `\M~AL` Match Any Line, accepts and skips over the fifth line
6. `\MSTATE` Passes if the word STATE is found in the sixth line

It is very unlikely that we would find 5 lines like this unless we were looking at a message in this format, so this series of commands is probably sufficient. We have also recognized all of the lines that will be needed for extraction, so can go on to the next phase.

## Action Extraction

The next thing is to extract those parts of the message that uniquely identify a particular point and state. Where Pattern Recognition focuses on the parts of the message that are always the same, extraction focuses on those parts that are different for different alarms. On the preceding page we decided that just three fields would be sufficient: the number following REPT:CELL, the number following SCAN POINT:, and the word following STATE. Remembering that we extract text into slots, and slots are connected together to form keys, we could extract just those three fields to form the following Action Keys:

1427ALARM      and      1427NORMAL

There is an obvious problem with this: when we string the two numbers together we can't tell where one ends and the next begins, and the same key would be generated by point 7 on cell 142. The solution is to put literals between numbers to act as separators. It doesn't matter what they are; in this case we will put a C before the cell number and a P before the point, which will help humans interpret the key as well as resolve ambiguity to the computer. The resultant Actions Keys are

C14P27ALARM      and      C14P27NORMAL

Having decided what the keys should contain, we now need to write rules to create them.



It is useful at this point to plan our slot usage by filling out a slot table, which is simply a list on paper of what will be going in the various slots. Action Keys are always generated by connecting the contents of slots 1-9 together in that order, ignoring empty slots. Site Keys are generated from slots 10-14 in a similar manner. In our example we don't need a site keys, so a possible slot table would look like this:

### Slot Contents

1. Literal 'C'
2. Cell number, numeric field following REPT:CELL on line 3
3. Literal 'P'
4. Point number, numeric field following POINT: on line 4
5. State, field following STATE: on line 6

It is now very easy to write the rules for the Action Extraction phase:

1. \T2\L1C\MCELL\F1\K2
  - Throw away the first two lines. Extraction starts over on the first line of text, but we don't need anything until line 3.
  - Put C in slot 1
  - Match (find) CELL, then skip to 1st field following
  - Put contents of that field in slot 2
2. \L3P\MPOINT:\F1\K4
  - Put P in slot 3
  - Match (find) POINT:, then skip to 1st field following
  - Put contents of that field in slot 4
3. \T1\MSTATE:\F1\K5
  - Throw away next line
  - Match (find) STATE:, then skip to 1st field following
  - Put contents of that field in slot 5

Planning the rules for Example 2 is now done. To test:

- Under Files - ASCII Devices, create a new device type named EX2.
- Complete the header record using spaces and carriage returns as soft separators, no hard separators, line feed as line terminator.
- Create Rule 10, enter the Pattern Recognition and Action Extraction commands described above.
- Bring up the debugger, select the alarm message under EXAMPLE 2, step through all commands, and verify the extracted key by viewing slot contents at the end of extraction.
- Repeat using the clear message under EXAMPLE 2 as input.

If this were to be an operational alarm, there is one more stage of databasing:

- A physical ASCII input port needs to be designated and set up with appropriate parameters.
- Under F1=Devices, set up address 0 with Device Type = EX2
- From the Device screen, select F1=Points to define an alarm corresponding to this ASCII message.
- From the Device screen, select F2= ASCII Actions. Enter the SET and CLEAR action strings derived above (SET=C14P27ALARM and CLEAR=C14P27NORMAL).
- If you have a way to send ASCII messages to your T/Mon (external terminal, etc) try sending the messages for EXAMPLES 2 from the ALDEMO.REP file. Actual alarm activity should occur. If you select Shift-F7 from the alarm summary screen, you can view the ASCII processing in action.

---

## Example 3: Exercise

This example works with the following input text:

(all lines end with the standard Carriage Return - Line Feed sequence)

Example of alarm occurring (first line starts in column 1, other lines have leading spaces):

```
**38  REPT: AP 1, RCS 210, ALARM, EQUIPMENT MALFUNCTION
      MICROCELL 1 SIGNALING LINK UNAVAILABLE [APPLNKU]
      PERCEIVED SEVERITY: MAJ
      FRAME 1, SLOT 1
      1999-12-03 09:15:34 REPORT FINAL
```

Example of alarm clearing (first line starts in column 2, other lines have leading spaces):

```
 39  REPT: AP 1, RCS 210, ALARM CLEARED
      MICROCELL 1 SIGNALING LINK UNAVAILABLE [APPLNKU]
      1999-12-03 09:16:50 REPORT FINAL
```

**AP** stands for Alarm Point, **RCS** stands for a particular cell site.

Write pattern recognition and extraction rules to build suitable keys from these messages, then test with the ASCII debugger.

## Example 4: Using ASCII Tables

This example works with the following three messages: (all lines start in column 1 and end with the standard Carriage Return - Line Feed sequence)

```
ALARM HISTORY - SCU 4 - 06/29/00
-----
Type          Date          Initial Current Count
-----
LOS,Line 06/29/00 13:00:00 ok ALARM 19
```

```
ALARM HISTORY - SCU 4 - 06/29/00
-----
Type          Date          Initial Current Count
-----
LOS,Line 06/29/00 14:00:00 ok ok 0
```

```
ALARM HISTORY - SCU 4 - 06/29/00
-----
Type          Date          Initial Current Count
-----
LOS,Line 06/29/00 15:00:00 ok ALARM 8
```

In this example, we will recognize the pattern by matching on the words ALARM, HISTORY, and SCU in the first line, and the series of hyphens in line 2 and 4.

We want to generate different alarms depending upon the Count found in line 5: no alarm if it is 0, a minor (level C) alarm if it is between 1 and 10, and a major (level B) alarm if it is more than 10.

The action key should contain the number following SCU on line 1, the Type field on line 5, and something to indicate the level that is derived from Count. ASCII Tables provide an ideal way to convert counts into keys, and are generally useful in any situation where keys need to be translated in some way from the text that is actually being received.

### Pattern Recognition Rules

1. \MALARM\MHISTORY\MSCU Search for the essential words in the first line.
2. \M----- Match enough dashes to be satisfied they are there.
3. \M~AL Use this to get to the next line.
4. \M----- Match some more dashes.
5. \M~AL We are satisfied we're looking at the right kind of message, and don't need any more pattern recognition, but need to accept line 5 here because it is going to be used in the extraction phase.

### Action Extraction Rules

1. \MSCU\F1\K1\KL2: Find the number following SCU and put it in key slot 1. Put a colon in key slot 2 as a separator.
2. \T3\K3\KL4:\A41\V1\XSCU Throw away 3 lines, then put the contents of the first field on line 5 in key slot 3 followed by a colon in slot 4. Go to absolute column position 41, put the contents of that field in Variable slot 1, and execute the ASCII table named SCU.

**ASCII Table SCU**

Build this table by escaping out of the ASCII Device Rules screen, then select ASCII Tables from the ASCII Devices menu. Select F)ind and enter SCU as the Table Name. There will be three entries in this table (for each, do a Find to set up the entry number):

**Entry 1:**

Descr:	SCU NO ALARM		
Condition 1:	Key: V1	Type: NUMERIC	OP: = Value: 0
Condition 2:	(leave blank)		
TRUE action:	Key: K5	New Value: NIL	Gen Key: N
FALSE action:	leave blank		

This entry says: if the numeric value contained in Variable Slot 1 equals 0, then put the word NIL in Key slot 5. Do NOT generate a key (and a subsequent alarm) at this point - this will happen automatically, one time, when extraction is complete.

**Entry 2:**

Descr:	SCU MINOR		
Condition 1:	Key: V1	Type: NUMERIC	OP: >Value: 0
Condition 2:	Key: V1	Type: NUMERIC	OP: <=Value:10
TRUE action:	Key: K5	New Value: MIN	Gen Key: N
FALSE action:	(leave blank)		

This entry says: if the numeric value contained in Variable Slot 1 is greater than 0, AND that same value is less than or equal to 10, then put the word MIN in Key slot 5.

**Entry 3:**

Descr:	SCU MAJOR		
Condition 1:	Key: V1	Type: NUMERIC	OP: >Value: 10
Condition 2:	(leave blank)		
TRUE action:	Key: K5	New Value: MAJ	Gen Key: N
FALSE action:	(leave blank)		

This entry says: if the numeric value contained in Variable Slot 1 is greater than 10, then put the word MAJ in Key slot 5.

Enter the ASCII rules and table on the appropriate screens and test with the debugger. Try with all 3 sample inputs, noting how the keys develop. Also note that all table entries are executed on each trial, even though only one of them takes effect.

In an actual application, you would define three different alarms to represent these three conditions:

The alarm with SET Action String= 4:LOS,LINE:MAJ would be defined as level B.

The alarm with SET Action String= 4:LOS,LINE:MIN would be defined as level C.

The alarm with SET Action String= 4:LOS,LINE:NIL would be defined as NOLOG.

Since there is no explicit CLEAR action, these alarms would have to be removed manually by highlighting on the Standing page, selecting F7=ASCII, then F3=Ack. You could also remove all standing ASCII alarms collectively by selecting Ctrl-F7 from the Standing page.

## Example 5: While Loops

This example works with the following message: (all lines start in column 1 and end with the standard Carriage Return - Line Feed sequence)

```
ALARM HISTORY -   SCU    4    -   06/29/00
-----
Type           Date           Initial Current Count
-----
LOS,Line       06/29/00 13:00:00   ok    ALARM 19
LOS,DTE        06/29/00 14:16:58   ok    ALARM 5
LOS,SCU        06/29/00 14:28:33   ok    ok    0
LOF,Line       06/29/00 17:05:22   ok    ALARM 7
-----
```

In this example, we will recognize the pattern by matching on the words ALARM, HISTORY, and SCU in the first line, and the series of hyphens in line 2 and 4. That heading may be followed by a variable number of detail lines - we don't know in advance how many there will be, so we will use a WHILE loop to process all of them. Loops are the exception to the rule that we must match at least as many lines in pattern recognition as we are going to use in extraction: when using loops, pattern recognition needs to go only to the beginning of the loop. We also need a way to recognize when the loop should be exited. Since a WHILE loop continues as long as some condition is true, we need to look for something that will always be there on a valid detail line and is absent otherwise. In this case we will look for the two colons in the time field and quit if we don't find them.

We want to generate an alarm whenever the Current field shows ALARM, clear it when it is ok.

For each detail line an action key should be generated containing the number following SCU on line 1, the Type field, and the Current field.

### Pattern Recognition Rules

1. \MALARM\MHISTORY\MSCU Search for the essential words in the first line.
2. \M----- Match enough dashes to be satisfied they are there.
3. \M~AL Use this to get to the next line.
4. \M----- Match some more dashes.

### Action Extraction Rules

1. \MSCU\F1\K1 Find the number following SCU and put it in key slot 1.
2. \T3\W\M:\M:\D\K2\A35\K3\E Throw away 3 lines, then start the While loop. Match a colon, then another colon; the loop will terminate if either match fails, otherwise Do the loop. Put the contents of the first field in key slot 2 (note that the pointer resets to the start of the line when the Do begins). Then go to absolute column position 35 and put the contents of that field in Key slot 3. A new key will be generated upon reaching the End command.

Enter the ASCII rules and table on the appropriate screens and test with the debugger. Observe the slot contents at the completion of each loop.

## Example 6: While Line Loops

This example works with the following message:

(all lines start in column 1 and end with the standard Carriage Return - Line Feed sequence)

```
FIRE SUPPRESSION ALARM
BLDG 37           ZONE 12
OVERTEMP, SMOKE, FIRE, HALON
```

In this example, we will recognize the pattern by matching on the words FIRE SUPPRESSION in the first line and the words BLDG and ZONE in line two. The third line may contain a variable number of detailed conditions separated by commas - we don't know in advance how many there will be, so we will use a While Line loop to process all of them.

For each detailed condition an action key should be generated that looks like the following:

```
FS:37:12:OVERTEMP:ALARM
```

FS stands for Fire Suppression, the numbers are Bldg and Zone respectively, Overtemp is the condition, and Alarm is the state.

In the header rule (rule 0), define commas as hard field separators, since they delimit the conditions.

### Pattern Recognition Rules

- |                        |  |
|------------------------|--|
| 1. \MFIRE\MSUPPRESSION | Search for the essential words in the first line.  |
| 2. \MBLDG\MZONE        | Search for the essential words in the second line. |
| 3. \M~AL               | Need this to get to the detail line.               |

### Action Extraction Rules

- |   |  |
|---|--|
| 1. \MSUPPRESSION\F1\K9                            | Put the word following ALARM in key slot 9.  |
| 2. \KL1FS:\MBLDG\F1\K2\KL3:\MZONE\F1\K4\KL5:\KL7: | Put FS: in key slot 1, put the field after BLDG in key slot 2, put a colon in key slot 3, put the field after ZONE in key slot 4, and put colons in key slots 5 and 7.   |
| 3. \WL\K6\*\FH1\EL\C0                             | \WL starts the While Line loop. \K6 puts the current field in slot 6, and \* command forces a key and resultant alarm to be generated from it on each iteration of the loop. The \FH1 command makes the loop step through the input line field by field. \EL marks the end of the loop. \C0 clears all slots and suppresses the normal generation of a key that would occur upon reaching the end of a rule -otherwise the last alarm (HALON) would be generated twice |

Enter the ASCII rules and table on the appropriate screens and test with the debugger. Observe the slot contents at the completion of each loop.

## Example 7: ASCII Auto-Databasing

(applies only if the auto-databasing module is installed).

This example works with the following input text, which is the same as that used for Example 2.

All lines start in column 1 and end with a standard Carriage Return - Line Feed.

Example of alarm occurring:

```
02/21/01 09:04:10 #25623
** 04 REPT:CELL 14 ALARM SCANNING
SCAN POINT: 27
ALARM: CELL SITE INTRUSION
STATE: ALARM
```

Example of alarm clearing:

```
02/21/01 09:04:10 #25674
** 04 REPT:CELL 14 ALARM SCANNING
SCAN POINT: 27
ALARM: CELL SITE INTRUSION
STATE: NORMAL
```

In Example 2 we developed the following rules:

### Pattern Recognition Rules

- |                 |  |
|-----------------|--|
| 1. \M/\M/\M:\M: | Looks for a line containing two forward slashes and two colons, passes if those characters are found anywhere in the line in that order. |
| 2. \M~BL        | Match Blank Line, accepts and skips over blank line following time stamp.  |
| 3. \MREPT:CELL  | Passes if the string REPT:CELL is found in the third line  |
| 4. \MSCAN       | Passes if the word SCAN is found in the fourth line  |
| 5. \M~AL        | Match Any Line, accepts and skips over the fifth line  |
| 6. \MSTATE      | Passes if the word STATE is found in the sixth line  |

### Action Extraction Rules

- |                        |  |
|------------------------|--|
| 1. \T2\L1C\MCELL\F1\K2 | Throw away the first two lines. Put C in slot 1, match (find) CELL, then skip to 1st field following, put contents of that field in slot 2 |
| 2. \L3P\MPOINT:\F1\K4  | Put P in slot 3<br>Match (find) POINT:, then skip to 1st field following, put contents of that field in slot 4                             |
| 3. \T1\MSTATE:\F1\K5   | Throw away next line, match (find) STATE:, then skip to 1st field following. Put contents of that field in slot 5                          |

The resultant alarm action key is C14P27ALARM, clear is C14P27NORMAL. We will develop a slightly different action key for auto-databasing use, plus a number of additional keys.

For an overview of the auto-databasing process, please review section M6-67 to M6-82 .

In this example, we will extend Example 2 to define an entire alarm. This means we have to extract from the message itself enough information to fill out many of the entries that are usually entered manually on the standard T/Mon point editing screen, including site, level (severity), description, display windows, text message number, and pager profile number. We also have to generate both a SET Action String and a CLEAR Action String and fill out the entries that are usually made on the ASCII Action Definition screen for each point. For this example, we will also define the following:

- A Pager Extract consisting of the site number followed by the alarm description.  
**Note:** 800 Entry limit for these sections — see alternative method in Software Module 6 (ASCII Interrogator).
- A window for this particular device type. In a real-world application this would probably be something like Alcatel Switch, but in this example it will just be a window named EX7.
- If the alarm description contains the word INTRUSION, we will associate the alarm with a text message reading Call Security 123-4321. For this example this will be text message number 2.
- Pager profiles dependent upon site and severity (different people are usually on call for different sites, and management may want to be paged for critical alarms). For this example, when site number is 14, we want to assign pager profile 1 for minor alarms, 2 for major alarms, and 3 for critical alarms.

**Note:** 800 Entry limit for these sections — see alternative method in Software Module 6 (ASCII Interrogator).

To do all of this, in addition to an action key we will need to create the following keys and strings:

- Alarm Description (goes in the standard alarm description field)
- Status Key (resolves to alarm or clear condition)
- Level Key (resolves to severity A-D)
- Text Message Key (resolves to the text message number)
- Pager Profile Key (resolves to the pager profile number)
- Category Keys (up to 6 keys, each resolving to an optional display window number)
- Pager ASCII Extract (string included in pager message)

30 key slots are available for auto-databasing. Slots 1-9 are reserved for the action key, 10-14 for the site key, the remaining slots may be used for any purpose. Through key mapping, individual slots may be used multiple times to build the keys and strings listed above.

**NOTE:** See section A-28 for ASCII Worksheet.

We have determined that the input message encodes information as follows. Remember that we are setting up rules to process all messages received in this format, not just the sample message itself.

- Severity is indicated by the number of asterisks beginning line 3. One asterisk is minor, two is major, three is critical. There is always a space after the last asterisk. These will be significant in setting up the Level Key, and possibly the Text Message, Pager Profile, and Category keys.
- The number following REPT:CELL is the cell number, which represents a site.
- The number following POINT: is an alarm identification number. It has no relation to the point number that will be assigned automatically when this alarm is auto-databased, but it does identify the point uniquely and should be used as part of the action key.
- The words following ALARM: on line 5 identify the alarm in human-readable form and would be useful in the Alarm Description and as a Pager ASCII Extract.
- The word following STATE: on line 6 (ALARM or NORMAL) will determine the Status key.

It is useful to plan slot usage by drawing up a slot table. It usually doesn't matter which slot numbers are used for what as long as we build the action key in slots 1-9, site key in slots 10-14, and keep straight where the contents is coming from and where it is going.



**ASCII Tables used with Example 7**

Table EX7STS changes the words ALARM and NORMAL in slot 5, extracted from the incoming message to indicate status, to the more standard words SET and CLR. There are two table entries:

**EX7STS Table Entries****EX7STS Table Entries****Table A.1 - Slot Table**

Slot	Contents	Usage	Source
1	Cell Number	Action Key	Line 3, field after REPT:CELL
2	Colon	Action Key (separates fields)	Literal
3	Alarm Number	Action Key	Line 4, field after POINT:
4	Colon	Action Key (separates fields)	Literal
5	Status SET/CLR	Action Key	Derive from Line 6 field after STATE:
10	Cell Number	Site Key, Pager Profile Key	Line 3, field after REPT:CELL
15	Severity	Level Key Text Message Key Pager Profile Key Category 1 Key	Line 3, asterisks at beginning of line
18	Description	Alarm Description	Line 5, words following ALARM:
26	EX7	Category 2 Key (device type)	Literal

It is now easy to write the rules. The message is the same as for Example 2, so we can recognize it the same way:

**Pattern Recognition Rules**

1. \M/\M/\M:\M: Looks for a line containing two forward slashes and two colons, passes if those characters are found anywhere in the line in that order.
2. \M~BL Match Blank Line, accepts and skips over blank line following time stamp.
3. \MREPT:CELL Passes if the string REPT:CELL is found in the third line
4. \MSCAN Passes if the word SCAN is found in the fourth line
5. \M~AL Match Any Line, accepts and skips over the fifth line
6. \MSTATE Passes if the word STATE is found in the sixth line

The extraction rules are expanded to get the added information needed for auto databasing:

**Action Extraction Rules**

1. \T2\M\*\K15\MCELL\F1\K1\K10\KL2:\KL4: Throw away the first two lines. Find the first asterisk, then put entire field in key slot 15 Match (find) CELL, then skip to 1st field following. Put contents of that field in key slots 1 and 10 Put colons in key slots 2 and 4 as separators.
2. \MPOINT:\F1\K3 Match (find) POINT: then skip to 1st field following. Put contents of that field in key slot 3
3. \MALARM:\F1\KA18 Match (find) ALARM: then skip to 1st field following. Put contents of that field in key slot 18
4. \MSTATE:\F1\K5\XEX7STS\KL26EX7\!AUTO>EX7SET Match (find) STATE: then skip to 1st field following. Put contents of that field in key slot 5 (ALARM or NORMAL). Execute ASCII table EX7STS (changes slot 5 to SET or CLR). Put literal EX7in key slot 26. Do auto-databasing using ASCII table EX7SET

## Entry 1:

Descr:	CHANGE 'ALARM' TO 'SET'		
Condition 1:	Key: K5	Type: STRING	OP:= Value: ALARM
Condition 2:	leave blank		
TRUE action:	Key: K5	New Value: SET	Gen Key: N
FALSE action:	leave blank		

## Entry 2:

Descr:	CHANGE 'NORMAL' TO 'CLR'		
Condition 1:	Key: K5	Type: STRING	OP: =Value: NORMAL
Condition 2:	leave blank		
TRUE action:	Key: K5	New Value: CLR	Gen Key: N
FALSE action:	leave blank		

Table EX7SET is executed by the !AUTO command and performs a very special function in auto databasing. Remember that the Action Strings for both SET and CLEAR conditions are going to be filled in automatically the first time a message setting a particular alarm arrives. It's easy to get the SET action string - it's exactly the same as the Action Key that we generated in slots 1-9 - but we do not at this time have a CLEAR key in hand. What we need to do is examine the clear message we expect to get for this alarm, look at the action key that would be generated from it, and use a table to change the SET key we already have into the CLEAR key we expect to get at some time in the future. The system will then enter it as the CLEAR Action String for this alarm. Referring to the slot table we filled out above and the translation to it made by table EX7STS, we can see that the keys for this message should look like this:

Set:	<b>14:27:SET</b>
Clear:	<b>14:27:CLR</b>

It is going to be very easy to change the SET key into CLEAR. All we have to do is change the word SET in slot 5 into CLR, using a single entry in table EX7SET:

## Entry 1:

Descr:	CHANGE 'SET' TO 'CLR'		
Condition 1:	Key: K5	Type: STRING	OP: = Value: SET
Condition 2:	leave blank		
TRUE action:	Key: K5	New Value: CLR	Gen Key: N
FALSE action:	leave blank		

Enter both of these tables, EX7STS and EX7SET, in the usual way - from the Master Menu, select Files - ASCII Devices - ASCII Tables, and use Fjind to create the new entries.

## Key Mapping

Remember that, in addition to the Action Key generated from slots 1-9 and the Site Key\* generated from slots 10-14, we need to generate the following for use with auto databasing:

- Alarm Description (goes in the standard alarm description field)
- Status Key (resolves to alarm or clear condition)
- Level Key (resolves to severity A-D)
- Text Message Key (resolves to the text message number)
- Pager Profile Key (resolves to the pager profile number)
- Category Keys (up to 6 keys, each resolving to an optional display window number)

The purpose of Key Mapping is to permit these items to be built from the limited number of slots available, and to permit a particular slot to be used in multiple keys if appropriate. Key Mapping takes place after extraction is complete, as the first step in auto processing. The Auto ASCII Key Mapping screens have 800 entries for associating alarm point information with the alarm key data. ASCII Tables should be used in any application that needs more than 800 association entries. In this example, after consulting the slot table filled out above, the Key Mapping screen should be completed as follows. This screen is reached from the Master Menu by selecting Files - ASCII Devices - ASCII Rules, N)ext or P)rev to ASCII Device EX7 Device Header (Rule 0), then F7=Auto, select Key Mapping.

Type	#1	#2	#3	#4	#5	#6	#7
Alarm Desc	18		(use slot 18 as is)				
Status	5		(use slot 5, contains SET or CLR)				
Level	15		(use slot 15, severity, contains 1, 2, or 3 asterisks)				
Text Message	18		(use slot 18 as is, build key same as Alarm Description)				
Pager Profile	1	15	(use slot 1=site number, followed by slot 15=severity)				
Category 1	15		(use slot 15=severity, will resolve to a severity window)				
Category 2	26		(use slot 26=EX7, will resolve to a device type window)				
Category 3			(remaining windows not used)				
Category 4							
Category 5							
Category 6							

**\*Note:** Site Key identifies a particular site. Each possible incoming alarm message from a particular site must generate a Site Key that is unique to that site. Several other keys may be generated if you are using ASCII Auto-Databasing.

## Alarm Status

This screen is reached from the EX7 Device Header (Rule 0) screen by selecting F7=Auto, then Alarm Status. Its purpose is to equate the Status Key resulting from the Key Mapping above to a Status Value ALARM or CLEAR. The ASCII processor uses this to determine what kind of key is being generated. For this example, the Alarm Status screen should be filled out as follows:

Entry	String	OP	Status
1	SET	EQUAL	ALARM
2	CLR	EQUAL	CLEAR

#### Alarm Level

This screen is reached from the EX7 Device Header (Rule 0) screen by selecting F7=Auto, then Alarm Level. Its purpose is to equate the Level Key resulting from the Key Mapping above to a Level Value A,B,C or D. The ASCII processor uses this to fill in the Lev entry under point definition. For this example, the Alarm Level screen should be filled out as follows:

Entry	String	OP	Level
1	*	EQUAL	C
2	**	EQUAL	B
3	***	EQUAL	A

#### Text Message

This screen is reached from the EX7 Device Header (Rule 0) screen by selecting F7=Auto, then Text Message. Its purpose is to equate the Text Message Key resulting from Key Mapping above to a Text Message Value, which is a message number. The ASCII processor uses this to fill in the Msg entry under point definition. For this example, the Text Message screen should be filled out as follows:

Entry	String	OP	Message Number
1	INTRUSION	CONTAINS	2

The message itself is defined under Files - Text/Messages, where Call Security 123-4321 would be entered. The result would be to display this message whenever an alarm description containing the word INTRUSION is received.

#### Pager Profile

This screen is reached from the EX7 Device Header (Rule 0) screen by selecting F7=Auto, then Pager Profile. Its purpose is to equate the Pager Profile Key resulting from the Key Mapping above to a Pager Profile Value, which is a pager profile number. The ASCII processor uses this to fill in the Pager entry under point definition. For this example, the Pager Profile screen should be filled out as follows:

Entry	String	OP	Pager Profile
1	14*	EQUAL	1
2	14**	EQUAL	2
3	14***	EQUAL	3

Pager Profiles themselves are defined under Files - Pager - Profiles, then F2 to assign pager operators to each profile. We would assign operators corresponding to the on-call technicians for site 14 to each of these profiles, along with operators corresponding to escalating management levels for minor-major-critical alarms.

#### Category 1-6

This screen is reached from the EX7 Device Header (Rule 0) screen by selecting F7=Auto, then

Categories and Category #. Its purpose is to equate the Category Key resulting from the Key Mapping above to a Window Value, which is a window number. The ASCII processor uses this to fill in the Windows entry under point definition. Up to 6 window categories can be entered by the ASCII processor. The windows themselves are defined under Files - Windows. This example assumes that windows 2, 3, and 4 have been designated for Critical, Major, and Minor alarm respectively. We will also use window 27 for equipment type EX7, which is our sample device type.

For this example, the Category 1 screen should be filled out as follows:

Entry	String	OP	Window
1	***	EQUAL	2
2	**	EQUAL	3
3	*	EQUAL	4

The Category 2 screen should be filled out as follows:

Entry	String	OP	Window
1	EX7	EQUAL	27

### Testing the Auto Databasing process

Fill out all of the screens described in this example, including the ASCII Rules, Tables, and Auto Definitions. Get into the debugger and select the sample message of an alarm occurring for Examples 2 & 7. Step through the commands, observing how the slots develop. Auto databasing takes place in two stages when extraction is complete. The first stage builds everything except the CLEAR key; observe slot contents and Auto Keys at that point, step through the final stage, and observe how the CLEAR key is created.

Then select the sample message for the same alarm clearing. Step through the commands again. This time auto databasing will terminate with no action because it all gets done only when a SET occurs. However, if you view the slots you will see that a normal action key was generated, and in an actual application this would interact with the previously auto-databased action string to CLEAR the alarm.

In similar fashion, in an actual application auto databasing would terminate with no action on subsequent SETs because the database for this alarm had already been created. However, the keys that were generated would interact with that database to SET the alarm.

In an actual application, you would need to set up a port and device as described under Remote Port Definition in the ASCII Auto-Databasing module. Although there is more up-front work to set up message processing under auto-databasing, the payoff comes here: this phase is much easier than the manual method and is almost incidental to the total process. All you need to do is define the device type as EX7 under address 0, then select F7=Auto to define the address, site name, and site window to associate with each possible site key. All other ASCII databasing will take place by itself.

## Example 8: TL1 Auto-Databasing

(applies only if the auto-databasing module is installed).

This example illustrates TL1, which is a very common and highly standardized telecom network management language. Alarm reports consist of a two-line header followed by a variable number of detail lines, each reporting a single alarm. This example uses the following input text. All lines start in column 1 and end with a standard Carriage Return - Line Feed.

```
FRESNO 00-06-18 15:21:27
A 000009 REPT ALM
"FRONT DOOR:MN,OPEN,, "
"TECH ON SITE:NA,,, "
;
```

The essential information encoded in this message is:

- Message type: REPT ALM always appears in line 2 of a message reporting an alarm.
- Location: the first word in the first line is a Source Identifier (SID), which corresponds to a network element. It may contain letters, numbers, or hyphens, and is always terminated by a space. (This attribute is sometimes called a Target Identifier - TID - which means the same thing.)
- Alarm type: the first group of words in a detail line is an Access Identifier (AID), which corresponds to an alarm point. It follows an opening quote and is terminated by a colon.
- Severity: given by the two letters following the colon on a detail line. These may be CR, MJ, MN, NA, or CL (critical, major, minor, not alarmed, or clear).

There may be additional fields present in a particular application, but for our purposes they may be ignored. The essential fields noted above will always be found in the same place in any TL1 alarm message. This makes it easy to do pattern recognition, extraction, and auto databasing.

- A unique Action Key can be expressed as SID:AID:STATUS, where status is ALM or CLR. Since TL1 does not directly report status, we will use a table to derive it from the severity: the point is in an alarm state if we receive a CR, MJ, MN, or NA. If we receive a CL, it is clear.
- The Site Key is just the SID.
- Levels A,B,C,D correspond directly to the severity CR,MJ,MN and MA.
- For Alarm Description we could use just the AID, but for illustration we will use the entire detail line, which could contain further useful information in some applications.
- We could derive Text Message numbers, Pager Extracts, Pager Profiles, and Categories in much the same way as in Example 7. For this example, we will leave them out.

A slot table for this example could be set up like this:

### Field Separators

TL1 uses commas, quotes, and colons as hard field separators. For this example, under Files - ASCII Devices - ASCII Rules, create an ASCII device named EX8, and under Rule 0 enter:

**Table A.2 - Slot Table**

Slot	Contents	Usage	Source
1	SID	Action Key	Line 1, first field
2	Colon	Action Key (separates fields)	Literal
3	AID	Action Key	Detail line, field after " and before colon
4	Colon	Action Key (separates fields)	Literal
5	Status SET/CLR	Action Key	Derive from detail line field after colon
10	SID	Site Key	Line 1, first field
15	Severity	Level Key	Derive from detail line field after colon
16	Description	Alarm Description	Detail line after " to end

Soft Field Separators : <SPC> <CR>

Hard Field Separators : , " :

Line Terminator (hex) : 0A <LF>

### Pattern Recognition Rules

1. \M-\M-\M:\M: looks for a line containing two hyphens and two colons, passes if those characters are found anywhere in the line in that order.
2. \MREPT\MALM confirm that this is an alarm message.

### Action Extraction Rules

1. \F1\K1\K10\KL2:\KL4:\!AUTO>TL1  
go to first field, put contents in slots 1 and 10 put colons in slots 2 and 4 set up for auto processing using table TL1
2. \M~AL  
skip line 2
3. \W\M''\D\FH1\KH3\FH1\KH5\KH15\KA16(5,80)\XTL1SET\E  
start While loop to process multiple detail lines continue loop if quotes are found on line Do body of loop: go to field after first hard separator (a quote) put Hard field in slot 3 (up to colon) go to field after next Hard separator (colon) put Hard field in slots 5 and 15 (up to comma) go to absolute column 5, put up to next 80 characters in slot 16 execute table TL1SET (translates slot 5 levels to SET or CLR) End loop. Generate keys, do auto processing, create subsequent alarms.

### Tbl A.3 - ASCII Table Entries

Auto Definitions (reached by F7=Auto from ASCII Rules - Device Header screen):

### Automatic Key Mapping Type

Table Entry	Entry #	Condition #1				True Action		
		Key (Slot)	Type	Operator	Value	Key (Slot)	New Value	Gen Key
TL1SET	1	K5	String	=	CR	K5	SET	N
	2	K5	String	=	MJ	K5	SET	N
	3	K5	String	=	MN	K5	SET	N
	4	K5	String	=	NA	K5	SET	N
	5	K5	String	=	CL	K5	CLR	N
TL1	1	K5	String	=	SET	K5	CLR	N

Action Key	1-9
Site Key	10-14
Auto Key	15-30

T/Mon will concatenate the entries upon processing. Entry #1 will be followed by #2 with no delimiters.

### Key Mapping

Type	#1	#2	#3	#4	#5	#6	#7
Alarm Desc		16	2	1	(use description, colon, and SID)		
Status		5			(use slot 5, contains SET or CLR)		
Level		15			(use slot 15, contains TL1 severity code)		
Text Message							
Pager Profile							
Category 1		15			(will resolve to a severity window)		
Category 2							
Category 3							
Category 4							
Category 5							
Category 6							

### Alarm Status

(based on slot 5 contents after tables have executed)

Entry	String	OP	Status
1	SET	EQUAL	ALARM
2	CLR	EQUAL	CLEAR

### Alarm Level

(assigns TL1 Severity codes in slot 15 to T/Mon Levels)

Entry	String	OP	Level
1	CR	EQUAL	A
2	MJ	EQUAL	B
3	MN	EQUAL	C
4	NA	EQUAL	D

### Category 1

(assigns TL1 Severity codes in slot 15 to T/Mon alarm level windows)

Entry	String	OP	Window
1	CR	EQUAL	2
2	MJ	EQUAL	3
3	MN	EQUAL	4
4	NA	EQUAL	5



## ASCII Worksheet

Slot 1-9 = (Action Key)	1	2	3	4	5	6	7	8	9
Purpose									
Suggested	Site Name	: (literal)	Description	: (literal)	State				
From extraction									

Slot 10-14 = Site Key	10	11	12	13	14
Purpose					
Suggested	Site Name				
From extraction					

Slot 15-23 = Auto Databas- ing Keys	15	16	17	18	19	20	21	22	23
Purpose									
Suggested	Severity	Paging	Window	Window	Window	Window			
From extraction			Category 1	Category 2	Category 3	Category 4			

Slot 24-30 = Auto Databas- ing Keys	24	25	26	27	28	29	30
Purpose							
Suggested							
From extraction							

Key	Description
Action Key	An action key is created by compressing contents of slots 1-9. For example, if you enter slot 1= Fresno, slot 2= Door, slot 3=Alarm, then the generated action key would be FresnoDoorAlarm. We use delimiters to make an action key unique. For example, if you enter slot 1= Fresno, slot 2= :, slot 3= Door, slot 4= :, slot 5= Door, the generated action key would be Fresno:Door:Alarm.
Site Key	Site keys tell the T/Mon in what address to populate the database alarm.
Auto Databasing Key	Auto Databasing keys are used to tell the T/Mon what characteristics to create for an alarm (ie. severity, text messages, what windows to populate for this alarm, etc.)

---

## Clearing Multiple ASCII Alarms with a Single Message

In order to clear multiple ASCII alarms with a single message, we need to use the table and variable functions of the ASCII processor.

For my example I will be using messages in which a 303 & 304 alarm are both cleared by a 300 alarm (see Figures A.1- A.8 for examples):

### 303 message:

```
WAVLSCXB02T CM      ** ENET303 JUL01 19:46:01 7214 SYSB ENET Plane: 1 Shelf:
  ENET PSLink state change. SET from OK ; PM detected link error
  PM: DTM 3    Port: 01 Capability: M,S
```

### 304 message:

```
WAVLSCXB02T CM      ** ENET304 JUN20 18:04:17 4866 SYSB ENET Plane: 1 Shelf:
  ENET PSLink state change. Set from CBSY ; CBSY recovery failed
  PM: MTM 1    Port: 01 Capability: M,S
```

### 300 clear message:

```
WAVLSCXB02T CM      ENET300 JUL01 19:46:40 2817 RTS ENET Plane: 1 Shelf:
  ENET PSLink state change. Set from SBSY ; PM Link error dropped
  PM: DTM 3    Port: 01 Capability: M,S
```

Using the ASCII rules, we will be creating keys, the goal is to create keys that look like this:

### 303 keys:

```
cm:enet303:set
cm:enet303:clr
```

### 304 keys:

```
cm:enet304:set
cm:enet304:clr
```

When we generate the clear message with the 300 alarm, instead of putting the “enetxxx” in a key slot, we will put it in a variable slot. We will then use this variable in a table to map to the clear keys of the 303 and 304 alarms. We will be using the \ \$ command in the clear message to skip normal automatic key generation at the end of the extraction phase. Instead we will be using the table to create the two clear keys. It is important that you omit the “!auto” tag from the clear rule, because we don’t want to make another alarm point, we just want it to generate the clear for the other alarms. In this case it does not matter if the clear message is seen by the ASCII processor before the alarm occurs.

**Note:** In the ENETCL table we set the GenKey option to yes.

```

ASCII Device Rules

ASCII DEVICE : ENET          Rule #      : 10
Descr : ENET 303 Set
Log Type : STANDARD
Special  : NONE
Ignore   : N

Pattern Recognition
1 \MWA\LSCH\MENET303
2 \MENET
3 \MPM:
4
5
6

Action Extraction
1 \MCM\K1\KL2:\MENET\K3\K15\KL4:\KL5SET\!AUTO>ENET
2
3
4
5
6

F)ind, E)dit, D)etele, N)ext, P)rev, M)ove, R)ead, Q)uit :
F4=Debug, F6=Manage, AF6=Import/Export, F10/Esc=Exit

```

Fig. A.1 - Rule for creating the 303 keys

```

ASCII Device Rules

ASCII DEVICE : ENET          Rule #      : 15
Descr : ENET 304 Set
Log Type : STANDARD
Special  : NONE
Ignore   : N

Pattern Recognition
1 \MWA\LSCH\MENET304
2 \MENET
3 \MPM:
4
5
6

Action Extraction
1 \MCM\K1\KL2:\MENET\K3\K15\KL4:\KL5SET\!AUTO>ENET
2
3
4
5
6

F)ind, E)dit, D)etele, N)ext, P)rev, M)ove, R)ead, Q)uit :
F4=Debug, F6=Manage, AF6=Import/Export, F10/Esc=Exit

```

Fig. A.1 - Rule for creating the 304 keys

```

ASCII Tables
Table Name   : ENET          Entry #       : 1
Descr       : generate clear for 303 & 304

-----Condition #1-----
Key: K5  Type: STRING  OP: =  VALUE: SET
-----Condition #2-----
Key:      Type:      OP:      :
-----TRUE Action-----
Key: K5  New Value: CLR  Gen Key: N
-----FALSE Action-----
Key:      New Value:      Gen Key:

F)ind, E)dit, D)elele, N)ext, P)rev, M)ove, R)ead, Q)uit : _
F10/Esc=Exit

```

Fig. A.3 - Table for generating the clear keys for 303 &amp; 304

```

ASCII Device Rules
ASCII DEVICE : ENET          Rule #       : 20
Descr       : ENET clear for 303 & 304
Log Type    : STANDARD
Special     : NONE
Ignore      : N

Pattern Recognition
1 \MMAVLSCX
2 \MENET
3 \MPM:
4
5
6

Action Extraction
1 \MCM\K1\KL2:\MENET\V3\KL4:\KL5CLR\XENETCL\$
2
3
4
5
6

F)ind, E)dit, D)elele, N)ext, P)rev, M)ove, R)ead, Q)uit :
F4=Debug, F6=Manage, AF6=Import/Export, F10/Esc=Exit

```

Fig. A.4 - Rule for defining the clear key as well as populating the variable

ASCII Tables			
Table Name	: ENETCL	Entry #	: 1
Descr : 300 alarm clears 303			
Condition #1			
Key: V3	Type: STRING	OP: =	VALUE: ENET300
Condition #2			
Key:	Type:	OP:	:
TRUE Action			
Key: K3	New Value: ENET303	Gen Key: Y	
FALSE Action			
Key:	New Value:	Gen Key:	
F)ind, E)dit, D)delete, N)ext, P)rev, M)ove, R)ead, Q)uit :			
F10/Esc=Exit			

Fig. A.5 - Table for creating two clear keys from the variable (for 303 key)

ASCII Tables			
Table Name	: ENETCL	Entry #	: 5
Descr : 300 alarm clears 304			
Condition #1			
Key: V3	Type: STRING	OP: =	VALUE: ENET300
Condition #2			
Key:	Type:	OP:	:
TRUE Action			
Key: K3	New Value: ENET304	Gen Key: Y	
FALSE Action			
Key:	New Value:	Gen Key:	
F)ind, E)dit, D)delete, N)ext, P)rev, M)ove, R)ead, Q)uit : _			
F10/Esc=Exit			

Fig. A.6 - Table for creating two clear keys from the variable (for 304 key)

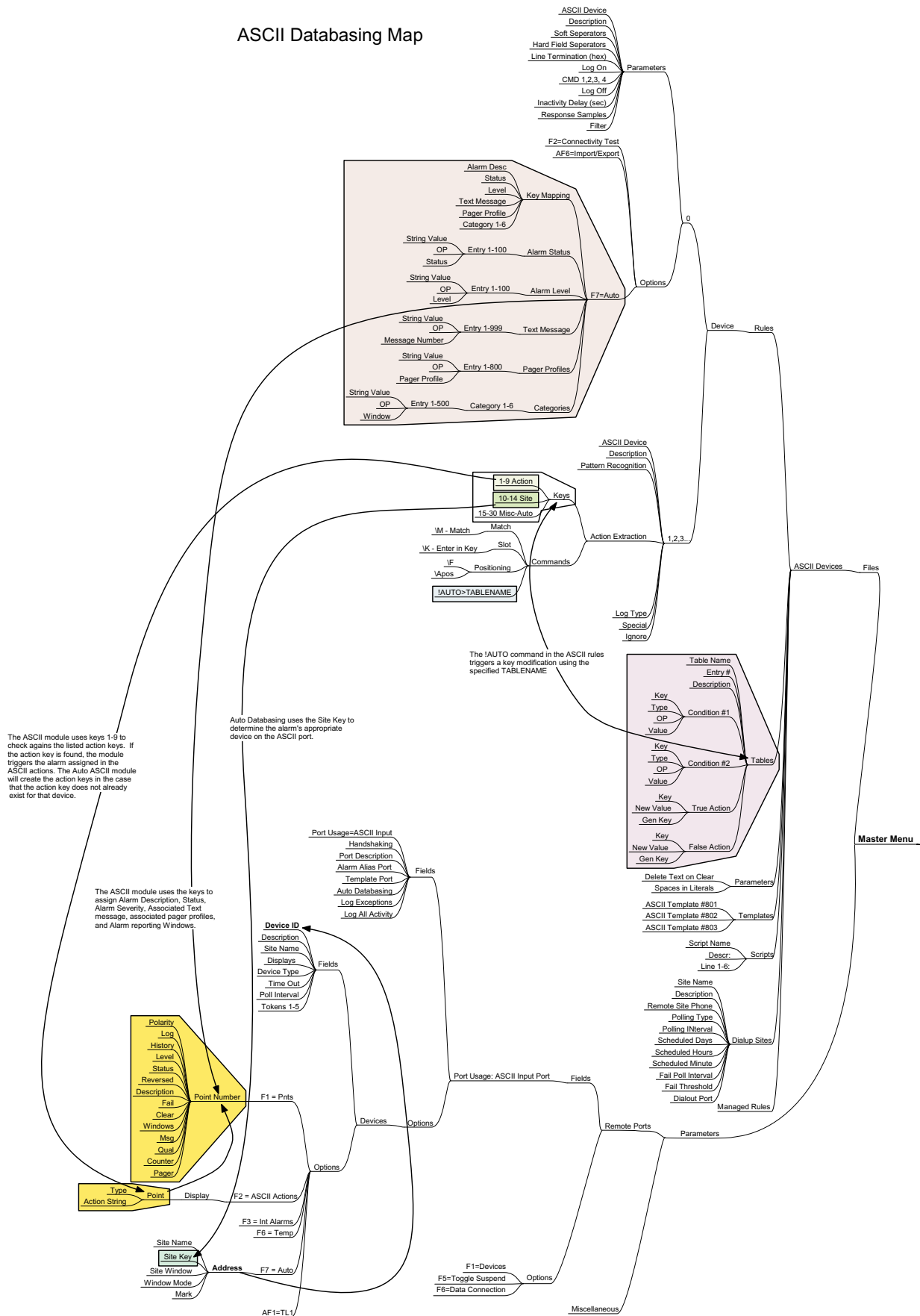


Fig. A.7 - ASCII Databasing Map

**This page intentionally left blank.**

# Appendix B

## Define Controller Cards

### Card Definition

Selecting Card ISA from the Parameters menu (press C to select Card and press Enter) will allow you to setup the operating parameters of the controller cards. This screen lets the system know how to talk to the cards. This is especially important for cards that have special provisioning requirements. On new T/MonXM systems these parameters have been set at the factory. However, you will have to use this screen when adding new cards.

Use the following steps to add define controller cards:

1. From the T/MonXM Master Menu, choose Parameters > Card PCI — see Figure B.1.
2. The ISA Card Definition screen will appear. Press Tab to select the appropriate card from List Box — see Figure B.2 and Table B.A.
3. Enter the address of the card.
4. If you are defining a 602 card, press F1 to and select the appropriate docking pad type — see Figure B.3.
5. Press F8 to save your changes.

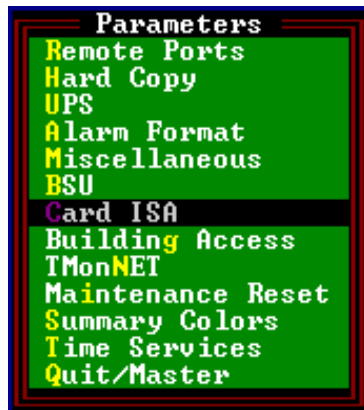


Fig. B.1 - Card ISA menu



Fig. B.2 - The card definition screen



**Table B.A - Fields in the Card Definitions screen**

Field	Description
Part #	The part numbers of the cards in the system. Press Tab to see a list of cards. D-PC-600-00 232 Ports D-PC-602-00 Modular Ports D-PC-603-00 1 Modular / 3 RS232 Ports D-PC-625-00 High Speed Modem Ports D-PR-240-00 X25 Card (1-4) D-PR-241-00 X25 Card (5-6) D-PC-215-00 Remote Ports 1-4 D-PR-211-00 Remote Ports 5-8 D-PC-212-00 Remote Ports 9-12 D-PC-213-00 Remote Ports 13-16 D-PR-205-10 X25 Card Data Scope
Description	This is the description of the card definition. It will be automatically entered when one of the listed card types is selected.
Address	Indicates the address of the card for those cards that are addressable (Any of the 600 group: 600, 602, 603, 625, etc). Valid addresses are 1-6. This must match the address setting on the card's DIP switches.

**Table B.B - Key commands available in the Card Definition screen**

Function Key	Description
Tab	This lists available options cards. (Ctrl-D also calls up a default box of available options.) See Table B.A for list.
F1	Opens the Docking Pad Provisioning Card screen. Press Tab to select the appropriate docking pad type.
F3	Deletes the current entry line.
F8	Saves the card definitions.
F9	On-line help.
F10/Esc	Exit

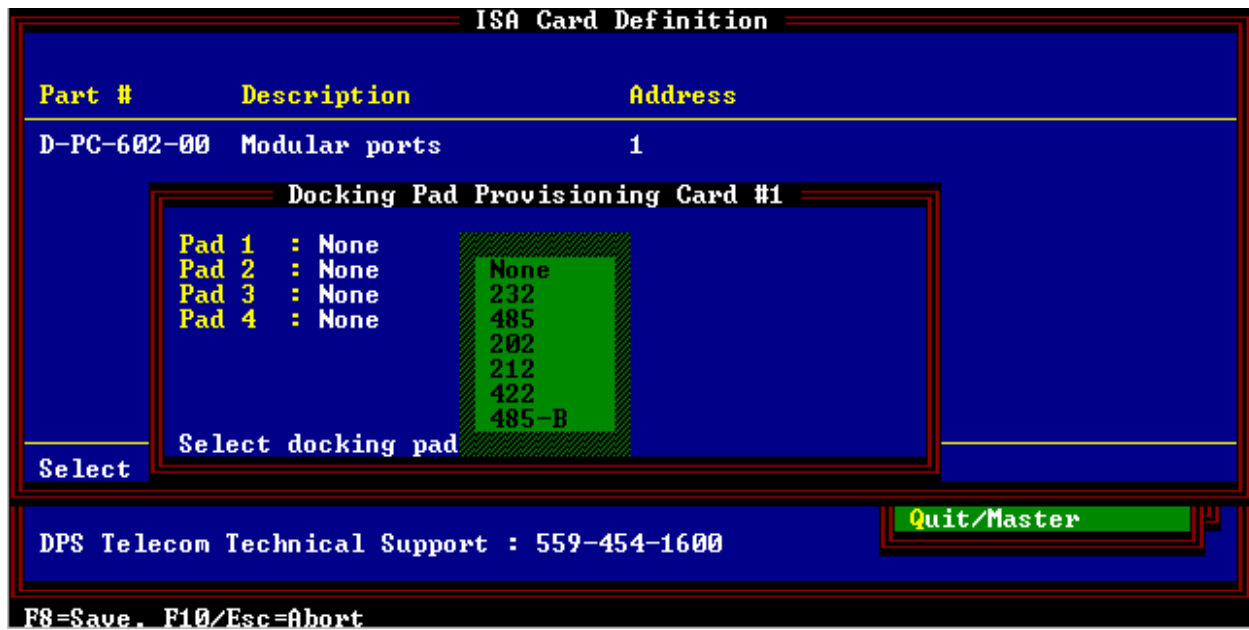


Fig. B.3 - Define the docking pad type in the Docking Pad Provisioning Card screen

Docking Pad Types available are as follows:

- RS-232
- RS-485
- 202
- 212
- 422
- 485B

**This page intentionally left blank.**

# Appendix C

## Configuring a X.25 Port Card

This appendix provides supplementary information for configuring the optional X.25 port card. (Part Number D-PR-240-10A-00). This card occupies a slot normally available for a 600 or 602 card in the T/MonXM WorkStation or IAM housing. Each card provides one X.25 port, to be used either for an ASCII input/output (I/O) port or for the TL1 Responder application. Up to four cards can be used.

The X.25 ports are numbered 25 through 28, regardless of the number of 600 or 602 cards in the system. Addressing of the card is separate from the 600/602 card addressing. The first card is addressed as X.25 card number 1, the second is X.25 card number 2, etc.

### Hardware Connections

The X.25 signal interface is via a DB25 connector on the back of the IAM or T/MonXM WorkStation housing. The figure and table below shows the physical location and pin-out of the connector. The figure also shows physical connections between the connector and the mainframe.

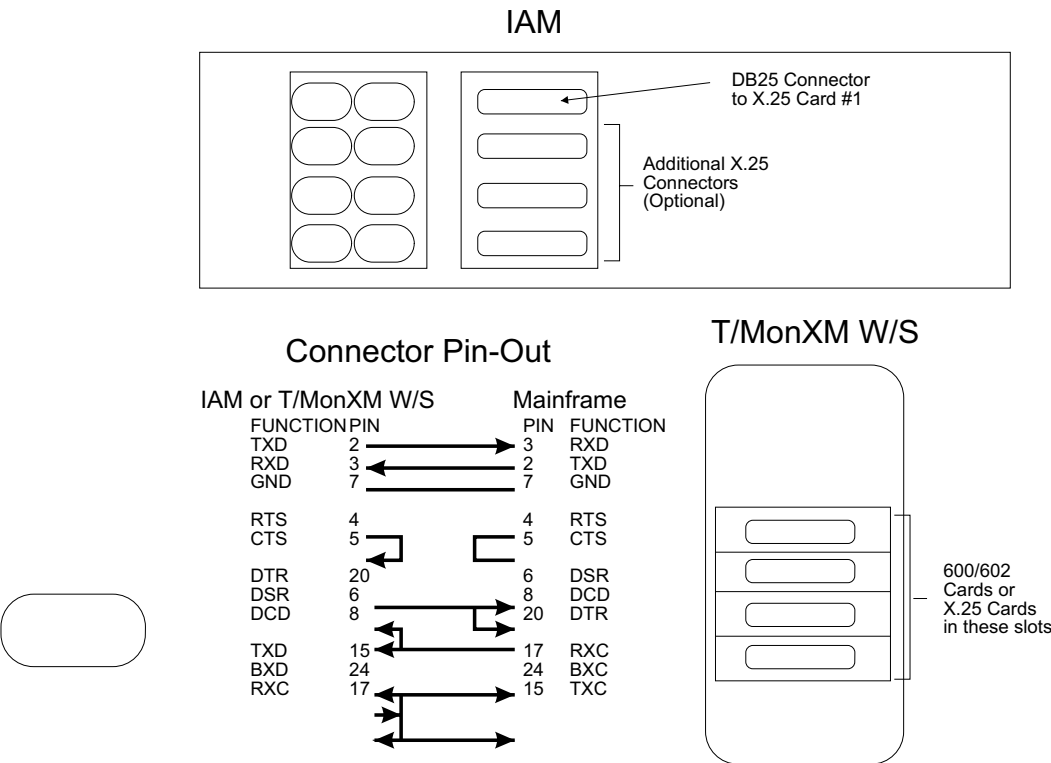


Fig. C.1 - X.25 Connector location and pinout

## Software Configuration

Steps to configure the X.25 Card:

The following applies only if your system is equipped with the TL1 Responder module:

A. If the port usage is X.25 TL1 Responder:

1. Define the Port (p. C-2)
2. Define the Device (p. C-4)
3. Define the Responder (p. C-5)
4. Define the LCN (pp. C-6)
5. Define the Card (page C-12)
6. Provision the card (pages C-14)

The following applies only if your system is equipped with an ASCII module:

B. If the port usage is X.25 I/O (for straight ASCII or Craft Port usage):

1. Define the Port (p. C-6)
2. Define the PVCs (p. C-7)
3. Define the SVCs (p. C-8)
4. Define Job ports (p. C-9)
5. Define the Device (p. C-11)
6. Define the Card (page C-12)
7. Provision the card (pages C-14)

## Port Definition/ X.25 TL1 Responder

To configure an X.25 card, begin at the Main Menu and select Parameters. Select Remote Ports to view the Remote Parameters screen. Press F and enter the port number. (Enter 25 to define the first port. Increase by one number for each additional port to be defined.)

Press “E” to edit the port. Press Tab and select X.25 TL1 Responder. Fill in the remaining fields on the screen according to Tables C.A and Table C.B.

**Note:** *You must initialize your system before changes can take effect.*



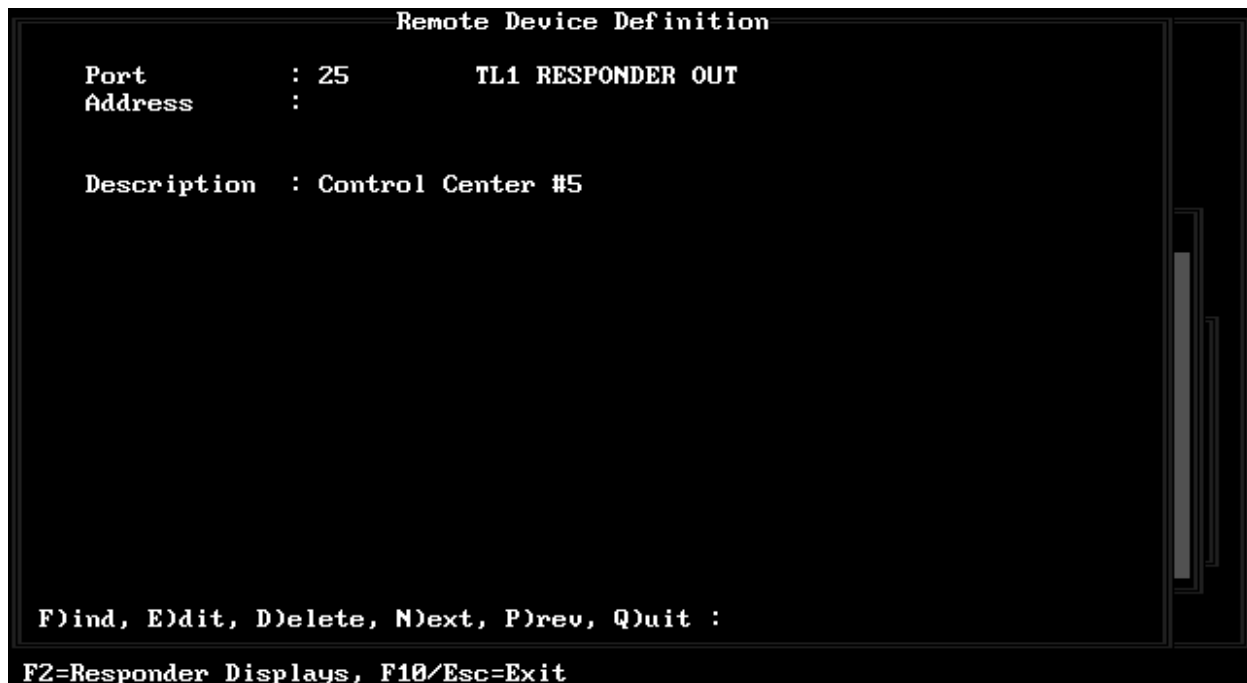
Fig. C.2 - Port Defined for X.25 TL1 Responder

**Table C.A - Fields in the Remote Parameters screen, X.25 TL1 Responder Port**

Field	Description
Port Usage	The Port Usage shows the selected port usage option.
Echo Input	If set to "Y", T/MonXM will echo back all commands/characters that are received. This field should be set to "N" if you are going to be connected to another computer. [N]
Null Aids Allowed	Enter "N" to force users to enter AIDs when entering TL1 commands (833 compliant). Enter "Y" to allow users to omit or enter null AIDs when entering TL1 commands. [N]
ATAG Width	Number of characters to output for ATAG (4-10).
One Alm/Report	For autonomous reports: Y=One alarm per header; N=Multiple alarms.
UID	User Identification. Used when TL1 OSS or other interrogating device queried with an ACT-USER command. The ACT-USER command is used for setting up a session when logging on to an external device (i.e.: switch, radio, multiplex channel, DPM, etc.). Use up to 10 alphanumeric characters. If left blank, cursor skips to Enforce Security field.
PID	Private Identifier or password. This field is entered only if a UID has been entered. It is also used in conjunction with the ACT-USER command, as explained above. Use at least 2 non-alpha characters in the string.
Enforce Security	Y = Require correct UID/PID (as entered above) with an ACT-USER command. N = Don't match UID/PID with an ACT-USER command.

**Table C.B - Key commands available in the Remote Parameters screen, X.25 TL1 usage**

Function Key	Description
F1	Devices. Takes you to the device definition screen.
F2	LCN. Takes you to the Logical Channel Number Definition window. (For TL1 responder port usage).
Up Arrow	Move to the previous field.
F8	Save (Available only in edit mode)
F9	Help (Available only in edit mode)
F10/Esc	Move to first field or exit without saving (depending on cursor location).
Tab	List port usages (while cursor is in the Port Usage field).



**Fig. C.3 - Device Definition screen**

#### Device Definition screen

When defining a TL1 responder, press F1 while in the parameters screen to define the devices. Refer to Software Module 14 - TL1 Responders.

#### Device Definition screen

Press F2 while in the Remote Device Definition screen to define the responder. Refer to Software Module 14 - TL1 Responders.



Fig. C.4 - X.25 TL1 Responder LCN Selection screen

**LCN Definition - TL1 Port**

Press F2 while in the Remote Parameters screen (TL1 Responder port usage) to define the Logical Channel Number (LCN). Enter information in the fields according to Table C.C.

**Table C.C - Fields in the Logical Channel Number Selection screen**

Field	Description
Type of LCN	Use Tab to select PVC or SVC. Selecting PVC moves cursor to the PVC field. Selecting SVC moves cursor to the SVC Address field (skips PVC Field).
PVC	Enter LCN (1-255)
SVC Address	Enter up to 14 digits for the address identifier or user equipment.
SVC Facility	Enter 2 digit facility code
SVC User Data	No entry required. (Reserved for future use)
SVC Calling Address	No entry required. (Reserved for future use)

Upon completion of the above fields, use the F10 or Esc key to return to the parameters menu.



## Port Definition/ X.25 I/O

To configure an X.25 card, begin at the Main Menu and select Parameters. Select Remote Ports. Press F and enter the port number. (The first port is 25. Increase by one for each additional port to be defined.)

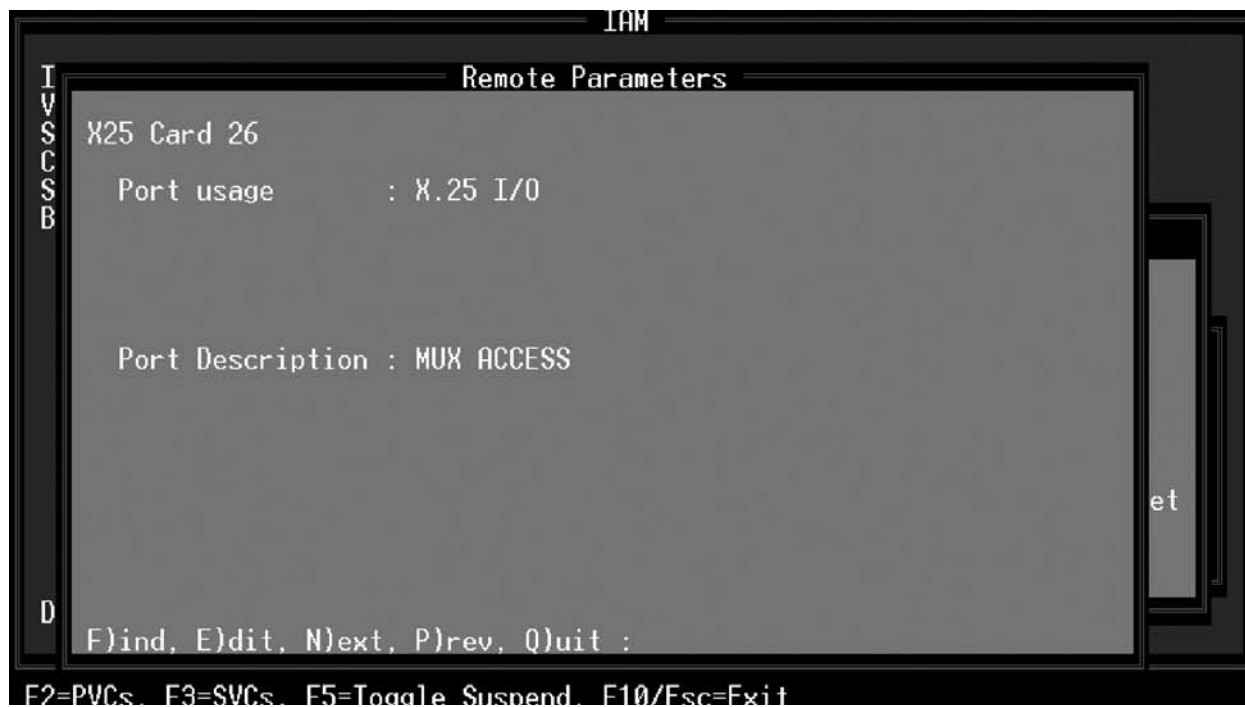
Press “E” to edit the port. Press Tab and select X.25 I/O. Fill in the remaining fields on the screen according to Table C.D and Table C.E.

**Table C.D - Fields in the Remote Parameters screen, X.25 I/O Usage**

Field	Description
Description	Description for the port (up to 30 characters).

**Table C.E - Key commands available in the Remote Parameters Screen, X25 I/O Usage**

Function Key	Description
F2	PVCs. Press to show the X.25 PVC Definitions screen.
F3	SVCs. Press to show the X.25 SVC Definitions screen.
F5	Toggle suspend.
F10/Esc	Exit.



**Fig. C.5 - Port defined for X.25 I/O**

X.25 PVC Definitions		
Entry	PVC	Description
1	443	Portland OSS
2	322	Seattle OSS
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		
13		
14		

Enter the PVC number (1-4096)

F1=GO TO, F3=BLANK, F8=Save, F10/Esc=Exit

Fig. C.6 - Define PVCs for X.25 I/O Port in the ACC X.25 PVC Definitions screen

#### PVC Definition - X.25 I/O Port

Press F2 while in the Remote Parameters screen (X.25 I/O port usage) to define the Permanent Virtual Channels (PVCs). Enter information in the fields according to the table below.

Fig. C.F.- Fields in the ACC X.25 PVC Definitions screen

Field	Description
Entry	Fixed line number (Uneditable), 1-128.
PVC	3 digit identifier for this PVC (for equipment at other end).
Description	Enter a description of the network element (up to 30 characters - for T/MonXM usage).

Table C.G - Key commands in the PVC and SVC Definition Screen (X.25 I/O Port Usage)

Function Key	Description
F1	Go to. Moves cursor quickly to another entry number.
F3	Blank. Deletes contents of entry line.
F8	Save.
F10/Esc	Exit.

X.25 SVC Definitions				
Entry	Address	Fac	User	Description
1	15934	adc	unity	oss controller
2	113445	ccd	fractured	oss sub-channel
3	.....			
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				

Enter the SVC address.

F1=GOTO, F3=BLANK, F8=Save, F10/Esc=Exit

**Fig. C.7 - Define SCVs for X.25 I/O Port in the ASC X.25 SVC Definitions screen**

#### **SVC Definition - X.25 I/O Port**

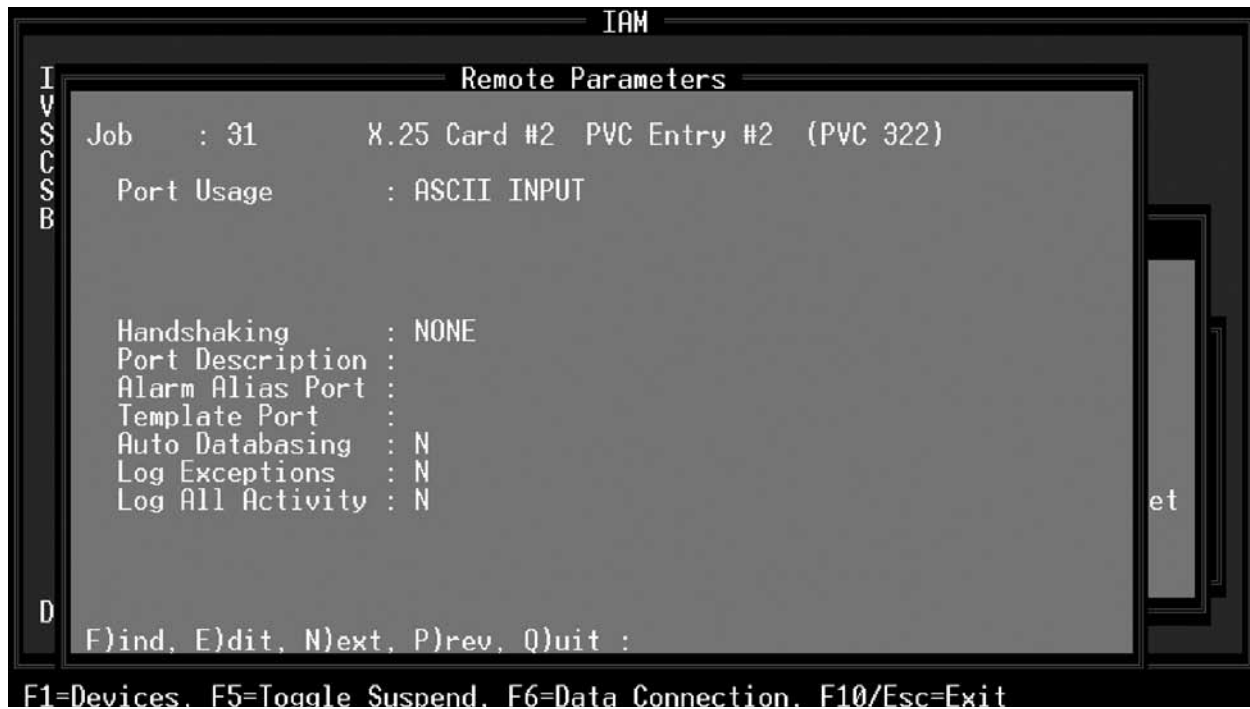
Press F3 while in the Remote Parameters screen (X.25 I/O port usage) to define the Switched Virtual Channels (SVCs). Enter information in the fields according to the table below.

See Table C.G for descriptions of hot keys in the SVC Definition Screen (X.25 I/O Port Usage)

When all PVCs and SVCs have been defined, go on in manual.

**Table C.H - Fields in the SVC Definition Screen**

Field	Description
Entry	Fixed line number (Uneditable), 1-128.
Address	14 digit address identifier of user equipment.
FAC	Only 2 digit facility codes or no codes allowed. Enter code or press enter for no codes.
User Data	Enter user data (up to 16 characters).
Description	Enter a description of the network element (up to 30 characters - for T/MonXM usage).



**Fig. C.8 - Define a Job Port for each PVC and SVC (ASCII input)**

### Job Ports

After PVCs and SVCs have been defined, return to the Remote Parameters screen. Use the "N" key to move to an undefined job port (Port number 30 through 157). Press "E" and fill in the fields per Table C.I and Table C.J.



**Fig. C.9 - Define a Job Port for each PVC and SVC (Craft Interface)**

Table C.I - Fields in the Job Port screen

Field	Description
Port Usage	Select ASCII Input, Craft Interface or Halted from the default box.
ASCII Input	
Handshaking	The handshaking field allows the user to select the type of handshaking the equipment is using to communicate. Valid entries are N (None), X (Xon/Xoff) and R (Rts/Cts). [N]
Port Description	30 character description of port for Craft Mode.
Alarm Alias Port	Number of Port whose (already) defined data base you wish to use for this port. Leave blank for None. If used, enter alias port number, then press F1 and set device rules. Port is then ready to use.
Template Port	Reference template port (801, 802 or 803). (Blank = None)
Auto Databasing	N. Enter Y only if port is to use auto databasing.
Craft Interface	
Handshaking	The Handshaking field allows the user to select the type of communicate handshaking that the equipment is using to communicate. Valid entries are N (None), X (Xon/Xoff) and R (Rts/Cts). [N]
Craft Description	This field is optional and allows you to simply enter a 30 character description for the port and the device that it is communicating with.
Full Duplex	Determines whether the terminal operates in Full Duplex mode. When Full Duplex mode is active, characters typed on the keyboard are assumed to be echoed back to the screen by the terminal device. Valid entries are Y (full duplex) or N (half duplex). [Y]

Table C.J - Key commands available in the Job Port Screen

Function Key	Description
F1	Devices. Opens the device definition screen. If you are not using auto databasing, refer to Software Module 5 - ASCII Processor. If you are using auto databasing, refer to Software Module 16 - Auto Databasing. F5
F5	Toggle suspend. Suspends port operation without changing configuration.
F6	Data connection. Opens the Data Connection Assignments Screen.
F8	Save. (Available only in edit mode.)
F9	Help. (Available only in edit mode.)
F10/Esc	Exit.

IAM

Data Connection Assignment

Job : 32    Usage : CRAFT INTERFACE

Data Connection : NONE

Teltrac Mux 6.3

Teltrac Mux 6.5

Teltrac Mux 6.7

X.25 Card #2    PVC Entry #1    (PVC 443)

X.25 Card #2    SVC Entry #1    (Add 15334)

X.25 Card #2    SVC Entry #2    (Add 113445)

[LIST BOX]    Cursor Keys=Move Highlight Bar, <ENTER>=Select, F10/Esc=Abort

**Fig. C.10 - Select PVC or SVC in the Data Connection Assignment screen**

#### Data Connection

Press F6 while in the Job Port Remote Parameters screen. The Data Connection Assignments screen will appear (Figure C.10). Fill in fields per Table C.K and Table C.L.

Upon completion of the Data Connection assignment, return to the job port screen and press F1 to define the device. If you are not using auto databasing, refer to Software Module 7 - ASCII Processor. If you are using auto databasing, refer to sections M7-67 to M7-82.

**Table C.K - Fields in the Data Connection Assignment screen**

Field	Description
Job	Job number assignment from previous screen.
Usage	Port usage assignment from previous screen.
Data Connection	Default box lists all available (unassigned) PVCs and SVCs. Use the Tab key to highlight the desired one and press Enter.

**Table C.L - Key commands available in the Data Connection Assignments screen**

Function Key	Description
Tab	Enters default box. Use cursor arrows or Tab to highlight a selection.
F10/Esc	Exit the screen without making an assignment.

Card Definition		
Part #	Description	Address
D-PC-600-00	232 ports	1
D-PR-240-00	X.25 card (1-4)	1
D-PR-241-00	X.25 card (5-6)	5
D-PC-602-00	Modular ports	3
.....		
Select card type		
DPS Telecom Technical Support : 559-454-1600		Quit/Master
Tab=List, F3=BLANK, F8=Save, F9=Help, F10/Esc=Exit		

Fig. C.11 - X.25 Card Definition screen

## Card Definition

Select Card from the Parameters menu. Refer to Appendix B for additional information. Remember that the address of an X.25 card is independent of the 600 and 602 cards. The address field for the X.25 card may have the same number as one of the other cards.

Factory-installed cards have all addresses preset. If a card is being added to an existing T/MonXM WorkStation or IAM be sure the address jumpers on the card are set according to Figure C.12 on the next page.

Table C.M - X.25 Card Addressing

X25 Card	X.25 Card Address	Remote Port Number
First	1	25
Second	2	26
Third	3	27
Fourth	4	28

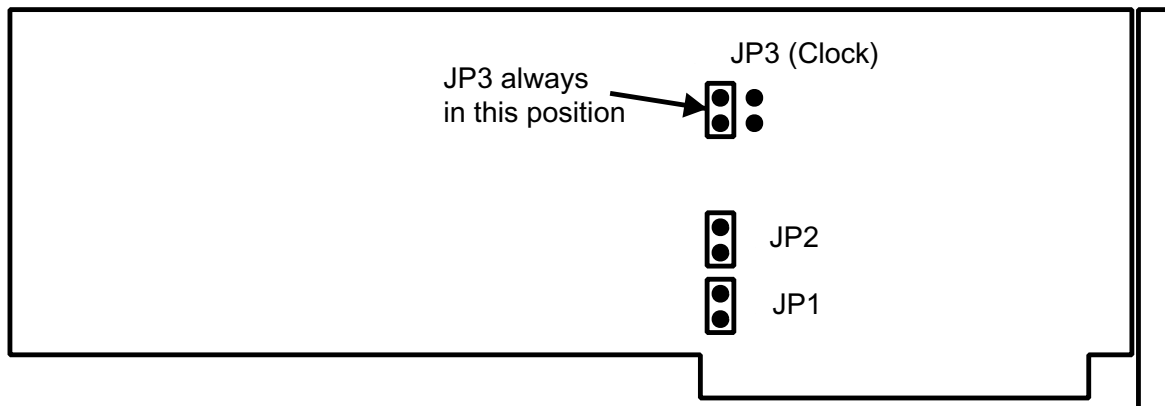


Fig. C.12 - Set X.25 Card Jumpers for Address

Table C.N - X.25 Card Address Jumper Positions

Address	JP1	JP2
1	IN	IN
2	IN	OUT
3	OUT	IN
4	OUT	OUT

**CAUTION:** Always observe electrostatic precautions when handling any hardware cards. Refer to Bellcore Technical Advisory #TA-TSY-00870 for further information.



```

Card Definition
-----
X25 Provisioning Card #1
-----
Baud      : 56000      T1 timer    : 2      Card Add: E000
Frame Window : 7      T2 timer    : 0
Equipment  : DTE      T4 timer    : 1
Packet Window : 2      N2 timer    : 10
Packet Default: 256    T10/20 timer : 90
Packet Maximum: 256    T11/21 timer : 90
                    T12/22 timer : 90
                    T13/23 timer : 90
                    T16/26 timer : 90
                    T28 timer    : 90
Min PVC     : 1      R10/R20    : 5
Max PVC     : 10     R12/R22    : 5
Min Incoming : 0     R13/R23    : 5
Max Incoming : 0     CCITT Comp  : 1988
Min Two Way  : 11     Facilities #1: 0000
Max Two Way  : 20     Facilities #2: 0000
Max Outgoing : 0
                    Baud at which X25 operates (press Tab for defaults)

Tab=Defaults, F8=Save, F10/Esc=Abort

```

Fig. C.13 - Enter card parameters in the X.25 Provisioning screen

## X25 Provisioning

Press F1 while the cursor is on the X25 Card Definition line in the Card Definition screen to reach the X25 Provisioning screen. Enter fields as defined in Table C.O.

Table C.O - Fields in the X25 Provisioning screen

Field	Description
Baud	Press Tab to see choices, Enter to select. Choices are EXT CLK, 1200, 2400, 4800, 9600, 19200, 38400, 45000, 56000, 74000, 112000.
Frame Window	Size of the frame window (k) (1-7)
Equipment	Device interface of this X25. Press Tab to see choices, Enter to select. Choices are DCE and DTE.
Packet Window	Size of the packet window (w) (1-7).
Packet Default	Default number of Bytes in the data field packet. Press Tab, highlight choice, enter to select. Choices are 16, 32, 64, 128, 256, 512, 1024.
Packet Minimum	Maximum negotiable number of Bytes in the data field packet. Press Tab, highlight choice, enter to select. Choices are 16, 32, 64, 128, 256, 512, 1024.
Min PVC	Lowest PVC that may be used. 1-4095, 0=not used.
Max PVC	Highest PVC that may be used. 1-4095. This field is skipped if previous field is 0.
Min Incoming	Lowest incoming SVC that may be used. 1-4095, 0=not used.

Table C.O - Fields in the X25 Provisioning screen (continued)

Field	Description
Max Incoming	Highest incoming SVC that may be used. 1-4095. This field is skipped if previous field is 0.
Min Two Way	Lowest two-way SVC that may be used. 1-4095, 0=not used.
Max Two Way	Highest two-way SVC that may be used. 1-4095. This field is skipped if previous field is 0.
Min Outgoing	Lowest Outgoing SVC that may be used. 1-4095, 0=not used.
Max Outgoing	Highest Outgoing SVC that may be used. 1-4095. This field is skipped if previous field is 0.
T1 Timer	T1 Timer - 1 to 30 seconds. 2-3 is typical.
T2 Timer	T2 Timer - 0 to 1 seconds. 0 is typical.
T4 Timer	ABM poll multiplier (1-240) x T1 Secs. 0 = disable, 1 = typical.
N2 Timer	Maximum resends at T1 intervals before error (1-30). 10 is typical.
T10/20 Timer	Timeout on restart indication or request. (15-255 seconds) 90 is typical. Rounded.
T11/21 Timer	Timeout on incoming call or call request. (15-255 seconds) 90 is typical. Rounded.
T12/22 Timer	Timeout on reset indication or request. (15-255 seconds) 90 is typical. Rounded.
T13/23 Timer	Timeout on clear indication or request. (15-255 seconds) 90 is typical. Rounded.
T16/26 Timer	Timeout on Interrupt Pkt Timeout (1-255) secs). 90 is typical.
T28 Timer	Timeout on registration request. (15-255 seconds) 90 typical. Rounded.
R10/R20	Retransmission count for Restart Indication/Request packets (0 - 250).
R12/R22	Retransmission count for Reset Indication/Request packets (0 - 250).
R13/R23	Retransmission count for Clear Indication/Request packets (0 - 250).
CCITT Comp	CCITT compatibility of packet layer. 1980, 1984, 1988.
Facilities #1	Enter facility in hex (Refer to manual for bit map).
Facilities #2	Enter facility in hex (Refer to manual for bit map).
Card Add.	Select from default box. Use DC00 for Pentium processors.

Table C.P - Key commands available in the X25 Provisioning Screen

Function Key	Description
Up Arrow	Move to the previous field
F8	Save
F10/Esc	Abort

**This page intentionally left blank.**

# Appendix D

## Ethernet Card Installation

(For Field Upgrades)

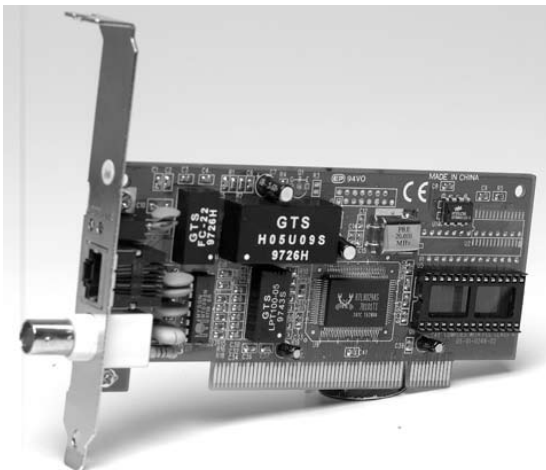
### Overview

Use this procedure to install hardware and software for an NE2000 Ethernet port on a DPS master / element manager (T/MonXM WorkStation or Intelligent Alarm Mediator (IAM)).

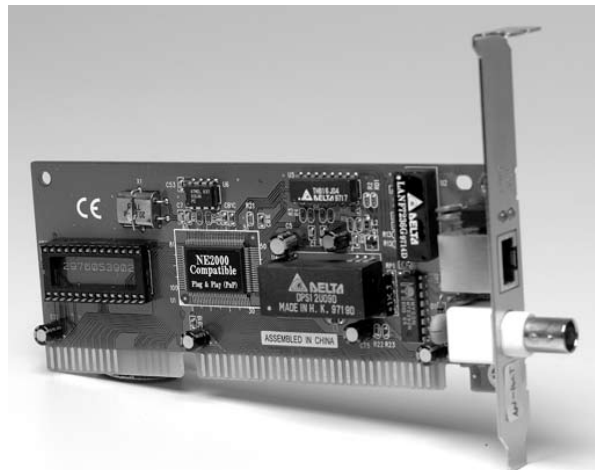
Two card slot formats are available, ISA (Figure D.1) and PCI (Figure D.2). ISA format cards are used in earlier versions of DPS masters, while the PCI format is found in most Pentium-based machines and some later 486's. Be sure to verify the format of your machine before ordering an Ethernet card for upgrading an existing T/MonXM or IAM. (DPS technical support can help if you are in doubt.)

T/MonXM can use LAN for a variety of tasks including: SNMP\*, RTU Interrogation (i.e. KDAs, Net Guardians, etc.), ASCII processing\*, Remote Access, E-mail notification of alarms, T/GrafX\*, and web browser remote access.

\* Additional software modules required.



**Fig. D.1 - Ethernet card in the PCI format is used in Pentium-based DPS element managers.**



**Fig. D.2 - Ethernet card in the ISA format is used in earlier T/Mon and IAM managers. This card is not available for new T/Mon units.**

---

## Installation

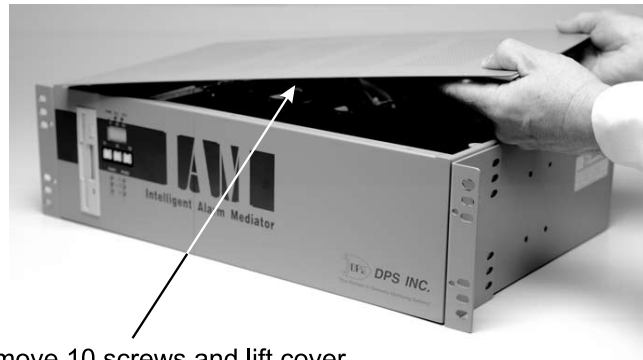
**NOTE:** Observe ESD precautions when handling the Ethernet Cards. (Use wrist strap and properly grounded work mat.)

1. Shut down element manager. Remove power cord or battery connection and open case.
2. If the card is being installed in an IAM, follow the illustrated steps in Figure D.3.
3. If the card is being installed in a T/MonXM WorkStation (tall tower case), follow the illustrated steps in Figure D.4.
4. If the card is being installed in a T/MonXM with a short tower case, follow the steps in Figure D.4, except for the case opening. A short tower case is opened by removing screws at the back and sliding the cover back and up.
5. Connect Ethernet.
6. Install software (see software installation procedure).
7. Perform database configuration in the T/MonXM software.
8. Test for proper operation.

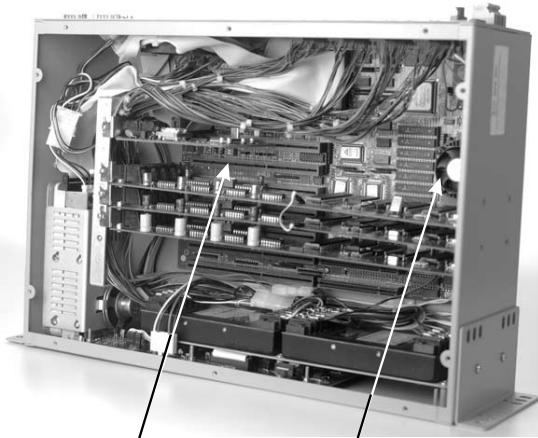
1. Cut off Bottom of Bracket Panel When installing in an IAM. (May have already been done at the DPS factory.)



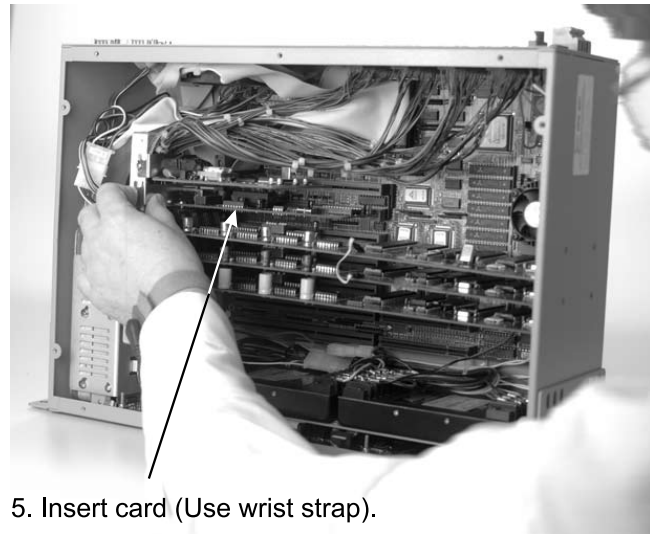
2. Remove IAM from rack or slide out, if equipped with DPS slide Rack.



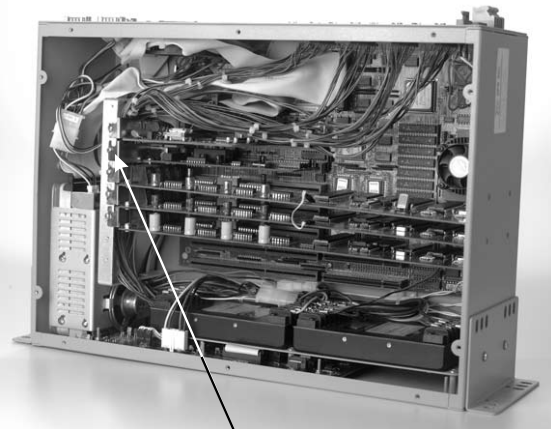
3. Remove 10 screws and lift cover.



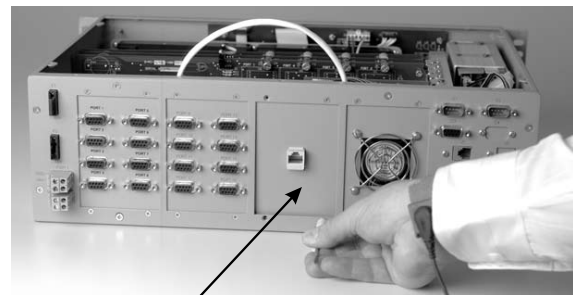
4. Locate empty slot. (Select one that is in line with the processor fan, if available.)



5. Insert card (Use wrist strap).



6. Secure panel/bracket with screw.



7. Remove a blank panel module from the back of the case and install RJ-45 panel.

8. Connect RJ-45 plug to RJ-45 jack on Ethernet card panel.



9. Replace cover and restore IAM to its rack location. Connect all cables and connect Ethernet to RJ-45 jack on rear.

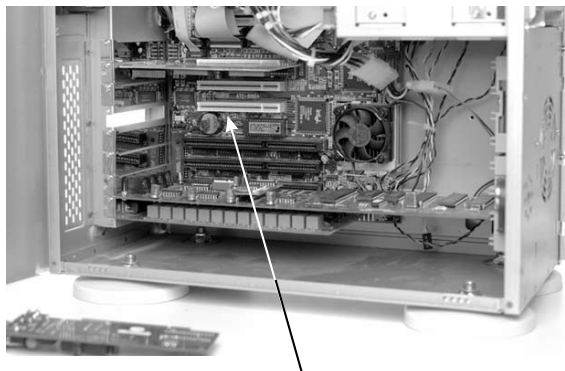
**Fig. D.3 - Follow these steps to install an Ethernet card in an older IAM**



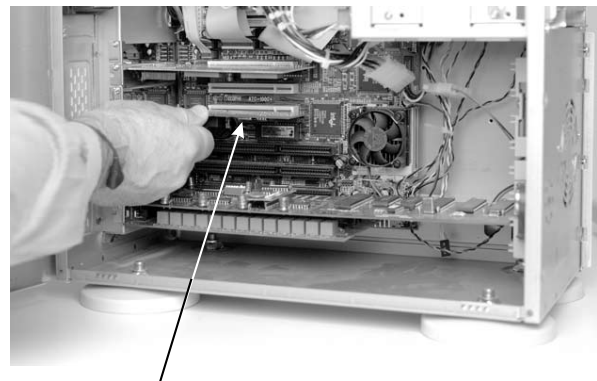
1. Remove front bezel by pulling out at bottom.



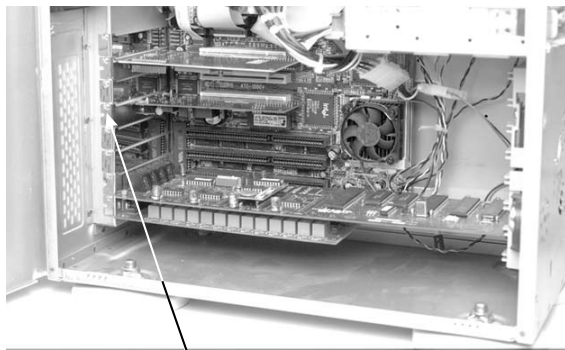
2. Loosen screws and swing side panel open to reveal cards.



3. Locate empty PCI slot and remove cover plate



4. Insert card (use wrist strap).



5. Secure panel/bracket with screw.

6. Close side panel, tighten screws and replace bezel.



7. Connect Ethernet at RJ-45 on back of case.

**Fig. D.4 - Follow these steps to install an Ethernet card in a T/MonXM tall tower case**

## Software Installation

Two disks are included with the NE2000 card, one from DPS and one from the card manufacturer. Begin the software installation with the DPS disk.

1. If the software is being installed on an IAM, turn up the IAM and connect the T/Access computer. Insert the disk in the IAM's drive and proceed to step 3.
2. If the software is being installed on a T/MonXM WorkStation, start the system. Insert the disk in the "A" drive and proceed to step 3.
3. Return to W/Shell and select Updates from the main menu. The T/INSTALL screen appears below (Figure D.5).



Fig. D.5 - Select Install from the T/Install main menu



```

T/Install
Program Information

Program       : NET SETUP           Version #    : 1.0A
Current disk # : Disk #1 of 1      Serial #     : 00002
Type of protection: Hardware       Release Date : MAR 3,1998
                                           Product Class: PROGRAM

ACTION  MEDIA      BY      DATE      TIME  COMMENT
----- (Last 3 Uses) -----
Installation

Destination drive(A-H): C           Volume Label : MS-DOS_6
Destination path       : \DPSNET
Name of installer     : ESTORM
Comment               : FIRST INSTALL.....

Enter comments for tracking purposes (Mandatory field)

ESC/F10/Up-arrow = Edit previous field

```

Fig. D.6 - Fill in fields in the installation window

4. In the Main Menu highlight Install <ENTER>. The installation window will appear (Figure D.6).

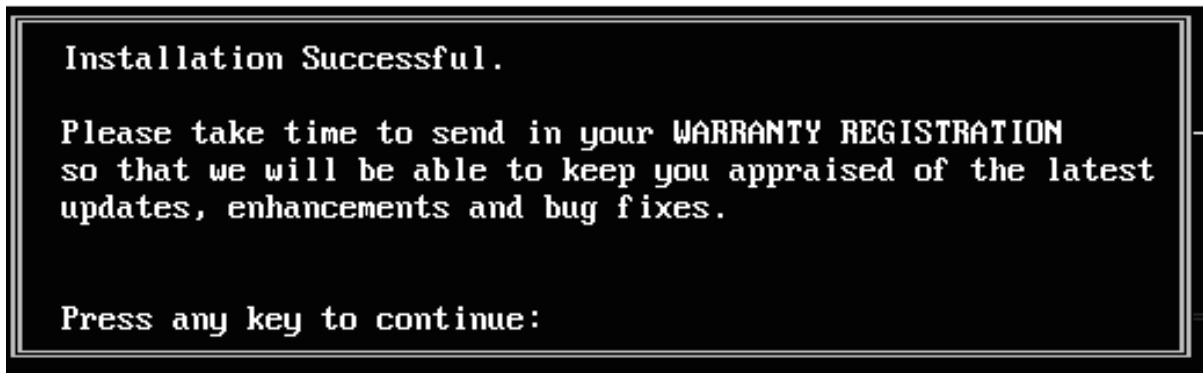


Fig. D.7 - T/Install reminds you to register



Fig. D.8 - Select Quit in the main menu

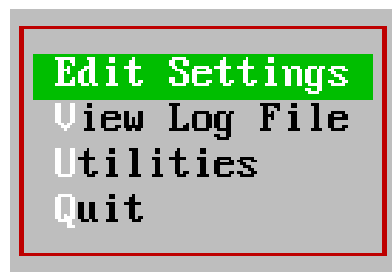
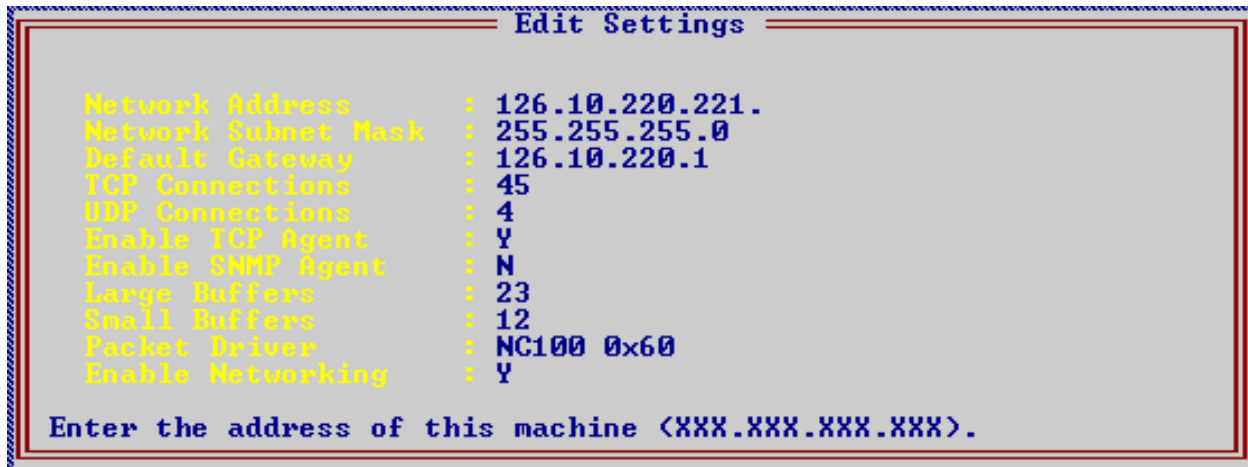


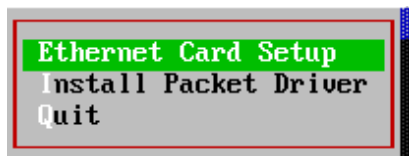
Fig. D.9 - Select network setup functions in the network setup main menu

5. Fill in the destination drive, destination path, your name or initials, and any desired comment, and press Enter
6. A confirmation box will ask “Do Installation?” Type Y and press Enter.
7. The bottom line of the screen will show the install progression. When installation is complete a reminder will appear telling you to send in the registration card (Figure D.7). Please remember to do this. Press any key to continue.
8. The Main Menu will again appear. (Figure D.8) Highlight Quit and press Enter.
9. A confirmation box will ask “Exit Program?” Type Y and press Enter.
10. The Shell screen will again appear. Select Network Setup and press Enter.

The Network Setup utility screen will appear (Figure D.9) A main menu will be displayed showing four selections. See Table D.A for an explanation of each selection.



**Fig. D.10 - Consult with your network manager to obtain network data for the edit settings window**



**Fig. D.11 - Select Ethernet Card Setup from the utilities sub-menu**

11. Select Edit Settings and fill in the fields (Figure D.10). Refer to Table D.A for an explanation of each field. Most of this information will have to be obtained from your network manager. Press <ENTER> when completed.
12. A confirmation box will ask "Are you sure you want to save these settings?" Type Y <ENTER>.
13. The prompt line at the bottom of the window will tell you to re-boot for changes to take effect. Press any key.
14. A confirmation box will ask "Re-boot now?"
  - a) For older ISA format users, type N and continue to step 15.
  - b) For new PCI format users, type Y, and reboot. Skip steps 15 to 24 and return to T/MonXM.
15. The Network Setup Main Menu will again appear. Select Utilities. The Utilities sub-menu will appear (Figure D.11).

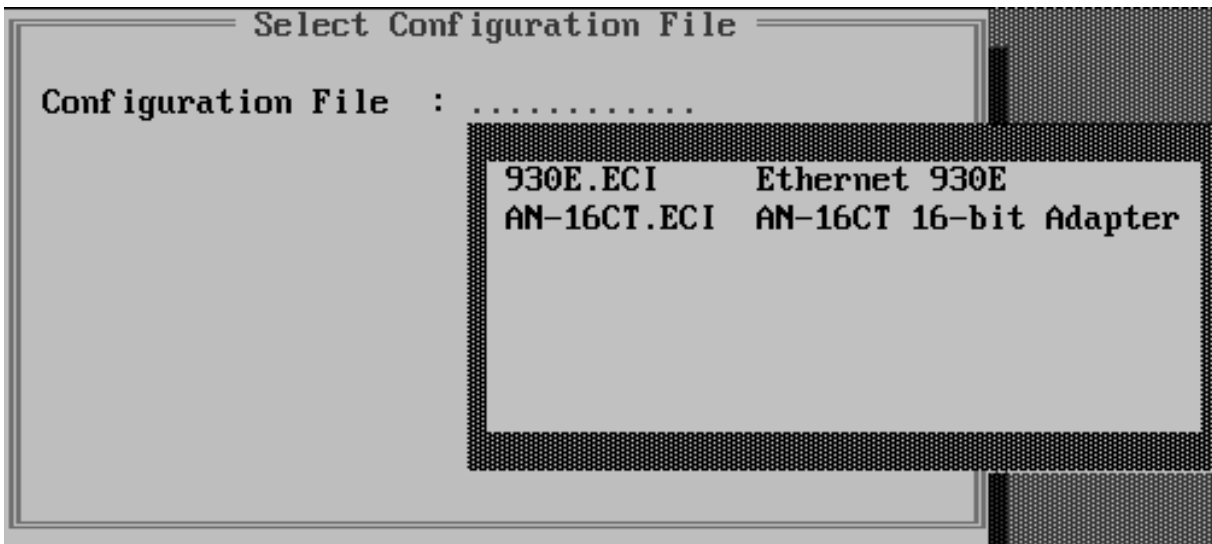


Fig. D.12 - Select the card type in the select configuration file window.

16. Select Ethernet Card Setup.  
The Select Configuration File window will appear (Figure D.12).
17. Press Tab and select the appropriate card type <ENTER>.
18. A red box will appear prompting you to insert the card manufacturer's disk (Figure D.13). Follow the directions in the red box. When the manufacturer's program has been loaded, follow the instructions on the screen and in the manufacturer's manual. Perform installation and any test procedures that are available.  
**Note:** *Boot ROM Option is not used.*
19. Upon completion of the Ethernet Card Setup program the Utilities menu will again appear (Figure D.14).

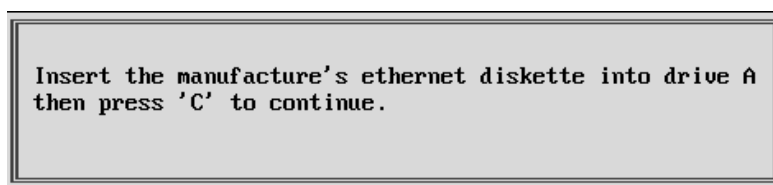


Fig. D.13 - A red box will prompt you to run the card manufacturer's program.

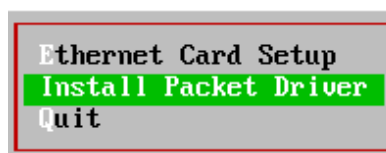


Fig. D.14 - Select install packet driver from the utilities menu.



**Fig. D.15 - Re-boot the system when all configuration is completed**

20. Select Install Packet Driver.  
The Select Configuration File window will again appear (Figure D.12).
21. Again select the appropriate card type <ENTER>.
22. A red box will again appear prompting you to insert the card manufacturer's disk (Figure D.13). Follow the directions in the red box. Follow the instructions on the screen to load the manufacturer's packet driver. Upon completion of the setup, the Utility Sub-menu will again appear.
23. Select Quit <ENTER>.  
A Notice will appear reminding you to re-boot (Figure D.15).
24. Remove the disk from drive A, press any key and the system will automatically re-boot.
25. Return to the T/MonXM program and perform databasing.  
SNMP Agent Application

**Table D.A - Network setup menu**

Menu Item	Field	Description
Edit Settings	Network Address	Enter the address of the T/Mon or IAM. (Address must be of the form XXX.XXX.XXX.XXX) *
	Network Subnet Mask	Enter the network subnet mask. (Mask must be of the form XXX.XXX.XXX.XXX) *
	Default Gateway	Enter the default gateway. (Gateway must be off the form XXX.XXX.XXX.XXX)*
	TCP Connections	Total TCP connections allowed. [Default value 40]
	UDP Connections	Total UDP Connections Allowed [Default value 4]
	Enable TCP Agent	Enable network communication. [Y]
	Enable SNMP Agent	Legacy provision, not applicable since 4.2B.
	Large Buffer	For adjusting network stack.
	Small Buffer	<b>Note:</b> Modify only after contact DPS Tech Support.
	Packet Driver	This field is automatically filled in when the card manufacturer's packet driver is loaded.
	Enable Networking	Enter "Y" to enable networking, "N" to disable networking
View Log File		This function displays a file of the network startup instructions that are used to boot the system. It is useful in trouble-shooting and may be called for by DPS technical support.
Utilities	Ethernet Card Setup	Prepares database for loading the Ethernet card's software (supplied with the Ethernet card). Use the Tab key to select the card type (Figure MD.12). Then follow instructions on screen.
	Install Packet Driver	Prepares database for loading the Ethernet card's packet driver file (supplied with the Ethernet card). Use the Tab key to select the card type (Figure D.12). Then follow instructions on screen.
Quit		Exits the program and re-boots the system to implement changes.

\*This information will have to be obtained from your network manager.

**This page intentionally left blank.**

# Appendix E

## Diagnostics

Diagnostics should be used only under these conditions:

1. During the initial install when problems arise.
2. When board level problems are suspected.
3. When instructed to by a DPS technician.

T/MonXM features diagnostics options that completely test the standard and optional devices that work in conjunction with T/MonXM (inside the computer). This will assist you in troubleshooting your WorkStation in the event that problems arise.

Each option from the Diagnostics menu will allow you to test each device individually. Selecting the Diagnostics option from the Master menu will open the Diagnostics menu.

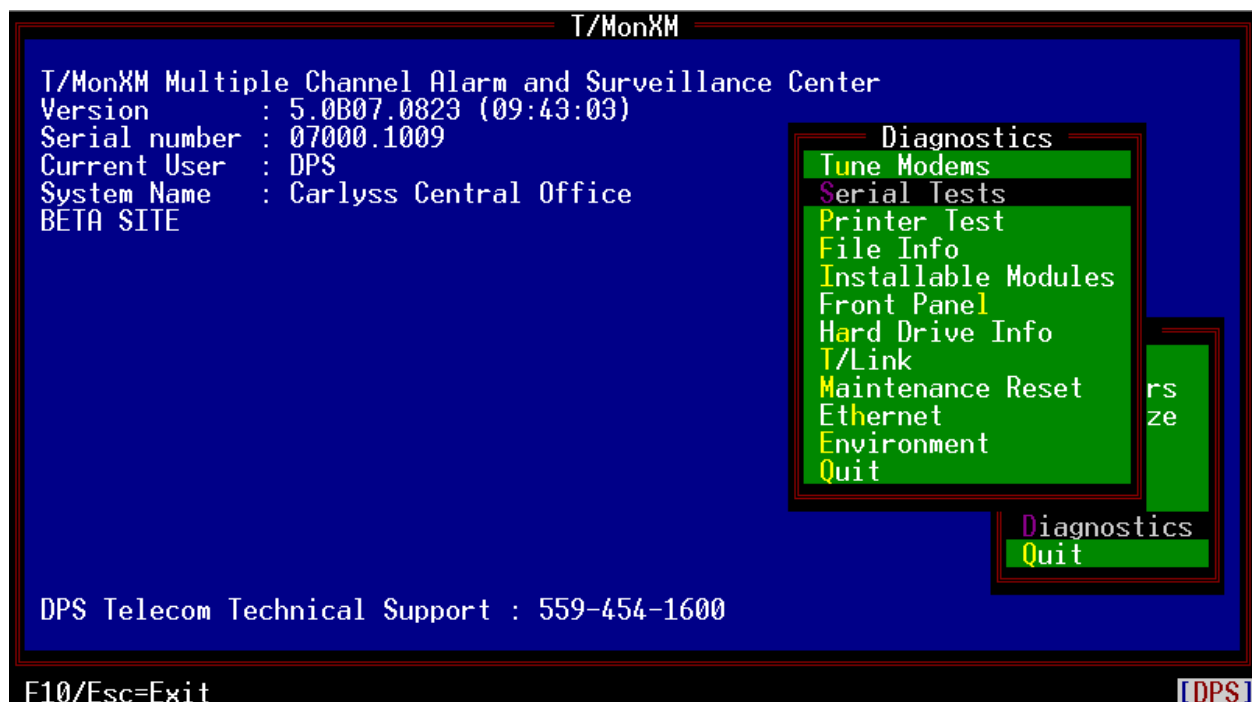


Fig. E.1 - Diagnostics mode is Selected from the Master menu



## Remote Access Cards

Selecting one of the Remote Access Card options from the Diagnostics menu will perform extensive testing of that Remote Access Card. To fully test the card, its ports must be physically looped-back. Two diagnostic cables have been provided for this purpose. Plug one end of a diagnostic cable into port 1 and the other end into port 2. Use the other diagnostic cable to do the same for ports 3 and 4.

Only RS232 ports can be looped back. i.e.:602 cards with 202 or 212 modems or RS485 cannot be looped. However, all other parts of the test are valid.

**WARNING:** Running Diagnostics while connected to the network can cause characters to be sent to network elements.

Figure E.3 illustrates the diagnostic cable connected to a remote access card for loop-back.

### Remote Access Card Test Screen

The Remote Access Card is the communication link between the T/MonXM WorkStation running the T/MonXM software and the remote card. If you execute this test option and a fail message occurs, contact DPS Telecom..

Successfully completion of this test confirms that data is exchanged between T/Mon software and remote cards.

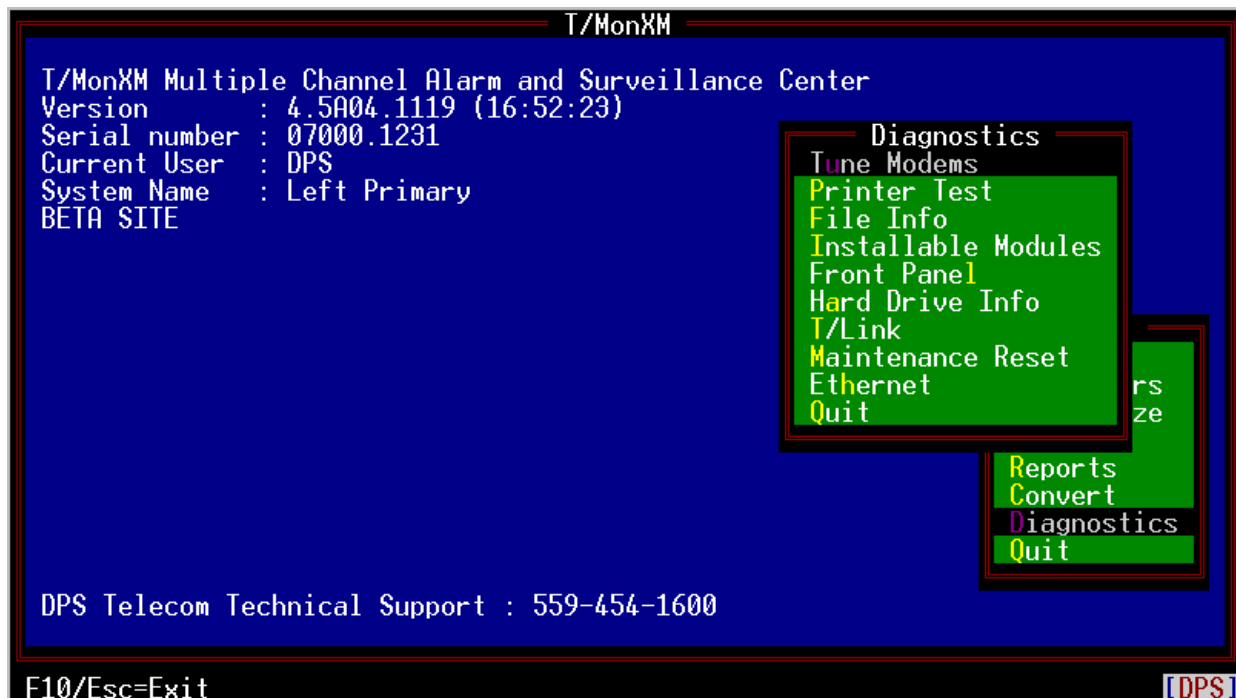


Fig. E.2 - Diagnostic mode menu provides selections for the installed options

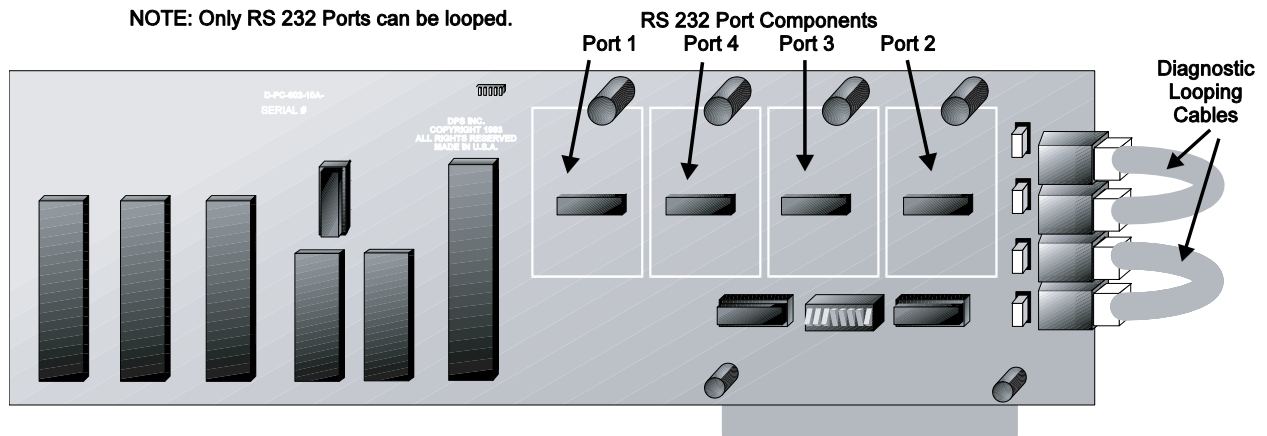


Fig. E.3 - A remote access card in loopback mode

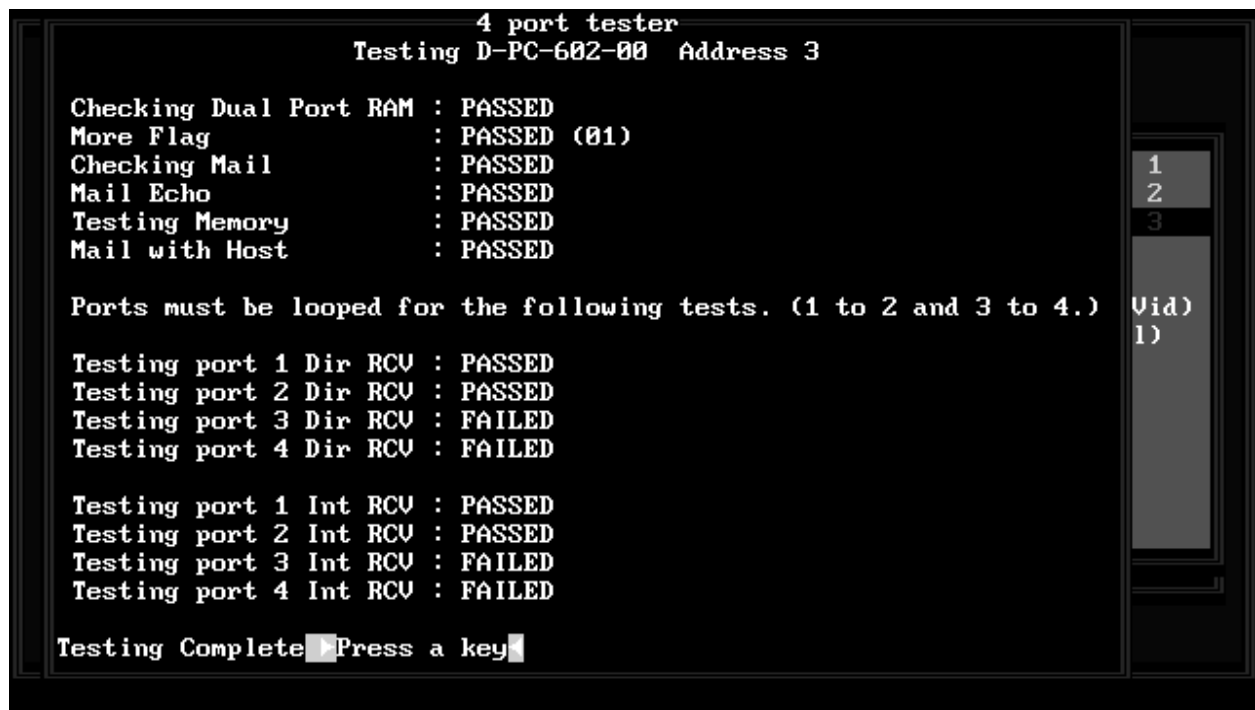


Fig. E.4 – Remote access screen shows test results.

## Tune Modems

Any of the four docking pads on your 602 Card may be populated with 202 modems. If they are, they may need to be tuned to optimize signal quality. The 202 modem levels are software adjustable. The modems are shipped from the factory with the levels set at approximately -13 db — the common industry standard.

Before tuning your modems, you must first select the pad they are on. After selecting a pad to tune, you will be in the Tune Docking Pad screen (see Fig. E.6). Refer to Fig. E.7 for an illustration of the card and connector. From here you tune the modem using the following procedures:

### Tuning procedures

1. Put either a V.F. meter or scope across the transmit leads of the 202 Modem.
2. Set Transmit Low Tone (5).
3. Press the 1 - 4 keys to bring the transmit level to the desired range. If the level is initially too low, use Coarse Up (1). If it is too high, use Coarse Down (4). Once the level approaches the proper range use the 2 and 3 keys to fine tune it.
4. Once tuned, press 7, followed by F10 to return to the monitoring screen.

Do not tune modem below -2 db as the wave forms become distorted.

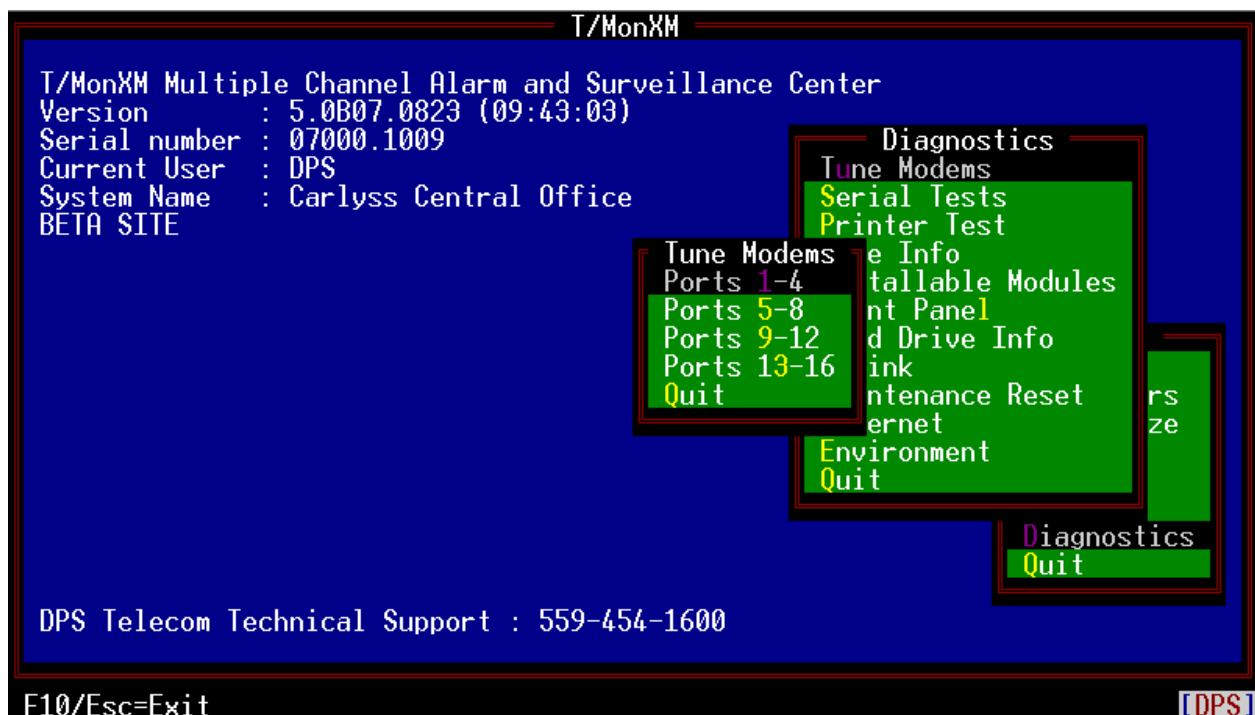


Fig. E.5 – Select four port controller card from the tune modems screen

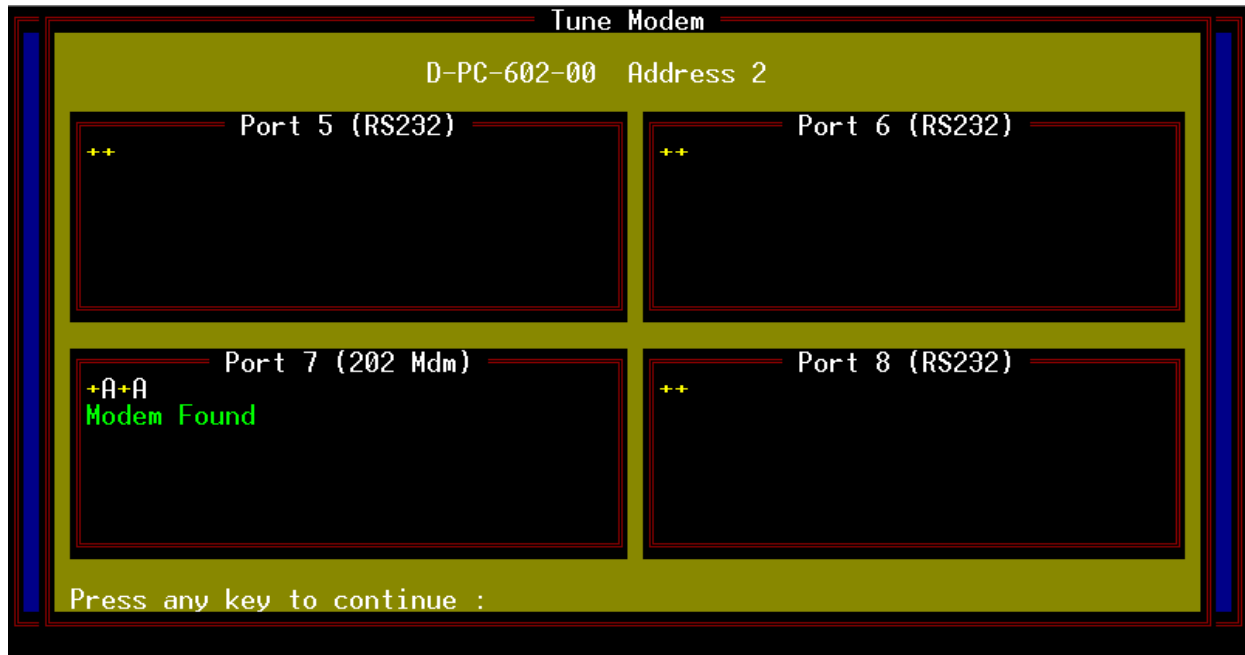


Fig. E.5A – The Tune Modems Window

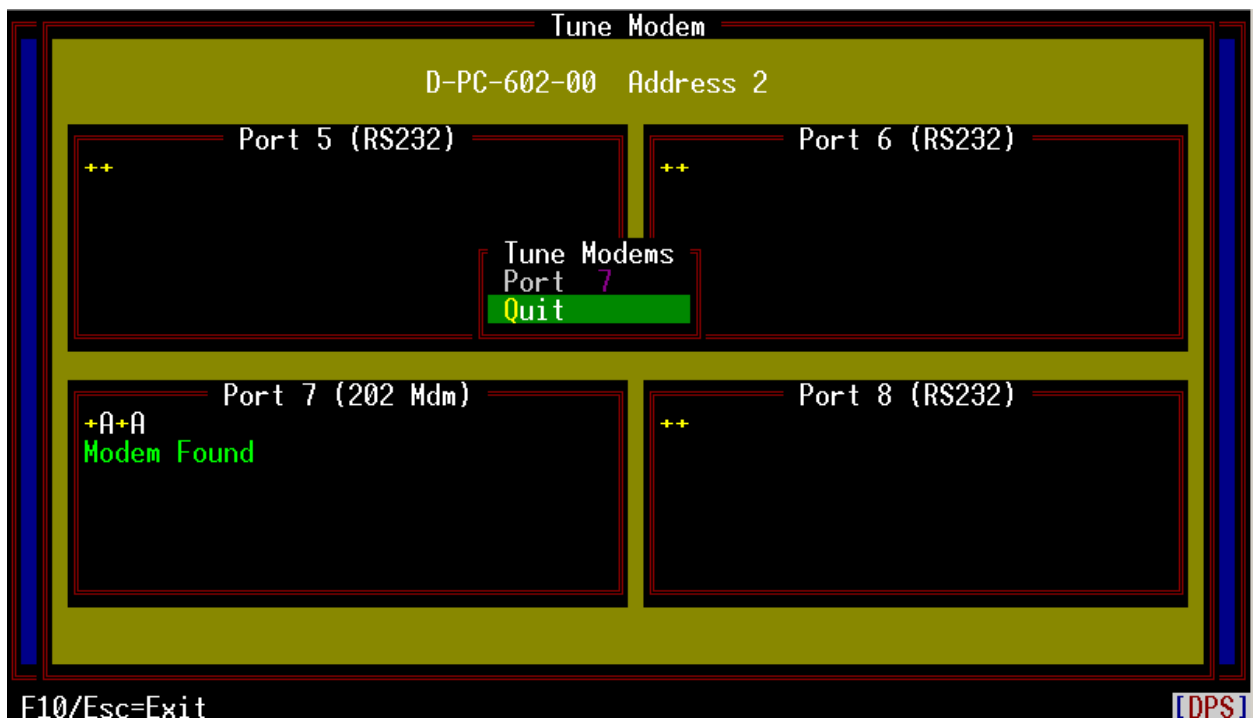


Fig. E.6 – Select pad from the tune modems window

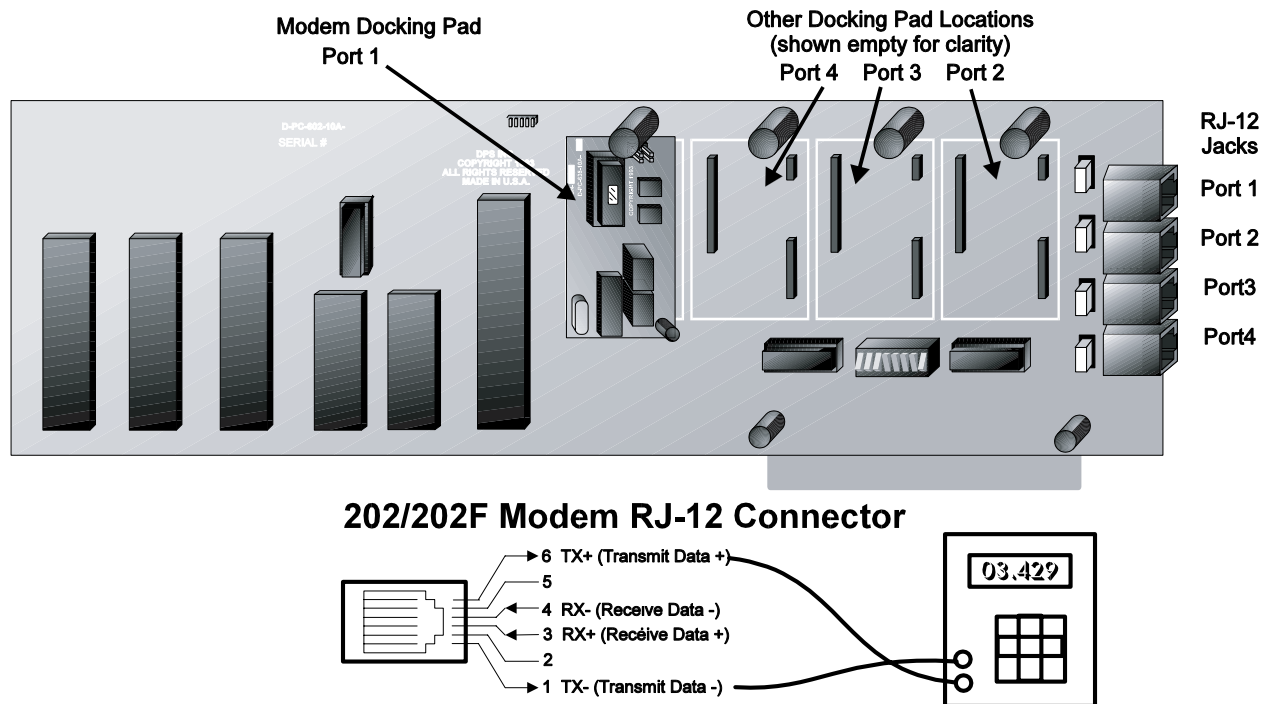


Fig. E.7 - Connect test leads to RJ-12 connector on controller card



Fig. E.8 - The tune docking pad window lists levels setting choices

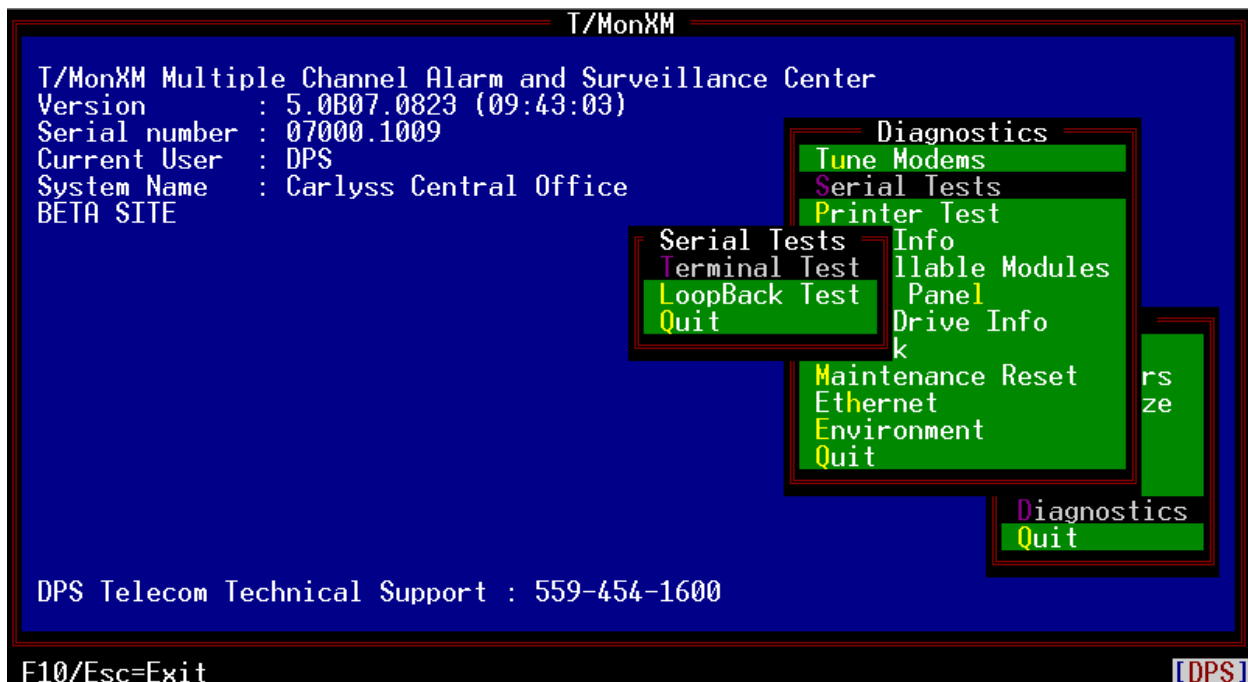
Table E.A - Fields in the Tune Docking Pad window

Field	Description
1. Coarse Up	Course (10 Step) LEVEL UP (hotter).
2. Fine Up	Single step LEVEL UP (hotter).
3. Fine Down	Single step LEVEL DOWN.
4. Coarse Down	Course (10 Step) LEVEL DOWN.
5. Transmit High Tone	Transmitter On - Xmit HIGH TONE.
6. Transmit Low Tone	Transmitter On - Xmit LOW TONE.
7. Transmit Off	Transmitter Off.
8. Transmit Square	Transmitter On - Xmit HIGH/LOW square wave.
F10/Esc	Exit.

## Serial Tests

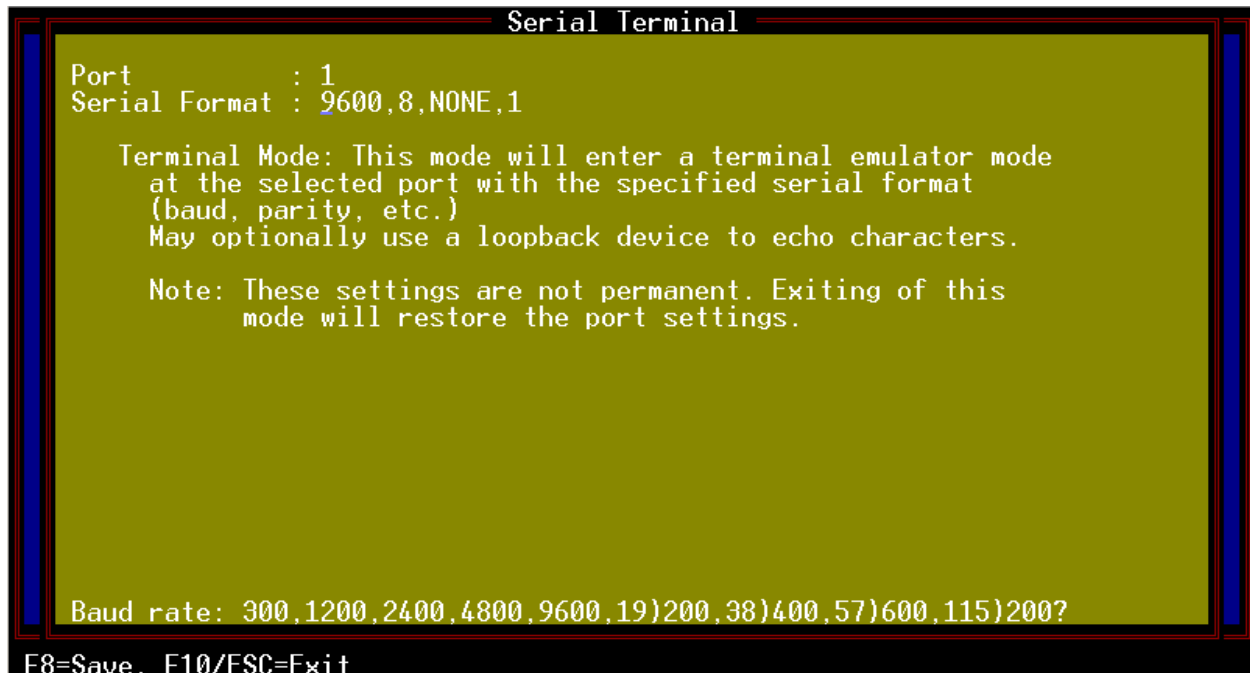
The purpose of this test is to verify that all RS232 ports are able to send and receive properly.

Serial tests consists of **2** modes: **Terminal Mode** and **Loopback Mode**.

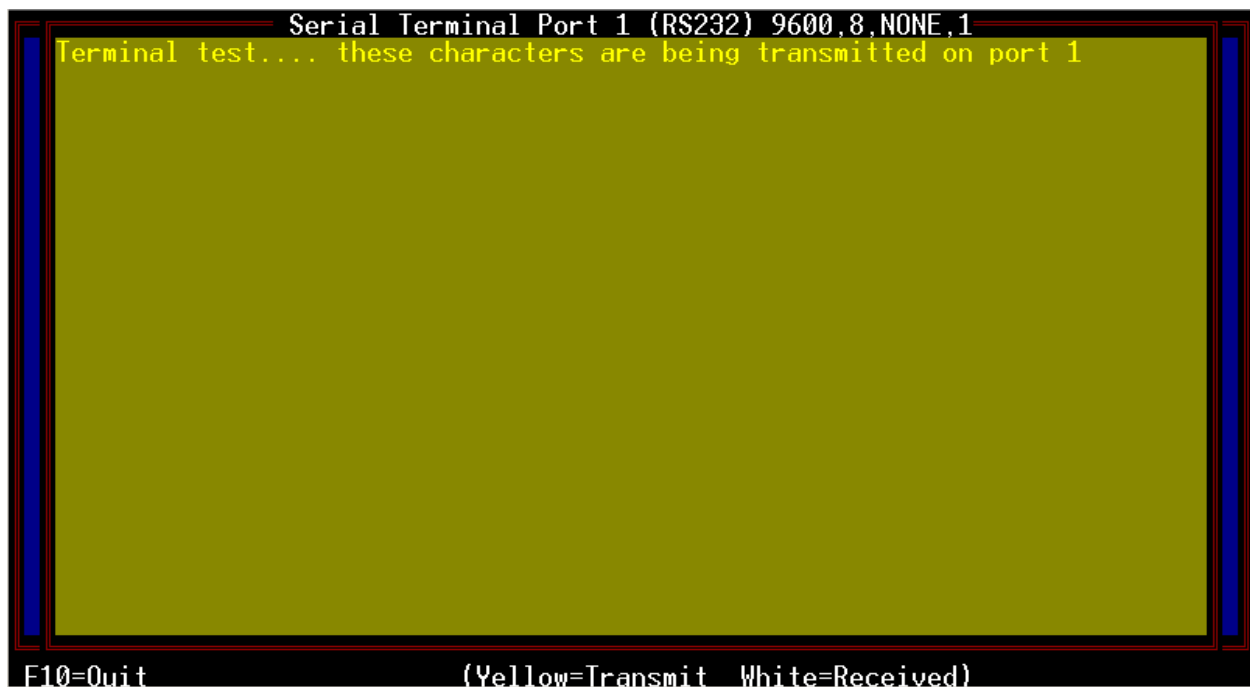


**Terminal Mode**

Terminal Mode will enter a terminal emulator for a specified port. This will allow a craft interface for a specific port without having to modify the database and running the craft mode in monitor mode.



These port settings will only be used for the terminal emulator. It will not affect how the port is data-based for monitor mode.

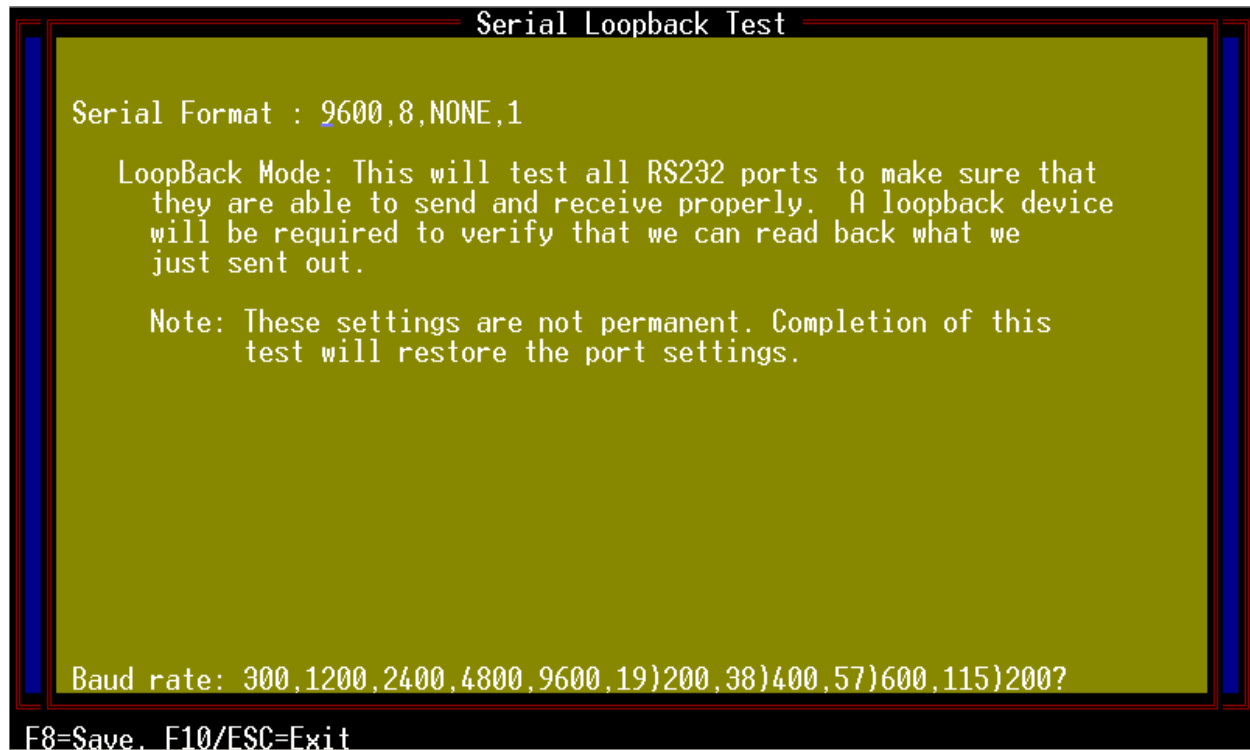


Characters may be entered and will be sent out the port. Transmitted characters will appear in yellow. Received characters will appear in white.

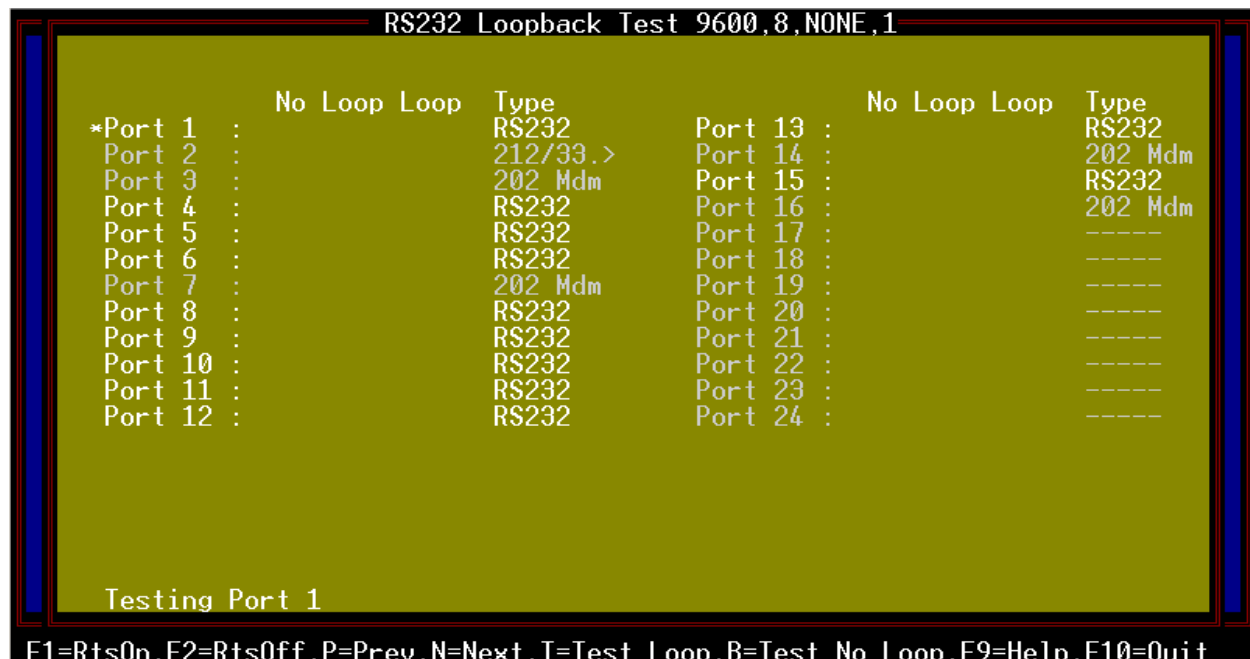
A loopback device may be used for testing purposes to receive characters back.

**LoopBack Mode**

LoopBack Mode will test all RS232 ports by sending out a known string and verifying that it is able to come back. A loopback device will be required for this test.



These port settings will only be used for the loopback test. This will not affect how the port is databased for monitor mode.





Once all of the port information has been entered, an empty status screen with all 24 ports will show up. An “\*” will mark which port is to be tested.

Move the marker to the next port by pressing N or Down arrow (next port). Move the marker to the previous port by pressing P or Up arrow (previous port). It will skip ports that are not defined as RS232 or if the PCI card was not detected.

Test the ports for loopback by pressing T or Right arrow. This will require a loopback device to be attached to the selected port to verify that transmitted data is coming back ok. The status will update once it has received and verified the data. “FAIL” will appear in black if the received data does not match what it had sent out or if it did not receive anything at all. “PASS” will appear in white if it was able to receive the same exact data that it had just sent out.

Test the port for no loopback by pressing B or Left arrow. This will require the loopback device to be removed so it does not receive anything after transmitting data. Data will be sent out the selected port and will fail if anything comes back.

#### Key commands available in RS232 LoopBack mode:

Function Key	Description
<b>F1</b>	Turns RTS on for the selected port.
<b>F2</b>	Turns RTS off for the selected port.
<b>P or Up Arrow</b>	Moves the marker to the previous available port. This will move up the list. (Marker will only stop on RS232 ports.)
<b>N or Down Arrow</b>	Moves the marker to the next available port. This will move up the list. (Marker will only stop on RS232 ports.)
<b>T or Right Arrow</b>	Will test the currently selected port for loopback. A loopback device will need to be attached for the transmitted data to be echoed back for verification. Will pass if the same string is received.
<b>B or Left Arrow</b>	Sends out data and expects nothing to come back. Remove any loopback devices currently attached to the port. This will test if there is a short between transmit and receive. Will fail if the port receives any data.
<b>F9</b>	Displays the help screen for the serial loopback test.
<b>F10/Esc</b>	Exit loopback mode.

## 108 Relay Card (Aud/Vid)

For diagnostic purposes only. This is not part of normal operation.

The 108 Relay Card is used to send controls to physical alarm indicators such as lights or buzzers/speakers connected to relays. The card reads the settings of cut-off switches and has an on-board speaker. The card comes with 4 relays for audio indicators, 4 for visual indicators and 4 for general purposes (identified as “Channel Cutoff” on the screen). The card also has a watchdog circuit that will automatically sense a critical operating condition within T/MonXM’s environment and issue a cold boot (the same operation as pressing the Reset switch on a PC) to the system when necessary. The 108 Relay Card supersedes the 101 Relay Card. Fig. E.7 illustrates the 108 Relay Card and connector.

When you enter the Diagnostics menu, T/MonXM will determine whether your system is running the 101 or 108 Card and will display the applicable card name on the menu (i.e., if you have an older 101 Card and run Diagnostics, you will see 101 Relay Card in the menu, not 108 Relay Card).



Fig. E.9 – Audio/visual relay card diagnostics screen tests A/V relay functions

Table E.B - Key commands available in the Aud/Vid Relay Diagnostics screen

Function Key	Description
F9	Online help.
F10/Esc	Exit.

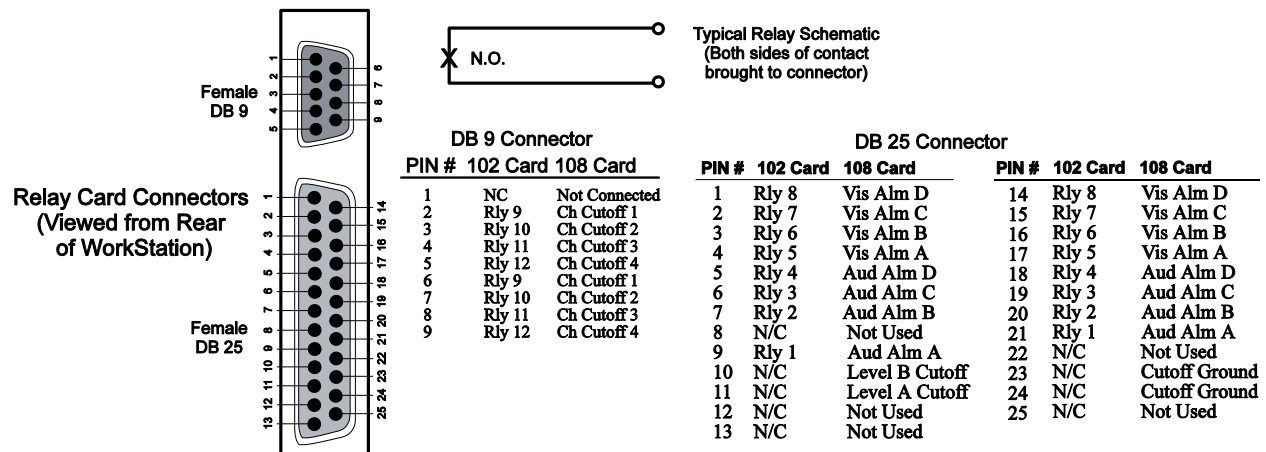


Fig. E.10 – Pinout for 102 and 108 relay cards is identical

### Relays

This option from the Audio/Visual Relay Diagnostics menu allows you to toggle on/off each of the relays. The table below shows the function keys available and their associated functions.

Relays					
RLY	State	RLY	State	RLY	State
1 [F1]	Open	5 [F5]	Open	9 [AF1]	Open
2 [F2]	Open	6 [F6]	Open	10 [AF2]	Open
3 [F3]	Open	7 [F7]	Open	11 [AF3]	Open
4 [F4]	Open	8 [F8]	Open	12 [AF4]	Open
Use the function keys to toggle the relays					

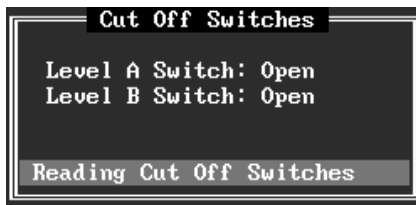
Fig. E.11 – A/V (108) relay diagnostic window

Table E.C - Key commands available in the Relays window

Function Key	Description
F1	Toggles Level A Audible relay.
F2	Toggles Level B Audible relay.
F3	Toggles Level C Audible relay.
F4	Toggles Level D Audible relay.
F5	Toggles Level A Visual relay.
F6	Toggles Level B Visual relay.
F7	Toggles Level C Visual relay.

**Table E.C - Hot keys available in the Relays window (continued)**

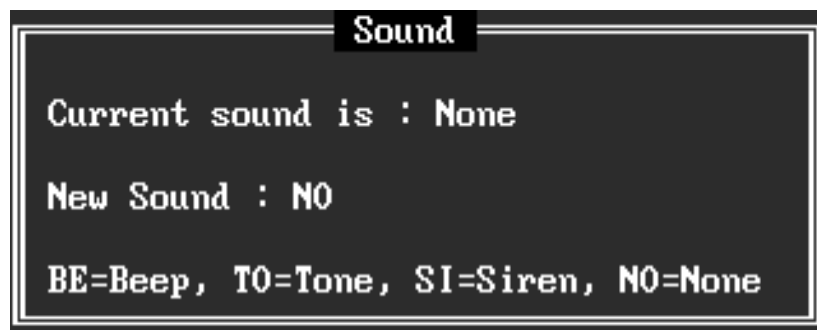
Function Key	Description
F8	Toggles Level D Visual relay.
Alt F1	Toggles General Purpose relay 1.
Alt F2	Toggles General Purpose relay 2.
Alt F3	Toggles General Purpose relay 3.
Alt F4	Toggles General Purpose relay 4.
Ctrl F1	Opens All relays.
Ctrl F2	Closes All relays.

**Cut Off Switches**

This option will read each of the two cutoff switches located on the Audible Alarm Card. After reading the switches, this option will indicate if they are open or closed.

**Fig. E.12 – Cut off switches diagnostic window****Table E.D - Hot keys available in the Cut Off Switches window**

Function Key	Description
F10/Esc	Exit.

**Fig. E.13 - Sound diagnostic window**

This section and Table E.E apply to the 102 Relay card as well.

**NOTE:** T/MonXM will not use the sound on the 102 card.

**Sound**

This option will allow you to test each of the three different tones that the audible alarm card will generate. The three available tones and their corresponding letters are given in the following table.

**Quit**

This option will allow you to quit the Relay Diagnostics menu and return to the Diagnostics menu.

**Table E.E - Test entry codes in the Sound window**

Entry	Description
BE	Periodic beeping sound.
TO	Steady sound.
SI	High and low pitch sound.
NO	No Tone generated.
F10/Esc	Exit.

## 102 Relay Card (local)

The 102 Local Relay Card is identical to the 108 Relay Card but doesn't have an audible sounding device and is set for a different I/O location.

### Relays

This option from the Relay Card Diagnostics menu allows you to toggle on/off each of the relays. The pin-out for the connectors on the 102 Relay Card are the same as those on the 108 Relay Card. Refer to Figure E.7. The table and window illustration on the next page show the function keys and their associated functions.

**Fig. E.14 – Local relay card diagnostics screen tests local relay functions****Table E.F - Key commands available in the 102 Local Relay Diagnostics screen**

Function Key	Description
F9	Online help.
F10/Esc	Exit.

Relays					
RLY	State	RLY	State	RLY	State
1 [F1]	Open	5 [F5]	Open	9 [AF1]	Open
2 [F2]	Open	6 [F6]	Open	10 [AF2]	Open
3 [F3]	Open	7 [F7]	Open	11 [AF3]	Open
4 [F4]	Open	8 [F8]	Open	12 [AF4]	Open
Use the function keys to toggle the relays					

Fig. E.15 – Local (102) relay diagnostics window

Table E.G - Key commands available in the Relays window

Function Key	Description
F1	Toggles relay 1 between open and closed.
F2	Toggles relay 2 between open and closed.
F3	Toggles relay 3 between open and closed.
F4	Toggles relay 4 between open and closed.
F5	Toggles relay 5 between open and closed.
F6	Toggles relay 6 between open and closed.
F7	Toggles relay 7 between open and closed.
F8	Toggles relay 8 between open and closed.
Alt F1	Toggles relay 9 between open and closed.
Alt F2	Toggles relay 10 between open and closed.
Alt F3	Toggles relay 11 between open and closed.
Alt F4	Toggles relay 12 between open and closed.
Ctrl F1	Opens All relays.
Ctrl F2	Closes All relays.

**Cut Off Switches**

Refer to Cut-Off Switches sub-section under the 108 Relay.

**Sound**

Refer to Sound sub-section under the 108 Relay.

**Quit**

This option will allow you to quit the Relay Diagnostics menu and return to the Diagnostics menu.

## Printer Test

Printer Test is only valid for printers directly connected to the T/Mon or IAM-5 unit.

Selecting the Printer Test option from the Diagnostics menu will perform a quick test on any parallel printer connected to either LPT1 or LPT2 printer ports. When the Printer Test option is chosen, the following printer dump will be sent to the printer:

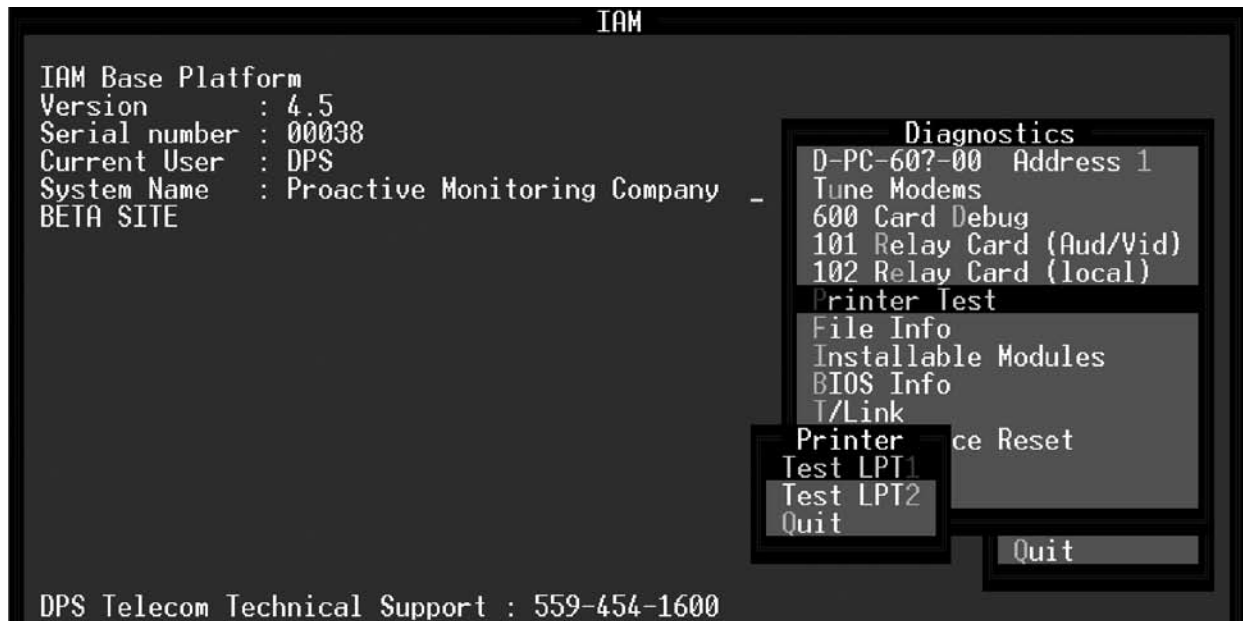


Fig. E.16 – Select printer port to test from the printer test screen

```

This is line 1 of 20 on LPT1      !"#$%&'()*+,-./0123456789;:@ABCDEFGHIJKLMNO
This is line 2 of 20 on LPT1      PQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz !"#$
This is line 3 of 20 on LPT1      %&'()*+,-./0123456789;:@ABCDEFGHIJKLMNOPQRST
This is line 4 of 20 on LPT1      UVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz !"#$%&'()
This is line 5 of 20 on LPT1      *+,-./0123456789;:@ABCDEFGHIJKLMNOPQRSTUVWXYZ
This is line 6 of 20 on LPT1      Z[\]^_`abcdefghijklmnopqrstuvwxyz !"#$%&'()*+,-./
This is line 7 of 20 on LPT1      /0123456789;:@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
This is line 8 of 20 on LPT1      _`abcdefghijklmnopqrstuvwxyz !"#$%&'()*+,-./0123
This is line 9 of 20 on LPT1      456789;:@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abc
This is line 10 of 20 on LPT1     defghijklmnopqrstuvwxyz !"#$%&'()*+,-./0123456789;:@ABC
This is line 11 of 20 on LPT1     DEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrst
This is line 12 of 20 on LPT1     uvwxyz !"#$%&'()*+,-./0123456789;:@ABCDEFGHIJKLMN
This is line 13 of 20 on LPT1     OPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz !"#$%&'()*+,-./
This is line 14 of 20 on LPT1     /0123456789;:@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`
This is line 15 of 20 on LPT1     'abcdefghijklmnopqrstuvwxyz !"#$%&'()*+,-./0123456789;:@AB
This is line 16 of 20 on LPT1     CDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstu
This is line 17 of 20 on LPT1     vwxyz !"#$%&'()*+,-./0123456789;:@ABCDEFGHIJKLMNO
This is line 18 of 20 on LPT1     PQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz !"#$%&'()*+,-./
                                     123456789;:@ABCDEFGHIJKLMNO
                                     PQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz !"#$%&'()*+,-

```

Fig. E.17 – Example printer test printout

## File Info

The File Info option in the Diagnostics menu will display the T/MonXM files that are in the current directory being used. This option allows you to read file information to a Technical Support person who is troubleshooting the system.



Fig. E.18 – The file info menu

### TASK Files

Selecting TASK Files will provide you with a list of files that T/MonXM uses to download the 4-port intelligent controllers. The file name, the date and time the file was created, the size of the file, the version number and the file usage is shown on the screen.

T/MonXM				
The .TSK Files				
File Name	Date	Time	Size	Comment
BOOT.TSK	4/12/91	1:42p	512	(C) 1990,91 DPS INC. BOOT - BOOT LOADER VER 1.1 RLS 4-12-91
COMINT.TSK	4/12/91	1:43p	4480	(C) 1990,91 DPS INC. COMINT - TEST PROG VER 1.1 RLS 4-12-91
IDLE.TSK	4/12/91	1:43p	256	(C) 1990,91 DPS INC. IDLE - TEST PROG VER 1.1 RLS 4-12-91
LOOP.TSK	4/12/91	1:43p	2304	(C) 1990,91 DPS INC. LOOP - TEST PROG VER 1.1 RLS 4-12-91
MAIL.TSK	4/12/91	1:43p	256	(C) 1990,91 DPS INC.

Cursor Keys=View, F10/Esc=Return to Menu

Fig. E.19 – Task files window



```

System Log
Mar 6,2000 16:17:55 System Log for serial number 00006
Mar 6,2000 16:17:55 [SYSTEM] REBUILT INDEX FILE : INTPT2.IDX
Mar 6,2000 16:17:59 [SYSTEM] KEY FILE SIZE CHANGED : DERVMON.IDX
Mar 6,2000 16:17:59 [SYSTEM] REBUILT INDEX FILE : DERVMON.IDX
Mar 6,2000 16:40:52 T/MonXM Version : 3.0w+2
Runtime Error 2 occurred at address 003D:0F38
Mar 6,2000 18:10:37 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:38 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:39 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:40 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:41 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:42 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:43 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:43 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:44 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:45 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:46 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:47 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:48 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:49 Error: ETYPE=250 ND=64 Code=9 SC=5
Mar 6,2000 18:10:50 Error: ETYPE=250 ND=64 Code=9 SC=5
File : TMONXM.SL Size: 3117786 Date/Time: Jun 12,2000 15:58:36
F2=File, F3=Search, F5=Top, F9=Help, F10/Esc=Exit

```

Fig. E.20 – The system log window

### System Log

Selecting the System Log option from the File Info menu will display the System Log screen and allow you to view system activity. Information shown includes the date and time of entry, the version number, and a listing of errors.

Pressing F9 (help) while at the System Log screen allows you see the function and cursor control keys. To view a file: Press F2 and place the cursor on the file name, then press Enter. The response on the screen will show the file name, file size, and date and time the file was created. The table below shows the function keys and their associated functions.

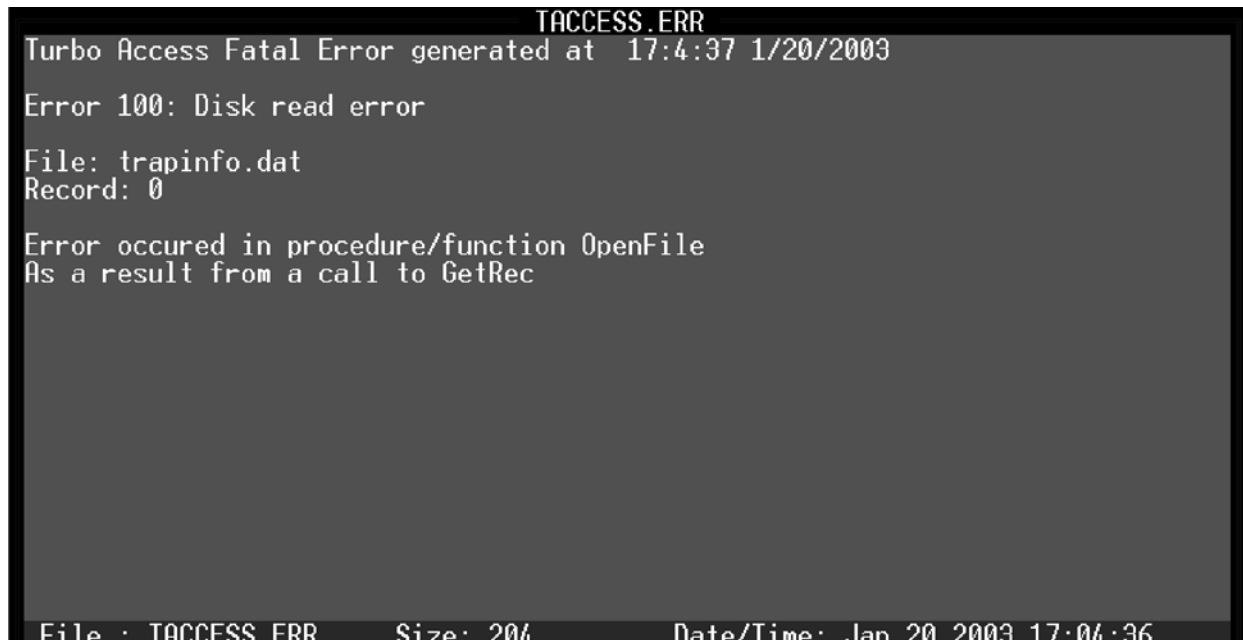
Table E.H - Key commands available in the Systems Log window

Function Key	Description
F2	Select a file to view.
F5	View the beginning of the file.
F9	Online help screen.
F10/Esc	Exit.
Up/Down Arrows	Move a line at a time.
PgUp/PgDn	Previous Page/Next Page. <b>Note:</b> If you page down past the buffer you may not be able to get to the top unless you press Home. T/Mon uses a 10k buffer for the incoming text from the System Log file.
Home (F5)	Move to the top of the file.
End (F6)	Move to the end of the file.
F3	Search for function.

**T/ACCESS.ERR**

The T/ACCESS.ERR option allows you to view the last disk access error generated by T/MonXM if an error condition should arise.

The following information is displayed in the T/ACCESS.ERR file: file name, size of the file, date, time and location of the error(s). An example of the T/ACCESS.ERR screen is shown in Figure E.21.



```

TACCESS.ERR
Turbo Access Fatal Error generated at 17:4:37 1/20/2003
Error 100: Disk read error
File: trapinfo.dat
Record: 0
Error occured in procedure/function OpenFile
As a result from a call to GetRec
File : TACCESS.ERR      Size: 204      Date/Time: Jan 20 2003 17:04:36
  
```

**Fig. E.21 – The TACCESS.ERR window**

**DTMF Greeting File**

The DTMF Greeting File is used to answer the phone and send out info from the current greeting file. This file can be viewed on screen. This file is used in connection with building access and special hardware peripherals.



```

Serial number : 00038
Current User  : DPS
System Name   : Proactive Monitoring Company
BETA SITE

Diagnostics
D-PC-607-00 Address 1
Tune Modems
600 Card Debug
101 Relay Card (Aud/Vid)
102 Relay Card (local)
Printer Test
File Info
Installable Modules
BIOS Info

File Info
TASK Files
System Log
TACCESS.ERR
DTMF Greeting File
Quit

e Reset
Quit

DPS Telecom Technical Support : 559-454-1600
  
```

**Fig. E.22 – The DTMF greeting file window**

# Installable Modules

Selecting the Installable Modules option from the Diagnostics menu will display the Modules menu. The Modules menu allows you to view software module installation status and provides module information.

## Installation Status

Selecting the Installation Status option from the Modules menu will display a list of the modules this version of T/MonXM can support. It also indicates which modules are installed and their capability or capacity. See illustration of window in Figure E.24 and table of fields on the next page. Refer to the Software Module sections of this manual for more information on individual software modules.



Fig. E.23 – The installable modules menu

Table E.I - Key commands available in the Installable Options window

Function Key	Description
PgUp	Move up one page.
PgDn	Move down one page.
Home	Go to beginning of Installable Options screen.
End	Go to end of Installable Options screen.
Up Arrow	Move up one line.
Down Arrow	Move down one line.

Installable Options	
Status	Option
UNRESTRICTED	Remote Access
255 PORTS	TBOS Responder
255 PORTS	DCPF Interrogator
INSTALLED	LED Bar
255 PORTS	E2 Responder
255 PORTS	TBOS Interrogator
255 PORTS	E2 Interrogator/Monitor
255 PORTS	DCM Interrogator
255 PORTS	Direct ASCII Interrogator
255 PORTS	TL1 Combiner
INSTALLED	Building Access
INSTALLED	Alarm Message Forwarding
255 PORTS	DCPF Responder
255 PORTS	FX8800 Interrogator
720	Alarm Windows
INSTALLED	VDM
INSTALLED	Pager
more ↓	

Fig. E.24 – Installation status window

Table E.J - Fields in the Installation Status window

Field	Description
Status	Indicates if option is installed and capacity: •Not Installed = Option not available, module not installed •Installed = Option is available •Unrestricted = Option available with no capacity restrictions •### = Option is available the number of times stated •# Ports = Number of ports the option covers (capacity).
Option	Description of the option.

### Module Information

Selecting the Module Information option from the Modules menu displays information about optional software modules that have been installed. This list includes only the modules present on the system. Refer to the Software Module sections of this manual for more information.

Module Information			
Program Serial Number : 00312			
File Name	Serial #	Type	Status
DFP00488.MOD	00312	DCP/DCPF Interrogator/Responder Mult. Port	OKAY
AQL00504.MOD	00312	ASCII Query Language	OKAY
MAP00503.MOD	00312	Modem ASCII Interrogator Multiple Port	OKAY
DLK00502.MOD	00312	Datalok 10 Multiple Port	OKAY
BAU00501.MOD	00312	Building Access (DTMF and BAU)	OKAY
DAP00500.MOD	00312	Direct ASCII Interrogator Multiple Port	OKAY
TLC00499.MOD	00312	TL1 Combiner	OKAY
TLP00498.MOD	00312	TL1 Responder Multiple Port	OKAY
RA400497.MOD	00312	Remote Access 4 Ports	OKAY
TBP00496.MOD	00312	TBOS Interrogator/Responder Multiple Port	OKAY
DMP00495.MOD	00312	DCM Interrogator Multiple Port	OKAY
E2P00494.MOD	00312	E2 Multiple Port	OKAY
AMF00493.MOD	00312	Alarm Message Forwarding	OKAY
PAG00492.MOD	00312	Pager	OKAY
VDM00491.MOD	00312	UDM	OKAY

Fig. E.25 – Module information window

## Front Panel Test

**Note:** The following section appears only on T/MonXM.

Selecting the Front Panel option from the Diagnostics menu will display the Front Panel Tests menu. This menu will allow you to run diagnostic tests on the front panel of the T/Mon NOC. The Front Panel menu option is only accessible on T/Mon NOC systems. It is necessary to be located in front of the T/Mon NOC when performing these tests in order to determine the results of the test (i.e. audio, screen drawing etc...).

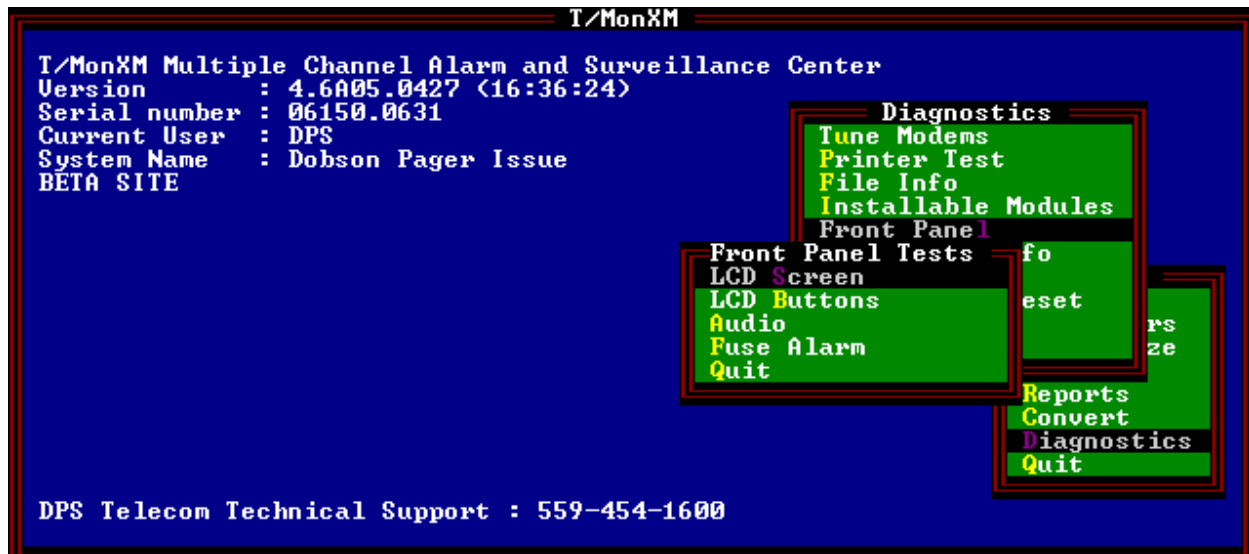


Fig. E.26 – The Front Panel Test menu

### LCD Screen

Selecting the LCD Screen option from the Front Panel Tests menu will display a list of diagnostic tests to perform on the front panel LCD. These tests include screen drawing and contrast changes.

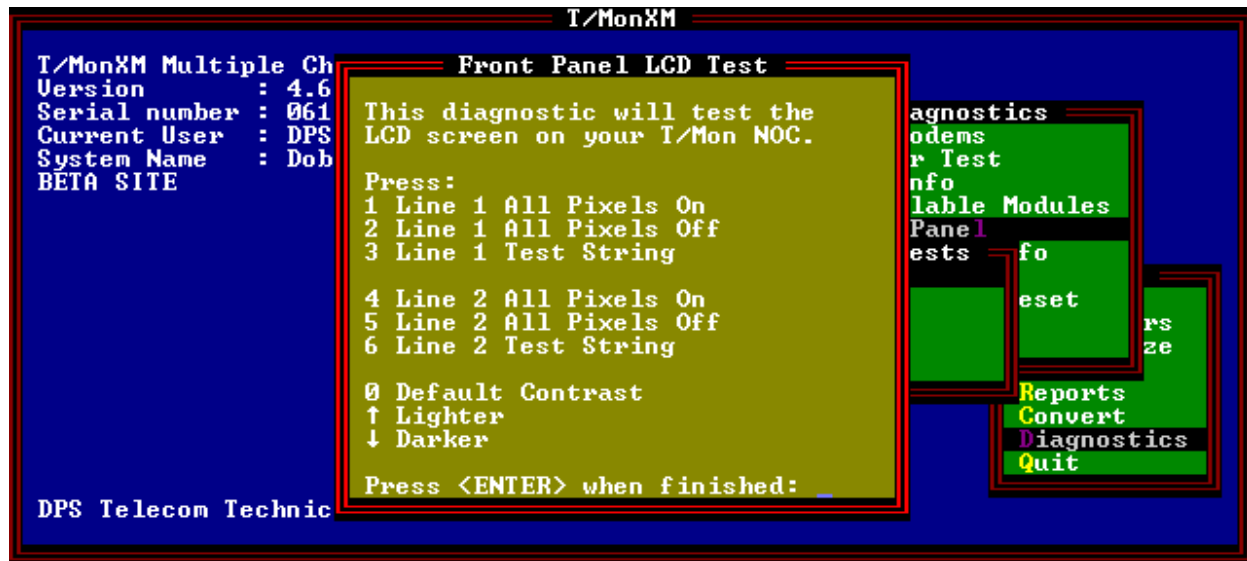


Fig. E.27 – The Front Panel LCD Test screen

### LCD Buttons

Selecting the LCD Buttons option from the Front Panel Tests menu will display the status of each LCD button. Pressing the buttons should alter their status.

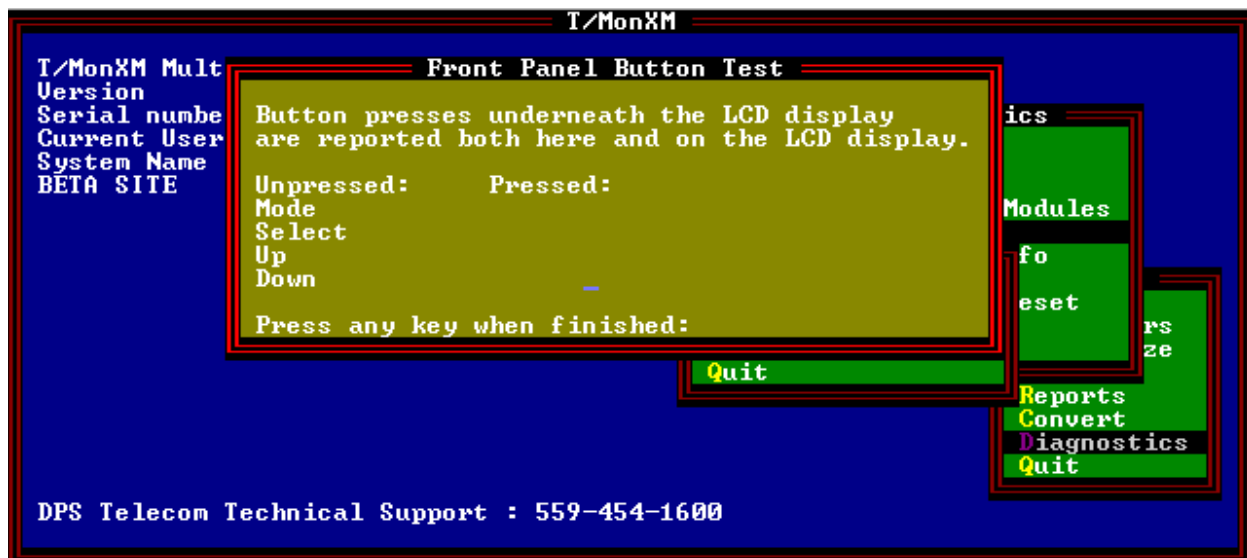


Fig. E.28 – The Front Panel Button Test screen

### Audio

Selecting the Audio option from the Front Panel Tests menu will display a list of diagnostic tests to perform on the front panel sound system. These tests include tone changes.

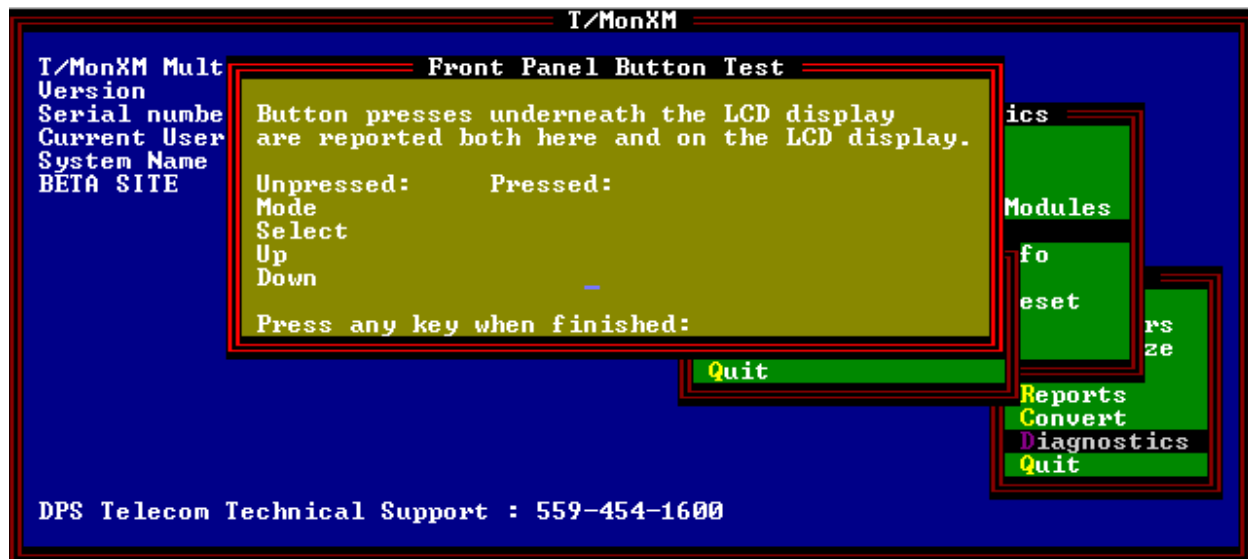


Fig. E.29 – The Front Panel Audio Test screen

### Fuse Alarm

Selecting the Fuse Alarm option from the Front Panel Tests menu will display the status of each fuse. Removing a fuse or inserting a blown fuse should alter their status.

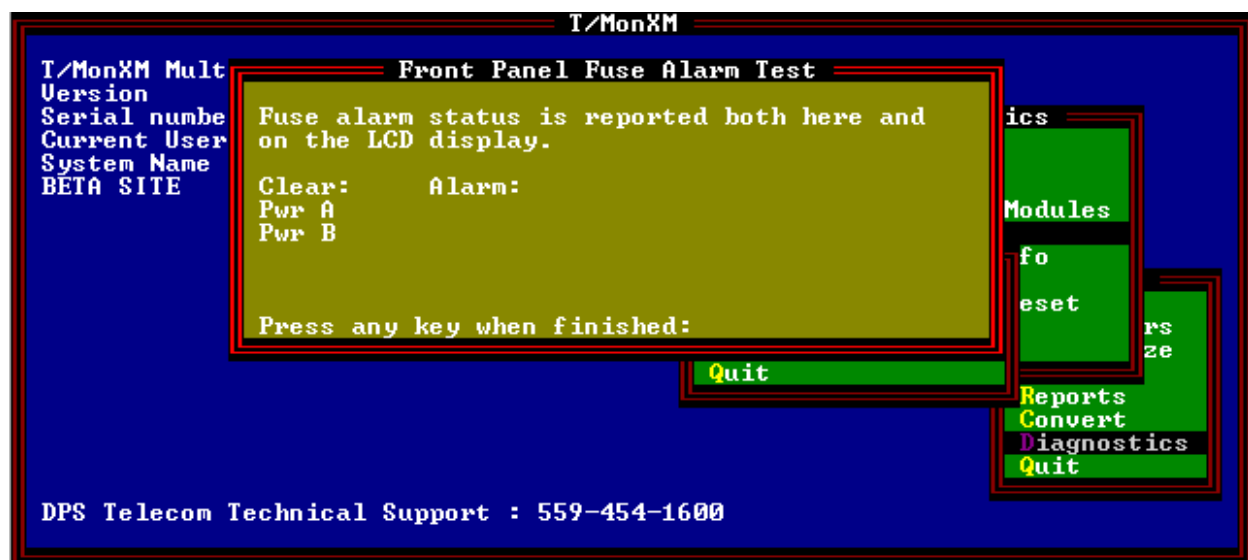


Fig. E.30 – The Front Panel Fuse Alarm Test screen

## Hard Drive Info

Selecting Hard Drive Info from the Diagnostics Menu will allow you to view the status of about the disk drives of your T/Mon. The volume label, disk usage, and the last time the history file was updated are all included.

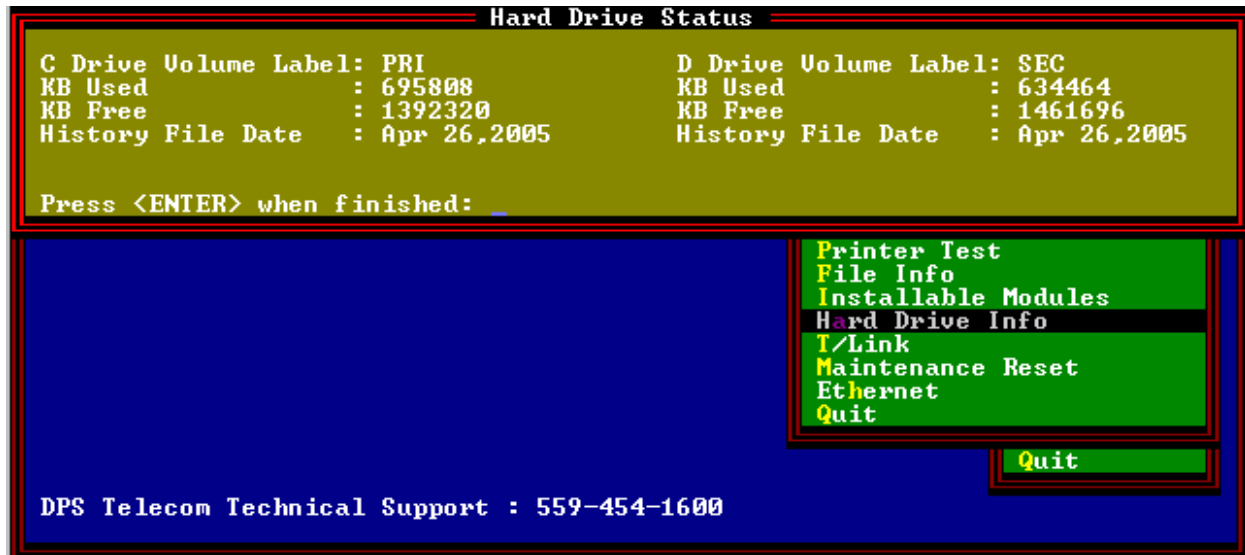


Fig. E.31 – The Front Panel Fuse Alarm Test screen

## T/Link

This T/Link screen is used only to verify the version of T/Link you are running in the case DPS Technical Support needs it. T/Link is used to remotely connect and control a T/MonXM master. See W/Shell documents for additional information.



Fig. E.32 – The T/Link screen



## Maintenance Reset

This function tests the watchdog reset function of the 108 Card. It causes the system to reset (cold boot). To run this test highlight Maintenance Reset in the Diagnostics menu and press Enter. Press M to test. Press F10/Esc to abort.

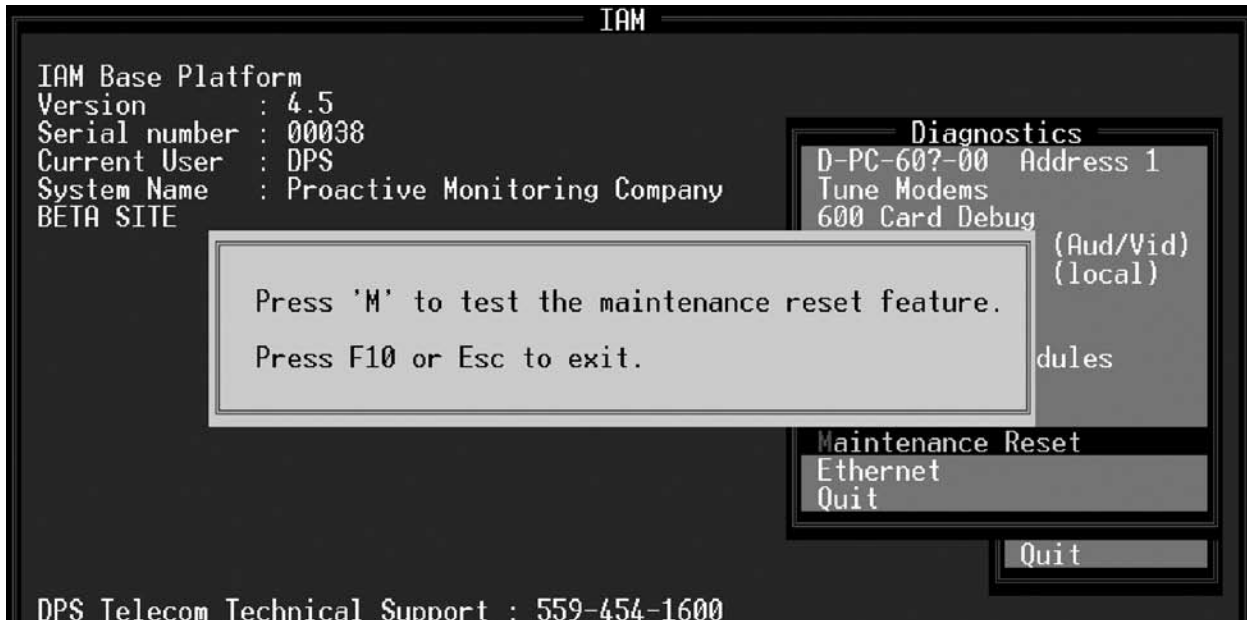


Fig. E.33 – Select maintenance reset from the diagnostics menu

## Ethernet

The ethernet screen is used to verify the version of the installed TCP agent and IP address of T/Mon.



Fig. E.28 – Ethernet menu item shows TCP agent version

# Appendix F

## Disk Files

---

### Program Files

The release disk contains the following files:

IAM.EXE	IAM executable files.
TMONXM.EXE	T/MonXM executable files.
TMONXM2.EXE	
TASK.TSK	
BOOT.TSK	4 Channel Communication controller file.
REMOTE.TSK	4 Terminal Controller file.
TEST.TSK	4 Channel and 4 Terminal Controller diagnostic files.
COMINT.TSK	
MLECHO.TSK	
LOOP.TSK	
IDLE.TSK	
MAIL.TSK	

---

### Database Files

As the system is used, the following files will be created in the T/MonXM account:

CTLCAT.DAT	Labeled Controls Files
CTLCAT.IDX	
CTLPNT.IDX	
CTLPNT.DAT	
DCTL2.DAT	Miscellaneous Files
DCTL2.IDX	

XMPNT.DAT	Point Files
XMPNT.IDX	
DEVADD.IDX	Address Files
DEVADD2.DAT	
DEVADD3.IDX	
EMHIST2.IDX	History Files
EMHIST2.DAT	
XMLIVE.DAT	Live Files
XMLVDAT.IDX	
XMLVDITEM.IDX	
EMMSG.DAT	Text Messages File
EMWIN.DAT	Window Files
EMWIN.IDX	
TMONEM.DAT	Program Data File
TRB.DAT	Trouble Log Files
TRBDATE.IDX	
TRBPNT.IDX	

**Note:** As the system is used, the names of the configuration files in the T/MonXM account follow the standard rule “SYSTEMNAME.EXT”.

# Appendix G

## Uninterruptible Power System



Fig. G.1 - The uninterruptible power system screen.

**Note:** Please contact DPS prior to using any UPS System to verify compliance with DPS Standards.

The Uninterruptible Power System is a hardware option that can be purchased for your T/MonXM WorkStation. The DPS Inc. Uninterruptible Power System (UPS) is line-interactive, meaning it can communicate directly with T/MonXM via T/MonXM's serial ports Com 2.

**NOTE:** This is a Com port, not a port on a four-port intelligent controller card.

The unit is computer-grade quality, has outstanding lightning and brownout protection, and RF noise filtering.

The DPS-supplied UPS comes complete with all cables and instructions for installation. Other UPS's can be used, but may require a special cable.

In the event of a power failure, the unit responds instantly to provide continuous AC power to T/MonXM. Because there is no break in power transfer between line power and UPS usage, you are able to maintain an orderly shutdown without corrupting alarm data files. T/MonXM can be set to shut itself and the UPS down from 0 to 60 minutes after loss of line power.

Selecting the UPS option from the Parameters menu (press U to select UPS and press Enter) will bring you to the UPS Parameters screen.

**Table G.A. - Fields in the UPS screen**

Field	Description
UPS Enabled	Set to Y if you are using the UPS option. Otherwise, this should be set to N. [N]
UPS Port	Enter the Serial Com Port number that is connected to the UPS.
UPS Time-out	<p>The amount of time, in minutes (0-60), after going to battery power before the workstation will be shut down. If the UPS' low battery indicator comes on during this period of time, the workstation will be shut down anyway. In the event of an extended overnight power failure this will permit unmanned operation. A value of 0 means the workstation will always wait for the low battery indicator from the UPS before shutting down.</p> <p>When power goes back on T/MonXM will restart the system, either:</p> <ol style="list-style-type: none"> <li>1) initialize and go into Monitor mode - if you were in Monitor mode when the system powered down or</li> <li>2) go to the Log On screen - if you were not in Monitor mode.</li> </ol>

# Appendix H

## Troubleshooting

This section is an overview of the most common software problems that may arise when installing and running T/MonXM. The error codes listed below are broken into two sections, Run-Time Errors and Security Errors. Each will give a description of what the error code means and the course of action that needs to be taken to alleviate the problem.

### Run-Time Errors

Run-time errors cause the program to display an error message and terminate. A run-time error will be displayed in the following format:

Run-time error nnn at xxxx:yyyy

The nnn is the run-time error number, and xxxx:yyyy is the run-time error address (segment and offset).

**Table H.A - Common software error codes, descriptions and actions**

Error Code	Description	Action
1	Invalid file handle.	Contact DPS.
2	File not found.	Contact DPS.
3	Path not found.	Contact DPS.
4	Too many open files.	Check CONFIG.SYS for the entry "FILES=200." Files should be 200.
5	File access error.	Error reading file. Corrupt file or bad media.
6	Invalid file handle.	Contact DPS.
12	Invalid file access.	Contact DPS.
15	Invalid drive number.	Contact DPS.
16	Cannot remove current directory.	Contact DPS.
17	Cannot rename across drives.	Contact DPS.
18	No more files.	Contact DPS.
100	Disk read error.	Contact DPS.
101	Disk write error.	Contact DPS.
102	File not assigned.	Contact DPS.
103	File not open.	Contact DPS.
104	File not open for input.	Contact DPS.
105	File not open for output.	Contact DPS.
106	Invalid numeric format.	Contact DPS.
150	Disk is write-protected.	Remove write protect tab.
152	Drive not ready.	Check drive. Make sure that the door on drive is closed.

**Note:** Table H.A continues on following page.

**Table H.A - Common software error codes, descriptions and actions continued**

Error Code	Description	Action
154	CRC error in data.	Media problem.
158	Sector not found.	Media problem.
159	Printer out of paper.	Check the printer and its cables.
160	Device write fault.	Check the drive and its cables.
161	Device read fault.	Check the drive and its cables.
162	Hardware failure.	Media problem.
198	Hardware failure.	Problem communicating with all remote cards
201	Out of range variable.	Contact DPS.
202	Stack overflow error.	Contact DPS.
203	Heap overflow error. Not enough memory.	Contact DPS.
216	General protection fault	Contact DPS.

---

## Security Errors

**Table H.B - Common security error codes, descriptions and actions**

Error Code	Description	Action
7010	Running under pre-DOS 2.0 operating system.	Reboot system with DOS 5.0 or later and rerun.
7024	Same program, different serial number with protection already on disk.	Contact distributor.
7034	Media contains no protection. Hardware may not be compatible with software.	Contact distributor.

**Note:** If any of these problems continue to exist after attempts to correct them, be sure to write down the “complete” error message. Please note what you were doing just prior to when the error occurred before contacting the distributor.

# Appendix I

## Quick Reference Tables



Fig. I.1 - Alarm Summary Mode screen

### Alarm Summary Mode Quick Reference

#### Alphabetic Listing of Key Commands

Alarm Indicator Control	Alt-F1
ASCII Analyzer	Shift-F7
Building Access Statistics	Ctrl-F3
Channel Summary	Alt-F9
Chat Mode	Ctrl-F9
Site Controls Screen (based on selected window)	F8
COS Alarms Mode	F3
Craft Mode	Ctrl-F7
Datalok Analogs	Shift-F8
DCPF Network	Shift-F10
Dialup Control	Shift-F4
English Analyzer Mode	Alt-F5
Log Off/Return to Master Menu	Esc/F10
Help Screen	F9
Labeled Controls	Ctrl-F8
Legend Window	F5
Pager Control/Status	Shift- F3
Performance/Statistics Window	F6
Protocol Analyzer Mode	Alt-F8
Report Menu Mode	Alt-F7



Reset Performance Statistics	Alt-F2
Set English Filter Window	Ctrl-F5
Silence Window Status	Alt-F3
Site Statistics	Shift-F6
Standing/Live Alarms Mode	F4
System Information Window	Ctrl-F6
TL1 Observation Mode	Ctrl-F2
Toggle Local Sound	Ctrl-F4
Toggle Printer Logging	Ctrl-F1
VDM Control	Shift-F5
X.25 Stats	Shift-F2
View the list of silenced items	Alt-F4

**Table I.A - Key commands available in the Alarm Summary Mode screen**

Key		Ctrl-	Alt-	Shift-
F1		Toggle Printer Logging	Alarm Indicator Control	
F2		TL1 Observation Mode	Reset Performance Statistics	X.25 Stats
F3	COS Alarms Mode	Building Access Status	Silence Window	Pager Status Control
F4	Standing Alarms Mode	Toggle Local Sound	Silenced Status	Dialup Control
F5	Summary Legend Window	Set English Filter	English Analyzer Mode	VDM Control
F6	Performance/ Statistics	System Information		Site Statistics
F7		Craft Mode	Report Menu Mode	ASCII Analyzer
F8	Site Controls	Labeled Controls	Protocol Analyzer Mode	Datalok Analogs
F9	Help Screen	Chat Mode	Channel Summary	
F10				DCP(F) Network

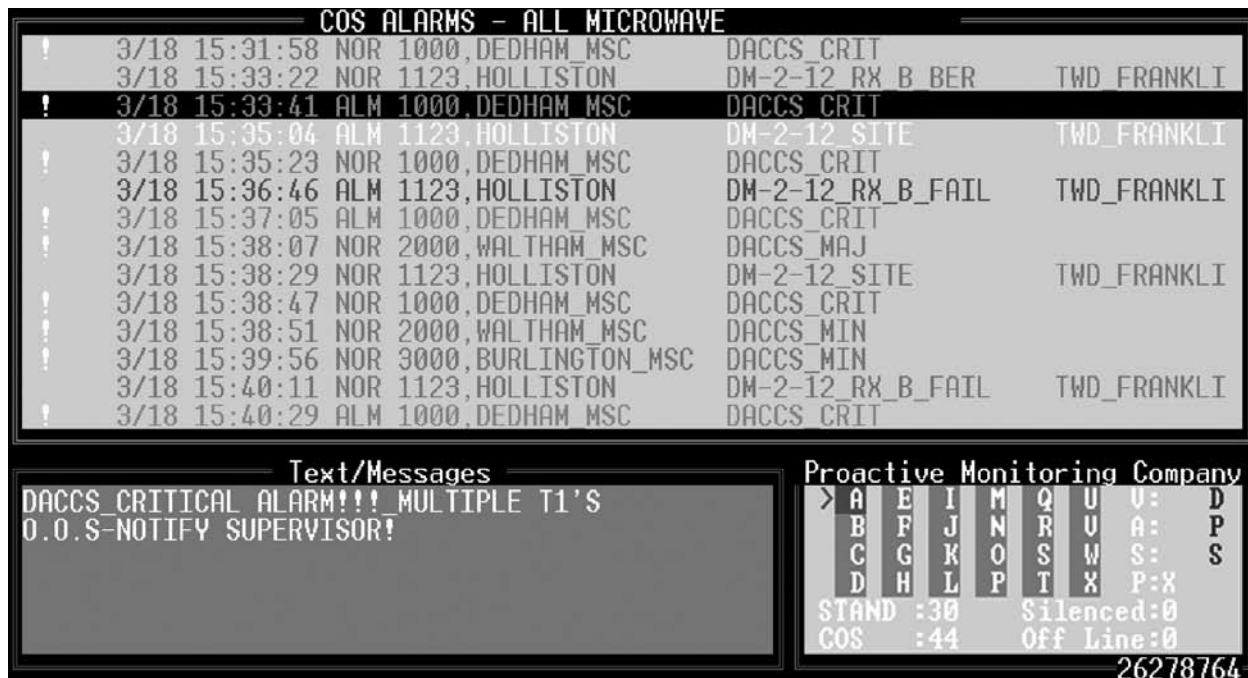


Fig. I.2 - COS Mode screen

## COS Mode Quick Reference

### Alphabetic Listing of Key Commands

Acknowledge Alarm	Enter
Acknowledge All Alarms (Current Wind)	Alt-F4
COS Window Report	Alt-F7
English Analyzer	Alt-F5
Exit COS screen	Esc/F10
First Alarm Window	Alt-F1
Go To First Alarm Page	Home
Go To Last Alarm Page	End
Go To Next Alarm Page	PgDn
Go To Previous Alarm Page	PgUp
Help Screen	F9
Last Alarm Window	Alt-F2
Next Window With Alarms	Ctrl-F2
Pan Alarm Screen	Tab
Performance/Statistics	Alt-F6
Previous Window With Alarms	Ctrl-F1
Protocol Analyzer	Alt-F8
Select Next Window	F2
Select Previous Window	F1
Silence Alarm	Alt F3
Site Controls (For current window)	F8
Standing/Live Alarms Mode	F4
Tag Alarm	Shift-F10
Text/Messages Window	F5
Toggle Sound On/Off	Ctrl-F4

Trouble Log  
View Analog

F6  
Ctrl-F6

**Tbl. I.B - Key commands available in the COS Mode screen**

Key		Ctrl-	Alt-	Shift-
F1	Select Previous Window	Previous Window with Alarms	First Alarm Window	
F2	Select Next Window	Next Window with Alarms	Last Alarm Window	
F3			Silence Alarm	
F4	Standing Alarms Mode	Toggle Sound On/Off	Acknowledge All Alarms in Current Window	
F5	Text/Message Window		English Analyzer on Selected Window	
F6	Trouble Log	View Analogs	Performance/Statistics	
F7			COS Window Report	
F8	Site Controls		Protocol Analyzer	
F9	Help online.			
F10	Exit			Tag Alarm
Tab	Pan Alarm Screen Over			
Home	Go to First Alarm Page			
End	Go to Last Alarm Page			
PgUp	Go to Previous Alarm Page			
PgDn	Go to Next Alarm Page			
Enter	Acknowledge Alarm			



Fig. I.3 - Standing Alarms screen

## Standing Alarms Quick Reference

**Note:** See Table I.B for key commands available in Standing Alarms screen.

### Alphabetic Listing of Key Commands

COS Alarms Mode	F3
English Analyzer (On Current Window)	Alt F5
Exit	Esc/F10
First Alarm Window	Alt F1
Go To First Alarm Page	Home
Go To Last Alarm Page	End
Go To Next Alarm Page	PgDn
Go To Previous Alarm Page	PgUp
Help Screen	F9
Last Alarm Window	F2
Live Window Report	Alt F7
Next Window With Alarms	Ctrl F2
Pan Alarm Screen Over	Tab
Performance/Statistics	Alt F6
Previous Window With Alarms	Ctrl F1
Protocol Analyzer	Alt F8
Select Next Window	F2
Select Previous Window	F1
Site Controls	F8
Tag Alarm	Shift F10
Text/Messages Window	F5
Toggle Sound On/Off	Ctrl F4
Trouble Log	F6
View Analogs	Ctrl F6

**This page intentionally left blank.**

# Appendix J

## Modem Initialization Strings

The following table lists some initialization strings for commonly used dial modems.

**Table J.A - Modem Initialization Strings**

Modem Model	Initialization String
A.T.&T. Paradyne PCMCIA 3760/62/63/64	AT V1 X4 Q0 SR41=3\Q0\N1
Hayes Accura	AT S7=120 E1 V1 M1 Q0 X4 &Q0 or AT&Q0
Intel Satisfaction (400 and 400E)	ATS7=120E1V1M1QX4\N\Q%C0%E-J&Q
Intel 14/14E	ATB5S7=120E1V1Q0X4\G\N\C-J
US Robotics Sportster 14400	AT&M0&K0E1V1Q0X4
Paradigm 14400	ATS7=120E1\G1%B1200%C0\N1
Megahertz PCMCIA CC3144	AT&F&C1&D2&Q&K&S1W2S95=\N# C\
Compaq 14.4 laptop	ATS7=120E1V1M1Q0X4\N1%C0\Q0
DPM Factory Default	ATS7=120E1V1M1Q0X4
Best Data Products, Inc. Model 9624FQ	ATE1V1L3M1Q0S7=120X4&Q0&D&C
U.S. Robotics Courier (33.6 / 28.8 kbps)	ATZ
Multi Tech (33.6 & 56K)	ATH0E0&C1S0=0V0X4\$MB9600\$SB9600\$&Q1

The following is an example of a common modem problem due to an initialization string error:

With the modem's audible monitor enabled, you can hear the modem dial and the response tone from the remote when it answers. But instead of a "connect" message you get a "no carrier" message. This is generally caused by a high speed modem taking too long to negotiate speed and protocol.

Check the modem initialization string in Table J.A. If your modem is not listed, consult your modem manual. Be sure that flow control, compression and error correction are off. If difficulty persists, contact DPS Technical Support. Please have your modem manual handy.

**This page intentionally left blank.**

# Appendix K

## LED Display Bar

---

---

### Basic Operation and Setup

LED Bar support is included for existing LED Bar users.

Alarms can be conveniently monitored by watching the LED Display Bar from a distance. The LED Display Bar displays alarm and other information a single line at a time. The user chooses an alarm window and T/MonXM will scan through alarms one-by-one and display alarm information.

#### Software Module Setup

The LED Display Bar software module must be installed before you can access the LED Display Bar. Refer Section 2 - Software Installation for installation procedures.

#### Hardware Setup

The D-PR-0490-00 LED Display Bar works with T/MonXM and other T/Mon products that support LED Display bars.

Plug the AC power adapter into a 110 VAC wall outlet and the round power connector into the LED Display Bar. Then, plug the DB9 plug into the LED Display Bar port and plug the RJ11 plug into a T/Mon remote access port. All subsequent LED bars use a DB9 to DB9 cable (D-PR-044-00)

#### LED Bar Specifications

There are four user assignable display colors. You have a choice of red, green, yellow and rainbow. Thirteen characters are visible at one time. Additional characters scroll to the left. The interface is RS422 (4 wire) at 300 to 9600 baud.

---

### LED Bar Remote Parameters

Selecting Remote Ports from the Parameters menu will allow you to select and define the LED Bar Port and baud parameters. Refer to Figure K.1.



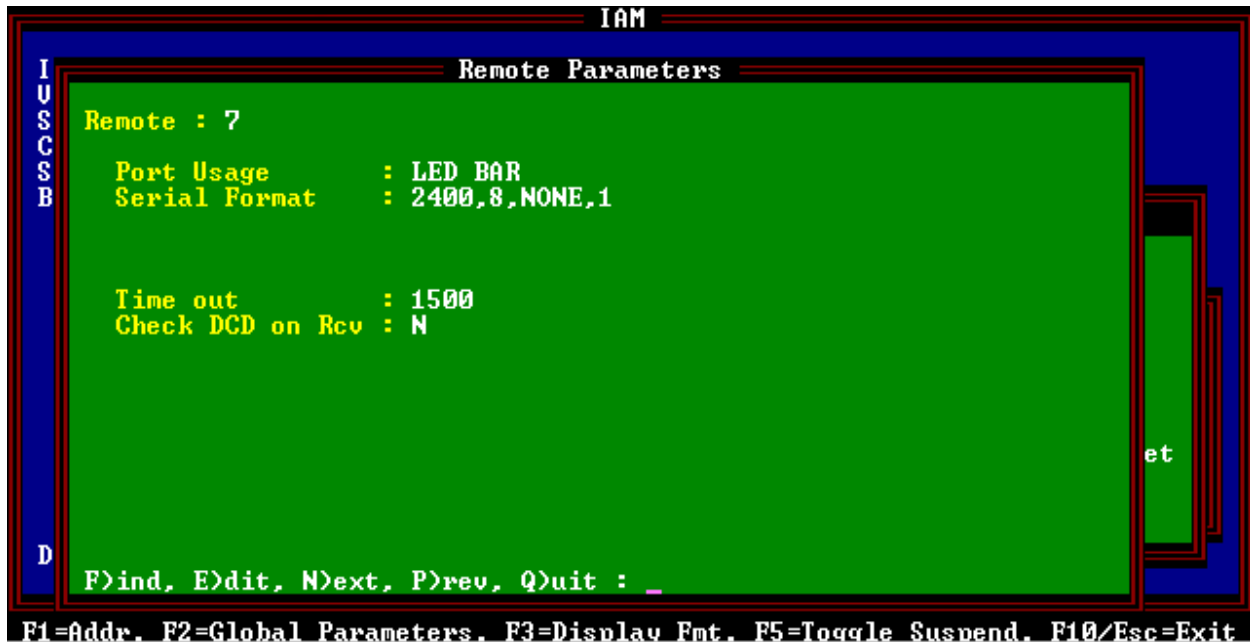


Fig. K.1- Remote Parameters screen

Table K.A - Key commands available in the Remote Parameters screen

Field	Description	
Port Usage	LED Bar	
Serial Format	Baud	Valid baud rates are 1200, 2400, 9600 and 38400. [2400]
	Data Bits	Data bits for the port. [8]
	Parity	Valid parity values are odd, even and none. [NONE].
	Stop Bits	Stop bits for the port. [1]

\* **Note:** The fields in the Remote Parameters screen vary according to port usage

Table K.B - Key commands available in the Remote Parameters screen

Function Key	Description
F1	Addresses. Allows you to access the LED Bar Definition Screen
F2	Global Parameters. Define the Message Delay, Character Separator, Separator Color, and Other Text Colors.
F3	Display Format. Define the display format data will appear in Monitor Mode.
F5	Toggle Suspend. Allows you to define but temporarily halt or suspend this function.
F10/Esc	Leaves the Remote Parameters Screen.



Fig. K.2 - LED Bar Definition screen

## LED Bar Address Definition

Pressing F1 (Addresses) from the Remote Parameters screen allows you to access the LED bar definition screen.

The field names for the LED bar definition screen are described below:

Table K.C - Fields in the LED Bar Definition screen

Function Key	Description
LED Bar Address	The LED Display Bar address
Alarm Window	The alarm window that the LED Display Bar will use to display alarms.
Description	Other information about the LED Display Bar. (e.g., its physical location.)

Table K.D - Function keys available in the LED Bar Definition screen

Function Key	Description
F1	GOTO. Moves the cursor to a selected address.
F3	BLANK. Deletes the current LED address from the database.
F8	Saves the LED Bar database.
F9	Help. On line help.
F10/Esc	Leaves the LED Bar database screen without saving any changes that may have been made.

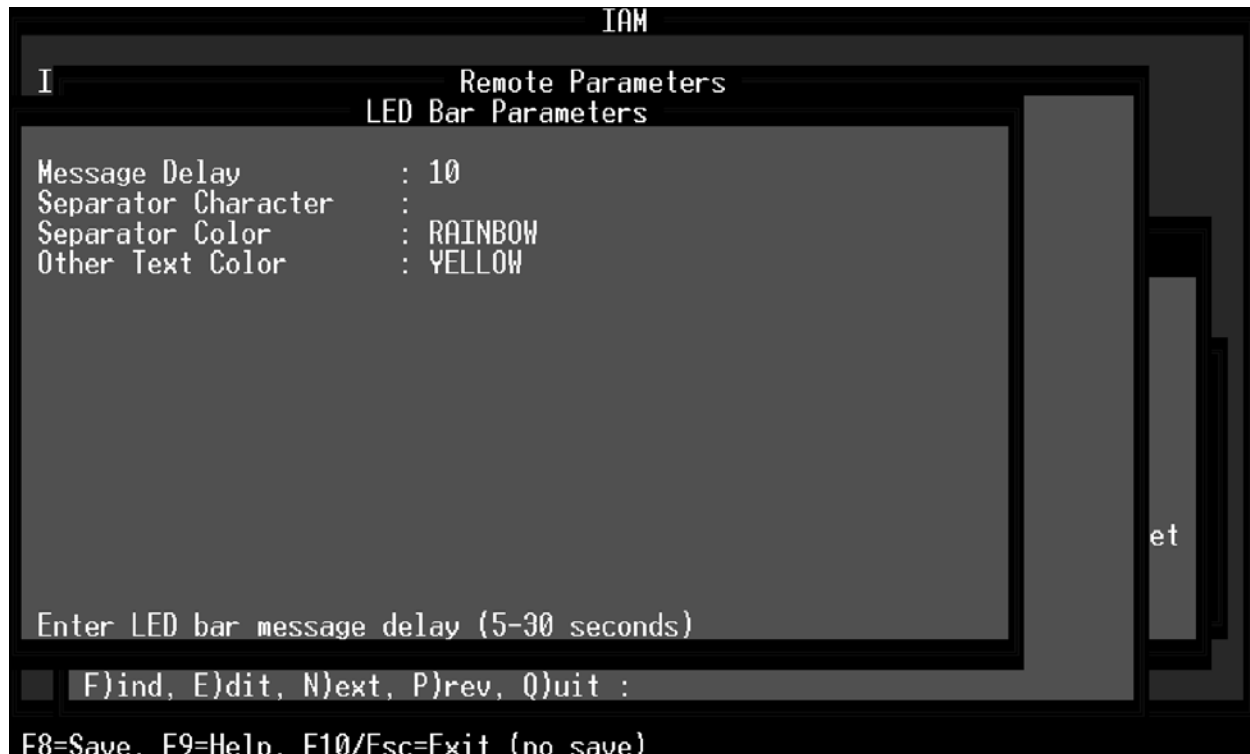


Fig. K.3 - LED Bar Parameters screen

## LED Alarm Color Definition

Pressing F2 (Global Parameters from the Remote Parameters screen allows you to specify which four colors the different alarms will show on the LED display bar. A different color can be assigned to each alarm level “A” through “D”.

See Table K.F for defaults in the LED Bar Parameters screen.

Table K.E - Fields in the LED Bar Parameters screen

Field	Description
Message Delay	The amount of time, in seconds, that the LED Display Bar will pause before displaying a new message (5-30 seconds). [10]
Separator Character	The character that is displayed between messages. [ ] <b>Note:</b> This character may be a space.
Separator Color	The color of the separator character. Choose from Green, Rainbow, Red, and Yellow. [Rainbow]
Other Text Color	The color used for messages such as “T/Mon Offline” and “No Alarms.” Choose from Green, Rainbow, Red, and Yellow. [Yellow]



Fig. K.4 - Edit LED alarm format screen.

# LED Alarm Format

Define the displayed alarm format by pressing F3 (Display Format from the Remote Parameters screen) in the Remote Parameters screen. The fields attributes are similar to the Master menu > Parameters > Alarm Format option. Refer to section 16-15 (Alarm Formatting) for more information.

**This page intentionally left blank.**

# Appendix L

## Frequently Asked Questions

The following questions were sent to DPS Telecom by T/MonXM users, and the answers were written by the DPS Telecom Technical Support staff.

The latest FAQs can be seen on the T/MonXM support page:

**[www.dpstele.com/support/techfaqs/tmoniam.html](http://www.dpstele.com/support/techfaqs/tmoniam.html)**

If you have a question about T/MonXM, please call us at:

**1-800-622-3314**

or e-mail us at

**[support@dpstele.com](mailto:support@dpstele.com)**.

### **Q. I'm not receiving pages from my T/MonXM. What's the problem?**

**A.** Possible Causes: the following sequence must be completed before a page will be delivered:

- The alarm must occur, and it must pass any qualification tests that have been programmed for it
- The alarm must generate a call to the pager in question
- The call must reach a paging facility
- The paging facility must be able to interpret the call and send the page
- The pager must be able to receive the page

Most paging problems are caused by relatively simple factors that interrupt this sequence.

### **Diagnosing T/MonXM Paging Problems:**

**A.** Verify that T/MonXM can successfully deliver a page to the pager in question:

1. From the Alarm Summary screen, use Shift-F3 to access the Pager Status screen.
2. Select F4=Send
3. Select the appropriate pager
4. Enter a test message and hit through remaining entries
5. Observe results, including reception of an actual page
6. If a page is not received, try the following:
 

Call the paging facility yourself, from any convenient phone, using the phone number programmed into the device. A paging system should answer.

  - If you still have problems, unplug the phone line from your T/MonXM system, plug in an ordinary analog phone, and call the paging facility using **exactly** the same number T/MonXM is set up to call. A paging system should answer. There is often a problem with forgotten factors such as having to dial 1 first to get an outside line being in a different area code than originally thought, or having a long-distance call-blocker on the line. Also verify that the line sounds clean, with no static, hum, or other noise.
  - If you still have problems, note exactly how the paging facility responds to calls:
 

If delivering a numeric page, there is generally a brief voice message after which the numeric message is entered. To step over this voice message, a delay before the

actual message is sent is specified under Files-Pager-Pager Carriers. Verify that the delay is appropriate for your system.

- If delivering an alpha page, the device expects to make an immediate modem connection when the facility answers - this comes across as a hissing sound.
  - Many paging facilities are enhancing their service by adding voice messaging capabilities and other features that deviate from these standard dialup sequences. In some cases, your device can be programmed to work around these exceptions; in other cases the paging facility may have a simplified dialup sequence available if you ask for it.
  - If you still have problems you may observe activity on the pager port itself by selecting the English Analyzer (Alt-F5) or the Protocol Analyzer (Alt-F8) from monitor mode, and use plus/minus to get to the pager port. You may use T/Remote to send a manual page as above, or trigger an alarm to generate a page. This may give you a hint as to what the problem may be.
- B.** If T/MonXM can page, but a particular alarm is not being received, you should check the chain of events that occurs when an alarm is triggered. Basically, the alarm calls a Pager Profile, the Profile calls one or more Operators, and the Operator pages the Carrier who is currently on call according to the weekly schedule.
1. Verify that the alarm is set up to be paged. Locate the alarm under Parameters > Remote Ports > Devices ( F1) > Points ( F1) > Edit, and scroll to the appropriate point. Press F4 to scroll right—the Pager Profile is set up in the far right column and is not ordinarily visible. A pager profile number should be entered there.
  2. Verify what the pager profile configuration. Exit to the Master menu, select Files > Pager > Profiles and scroll to the appropriate profile number. Press F2 to view Pager Entries—these list Pager Operators, the types of notifications they are to receive, and any delays that may be involved. It is possible that your operator is not set up to receive the type of page you are expecting, or alarms are being acknowledged before delays expire.
  3. Verify your pager information. Exit to the Pager Carrier item on the Pager menu and confirm the pager number, carrier's initials, phone, etc.
  4. Verify that this carrier is assigned to one of the operators identified in step 2.2. Go to the Pager-Weekly Schedules menu item, enter the appropriate operator number, and confirm that this carrier is scheduled at the time you expected to receive a page. Also confirm that the normal schedule was not overridden by a Schedule Exception.

**Q. Why can't I see all my windows? Activate controls? Acknowledge alarms? Etc.**

- A.** Privileges for all of these items, and many more, are controlled from the System Users item on the File Maintenance menu. The system identifies you through your logon initials and only allows activity specified on the System Users screen. The ability to change these privileges is itself a controllable privilege.

**Q. XMEdit is missing screens/menu items/options.**

- A.** If your XMEdit seems to be missing features that are available in your T/MonXM system, there are probably optional software modules that have been installed in one but not the other. You can determine what has been installed by selecting Diagnostics > Installable Modules > Installation Status on the master menu. If XM/Edit is missing anything, run T/Install from the original installation floppy for each missing module. Only install the single

disks sets that begin with XM (i.e. XMASC, XMPAG, XMRMT1). **Make sure it gets installed into the XM/Edit directory**, not the default T/MonXM directory.

**Note:** XMEdit can use the same modules as the original T/Mon or IAM system and does not necessarily need an additional module set for the XMEdit Software.

**Q. I want to upgrade my T/MonXM system from Version 2.4 to the most current 4.5. Are there any special hardware changes I must have before I can proceed with my upgrade?**

A. Generally not. The only primary option is to have a minimum of 64MB of memory installed on your system. Version 2.4 only requires 4MB maximum to run. Contact DPS Telecom for pricing on available upgrade features.

**Q. Why should I do a backup of my current database before I upgrade or change my T/MonXM system?**

A. We encourage all users to back up their current database before any modification takes place. This will eliminate the possibility of losing your data files, in case of any difficulty during the upgrade or modification.

**Q. I get a Runtime Error 5 @ address 0065:0099 every time I try to restore a backup of my database to my T/MonXM system. What's the problem?**

A. This runtime error is usually caused by the two files from your backup disk, (ARCHIVE.DPS & CTRL.DPS) having read-only file attributes assigned to them. You can remove the read-only option by inserting the disk in a Windows-based computer. Open the (A) drive, right-click on the file, choose Properties, and uncheck the Read-only check box. You can also do this from a DOS-based computer by using the attribute and -r command. (A:\attrib -r archive.dps and A:\attrib -r ctrl.dps)

**Q. How do I delete reports from my T/MonXM system?**

A. From the Master menu choose Files > Utilities > Report Maintenance > Delete Report File. You will be prompted to choose which file to delete. Use caution upon deleting files. There is no Undo command to bring these files back.

**Q. How can you temporarily suspend the automatic restart of a T/MonXM system?**

A. You can edit the autoexec.bat file as follows:

```
if not exist c:\resume.dat goto shell
copy c:\resume.dat c:\resume.off
del c:\resume.dat
:shell << existing line for reference only
```

With the file edited to include these lines, the T/MonXM system will not automatically restart after interrupted operation. This mode is helpful during diagnostic or maintenance type functions but the lines should be removed (or at least REMed out) before returning the system to normal operation.

**Q. Why can users Ack alarms from T/Remote for Windows, but not the Web Browser?**

A. Alarms can only be acknowledged from the Web Browser if the "ACK INITIALS" have been included in the standard alarm formatting—this option can be selected from the Parameters > Alarm Format menu in T/MonXM.



**Q. How do I transfer a database from an older T/MonXM system to a newer system running a newer version of the software?**

- A. Follow these steps:
1. Exit W/Shell on the older system.
  2. Change the directory to C:\TMONXM.
  3. Copy all the \*.DAT & \*.IDX files to a floppy disk.
  4. Restart W/Shell on the older system.
  5. Insert the floppy disk in the new system.
  6. Exit W/Shell on the new system.
  7. Change the directory to C:\TMONXM
  8. Delete all \*.DAT & \*.IDX files.
  9. Copy all the files on the floppy disk to the hard drive.
  10. Restart W/Shell on the newer system.
  11. Launch T/MonXM.
  12. T/MonXM will automatically update the database.

**Note:** The T/Mon FTP Server can be used rather than the floppy disk, if the files are too large.

**Q. Where does T/MonXM derive the tmonADispDesc that is sent in a SNMP Trap?**

- A. The tmonADispDesc is filled with the contents of the “Display Desc” field on the Point Definition form (Parameters > Remote Ports > Devices > Points or the equivalent from one of the Files menu options).

**Q. Where does T/MonXM derive the tmonAAuxDesc that is sent in a SNMP Trap?**

- A. The tmonAAuxDesc is filled with the contents of the ‘AUX Description’ field for each point on the Point Definition form (Parameters > Remote Ports > Devices > Points or the equivalent from one of the Files menu options).

**Q. How do I get AUX Descriptions to appear for each point on my Point Definition form?**

- A. Change Parameters > Miscellaneous > Edit AUX Desc to “Y.”

**Q. How can a device be halted so it is not polled on a specified port for the duration of that T/MonXM session?**

- A. From the Alarm Summary window press Shift F6. Using the + and - keys, find the port with the devices you want to halt. Using the arrow keys, select the device and press F5 to halt it or F4 to put a halted device back online.

**Q. Why is my T/MonXM not reading correctly from the NetGuardian internal temperature sensor?**

- A. To scale the reading of the NetGuardian internal temperature sensor on the T/MonXM system you need to enter the following scaling factors; Voltage Value 1: 1.0 Unit Value 1: 4.217 Voltage Value 2: 10.0 Unit value 1: 42.170.

**Q. XM Edit - How come I don't have access to some of the configuration screens that I have on my full master? (IE: ASCII, missing alarm windows, remote access use exceeded ...)**

- A. You need to install those various software modules on your XM edit machine. Be sure to set the installation path to the location where XM Edit has been installed. Only install the single disks sets that begin with XM (i.e. XMASC, XMPAG, XMRMT1).

**Q. Why does my XMEdit not show all the database from T/MonXM?**

**A.** Make sure that all of your software modules are loaded into your XMEdit directory.

**This page intentionally left blank.**

# Index

\KDlit M6-24, M6-31, M6-49  
 108 Audible Alarm Card 16-39  
 16 Channel Analog M3-21  
 202 Modem Docking Module M-15  
 212 Modem docking module M3-28  
 21SV Interrogator M18-1  
     Define Controls for the 21SV/RA or 21SV/EXP 32 DO  
     M18-8  
     Point Mapping M18-4  
     Provision the NEC 21SV Device M18-5  
         Monitor Points Provision M18-6  
         Provision Control Points M18-7  
 8 Analog and 4 TBOS Expansion Card M3-25  
 8 Port Teltrac MUX Interrogator M20-1  
 8-port ASCII MUX M21-1-M21-5

## A

ACK Alarms 16-27  
     Key commands 16-27  
 Acknowledging alarms FAQs L-3  
 ADC M3-28  
 Address Statistics (Monitor Mode) M1-16  
 AID (Access IDentifier) M13-3  
 Alarm Formatting 16-15  
     Level and Status Attributes 16-19  
     Level and Status Matrix 16-20  
 Alarm Indicator Control 16-39  
 Alarm Message Forwarding 16-21, M23-1  
     Alarm Forward Parameters 16-22, M23-2  
     Basic Operation and Setup 16-21  
 Alarm Printer Logging 5-11  
 Alarm Summary Colors 16-23  
 Alarm Summary Mode Quick Reference I-1  
 Alarm Windows Modules 6-3  
 AlphaMax M3-28, M3-30  
     Alarm Provisioning M3-37  
     Provisioning M3-35  
     Relay Provisioning M3-39  
 AlphaMax 82A and 82S Sites M3-3  
 AlphaMax 82A Sites M3-28  
 Alphanumeric Pager Formats 8-17  
     define level and status attributes 8-20  
 Alt Path Switch M1-39  
 alternate communication pat 20-1  
 Analog display worksheet M3-22  
 AQL - ASCII Query Language M26-2  
 ASCII M6-1  
     Action Definitions M6-88  
     Alarm Counter M6-84  
     Alarm History M6-82  
     Alarm Qualification M6-83  
     Analyzer M6-65  
         Display Modes M6-65-M6-66  
     Block Copy M6-27  
     Connectivity Test M6-10  
     Detailed Logging M6-35  
     Device Rules screens M6-7  
     Logging M6-66  
     Loop Commands M6-28  
     Message Processing M6-6  
     Parameters M6-36  
     Repeat Loops M6-28  
     Rules M6-6  
         Header Rule (Rule 0) M6-6  
         Numbered Rule M6-6  
     Scripts M6-37  
     Tables M6-34  
     Template Site Definition M6-64  
     Templates M6-63  
     Terms/Glossary M6-3-M6-4  
     While Line Loops M6-30  
     While Loops M6-28  
 ASCII Databasing Map A-33  
 ASCII Debug M6-41  
 ASCII Dial-Up M6-45, M6-50  
     device definition M6-50  
     Incoming Call Device Type Identification M6-47  
         !!!SET\_DEVICE!!! M6-47  
         \KDlit M6-49  
     Remote Ports parameters M6-45  
     Remote Site definition M6-50  
 ASCII Import 18-15  
 ASCII Messages A-2  
     Lines, Columns, Fields and Separators A-7  
 ASCII MUX Interrogators and Responders M21-1  
 ASCII Processing M6-1  
     Basic Concepts M6-5  
     Numbered Rules M6-11  
     Overview M6-44  
 ASCII Processing Language M6-14  
     Directives M6-28  
     Loop Commands M6-25  
     Match commands M6-13  
     Positioning Commands M6-19  
     Quick Reference M6-30  
     Slot Commands M6-19  
 ASCII Processor A-3  
     Message Processing A-3  
         How message processing works A-3  
         How the alarm processor works A-4  
         Recognizing patterns in messages A-5

- ASCII Query Language M26-1
- ASCII Scripts M6-40
- ASCII Sites M3-6, M3-29
- ASCII Syntax Checker M16-13
- ASCII Tables M6-37
- ASCII Tutorial A-1
  - Auto-Databasing A-18-A-27
  - Exercise A-13
  - multi-line input message A-10
  - Tables A-14
  - TL1 Auto-Databasing A-25-A-27
  - Using Separators A-8
  - While Line Loops A-17-A-27
  - While Loops A-16-A-27
- Assigning a Data Connection 3-4
  - Remote Device Definition 3-6
- Auto-Databasing ASCII M6-71
  - \!AUTO Command M6-85
  - Added features in M6-71
  - Alarm Counter M6-84
  - Alarm History M6-82
  - Alarm Level M6-77
  - Alarm Qualification M6-83
  - Alarm Status M6-75
  - Auto-ASCII Site Definition M6-89
  - Categories (Windows) M6-80
  - Input Device Definition M6-80
  - Key Mapping M6-74
  - Pager Profile M6-79
  - Point Definition M6-91
  - Remote Port Definition M6-87
  - Screen Log M6-81
  - Slots and Keys M6-72
  - Text Message M6-78

Automatic Backup 2-17

## B

- Badger Interrogator M4-1
  - Define Alarm Points M4-4
  - Define Analog Points M4-6
    - Analog Display Worksheet M4-7
  - Define Badger Remote Devices M4-2
  - Define Control Relays M4-9
  - Define Internal Alarms M4-8
  - Define the Remote Port M4-1
- BAS M22-1
  - Building Access Unit (BAU) M22-23
    - alarm forwarding variables M22-23
  - BAU Access Parameters M22-25
  - Login M22-30
  - Logoff M22-31
  - Monitor M22-30
  - Personal IDNumber M22-29

- site IDnumber M22-30
- TBOS Controls Sent to the BAU M22-29
- TBOS Display Interpretation M22-27
- DTMF Access M22-16
  - alarm forwarding variables M22-18
  - Login M22-22
  - Logoff M22-22
  - Monitor M22-22
  - personal IDnumber M22-21
  - site ID number M22-21
- for KDA M22-13
- for NetGuardian M22-2
  - BAS User Profiles M22-7
  - ECU mapping M22-9
- BAS Global M22-11
- BAS Profiles M22-7
- Black Box DTMF-ASCII Converter M17-1
- Building Access System M22-1
- Building Status Unit Controls 13-1
  - Assign Controls 13-2
  - Configure Sanity Frequency 13-4
  - local operation 13-2
  - remote operation 13-2
  - Update Frequency 13-3, 13-4

## C

- Card Definition C-12
- Change Of State (COS) Alarms 16-25
- Changing Terminal Drivers 5-9
- Channel Summary 16-48
- Chat Mode 16-53
- Compile MIB Files M12-6
- Controls 12-1
  - Derived Alarms/ Controls 12-10
  - Defining Term Syntax 12-12
  - Rules 12-13
  - Evaluation 12-14
    - for events that don't happen 12-15
    - ignoring silenced alarms 12-10
  - Labeled Controls 12-6
    - Category Definition 12-7
    - Control Point Definition 12-8
  - Site Controls 12-1
    - Control Point Definition 12-4
- Core Prep 16-14
- COS 16-1, 16-25
- COS Mode Quick Reference I-3
- Craft Interface 9-7
  - remote parameters 9-8
- Craft Mode 16-53

## D

- Datalok 10D Sites M3-5, M3-29
- DCM Interrogator M8-1
- DCP(F) 16-32
- DCP(F) Database Transfer M1-11
- DCP(F) Device Definition M1-4
  - Analog Point Definition M1-8
  - Analog Display Worksheet M1-9
  - Control Relays M1-10
  - Defining an Address M1-5
  - Device Failures/Offlines M1-10
  - Point Definition M1-7
- DCP(F) Dial-Up M1-53
- DCP(F) Interrogator M1-1
- DCP(F) Network Status (Monitor Mode) M1-15
- DCP(F) Responder M1-19
  - Remote Device Definition M1-20
  - Responder Definition M1-21
- DCP1 Remotes M1-33
  - Harris DS5000 M1-33
  - Provision the Accumulator Timer M1-36
- Dedicated ASCII M6-54
  - ASCII Input port M6-54
  - Device Definition M6-56
  - Point Definitions M6-58
  - Remote Parameters M6-54
- Define Controller Cards B-1
- Defining TL1 Source Interrogators M13-5
  - SID Definition M13-5
- Deleting report files L-3
- Derived Alarms/Controls 12-10
- Diagnostics E-1
  - 102 Relay Card E-10
  - 108 Relay Card (Aud/Vid) E-7
  - BIOS Info E-21
  - Ethernet E-22
  - File Info E-13
  - Installable Modules E-16
  - Maintenance Reset E-22
  - Printer Test E-12
  - Remote Access Cards E-2
  - T/Link E-21
  - Tune Modems E-4
- Dial-Up MAT (400) M1-51
- Dial-Up Remotes M3-28
- Dialup Site Monitor 16-49
- Disk Files 18-19
  - Database Files 18-19-18-20
  - Program Files 18-19-18-20
- Display Mapping Guide 11-1
  - KDA Remotes 11-4
    - Housekeeping alarms 11-8
    - TBOS Device Failures 11-8
  - Modular Alarm System 11-10
  - NetGuardian 216 11-2
  - NetGuardian 832A/ NetMediator 11-1

- Relays/Housekeeping alarms 11-2
- NetGuardian- Q8 11-3
- NetMediator T2S 11-11
  - JungleMux 11-18
  - MDR-4000E DS-3 11-13
  - MDR-6000 11-14
  - MDR-7000 11-15
  - MDR-8000 DS-1 11-17
  - MDR-8000 DS-3 11-16
  - Multiplex Lynx SC 11-19
  - Relay/Housekeeping Alarm 11-12
- Protection Switch 11-11
- TBOS Protocol 11-9
  - KDA 864 Device Failure Alarms 11-9
- DNS 21-1
- DPM M3-28, M3-30
  - Alarm Provisioning M3-37
  - Provisioning M3-35
  - Relay Provisioning M3-39
- DPM 216 Sites M3-28
- DPM Sites M3-2, M3-28
- DPS Telecom MIB M11-1
- DTMF On-Call M17-1
  - Barge-In Feature (Bypass Automated Menu Prompts) M17-2
  - Operation M17-3
  - Problem Message Numbers M17-4
  - Response Options M17-2

## E

- E2A Interrogators M7-1
- E2A Responders M7-7
- ECU Display Mapping M22-9
- Email Alarm Notification 8-1
  - Email Alarm Notification Port Setup 8-7
    - Mail Incoming POP3 8-9
    - Mail Outgoing SMTP screen 8-8
    - POP3 Data Connection 8-9
    - SMTP Data Connection 8-8
  - Entering Email Addresses 8-12
- English Analyzer Mode/English Filter 16-42
- Ethernet Card D-1
  - Installation on older units D-1
- Ethernet I/O 3-1
- Exit Monitor Mode (Log Off/On) 16-65

## F

- FAQs L-1
- File Maintenance Menu
  - Utilities 18-1
- File Utilities Menu 18-1
  - Back Up Data Files 18-1

- Compress History 18-5
- Compress Points 18-6
- Delete Live Files 18-11
- Delete System Log 18-10
- Disk Information 18-6
- History File Purge 18-4
- Rebuild Key Files 18-8
- Report Maintenance 18-7
- Restore Data Files 18-3
- Format Floppy Disk 2-15
- Frequently Asked Questions L-1
- FSK Converter M5-1
- FTP Server M15-1
- FX 8800 Alarm Output Mapping M10-5
- FX 8800 Interrogator M10-1

## G

- Groups 8-25
- GET Commands M12-19

## H

- Hard Copy 19-40
- Hard Drive Recovery Program M25-2
  - Abnormal Hard Drive Recovery M25-3
  - Hard Drive Recovery Status Messages M25-3
- Harris DS5000 M1-33
- HDLC Stats 16-62
- HTTP 17-1, 17-4
- HTTPS 17-1, 17-4, 17-5, 17-6

## I

- IAM-5
  - Front Panel Operation M-7
  - Fuse Alarm M-8
  - Installation M-2
  - Intelligent Controller Card Pinouts M-11
  - Modem M-10
  - Mounting M-2
  - Power and connector locations M-4
  - Printer Port M-9
  - Remote Terminal Cable Connections M-11
  - Serial Ports M-9
  - Slide Rack M-5
  - Specifications M-1
  - UPS Cable Connections M-10
- ICMP 3-3
- Import Alarm Definitions 18-12
- Import MIB Files M12-6
- Initialization 16-13
- Integrated SNMP Agent M11-1

## M-4 Index

- Performance/Stats M11-4
- Read Community M11-2
- Trap Community M11-2
- Write Community M11-2
- Internal Alarms 14-1
  - Address 0 Display 1 Alarms 14-6
  - Address 0 Display 2 Alarms 14-10
  - Address 13 Display 1 Alarms 14-11
  - Internal Alarms Assignments 14-11
  - marked with an asterisk 14-6
  - Offline and Device Failure alarms 14-6
  - Point Definition Screen 14-3
  - Standard Alarms 14-4
  - User Defined 14-13
    - How To Create User Defined Internal Alarms 14-14
- ISA Card Definition B-1

## K

- KDA 832-T8 Sites M3-5
- KDA 864 and KDA 832-T8 Sites M3-4
- KDA 864, KDA-TS, KDA 832-T8 Sites M3-28
- KDA Shelves M3-7
  - address definition M3-10
  - Advanced KDA Provisioning M3-19
  - Alarm point provisioning M3-13
  - Alarm Qualification Units M3-14
  - Control Periods M3-15
  - DCP, DCPX or DCPF M3-16
  - DSAT M3-17
  - provisioning target menu M3-11-M3-12
  - Responder Provisioning M3-15
  - UDP M3-18
- KDA-TS Sites M3-5
- Key Command Quick Reference Tables I-1

## L

- Labeled Controls 12-6
- Labeled Controls Mode 16-55
  - Issuing Labeled Controls 16-56
  - Point Selection 16-57
    - Batch Point Operation 16-59
    - Individual Point Operation 16-57
- Labeled Controls Point Selection 16-57
- LAN-Based Remotes M1-22
  - NetGuardian M1-22
- Larse Interrogator M5-1
  - Define Alarm Points M5-10
  - Define Control Relays M5-11
  - Define Internal Alarms M5-10
  - Define Larse/Badger Remote Devices M5-2
  - Define T/MonXM Analog Alarm Thresholds M5-7
  - Analog Display Worksheet M5-8

- Note on Analog Alarms M5-9
- Define the Remote Port M5-1
- Provision the Larse/Badger Remote Unit M5-4
- LED Alarm Color Definition K-4
- LED Alarm Format K-5
- LED Display Bar K-1
- LR-24 Relay Card M3-24

## M

- MAS Sites M3-6, M3-29
- master T/Mon 20-1
- MIB (Management Information Database) M12-6
- MIB file M11-1
- Miscellaneous Parameters 15-1
  - Alarm Analog History Period 15-3
  - Alm Pan Time-out 15-3
  - Aud Rly Polarity 15-2
  - Aud Rly Release 15-2
  - Auto Scroll Alarms 15-2
  - DB Backup Alarm 15-3
  - Debug Port 15-3
  - Default Level 15-1
  - Disable Audio 15-3
  - Edit Aux Desc 15-3
  - Fast menus 15-3
  - Full Display 15-2
  - Hist Auto Purge 15-2
  - History Path 15-2
  - Live Path 15-2
  - Max COS Entries 15-3
  - Normal Analog History Period 15-3
  - Pulse Aud Relays 15-3
  - Screen Saver 15-2
  - System Name 15-3
  - Undef Polarity 15-2
  - Undef Reverse 15-2
  - Use Alarm Qual 15-1
  - Use Display Desc 15-1
- Modbus Interrogator M19-1
  - Modbus Addressing M19-7
    - data model M19-7
    - Modbus Addressing Model M19-9
- Modem Initialization Strings J-1
- Modular Alarm System (MAS) M3-29
- Modular Alarm Transmitter - MAT (400) M1-51
- Modular Alarm Transmitter (MAT) M3-28
- Monitor Mode 16-1
  - Alarm Summary Screen 16-3
    - Key commands 16-8
  - COS Alarm screen 16-2, 16-25
  - Monitor Alarm Point Descriptions 16-11
  - Monitor Mode Operation Notes 16-12
    - Automatic Alarm Acknowledging 16-12

- Automatic History Purging 16-12
- Standing Alarm Virtual Mode 16-12
- Page Index 16-2
  - Page Index Window 16-6
- Summary Legend window 16-8
- MyODBC M24-1
- MySQL M24-1

## N

- Net Dog M3-30
- NetGuardian FAQs L-4
- NetMediator 4-Port TBOS/TABS (expansion module) M1-32
- Network Setup 3-1
- Network Setup Utility D-7
- Network Time (NTP) 9-9
  - performance statistics 9-10
- No Data Connection prompt 3-5
- nuisance alarm 16-30

## O

- OID M12-9-M12-11
- Option Cards M-12
  - 102 Local Relay Card M-18
  - 108 Audible Alarm Card M-17
  - Audible and Visual Alarm Card M-19
  - Intelligent Controller Card M-13
    - 603 Card Jumpers M-16
      - Address and Interrupt Settings M-14
      - Docking Module Jumpers M-15
      - Overhead Jumper M-16

## P

- Pager 8-1
  - Operators 8-4
  - Pager Alarm Notification Port Setup 8-5
    - Multi Alpha Pages 8-6
    - Pager Speaker 8-5
  - Pager Carrier 8-4
  - Pager Profiles 8-3
  - Pager Scheduling 8-3, 8-4
  - Parameters 8-3
  - System Security 8-3
- Pager and email function flow diagram 8-4
- Pager Carriers 8-10
  - Pager Carrier Response Options 8-13
- Pager Profiles 8-21
  - Alpha pager settings 8-22
  - Entering Pager Profiles 8-24
  - Numeric pager settings 8-22
- Pager Status in Monitor Mode 16-60



- Flush Pager Queue 16-61
- Lock Function 16-60
- Sending Pager Messages 16-61
- Paging Problems L-1
- Performance/ Statistics Mode 16-31
- Ping Interrogator 9-4
  - Device Definition 9-5
  - TCP Port Definition 9-4
- Point Definition shortcuts 10-1
  - Cloning Entire Displays or Sites 10-21
  - Cloning Part of a Display 10-22
  - Column (Attribute) Entry 10-13
  - Description Modification 10-14
  - DeviceTemplates 10-24
  - Editing Shortcuts 10-9
  - Point (Line) Copying 10-11
  - Point (Line) Editing 10-11
  - Point Editing 10-2
  - Windows Modification 10-19
- Port Interface Cartridges (PICs) 1-11
- Preventive Maintenance 18-12
- Profiles 7-2
- Protection Switch M1-49
- Protocol Analyzer 16-46
- Pulsecom Datalok M16-1
  - Alarm Point Mapping M16-22
  - Analog Image Alarm Mapping M16-26
  - Configuration Tables M16-22
  - Control Mapping M16-25
  - Housekeeping Mapping M16-24
  - Operational Summary M16-1

## R

- Redundant Dual T/Mon Backup 20-1
- Re-installing T/MonXM 2-5
- Remote Access 5-1
  - Cursor Movement Keys 5-11
  - Log On/Off 5-8
  - Remote Access Audible Options 5-3
  - Remote Access Server 5-4
  - Selecting Function Keys on Remotes 5-10
- Remote Ports 9-1-9-2
  - Defaults 9-3
  - port numbers and functions (IAM-5) 9-2
  - port numbers and functions (T/Mon NOC) 9-2
  - usages 9-3
- Remote Terminal Control Keys 5-9
  - Refreshing the Terminal Display 5-9
- Remote Users over LAN 5-12
- Remotes M3-1
  - AlphaMax M3-1
  - DPM M3-1
  - KDA M3-1

- 16 Channel Analog M3-21
- 4-TBOS card M3-25
- 8-analog card M3-25
- Analog provisioning M3-22
- Downloading the Provisioning File M3-27
- KDA shelf definition M3-7
- LR-24 Relay Card M3-24
- Modular Alarm System M3-1
- Net Dog M3-1
- Report Mode 16-44
- Reports 19-1
  - Alarm Database Report 19-17
  - Dial-Up History Report 19-15
  - Export History 19-9
  - History Report 19-5
  - Labeled Controls Report 19-30
  - LED Bars Report 19-31
  - Pager 19-33
  - Reports available in the Report Mode menu 19-3
  - Reports in Monitor Mode vs. Reports under the Master Menu 19-1
  - Running Reports from T/RemoteW 19-5
  - Site Controls Report 19-31
  - Users Report 19-32
  - View Report File 19-37
- Ring Polling M1-37

## S

- Schedule Exceptions 8-16
  - copy another exception schedule 8-16
- Screen Log M6-81
- secondary T/Mon 20-1
- Security Help 7-4
- security permissions options 7-2
- SET Commands M12-19
- SID (Source IDentifier) M13-2, M13-5
- Silence Alarms/Windows 16-30
- Site Controls 12-1, 16-34
  - Point Selection 16-36
    - Batch Point Operation 16-38
    - Individual Point Operation 16-36
- Site Controls Point Selection 16-36
- Site Log In Status M22-12
- Site Report M22-31
- Site Statistics 16-62
- Silence Alarms 17-9
- SNMP M11-1
- SNMP Agents M12-7
- SNMP Databasing Map M12-16
- SNMP Manager Display M11-5
- SNMP Responder (File Maintenance Menu) M11-2
- SNMP Trap Processor M12-1
  - Associate SNMP Traps with Alarm Points M12-9

- SNMP Traps Defined M12-9
- Verify Ethernet Port Assignment M12-2
- SNMP traps FAQs L-4
- SNPP 8-8
- Standard Dial-Up Remotes M3-28
- Standard Internal Alarms 14-3
  - display 1 14-4
  - display 2 14-5
- Standing Alarms 16-28
- Standing Alarms Quick Reference I-5
- System Information 16-51
- System query window 16-65
- System Time 2-15
- System Users 7-1
  - Define System Users 7-2
  - Password 7-1
- System Users FAQs L-2

## T

- T/AccessMW 5-1
- T/Install 2-9
- T/KDAW M3-27
- T/Link 2-13
- T/Mon DTMF Voice Interface M17-1
- T/Mon Hard Drive Mirroring M25-1
- T/Mon NOC 1-1
  - Back Panel Connections 1-5
    - 110 VAC Models 1-6
    - Dual –48 VDC Models 1-5
  - Hardware Installation Guide 1-1
  - LCD Display 1-14
  - Network Connections 1-8
    - Internal Modem Connection 1-8
    - LAN Connection 1-8
  - Power Connections 1-5
  - Rack Mounting 1-4
  - Security Key 1-7
    - Error message 1-7
  - Serial Ports 1-9
    - Serial Port Pinouts 1-10
      - IAM-Compatible Port Pinouts 1-10
      - T/MonXM WorkStation-Compatible Port Pinouts 1-11
  - Slide Rack Mounting 1-2
  - Specifications 1-1
- T/Mon SQL M24-1
  - Data Dictionary M24-5
  - Internal Alarms M24-10
  - Performance/Stats in Monitor Mode M24-10
  - TCP Socket Connection M24-4, M24-5
- T/Mon SQL Agent M24-1
  - Changing Instances M24-3
  - Creating New Configuration Files M24-4
  - Debug port M24-4
  - Debug Reset Counter M24-4
  - Hide the Application Window M24-4
  - Instance configuration settings M24-2
  - Reset Counter M24-3
  - Restarting M24-3
  - Settings for the T/Mon SQL Agent M24-7
- T/MonXM 4-1, F-1, M-1
  - Disk Files F-1
    - Database Files F-1
    - Program Files F-1
  - Hot Key Edit Commands 4-4
  - Interface 4-1
    - Fast Menus feature 4-1
    - Field Editing 4-5
    - Function Keys 4-2
    - List Box 4-3
    - Menus 4-1
  - Software Specifications M-1
- T/MonXM WorkStation M-21
  - 33.K Baud Dial Modem M-26
  - Installation M-22
  - Intelligent Controller Card Pinouts M-27
  - Remote Terminal Cable Connections M-27
  - Serial Ports M-25
  - Specifications M-21
  - UPS Cable Connections M-26
  - Video Monitor M-25
- T/RemoteW 5-1, 16-1, 16-45
- T/Windows 5-1, 16-1, 16-45
- TABS Responder M14-1
  - Mapping Devices to the TABS Display M14-3
  - Protocol Mediation M14-1
- TAG Alarms 16-30
- TAP Interrogator M27-1
- TBOS Interrogator M9-1
- TBOS Responder M9-6
- TCP Ports 3-3
- TELNET 3-3
- TELNET-Raw 3-3
- Text/Message Definition N-1
  - Defining a Message N-1
- Text/Messages Window 16-29
- Time Service 9-11
- Time-Stamp KDA M3-28
- TL1 M13-1
  - Alarm Definition Commands M13-9
  - Command Definitions M13-27
  - Command Overview M13-24
  - Commands, Messages and Codes M13-20
  - Configuration Tables M13-22
  - User Input Command Errors M13-19
- TL1 Glossary M13-23
- TL1 Interrogators M13-1
  - Defining TL1 Alarm Points M13-7

- Defining TL1 Control Points M13-13
- Remote Device Definition M13-5
- Setup Procedure M13-4
- SID Definition M13-5
- TL1 Responders M13-15
  - Defining TL1 Responders M13-15
  - Remote Device Definition M13-17
  - Remote Parameters M13-16
  - Responder Definition M13-18
- TMonNET 20-2, M1-11
  - TMonNET Address 20-5, M1-12
  - TMonNET Network Port 20-3
  - TMonNET Node Definition 20-6
  - TMonNET Nodes M1-13
  - TMonNET Other Parameters 20-10
  - TMonNET Port M1-11
  - TMonNET Transfer 20-9
- TMonNET Alt. Path 20-11
  - Databasing 20-11
  - English Messages 20-13
  - Housekeeping Alarms 20-14
  - Testing the Alternate Communication Path 20-15
- TMonNRI 20-16
- Transaction Language 1 (TL1) M13-1
  - Tutorial M13-1
- Transfer MIB files M15-1
- Transferring databases between T/MonXM systems L-4
- Trap Association M12-14-M12-15
  - Translate screen M12-14-M12-15
- TRIP 16-32, M2-1
- TRIP Dial-Up M2-1
- Trouble Log 19-42
  - Compile Reports 19-45
- Troubleshooting H-1
  - Security error codes H-2
  - Software error codes H-1, H-2

## U

- UDP 3-3
- Uninterruptible Power System G-1
- Upgrading T/MonXM 2-2
  - CD 2-2
  - Floppy Disks 2-6
  - T/Install 2-9
- UPS G-1
- User Profile 7-2

## V

- View Analogs 16-64, M1-18
- virtual ports 9-1-9-2

## W

- W/Shell 2-1
- Warranty iii
- Web Browser Interface 17-1
  - Compatibility 17-1
  - Connecting via Web Browser 17-6
  - Preferences 17-10
    - Alarm Summary page control 17-10
    - Alarm Summary refresh frequency 17-10
    - page index refresh frequency 17-10
  - Using the Web Browser Interface 17-7
- Weekly Operator Schedules 8-14
  - Weekly Schedule 8-14
- Window Definition 6-3
- Windows 6-1
  - All Alarms window 6-3
  - Recommended window assignment 6-1
  - Severity windows 6-2
  - Type/Equipment windows 6-2
  - Using windows to sort reports 6-1
  - Window Definition screen 6-3
- Workstation Info Menu 2-16

## X

- X.25 Card C-1
  - Hardware Connections C-1
  - Software Configuration C-2
  - X.25 TL1 Responder C-2
  - X25 Provisioning C-14
- X.25 Card Software Module C-1
- X.25 I/O Port Usage C-6
- XMEdit FAQs L-2

# End User License Agreement

All Software and firmware used in, for, or in connection with the Product, parts, subsystems, or derivatives thereof, in whatever form, including, without limitation, source code, object code and microcode, including any computer programs and any documentation relating to or describing such Software is furnished to the End User only under a non-exclusive perpetual license solely for End User's use with the Product.

The Software may not be copied or modified, in whole or in part, for any purpose whatsoever. The Software may not be reverse engineered, compiled, or disassembled. No title to or ownership of the Software or any of its parts is transferred to the End User. Title to all patents, copyrights, trade secrets, and any other applicable rights shall remain with the DPS Telecom.

DPS Telecom's warranty and limitation on its liability for the Software is as described in the warranty information provided to End User in the Product Manual.

End User shall indemnify DPS Telecom and hold it harmless for and against any and all claims, damages, losses, costs, expenses, obligations, liabilities, fees and costs and all amounts paid in settlement of any claim, action or suit which may be asserted against DPS Telecom which arise out of or are related to the non-fulfillment of any covenant or obligation of End User in connection with this Agreement.

This Agreement shall be construed and enforced in accordance with the laws of the State of California, without regard to choice of law principles and excluding the provisions of the UN Convention on Contracts for the International Sale of Goods. Any dispute arising out of the Agreement shall be commenced and maintained only in Fresno County, California. In the event suit is brought or an attorney is retained by any party to this Agreement to seek interpretation or construction of any term or provision of this Agreement, to enforce the terms of this Agreement, to collect any money due, or to obtain any money damages or equitable relief for breach, the prevailing party shall be entitled to recover, in addition to any other available remedy, reimbursement for reasonable attorneys' fees, court costs, costs of investigation, and other related expenses.