Hewlett-Packard A5799A Terminal Server Reference

Edition 1

HyperPlex
Datacenter Solutions

Manufacturing Part Number: A5547-90003
E0499

United States

Legal Notices

The information in this document is subject to change without notice.

Hewlett-Packard makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty. A copy of the specific warranty terms applicable to your Hewlett-Packard product and replacement parts can be obtained from your local Sales and Service Office.

Restricted Rights Legend. Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c) (1) and (c) (2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

HEWLETT-PACKARD COMPANY
3000 Hanover Street
Palo Alto, California 94304 U.S.A.

Use of this manual and flexible disk(s) or tape cartridge(s) supplied for this pack is restricted to this product only. Additional copies of the programs may be made for security and back-up purposes only. Resale of the programs in their present form or with alterations, is expressly prohibited.

Trademark Notices. NT and Microsoft are U.S. registered trademarks of Microsoft Corporation. X Window System is a trademark of the Massachusetts Institute of Technology.

Table of Contents

GLOSSARY OF COMMAND REFERENCES 149

PREFACE

Overview

The Hewlett-Packard Terminal Server is a muliplexer device that enables console access to multiple datacenter servers through a single web browser interface. It is one of the components of the Central Web Console (CWC) Kit. The Central Web Console is a systems management tool for the HP 9000 family of Enterprise Servers. The Terminal server allows Telnet communication to 28-host console ports through RS-232 connections. The Terminal server connects to a Windows NT Server through an Ethernet link.

The *Hewlett-Packard Terminal Server Reference* describes the features of the and provides a reference of user commands for system administrators. The terminal server is pre-configured for use with the Central Web Console. This manual introduces many of its features and functions; use of this component beyond the scope of this manual and the *HP Central Web Console Administrator's Guide* is not recommended.

This manual should be used in conjunction with the *HP Central Web Console Administrator Guide* and the *HP Central Web Console Installation Guide*.

A glossary of common terms can be found in the *HP Central Web Console Administrator's Guide*.

Audience

The HP Terminal Server Reference is designed as an aid during setup, troubleshooting, and terminal server maintenance for site system

administrators.

Conventions

You will find the following terms and notation used throughout this manual.

Terms

Authentication method – A security function that verifies the user, attempting to access the terminal server, is authorized. The terminal server uses a Password/Callback authentication method. An internal database stores information about each authorized user. See Chapter 2 for further information about adding, deleting, or modifying user information.

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

System prompt – The system prompt includes the site name followed by the “greater than” symbol (>). Terminal server commands are typed at this prompt.

SYSOP session – Identifies a communication session between a terminal server and the CWC server through either a Telnet, dial-up, or an AUX port connection.

Direct connection – Identifies a communication session between a terminal server and a Telnet capable device, a dial-up connection, or an AUX port connection.

Notation Used in this Manual

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

In This Book

This book consists of the following chapters:

Introduction

Chapter 1, **Overview of Features -** An overview of the terminal server features and operation.

Chapter 2, **The User Database -** Explains how to add, delete and change information in the user database.

Chapter 3. **System Parameters -** Includes instructions on how to set up the network parameters, such as the IP and Ethernet addresses.

Chapter 4, **File Buffering -** Describes how the terminal server stores data from host ports and how to manage and retrieve data buffers and files.

Chapter 5, **Modem Port Setup -** Explains how to configure a terminal server modem port. All parameters to set up modem ports are described.

Chapter 6, **Troubleshooting -** Explains how to reset all unit parameters to factory defaults and manually configure the system using a saved configuration file.

Chapter 7, **Action and Event Tables -** Explains how the terminal server manages alarms. This chapter also explains how to create, modify, and test Action Tables.

Chapter 8, **Action and Event Routines -** Describes each internal event and standard action routine. Examples are also included.

1. OVERVIEW OF FEATURES

What This Chapter Contains

This chapter provides an overview of the features and functions of the terminal server.

- Hardware Configuration
- Software Configuration
- How to Display Menus and Issue Commands
- Editing Modes
- Functionality Overview

Hardware Configuration

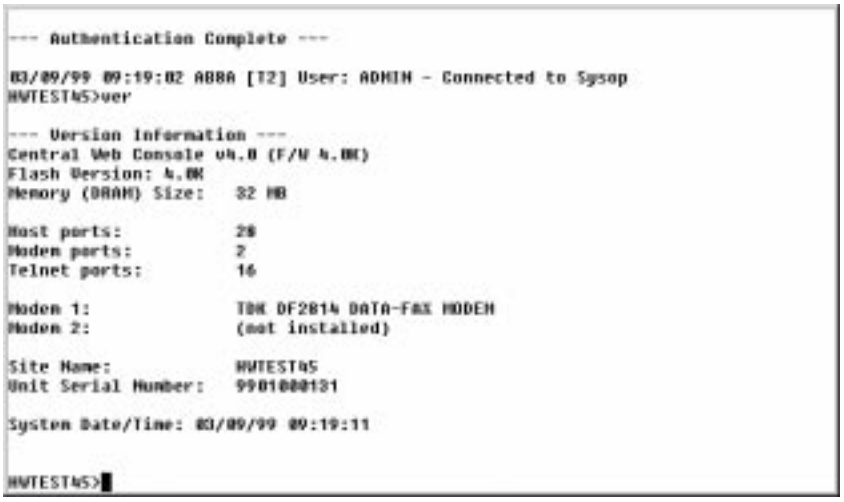
The terminal server is pre-configured for use with the Central Web Console. Many of the features and functions included with the terminal server are not supported for use with this environment. Use of the terminal server beyond the scope of this manual and the *HP Central Web Console Administrator Guide* is not recommended.

The hardware configuration consists of the following:

- Two expansion boards providing 28 host-console ports.
- Two Auxiliary (AUX) ports for initialization and direct communication with the terminal server.
- One PCMCIA modem.
- 48V-battery sensor (not used in this environment).
- 50-pin connector reserved for future use.

Software Configuration – VER Command

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



Displaying Menus and Issuing Commands

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

To go from one menu to another, enter the command letter assigned to that group at the system prompt. The menu mnemonics, names, and descriptions are listed below:

Command	Menu	Description
U	**User Maintenance Functions**	Displays list of commands to modify the user database.
S	**System Functions**	Displays list of commands to specify site and scheduling

Command	Menu	Description
		information.
A	**Action and Alarm Functions**	Displays list of commands to view and modify the Action Table.
L	**Log Functions**	Displays list of commands to view and modify logs.
F	**File Maintenance**	Displays list of commands to configure file buffering and management.
P	**Port and Session Control Functions**	Displays list of commands to view port status, port signals, host sessions, and to display and modify network parameters.
X	**User Commands**	Displays list of custom commands added as part of the device configuration. If X returns one of the menus listed above, the terminal server does not contain custom commands.

NOTE: All commands may be entered at the system prompt. The menu does not have to be displayed first. The access class of each user determines the commands displayed.

Entering/Selecting Parameters

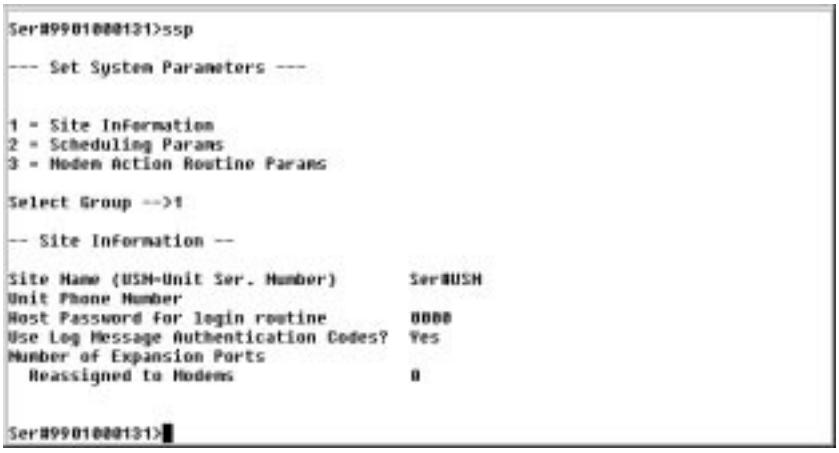
Parameters are entered or changed by either typing them in or by selecting them from a list of options. The method depends on the command.

For example, at the system prompt type **DH** (**D**isplay **H**ost) and press ENTER. The unit will respond with a message of '--- Display Host Port Params ---' and then a list of host ports to select. Type in the number of the Host port whose parameters you wish to view, press ENTER. The user may view these parameters in one step by typing **DH x** (where x is the Host Port number) and pressing return. The parameters for the selected Host Port will be displayed.

In some cases, the terminal server system provides you with several options. If the option displayed is not appropriate, scroll through the list by pressing the space bar. When the selection you want appears in the field, press the Enter key to select that item.

In the **S**et **D**ate and **T**ime (**SDT**) command, there are 10 different date codes available. Type **SDT** at the system prompt and the current date format will be displayed. Press the space bar and another format will be displayed, there are ten date format options. Once the desired format is displayed, press ENTER to accept the format. The display is now today's date shown in the format just entered. Press the ENTER again to display the current time. Pressing ENTER again returns the system prompt (>).

Some commands require that certain parameters be specified. For example, when you type **SSP** the Set System Parameters screen is displayed. The example below shows the parameters for Site Information (Option 1).



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

LA .H (or la .h)

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

Editing Modes

The terminal server supports editing in TTY and VT-100 modes. VT-100 mode displays all required information and then allows you to move up, down and across the screen to edit lines. In TTY mode, the lines are displayed one line at a time and must be edited left to right. TTY mode is the default mode for all access ports on the terminal server.

Use the SYSOP command **VT ON** to select VT-100 as the terminal mode during the current SYSOP sessions, regardless of the connection (AUX, Telnet or Modem). Typing **VT OFF** during the current SYSOP will turn the session back to TTY.

The user may change the default port editing setting (TTY) for access ports on the terminal server. To change the parameters for the AUX port, Telnet port(s), or Modem port(s), issue the **SA, ST,** or **SM** commands for each port respectively, and change the "Terminal Emulation" parameter by toggling from TTY to VT-100.

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

TTY Mode

Information is displayed one line at a time for editing. After the Enter key is pressed the next line is displayed for editing. In this mode it is impossible to return to "entered" lines to modify them.

VT-100 Mode

If you have a VT-100 terminal (or your computer is emulating a VT-100 terminal) you can execute SYSOP commands in VT-100 mode. In this mode all of the prompts will be displayed on the screen at once along with the data to be edited. The cursor will initially appear at the beginning of the first field.

At this point the arrow keys can be used to move from line to line performing edits in any order. Pressing the Enter key with the cursor on the last line of the display completes the function.

Using the Editing Keys

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

If your terminal emulation program has an option to set Destructive Backspace or Non-Destructive Backspace, choose the latter.

The following editing keys can be used whenever a field is presented for modification.

Editing Function	Keys
Move cursor to the right	[CTRL] R
Move Cursor to the Left	[CTRL] L
Delete the character at the cursor	[CTRL] D
Toggle overstrike on or off (default is off)	[CTRL] O
Delete text to the End of Line (EOL)	[CTRL] X
Move the cursor to the beginning of the line	[CTRL] B
Move the cursor to the end of the line	[CTRL] E
Backspace and delete	[←] (Backspace key)
Restart field (clears all new data and returns previous data)	[CTRL] Z
Abort (ends edit and does not change any pre-existing data)	[CTRL] A
Complete a line and go to next line	[↵] (Enter key)
Toggle choices (an example of a toggle choice is Yes or No)	Space bar

Functionality Overview

The terminal server provides several basic functions: security, site connectivity, alarm processing, and data buffering.

Function	Description
Security	The terminal server, as a front end, provides secured access to host devices. , All users connecting to the terminal server through the network, modem, or the AUX Port need to authenticate before being passed through to a host device or permitted to administer the terminal server. The terminal server also provides a logical switching function that allows an authorized user to connect to any host device listed in the user's profile.
Site Connectivity	The terminal server acts as a central point for connection to all hosts and other serial devices at a site. It enables connections through a local terminal, dial-up modem, and Ethernet. A dial-up modem also provides a PPP connection, allowing remote access to networked devices.
Alarm Processing	When attached to a maintenance port, the terminal server can process alarm messages and other ASCII based data streams. Alarm messages can be delivered via a modem or network connection. Using either PPP or network connectivity, the terminal server can deliver SNMP traps to network managers. The terminal server can convert ASCII-based alarms received on its host ports to standard SNMP traps. Acting as a SNMP trap proxy agent, the terminal server allows legacy equipment to be managed and provides alarm-reporting functions.
Data Buffering	The terminal server can buffer all data transmitted to a host port by the attached

Function	Description
	device. Data is collected on a RAMdisk as either buffered data or files. Error messages, buffered console output, traffic data and other information can be subsequently delivered to a central location through a dial-up or network connection.

Security Management

The terminal server maintains a database of authorized users. Only users listed in the database who successfully authenticate are allowed access. Supported authentication methods include the following password-oriented methods: Password, Callback and Variable Callback. The terminal server is configured for use with the following token methods, but the current version of the Central Web Console does not support their use: PassKey, and Pager.

The terminal server supports five access classes. Only a system administrator, logged into a SYSOP session as Master, can modify user profiles or the user database. The access class determines which ports can be addressed and what information can be viewed or modified within the terminal server.

Network Capabilities

The terminal server has both an Ethernet and a PPP TCP/IP network connection. Network connections support Telnet—to the terminal server and to attached hosts, FTP—for buffer and file delivery, and SNMP—for TRAP delivery to network management stations. In addition, the terminal server routes traffic between its network interfaces, allowing it to act as a secure, remote-access server for maintenance applications.

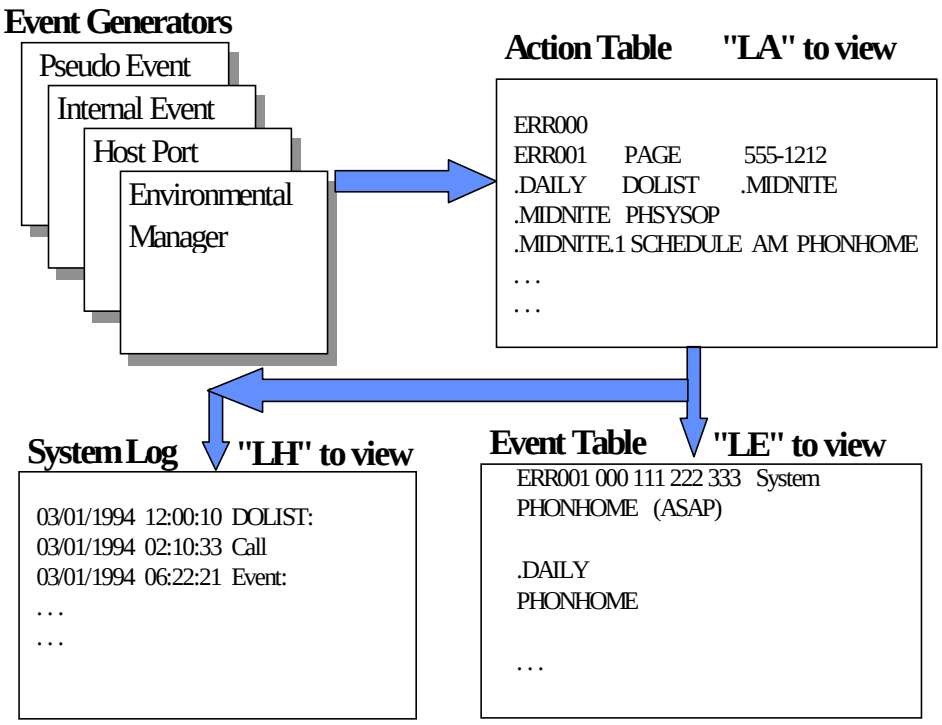
Alarm Management

Alarms and events originate from a number of sources: data received on a serial port, Timer events, as well as other activities internal to the terminal server.

When the terminal server processes an alarm or event, it checks the Action Table to determine if it is listed. If the alarm matches one listed in the Action Table, the event is placed in the Event Table for processing and listed in the System Log for reference. To process the event, the terminal server performs the associated Action Routine, which performs a task associated with the alarm.

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

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



Logs

The terminal server maintains logs containing details of alarms, accesses, host port activity, and system information. These logs are useful for site management, security management, and troubleshooting. The terminal server maintains all logs even without system power. A description of each log type follows:

Access History - The terminal server records each successful access. The time, date, user ID, duration of session and type of session are included in each record.

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

Log History - This log records the activity of the terminal server and the devices to which it is connected. Activities include modem connections, received calls, SYSOP sessions, and detected alarms and events.

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

Data Buffering

Each host port of the terminal server receives data from the resource to which it is connected. This data may be *buffered*, or collected in a file, which is temporarily stored on the terminal server RAMdisk. The RAMdisk reserves up to 1MB per port. The file may be sent to the administration PC for later review or importation into another software package.

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

2. THE USER DATABASE

What This Chapter Contains

The system administrator must create the user database once the terminal server is installed and all required ports initialized. The Central Web Console application requires a minimum of three user-access records: a Master user, a buffer manager, and a joint session manager. This chapter explains how to create and manage the user database.

The terminal server maintains a database of authorized users . Each user who accesses the terminal server or a host(s) through a secured web connection, a dial-up port or network connection must have a user record in the database. By limiting access through each of the ports, the terminal server provides access security to both the terminal server and protected host devices.

The user database resides on the RAMdisk and contains detailed information about each user: such as user name, access class, and authentication method. The user database can hold information for 90-plus users.

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

Overview

This chapter covers functions related to adding, modifying and deleting users from the database.

The database will be destroyed if the terminal server encounters a failure. Save the latest version of the database to an FTP directory; this helps you recreate a current database in the case of a failure.

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

User Name (ID)

Access Class

Whether user access is blocked

User Access Expiration Date

Number of sessions allowed

Primary and Secondary Authentication Methods

Auto Execute Command

Comments

Access Classes

Each user is assigned an access class that determines his/her access and administrative privileges. Users assigned the access class “Host” can only access host ports and have no administrative privileges on the terminal server. Sysop and Master users can administer the terminal server in addition to accessing the host ports.

NOTE: Only a user with Master access privileges can add, delete or modify user profiles in the database.

Master – Master access permits the user to change all information in the terminal server. The Master user controls when and how alarms are reported, add and delete users from the user database, change user

profiles, modify Action and Event tables, manage data buffering and access all hosts. The Master class is the highest level of access.

Sysop 3 – A Sysop 3 user can perform all functions listed above with the exception of modifying the user database. A Sysop 3 user can access all host ports and has access to the file commands used to manage data buffering, can make changes in how the terminal server responds to alarms, and change the port configuration of the unit.

Sysop 2 – A Sysop 2 user can view all alarm and event information, and manipulate pending alarms. The Sysop 2 user cannot change the way the terminal server responds to alarms. The Sysop 2 user can access all host ports.

Sysop 1 – A Sysop 1 user can view pending alarms, but cannot create or save changes. Data buffering commands are not available to the Sysop 1 user. The Sysop 1 user can access all host ports.

Host 1 to Host n – The host user only has access to a single host device. The host user cannot access any of the terminal server functions.

Displaying the User Maintenance Functions Menu

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

To display the User Maintenance Functions Menu, type **U** at the system prompt and press Enter. All commands associated with maintaining the user database are shown on this menu.

```
System Date/Time: 02/12/99 13:42:52


Ser#9901000131>u

- - - USER MAINTENANCE FUNCTIONS ( Master ) - - -

--- User Maintenance Functions ---

    LU    List Users                    DU    Display User Record
    AU    Add User                      CU    Change User
    XU    Delete User
Other Menus: S -System  A -Alarm  L -Log  F -File  P -Port  X -Extra

Ser#9901000131>
```

Command Summary

This database contains the records for authorized users of the terminal server system.

The following table lists commands to administer the user database. The table includes a brief description of each command and lists the access level that a user must have to successfully issue the command.

Function	Description	Access Class Required
AU – Add User	Adds a user profile to the database.	Master
CU – Change User	Changes the information associated with a user who has already been entered into the system using the Add User command.	Master
DU – Display User Record	Displays entire record for the user selected.	Sysop 2, Sysop 3, Master
LU – List Users	Displays list of all users in the database.	Sysop 2, Sysop 3, Master

Function	Description	Access Class Required
XU – Delete User	Deletes a user and removes all records associated with that user from the terminal server database.	Master

Adding a User – AU Command

The AU command allows you to add a user to the terminal server system. To access the system, a password is required. The first user entered into the database should have an access level of master. A master level user can access all the features of the terminal server and can add and delete users from the user database.

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

For example:

AU Carol

or **AU**

then **Carol** at the User Name prompt

Field	Function
User Name	Enter a user name. User names may be up to 15 alphanumeric characters in length, including spaces. ***NOTE: The terminal server converts alphabetical characters to upper case.***
Access Class	To select the Access Class, press the **space bar** until the desired choice is displayed. ***NOTE: The first user entered should be a master level user. A master user should be maintained in all systems at all times.***
Block Access	Initially No (the default) appears on the screen. Press the space bar to toggle to Yes. No enables access to the terminal server. Yes blocks access to the terminal server.
Sessions Allowed	Press the Enter key to allow unlimited sessions. Enter a number from 1 to 999 and press Enter to limit the number of successful sessions allowed for that user.
User Expiration Date	Enter the date in month/day/year to set the end of the user's access period. No date signifies the user has an unlimited access period.
Primary Authentication Method	Press the space bar until Password/Callback displayed. ***NOTE: The Pager and PassKey options are not supported with this version of the Central Web Console.***

Field	Function
Secondary Authentication Method	(Optional) Select a second means of authentication for a user. Press the space bar until the desired choice is displayed.
Auto Execute Command	(Optional) Enter a command that's executed automatically after user authentication. For example, if you enter LH - the log history will be displayed in reverse order after the user authenticates. This option is available only to users who sign on as a Sysop 1 level or higher.
Comments	Enter up to 40 alphanumeric characters on the *Comments* line. After you have entered comments in the Comments field, press Enter.

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

Password/Callback Authentication Method

If Password/Callback was selected as the primary authentication method, the terminal server will display the following information.

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

Field	Function
Enter a password	The password may be up to 15 alphanumeric characters. Asterisks appear on the screen as you type to prevent your password being displayed on the screen. Press Enter. ***NOTE: Passwords are case sensitive.***
Verify password	Retype the password exactly as you entered it the first time, and then press Enter.
Access Options	Press the space bar until the desired choice is displayed. Three options are available: Regular Callback, Passthru and Variable Callback. Each option is discussed in subsequent paragraphs.

Access Option: *Regular Callback*

Regular Callback requires the user to have a specific phone number listed in the terminal server user database, in addition to the password. The user calls the terminal server and enters their user name and password. After receiving the information the terminal server terminates the call and dials the caller back using the number in its database for that user. The user is requested to re-enter their password. After the password is authenticated, the user is allowed access.

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

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

Access Option: *Passthru*

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

Access Option: *Variable Callback*
Variable Callback requires a user name and corresponding password. After dialing in to the terminal server and entering the correct user name and password, the user enters a phone number for the terminal server to call back. The terminal server disconnects and the user hangs up. The terminal server then calls the user back at the phone number provided.

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

Listing Users – LU Command

Type **LU** at the system prompt, and press the Enter Key to display the list of users authorized to initiate a Sysop or Host session with the terminal server. The following information is displayed for each user:

User name

Access class [Acc. Class]

Whether user access is specifically blocked [Blk?]

Expiration date [Exp. Date]

Number of sessions allowed [# Ses. Exp?]

Primary authentication method [Auth. Mode(s)]

Secondary authentication method [Auth. Mode(s)]

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

```
--- List Users ---

User Name       Acc.Class   Blk?  Exp.Date    #Ses. Exp?  Auth.Mode(s)
ADMIN           Master                                    PwdCB
HOST1           Host 1                         1          PwdCB
HOST10          Host 10                        1          PwdCB
HOST11          Host 11                        1          PwdCB
HOST12          Host 12                        1          PwdCB
HOST13          Host 13                        1          PwdCB
HOST14          Host 14                        1          PwdCB
HOST15          Host 15                                   PwdCB
HOST16          Host 16                                   PwdCB
HOST17          Host 17                                   PwdCB
HOST18          Host 18                                   PwdCB
HOST19          Host 19                                   PwdCB
HOST2           Host 2                         1          PwdCB
HOST20          Host 20                                   PwdCB
HOST21          Host 21                                   PwdCB
HOST22          Host 22                                   PwdCB
HOST23          Host 23                                   PwdCB
HOST24          Host 24                                   PwdCB
HOST25          Host 25                                   PwdCB
HOST26          Host 26                                   PwdCB
-- More to Come - Press ENTER (Ctrl+A to quit) --
```

Field	Function
User Name	List of all users authorized to access the terminal server, or other device connected to the terminal server.
Acc. Class	The Access Class defined for that user. For a description of the access classes, see "Adding a User."
Blk?	This column shows whether a user's access is

Field	Function
	blocked. "No" means that access is permitted. "Yes" means that access for that user is blocked.
Exp Date	If a date appears in this field, the user will not be allowed access to the terminal server after this date.
# Ses. Exp?	If a number appears in this field, the user will not be allowed access to the terminal server system after he or she has successfully accessed the system the number of times displayed. This field is blank if the user's expiration date or number of sessions allowed has not been exceeded. A Yes appears in this field if the expiration date has past or the number of successful sessions has been exceeded.
Auth. Mode(s)	The primary and secondary (if used) methods of authentication for the user are displayed in this column. Password/Callback is the only authentication method supported for this version of the Central Web Console For a description of the authentication methods, see "Adding a User" at the beginning of this chapter.

Deleting a User Profile – XU Command

The Delete User command deletes all records associated with that user from the terminal server database. After a user profile has been deleted, the user cannot access the terminal server. To reinstate access privileges, a user profile must be added to the database, see "Adding a User."

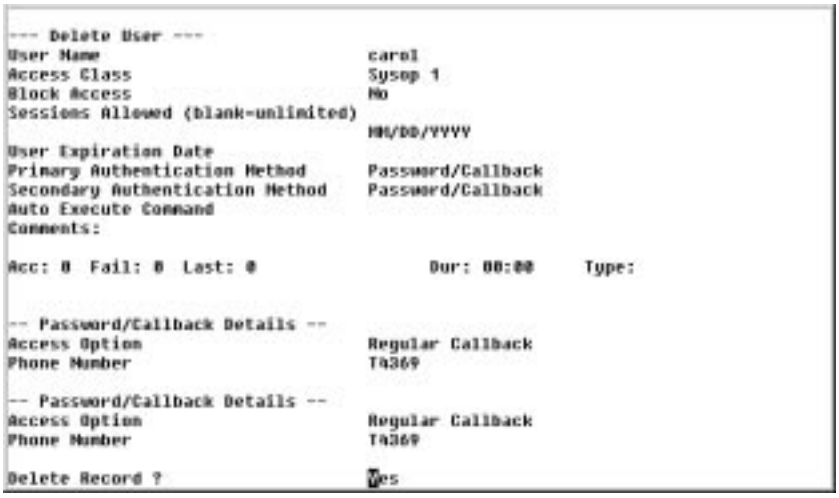
Type **XU** at the system prompt and press the Enter key to display the Delete User information screen.

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

For example:

```
>XU or
>XU Carol
```

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



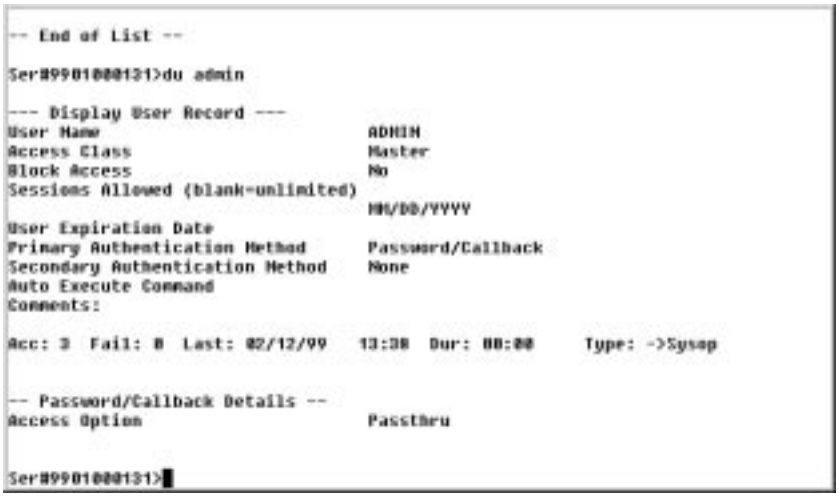
The prompt Delete Record? appears at the bottom of the screen requiring you to confirm that you want to delete that user. Initially No appears on the screen. To delete the user, toggle the field to Yes by pressing the space bar and then press the Enter key.

NOTE: To temporarily remove a user from the database, use the block access option in the user profiles. The user will not be allowed access, but all his/her access information will be maintained.

Displaying a User Record – DU Command

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

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



Field	Function
User Name	Enter the user name as it appears in the List User display, and then press the Enter key. You may also type the user name as part of the command. For example: **>DU** *or* **>DU CHRIS**

The User Record information screen for that user will be displayed.

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

For a description of the fields in the Display User Record Screen, refer to "Adding a User".

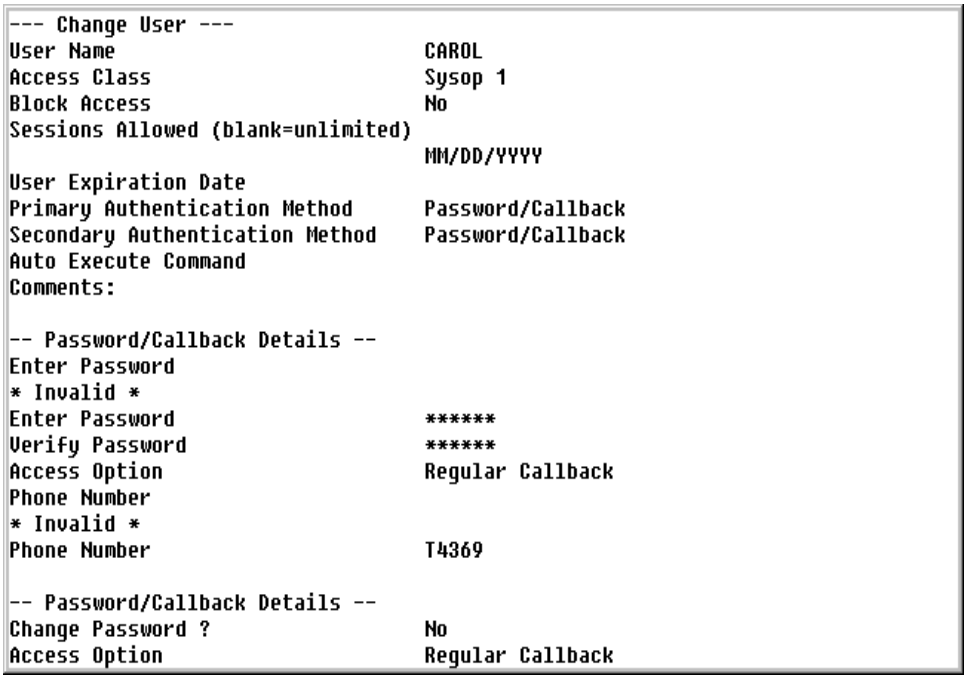
Changing User Information – CU Command

The Change User command allows you to change the information of an authorized user in the user database.

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

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

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



```
--- Change User ---
User Name                          CAROL
Access Class                       Sysop 1
Block Access                       No
Sessions Allowed (blank=unlimited)
                                   MM/DD/YYYY
User Expiration Date
Primary Authentication Method      Password/Callback
Secondary Authentication Method    Password/Callback
Auto Execute Command
Comments:

-- Password/Callback Details --
Enter Password
* Invalid *
Enter Password                     ******
Verify Password                    ******
Access Option                      Regular Callback
Phone Number
* Invalid *
Phone Number                       T4369

-- Password/Callback Details --
Change Password ?                  No
Access Option                      Regular Callback
```

Field	Function
User Name	Enter the user name as it appears in the List User display. You may also type the user name as part of the command. For example: >**CU** *or* >**CU TOM**
Access Class	To change the Access Class, press the space bar until the desired choice is displayed.

Field	Function
	When the appropriate selection is displayed, press the Enter key. If you do not wish to change this parameter, press the Enter key to move the cursor to the next field.
Block Access	Initially No (the default) appears on the screen. Press the space bar to toggle to Yes. No enables access to the terminal server. Yes blocks access to the terminal server.
Sessions Allowed	Press the Enter key to allow unlimited sessions. Enter a number from 1 to 999 and press Enter to limit the number of successful sessions allowed for that user.
User Expiration Date	Enter the date in month/day/year to set the end of the user's access period. No date signifies the user has an unlimited access period.
Primary Authentication Method	Press the space bar until Password/Callback is displayed. ***NOTE:*** ***The Pager and PassKey options are not supported with this version of the Central Web Console.***
Secondary Authentication Method	(Optional) Select a second means of authentication for a user. Press the space bar until the desired choice is displayed.
Auto Execute Command	(Optional) Enter a command that's executed automatically after user authentication.

Field	Function
	For example, if you enter LH - the log history will be displayed in reverse order after the user authenticates. This option is available only to users who sign on as a Sysop 1 level or higher.
Comments	Enter up to 40 alphanumeric characters on the *Comments* line. After you have entered comments in the Comments field, press Enter.

After pressing Enter, you will be prompted for more information about the authentication method that you selected. For complete information on each of the authentication methods, refer to "Adding a User."

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

3. SYSTEM PARAMETERS

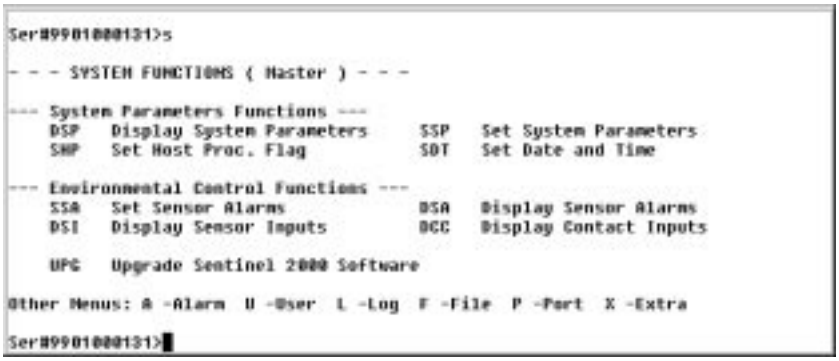
What This Chapter Contains

The terminal server menus provide commands for setting and displaying system parameters. The System Parameters are used primarily for information purposes. For example, the site name, IP address, and the phone number of the unit are specified by these parameters. The FTP and network parameters must also be set before the Central Web Console can communicate with all system components.

- Overview
- Site Information Parameters
- Software Upgrade Information
- Network Parameters
- FTP Parameters

Systems Functions Menu

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



The System Parameters Functions menu has three functional groups: System Parameters Functions, Environmental Control Functions and Upgrade Central Web Console software.

System Parameters Functions

The commands in this functional group enable you to set and display system parameters including the host processing flag and the date and time of the terminal server.

Environmental Control Functions

These functions are not supported in this version of the Central Web Console.

Upgrade Terminal Server Software

The terminal server software, CCL interpreter and the flash memory of the terminal server may be upgraded.

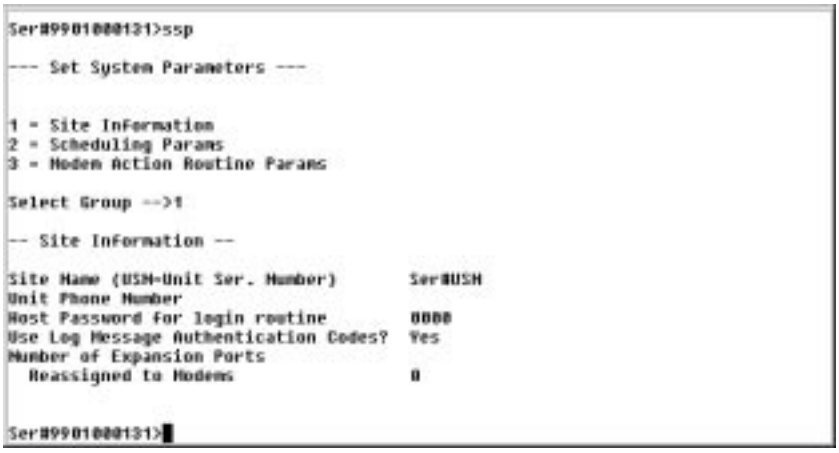
Set System Parameters – SSP Command

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

Type **SSP** to select which parameter group you want to be displayed. The following screen appears. This chapter only covers the Site Information parameters.

Site information

Type **1** to set Site Information. Site information includes site name, terminal server phone number and the host password. The system prompt displays the site name.



When the terminal server pages or phones in response to a particular alarm or event, it sends its site name and unit phone number along with the error message and other information that enables the receiver to contact the correct terminal server.

Field	Function
Site Name (USN = Unit Ser. Number)	Descriptive name of the terminal server location. When information is sent to another device, the site name is included automatically. The site name is displayed at the prompt. The site name may have a maximum of 30 alphanumeric characters. Only the first 15 characters appear at the prompt. The default site name is the unit's serial number. If you have more than one terminal server at a site, using the serial number as the site name is useful. If a site name is not entered, only the command prompt is displayed.
Unit Phone Number	Enter the phone number of the terminal

	server. This number is sent by the PHONHOME Action Routine.
Host Password for login routine	Enter the password for the host system for automatic login. The password may have a maximum of 16 alphanumeric characters.
Number of Expansion Ports Reassigned to Modems	The terminal server has been configured to use all expansion ports as host console ports.

Upgrading the Software

Your Hewlett-Packard service representative notifies you when an internal software upgrade is necessary. Installation instructions are dependent on the type of upgrade required.

Specify Network Parameters

Communication with the terminal server occurs across a TCP/IP network through either an Ethernet connection or a PPP link.

An Ethernet connection physically connects the terminal server to the network. PPP (point-to-point protocol) allows a network connection to a remote device via a modem connection. After a PPP link has been established you can perform network functions, such as Telnet or FTP, to the terminal server or to specific serial devices on the network. To establish a PPP link or to initiate a Telnet session, you must have the appropriate commercial software package installed and setup on the remote PC. Connection to the network provides for the following services:

- Ping
- Telnet communication

  - Network access to the terminal server for unit administration
  - Network access to the devices connected to the host ports
  - Network access to other devices on the network, using the terminal server as a RAS

- SNMP trap delivery
  - Delivery of SNMP traps for errors detected in the terminal server
  - Delivery of SNMP traps for alarms conditions detected in the devices connected to the host ports

- FTP file delivery (Client)
  - Delivery of buffer files from the terminal server to a network file server

Setting Network Parameters – SNP Command

If the terminal server is part of a network, it is necessary to set the Network Initialization Parameters *prior to starting the network module of the terminal server.* Changes made to the Network Initialization Parameters will only take effect if the *network has not yet been started*, or by *restarting the terminal server*. You can restart the terminal server by either using the key switch on the front panel to power-cycle the unit (off then back on – a 'hard' boot) or by issuing the **BOOT** command from the command prompt to perform a 'soft' boot.

Each device on a network must have a unique Ethernet and IP address. The Ethernet address of each terminal server is calculated by using a registered OUI and the terminal server's serial number. This ensures that all terminal servers on the same network will have different Ethernet addresses.

Before connecting the terminal server to your network, contact your network administrator and obtain the following information:

- IP address to be assigned to the terminal server
- IP address to be used for PPP connections
- Subnet mask for the network segment to which the terminal server will be connected
- IP address of the default gateway to be used by the terminal server

The terminal server allows a user to establish a PPP connection to the internal modem. This connection allows a Telnet session to either the terminal server or another device on the network attached to the terminal server. In the latter case the terminal server acts as a dial-up security server.

When a remote user attempts to access other network devices via a PPP session, those devices must know how to direct their responses back to the user. The simplest way to accomplish this is with a router that supports RIP, the standard Router Information Protocol. The strategy is to make the devices on the network direct their responses to the router, and then have the router forward the data to the terminal server. To do this, ensure that a RIP-enabled router is on the network, and configure the other devices to use it as their default gateway. The terminal server will automatically use RIP to tell the router how to forward data addressed to the remote user when a PPP link is established.

NOTE: The network number (the first set of numbers) for the PPP connection in the terminal server should be different than the network number used for the network IP address. If the network address of the terminal server is 193.1.1.1 then the PPP address should not begin with 193.

To set network parameters, type **SNP** at the system prompt and press the Enter key. Each prompt is explained in subsequent paragraphs.

```
02/17/1999 12:30:33 255A [T2] Set Network Params - O.K.
Ser#99010000131>snp

--- Set Network Params ---


1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params
4 = PPP Params
5 = Telnet Params

Select Group -->1
```

Network Initialization Parameters

The Network Initialization Parameters are set using the **SNP 1** command:

```
--- Set Network Params ---


1 = Network Initialization Params
2 = SNMP Manager Params
3 = FTP Params
4 = PPP Params
5 = Telnet Params

Select Group -->1
*****************************************************************
***            The Network is Already Running.                ***
***        Changes made to the IP address will not            ***
***     take effect until the Sentinel 2000 is restarted.     ***
*** To restart unit, power cycle or use the BOOT command. ***
*****************************************************************

Restore Factory Defaults ?         No
-- Network Initialization Parameters --
Start Network on Power-up ?        Yes
IP Address (nnn.nnn.nnn.nnn)       15.43.215.197
PPP Address (nnn.nnn.nnn.nnn)      192.9.200.3
Subnet Mask (nnn.nnn.nnn.nnn)      255.255.248.0
Default Gateway (nnn.nnn.nnn.nnn)  15.43.208.1
Enable RIP?                        No
Network-Loss Alarm Delay Time      60


02/12/1999 15:32:29 8FBC [T2] Set Network Params - O.K.
Ser#99010000131>
```

Field	Function
Restore Factory Defaults?	Initially No appears on the screen. Press the space bar to toggle to Yes. Select Yes to reload the values set at the factory.
--Network Initialization Parameters--Start Network on Power-up?	Initially No appears on the screen. Press the space bar to toggle to Yes. Yes will start the network module on unit power-up using the parameters defined with the SNP command.
IP Address (nnn.nnn.nnn.nnn)	Enter the IP address of the terminal server. Each device on the network must have its own unique IP address. The IP address assigned to the terminal server at the factory may not be appropriate for your network. The IP address must be set before the network module of the terminal server is started. Once the network has been started, changes to this parameter will take effect only after the terminal server is power-cycled (rebooted).
PPP Address (nnn.nnn.nnn.nnn)	Enter the PPP address of the terminal server. This is the IP address that is used to identify the terminal server over a PPP link. The network portion of the PPP address must be different from the IP address used above.
Subnet Mask (nnn.nnn.nnn.nnn)	The subnet mask determines which part of the terminal server's IP address represents its network number and which part represents its node number. Obtain an appropriate value from your network administrator.

Field	Function
Default Gateway (nnn.nnn.nnn.nnn)	The default gateway is the IP address of the router or other equipment on the local network segment that is used to direct traffic to and from the segment. Obtain an appropriate value from your network administrator.
Enable RIP?	Initially Yes appears on the screen. Press the space bar to toggle to No. Yes allows the terminal server to direct routers on the local network segment to use it as the gateway to devices connected to the terminal server via PPP.
Network-Loss Alarm Delay Time	Enter a time in seconds, from 0 to 255. If no network activity is detected for longer than the specified amount of time, the terminal server will generate a .NETDOWN alarm.

Overview of SNMP Support by Terminal Servers

SNMP (Simple Network Management Protocol) is a TCP/IP protocol for network management. It allows compliant devices to be configured and/or to send error messages to Network Management software packages.

The terminal server can send SNMP traps based on alarm conditions detected in host devices or in the terminal server itself. Any alarm condition that can be listed in the Action Table can be sent to a management system via an SNMP Trap. Thus, the terminal server acts as an SNMP trap proxy agent for devices that deliver alarms via asynchronous RS-232 communication, via contact closures, or other non-network mechanisms.

MIBs

SNMP uses a data structure known as Management Information Base, or MIB, to store information. Each piece of information, or object, in the MIB has a unique Object Identifier. Object identifiers are indices based on a tree structure. The information is held in a "node" at the end of a "branch" in the tree. The Object Identifier shows the path by listing each branch needed to reach the node.

The identifier serves to name or reference the object. MIBs for specific companies are allocated to the MIB branch known as enterprise. Thus, each company branches from the general branch known as enterprise. From that point on in the MIB, the company developing the MIB controls the information and Object Identifier used to reference the data. This information is required to coordinate the sending and receiving of data between an SNMP-compliant device and an SNMP-based network management system.

When both the SNMP Agent and SNMP Management system have the same MIB structure, data can be easily transferred and used. SNMP data packets, each containing an object identifier and information associated with that object, are passed between the device and management system to populate the appropriate fields in the receiver's MIB. Both the Agent and Management System can then reference the object and process the data as needed.

The terminal server has a general MIB as well as proprietary MIBs for companies that use the terminal server as an SNMP trap proxy.

The following table shows the basic set-up of a MIB and provides information about:

- Object Identifiers – The index used to identify the information in the MIB.
- Object Data – The information contained in the referenced data node.

- Object Source – The field in the terminal server where the information is located.

Object Identifier	Object Data	Object Source
1.3.6.4.1.1476.1.1.1	trapId	Alarm Severity. Placed in the Action Table Parameter Field. The value can be from 1 to 10.
1.3.6.4.1.1476.1.1.2	trapSiteDesc	Site name in System Parameter.
1.3.6.4.1.1476.1.1.3	trapSource	SNMP Agent.
1.3.6.4.1.1476.1.1.4	trapDesc	Alarm or error code. This is the alarm as delivered by the host device or terminal server system. It includes all parameters.
1.3.6.4.1.1476.1.1.5	trapComment	Comment Field in Action Table. The date and time of alarm are also included in this field.
1.3.6.4.1.1476.1.1.6	trapExtraInfo	Extra information associated with this message. Assigned by custom Action Routine.
1.3.6.4.1.1476.1.1.7	trapExpertData	May contain up to 161 characters, and provides additional data to the technician that helps in the isolation or correction of the problem.

An SNMP Management System can be configured to receive and use SNMP traps sent by the terminal server by using the above information.

NOTE: Configuration of the SNMP Management System may require the assistance of your LAN Administrator. Please contact him/her to determine how to compile the appropriate MIB for your particular system.

Delivering SNMP Traps

The terminal server can send SNMP traps using one of the following methods:

- If the Network Manager is on the same LAN or WAN as the terminal server, the trap can be sent with the SNMPTRAP Action Routine using the Ethernet connection.

- If the Network Manager is not on the same LAN or WAN, the terminal server can establish a PPP link through a modem and deliver the SNMP Trap.

SNMP Traps via Ethernet (Network)

Set all required network information using the SNP command. In the Action Table, place an entry similar to the following:

Alarm	Action Routine	Parameter	Comments
ERR123	SNMPTRAP	1	This is a major alarm

When the ERR123 alarm is detected, an SNMP trap is sent to the management system(s) identified in the network parameters. All information contained in the MIB is sent automatically. The parameter for the SNMPTRAP routines sets the trap level (1-10). This parameter is the enterprise specific trap ID and depends on the trap format (Nortel or standard).

SNMP Traps via PPP

To denote that an SNMP trap is to be delivered via a PPP link, set the appropriate field in the SNP command. When an SNMP trap is to be

delivered via a dial-up PPP link, the terminal server generates a .PPPREQ event. Include entries similar to the following in your Action table:

Alarm	Action Routine	Parameter	Comments
ERR001	SNMPTRAP	2	This is a minor alarm.
.PPPREQ	PHPPP	5551212	Create the PPP link.

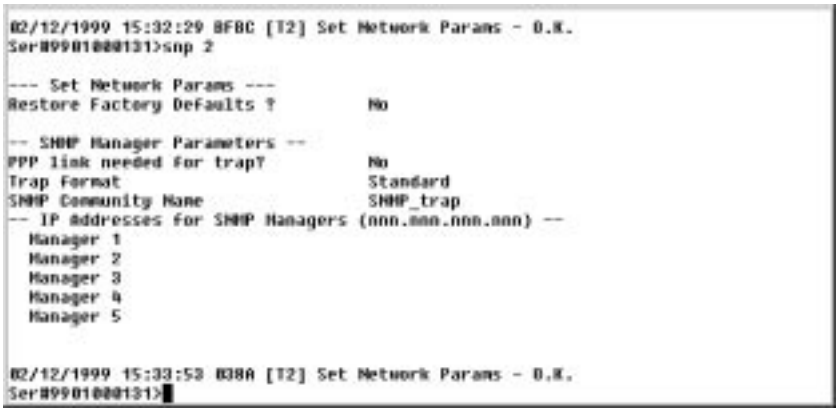
The telephone number can be specified directly, or any of the default telephone numbers specified in the system parameters can be referenced. PHPPP is not compatible with firewalls or any security measures on the remote access device.

Setting Terminal Server Parameters for SNMP Traps

The terminal server responds to “alarms” (such as an error condition on a host) by performing an appropriate user-defined action. A typical action might be connecting to a remote computer over a modem link and sending error information from the host to that computer. SNMP provides a standard way for the terminal server to report alarms to one or more computers that are connected via network.

SNMP Manager Parameters

You can configure the terminal server to send a message, or “SNMP trap,” to one or more supervisor computers, which are called SNMP managers, in response to alarm conditions. These parameters are set using the **SNP 2** command:



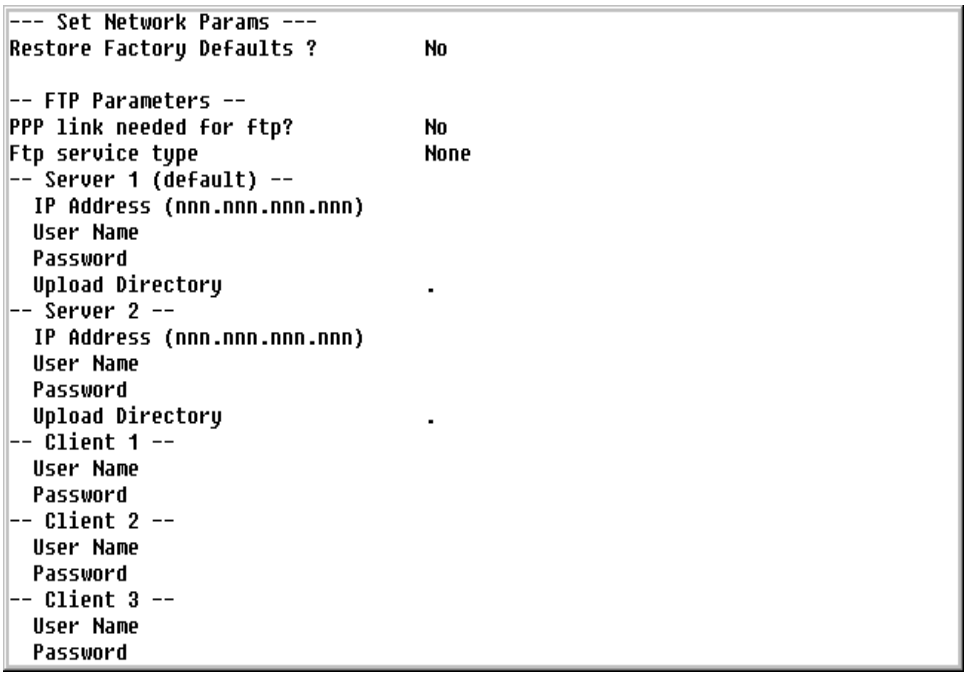
Field	Function
Restore Factory Defaults?	Initially No appears on the screen. Press the space bar to toggle to Yes. Select Yes to reload the values set at the factory.
--SNMP Manager Parameters-- PPP link needed for trap?	If the terminal server is not connected to the same network as its SNMP Manager, it can reach the manager over a modem link by using the "Point-to-Point Protocol" (PPP). Initially No appears on the screen. Press the space bar to toggle to Yes. Set this option to Yes to establish a modem link to *only one* SNMP manager. Additional steps may be necessary to configure the dial-out process. Select No if the trap will be sent via the network connection.

Field	Function
Trap format	This option selects one of the active MIBs to format the SNMP Trap. Two formats are available: Standard and Nortel. Press the **space bar** until the desired choice is displayed.
SNMP Community Name	Enter the SNMP community name (up to 20 characters can be used as a name).
--IP Addresses for SNMP Managers- *Manager 1* *Manager 2* *Manager 3* *Manager 4* *Manager 5*	A maximum of five IP addresses can be entered as SNMP Managers to accept SNMP traps. If the IP address is not on the terminal server's network segment, make sure the default gateway is set and all routers have been programmed with the proper routes.

Setting FTP Parameters

The terminal server supports FTP Client Send commands. Files can be sent from the terminal server to an FTP server using FTP (File Transfer Protocol) protocol. To do this, you must set parameters in the Set Network Parameters screen. After the parameters have been specified, you may issue the SEBUF or SEND command with the appropriate parameters.

To specify the FTP parameters, type **SNP 3** to display the Network Parameters menu, FTP Parameters option.



NOTE: In setting the user name and password, remember that they are case-sensitive.

Field	Function
Restore Factory Defaults	Press the space bar until the desired choice is displayed. Select “Yes” to restore original factory settings. Select ‘No’ to keep the current values.
PPP link needed for ftp?	Select this option if the terminal server needs to dial out with a PPP session to send files via FTP. (See

Field	Function
	the PPPREQ alarm and PHPPP Action Routine in Chapter 8.)
FTP service type	Select the type of FTP service (None or Client Only). Press the space bar until the desired choice is displayed.
Server 1 (default) – IP address (nnn.nnn.nnn.nnn)	Enter the IP address of the server. The files transmitted by FTP are sent to this address automatically unless specified otherwise.
User name	Enter the name used to log onto the server. This entry is case-sensitive
Password	Enter the password for the user named above. This entry is case sensitive.
Upload directory	Enter the name of the directory that should receive the file. A period denotes the root directory.
-- Server 2 --	
IP address (nnn.nnn.nnn.nnn)	Enter the IP address of the server. The files transmitted by FTP are sent to this address automatically when server 2 is specified.
User name	Enter the name used to logon onto the server. This entry is case-sensitive
Password	Enter the password for the user named above. This entry is case sensitive.

Field	Function
Upload directory	Enter the name of the directory that should receive the file. A period denotes the root directory.
-- Client 1 -- *User name*	Enter the name of the first user who will log in as an ftp client. This entry is case-sensitive
Password	Enter the password for the user named above. This entry is case sensitive.
-- Client 2 -- *User name*	Enter the name of the second user who will login as an ftp client. This entry is case-sensitive
Password	Enter the password for the user named above. This entry is case sensitive.
-- Client 3 -- *User name*	Enter the name of the third user who will login as an ftp client. This entry is case-sensitive
Password	Enter the password for the user named above. This entry is case sensitive.

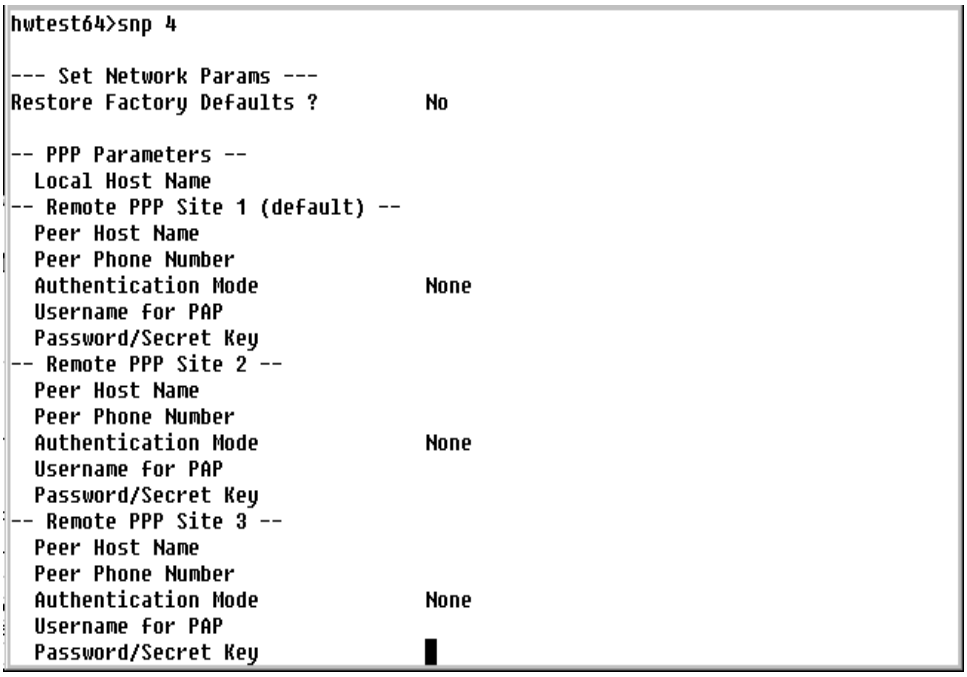
The Terminal Sever can establish a PPP link after establishing a SYSOP through a dialup (modem) connection. Set the parameters for your terminal dial-up package according to the manufacturer's instructions and authenticate into the terminal server. At the system

prompt, type the command **PPP** and press enter. Send the terminal server a “BREAK” from your terminal communication package and await notification that a PPP link has been established. When conformation has been received, you may open up a telnet window and establish a PPP link directly to the terminal server.

When connecting to a remote host via PPP, the are two standard options of authentication: PAP (Password Authentication Protocol) and CHAP (Challenge-Handshake Authentication Protocol). In the PAP authentication process, the terminal server sends the username and the password to the remote host. The remote host then determines whether or not the user is allowed to establish the PPP link.

The CHAP option of authentication offers a higher-level of security since the authentication process is encrypted. In this process, the terminal server and the remote host have a shared secret key. The terminal server transmits the local host name and the remote host responds with a “challenge” number (random number). The “challenge” number is then encrypted with a response back to the remote host, which encrypts the challenge using the same secret key. If the responses match, the PPP session is established.

Type **SNP 4** to display the Network Parameters menu, PPP Parameters option.

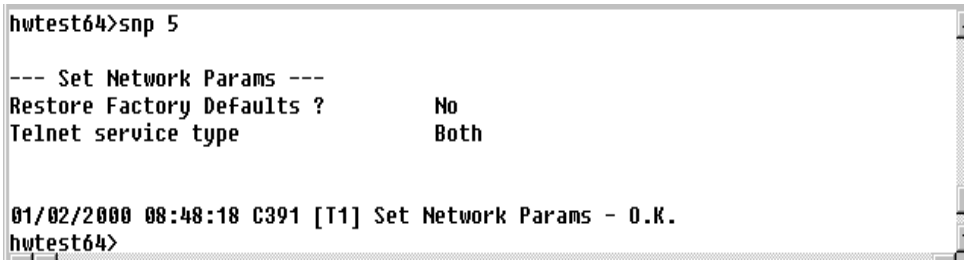


These parameters are set using the **SNP 4** command:

Field	**Function**
Restore Factory Defaults	Press the space bar until the desired choice is displayed. Select “Yes” to restore original factory settings. Select ‘No’ to keep the current values.
Local Host Name Remote PPP Site 1	Enter the host name to be used with the CHAP authentication option.
Peer Host Name	Enter the name of the remote host which to establish a PPP link.

Field	Function
Peer Phone Number	Enter the telephone number of the host to which a PPP link will be established.
Authentication Mode	Press the spacebar to select the authentication method to be used (PAP, CHAP or None).
Username for PAP	Enter the username for PAP authentication.
Password/Secret Key	Enter the password, if PAP option has been selected for authentication. Enter the secret key, if CHAP has been selected for authentication.

Type **SNP 5** to display the Network Parameters menu, Telnet Parameters option.



These parameters are set using the **SNP 4** command:

Field	Function
Restore Factory Defaults	Press the space bar until the desired choice is displayed. Select “Yes” to restore original factory settings. Select ‘No’ to keep the current values.

Field	Function
Telnet service type?	Press the space bar until the desired choice is displayed (None, Both, Client Only, Server Only)

4. FILE BUFFERING

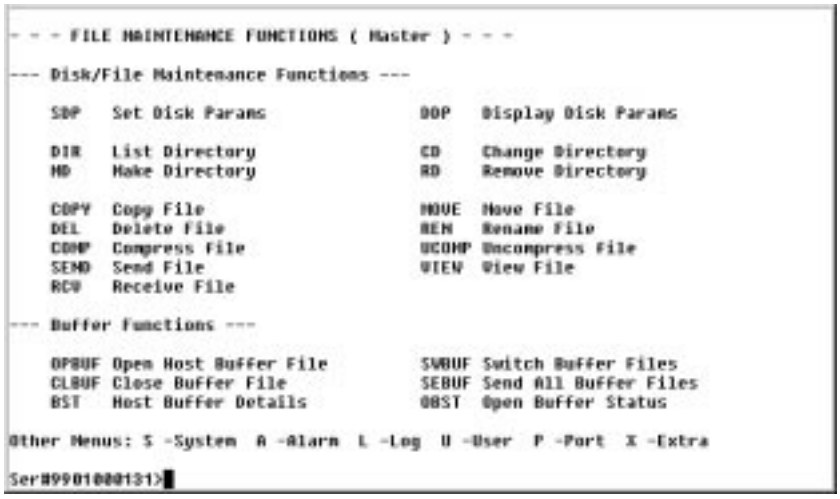
What This Chapter Contains

The File Management Menu is organized into two sections: Disk/File Maintenance Functions and Buffer Functions. The Disk/File Maintenance Functions section lists the commands by which the user may edit or manipulate files from the terminal server RAMdisk. The Buffer Functions section lists commands for collecting data into files and for sending files to the administration PC.

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

File Management Menu

To view the File Management Menu, type **F** at the system prompt and press the Enter key.



File Command Summary

Command	Function
DIR	Displays the files in the current directory. Directories are indicated by <DIR> adjacent to the name, along with their creation date and time.
MD	Makes a new directory under the current directory. MD <newdirectoryname> Example: MD newdir Creates a new directory named newdir under the current directory.

Command	Function
CD	Changes the current directory to a directory specified by the user. Note that a space MUST follow this command. Example: CD \ to return to the root directory. CD **..** to go up one level.
RD	Removes the specified directory. An error is displayed if the specified directory is not empty. RD <directoryname> Example: RD NEWDIR
COPY	Copies the specified file to a specified location. The destination directory must exist before the file can be copied. COPY <source directory>\<filename> <destination directory>\<filename> Examples: COPY \sentfiles\H4961212.2A \newdir\H4961212.2A To copy a file from the current directory to a new directory COPY H4961212.2A \newdir\H4961212.2A
DEL	Deletes a file from the RAMdisk. DEL <source directory>\<filename> It is not necessary to specify the directory if the file to be deleted is in the current directory. Example: DEL \sentfiles\H4961212.2A

Command	Function
MOVE	Copies a file to a new directory and then deletes it from the source directory after the file has been copied. MOVE <source directory>\<filename> <destination directory>\<filename> Examples: MOVE \sentfiles\H4961212.2A \newdir\H4961212.2A To move a file from the current directory to a new directory MOVE H4961212.2A \newdir\H4961212.2A
RCV	Command to receive files from the active port into the current directory on the terminal server using XMODEM or ASCII transfer. If FTP capability is available and the FTP parameters have been set properly, RCV can also be used to receive a file via FTP.
REN	Renames the specified file REN <filename> <new filename> Example: *REN H4961212.2A DAYONE* The file H4961212.2A is renamed as DAYONE.
SEND	Sends the specified file using either XMODEM or ASCII transfer protocol. If FTP capability is available and the FTP parameters have been set properly, SEND can also be used to transmit a file via FTP.
VIEW	Displays the contents of the specified file, one page at a time. Scroll through the file by pressing <ENTER> to view the next page. <CTRL-A> will return you to the prompt.

RAMdisk Organization

There are 32 Mbytes available on the RAMdisk. You may create and remove subdirectories, and copy, move, rename and delete files.

The directories listed below are automatically created by the system:

- A subdirectory is created for each host port that has buffering enabled, 1MB maximum per port. The data collected from the host port is stored in this subdirectory. The subdirectory is given the same name as the host port by default. To view the host port directory, type **OPBUF*h#*** *(Where h# is the desired host port number)* at the system prompt.

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

- The \LOGFILES directory contains files that are generated each day by the terminal server to maintain a record of that day's activities. These files are of two types: Event files, which list the alarms that were processed during one day, and Log files, which contain a copy of one day's log history.

Host Port Buffer Naming

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

Buffer File Naming Conventions

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

Examples: 101296AM.100
REPORT.01
IMPORTANTLOG

Note that in the screen above the default filename is *CURRENT.0.* The current buffer file for a host port is always named either *CURRENT.0* or *CURRENT.1*. When the buffer is switched, the buffer file is renamed to indicate the host port number from which the data was collected and the date and time the buffer was opened.

Files collected via host port data by the terminal server are stored in the directory of that host port and are assigned sequential names in order to provide the user a means of identifying when and where the data in the file was gathered. The terminal server uses following naming convention:

H*nyymmdd.hhq*

Where: H = the letter H
n = host port number [1-9, A-T represents ports 10-28]
yy = year
mm = month
dd = day
hh = hour
q = a letter (starting with 'A') used to differentiate multiple files opened during the same hour.

Example 1: H2981218.14A

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

Example 2: HG980709.08D

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

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

The Event and Log files that are generated by the terminal server have names of the form listed below:

EVyymmdd.LOG (for Event files)
LGyymmdd.LOG (for Log files)

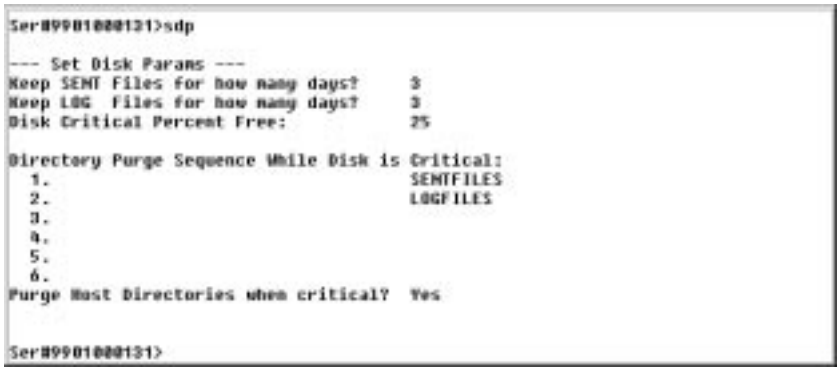
Where: EV = the letters EV
LG = the letters LG
yy = the last 2 digits of the year
mm = the month
dd = the day
.LOG = the letters .LOG

Setting the RAMdisk Protection Parameters

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

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

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



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

Field	Function
Disk Critical Percent Free:	Enter the percentage of disk space that must be free. When this percentage is reached, files will be deleted in the order specified by the entry for the *Directories to Purge* prompt.
Directory Purge sequence While Disk is Critical: - *SENTFILES* - *LOGFILES* - *sh* *4* *5* *6*	Enter the names of the directories that will be purged in sequence. When disk space is critical, files will be deleted from the first directory, oldest files first, followed by the second directory, etc. until disk space is no longer critical.
Purge Host When Critical	Initially **No** appears on the screen. Press the space bar to toggle to **Yes**.

RAMdisk Events

The terminal server, in response to certain RAMdisk conditions, will generate events that are part of the standard software/firmware. These standard events are as follows:

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

Buffering Data Received by a Host Port

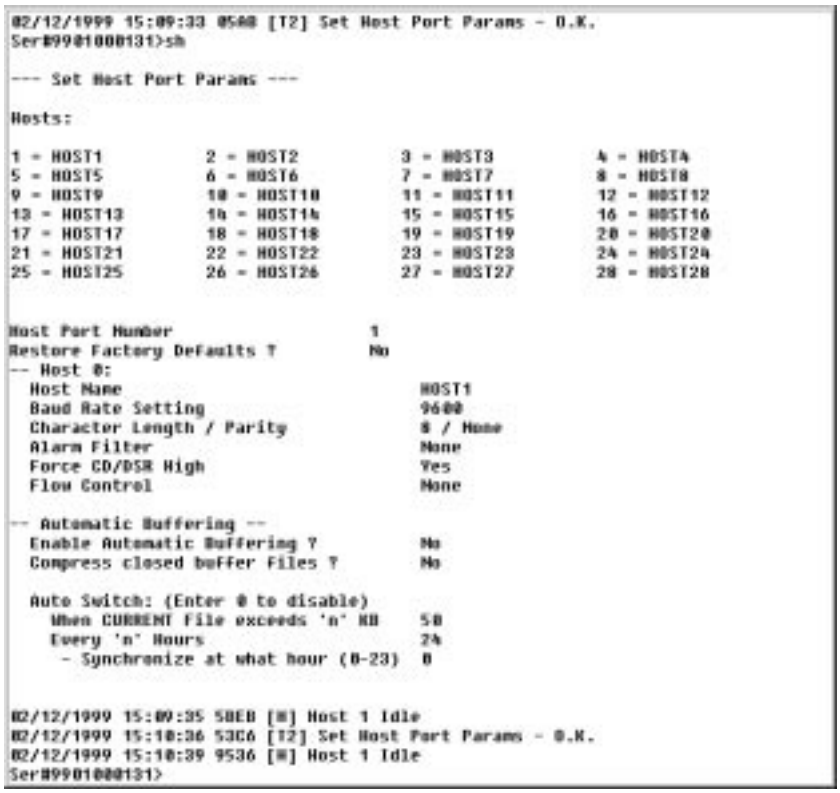
The terminal server provides both automatic and manual control of data buffering from the host ports. If automatic buffering is selected, a buffer file for the specified port will be opened and data collected until either a specified time or file size is reached. The current buffer file is then closed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

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

Automatic Buffering

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

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



Field	Function
Enable Automatic Buffering	Initially No appears on the screen. Press the space bar to toggle to Yes. Select Yes for automatic buffering. Select No to disable it.
Compress closed buffer files?	Initially No appears on the screen. Press the space bar to toggle to Yes. Select Yes to compress buffer files automatically when they are closed. The compression ratio is typically 4:1, but the ratio may vary because

Field	Function
	it is dependent on the data.
Auto Switch (enter 0 to disable) When CURRENT File exceeds 'n' KB	Enter the file size (in KB) at which the buffer should be switched. Note that the *CURRENT.x* file is renamed using the convention described in this section. Enter 0 to disable this feature.
Every n hours	Enter the number of hours between the switching of buffers.
Synchronize at what hour (0-23)	Indicate the hour at which the buffer should be switched. If the value is set to 2 and the previous value is set to 8, the buffer will switch at 200, 1000, and 1200 hours.

NOTE: If both the Current File exceeds 'n' KB and the Every n hours parameters are set, the buffer is switched when the first condition is met.

Manual Buffering

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

Command	Function
OPBUF	Open buffer Opens a buffer for a port. You will be prompted for the port number.
CLBUF	Close buffer Closes the buffer file for a particular port. You will be prompted for the port number.

Command	Function
SWBUF	Switch buffer Closes the buffer for the specified port and opens a new one. You will be prompted for the port number.
BST	Buffer status Displays the status of all open and closed buffer files for a specific host port.
OBST	Status of open buffers for each host port. Displays the status of all open buffer files. Status includes creation time, file size, and the time and size at which the buffers will be switched (if automatic buffering is enabled).

Using FTP to Send Files to an FTP Server

The terminal server supports FTP Client Send commands. Before you can send a file via FTP, the following must have been done.

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

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

Files may be sent using FTP from the terminal server to another device by issuing the **SEND** or **SEBUF** command. However, you must set the FTP parameters prior to using these commands.

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

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

Command: **SEND**

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

Files are sent from the current directory.

Examples:

To send the file NEW.CFG to server #1 (the default server entered using the **SNP 3** command) from the directory TEST while in the current directory, the command format is:

SEND \TEST\NEW.CFG,F,1

Where:

<TEST>	= name of the Host port Directory
<NEW.CFG>	= name of file to send
F	= use ftp protocol.
<server#>	= Number of the server that will receive the file, as listed in the Network Parameters table.

To send a file from the current directory, you need not enter a directory name:

SEND NEW.CFG,F,1

Files can also be sent to a server whose profile was not entered into the terminal server with the **SNP 3** command. To do this enter the following information:

SEND
<filename>,F,<IPaddr>,<user>,<password>,[directory]

Where:

<filename>	= name of file to send.
F	= use ftp protocol.
<IP addr>	= IP address of the server that will receive the file.
<user>	= login name of the ftp user on the server.
<password>	= password of the ftp user on the server.
[directory]	= directory on the server into which the file will be transferred. Enter the directory or specify "." to use the current ftp directory.

Command: **SEBUF**

Description: This command is used to send all closed buffer files in a specific host port buffer directory to either server entered with the **SNP 3** command:

Syntax: **SEBUF** <host#>,F,<server#>

Where:

<host#>	= is the number of the host port on the terminal server
F	= use ftp protocol.
<server#>	= Number of the server that will receive the file, as listed in the Network Parameters table.

SEBUF
<host#>,**F**,<IPaddr>,<user>,<password>,[directory]

Where:

<host#> = is the number of the host port on the terminal server

F = use ftp protocol.

<IP addr> = IP address of the server that will receive the file.

<user> = login name of the ftp user on the server.

<password> = password of the ftp user on the server.

[directory] = directory on the server into which the file will be transferred. Enter the directory or specify "." to use the default ftp directory.

Examples:

To send all buffer files from Host port 1 using server profile 2 and the FTP protocol, enter:

SEBUF 1,F,2

To send all buffer files from Host port 3 to a server at address 193.1.1.241 with the username and password of ftpuser, to the directory **recdir** enter:

SEBUF 3,F,193.1.1.241,ftpuser,ftpuser,\recdir

NOTE: Parameters are case-sensitive.

Using FTP to Receive Files from Another Device

The terminal server supports FTP Client Receive commands. Files can be sent from the FTP server to a terminal server using FTP (File Transfer Protocol) protocol. To do this, you must set parameters in the Set

Network Parameters screen. After the parameters have been specified, you may issue the RCV command with the appropriate parameters.

5. MODEM PORT SETUP

What This Chapter Contains

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

Each unit is shipped with factory defaults for the modem(s) installed in the terminal server. If you add or replace a modem with one of a different make or model, you must check the modem port parameters to be sure that they are set correctly for the installed modem. In particular, pay special attention to the modem initialization string. An incorrect modem initialization string can result in many problems. Consult the manual supplied with the modem for detailed information.

- Overview
- How to Display and Set Modem Parameters
- Explanation of Each Parameter

Modem Port Parameters

Display Modem Port Parameters – DM Command

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

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

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

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

Modem Control Strings ( Use '|' for ENTER; '~' for 1 second delay )

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



Ser#9901000131>
```

Set Modem Port Parameters – SM Command

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

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

Field	Function
Modem Number	Select the modem whose settings you wish to change.
Restore Factory Defaults?	Initially No appears on the screen. Press the space bar to toggle to Yes. Select Yes to restore the factory settings. Select No to keep the current settings. The factory default settings are listed in the appendix.
Baud Rate Settings:	
Modem Control Strings	The speed at which the terminal server transmits data to the modem (internal or

Field	Function
	external). An AT modem will not usually establish a session with a remote modem at a speed greater than the speed at which it was set up. The actual speed of the user session is a function of the type of connection that is made between the remote modem and the terminal server modem. Press the space bar until the desired choice is displayed. When the speed you want appears in the field, press Enter key to select that speed and advance to the next parameter. Available baud rates are 300,1200, 2500, 4800, 9600, 19200, 38400 and 57600.
User Session	The speed at which the terminal server communicates with its modem. When a connection is made to a remote modem, the modems negotiate the appropriate speed for the link. After the speed has been determined, a message is sent to the terminal server modem such as "CONNECT 2400" or "CONNECT 9600". Normally, the modem switches to the speed in the message. Some modems, however, (and most modems at some connect speeds) do not indicate the speed with a CONNECT message. In these instances, the speed must be derived some other way. Usually an Auto Baud routine is used to sense the speed of the incoming data. Sometimes it is preferable to force the incoming session at a particular speed. CONNECT **n** sets the speed of the session to the speed in the CONNECT message. If

Field	Function
	CONNECT **n** is chosen, and no CONNECT message is sent to the terminal server modem, it reverts to Auto Baud. Press the space bar until the desired choice is displayed. When the speed you want appears in the field, press the Enter key to select that speed. Speeds available are CONNECT n, 57600, 38400, 19200, 9600, 4800, 2400, 1200, 300 and Auto.
Char. Length/Parity	Use the space bar to select the character length and parity characteristics of the Modem Port. Available entries are 7 or 8 data bits, with Even, Odd, Mark, Space or no parity. The Auto entry initiates an auto-parity routine with the user.
Terminal Emulation	Specify the type of terminal that your computer is emulating when your computer is connected to the Modem Port via a remote modem. Press the space bar to toggle between TTY and VT100. If your computer is emulating a DEC VT-100 terminal, select VT100. If your computer is *not* emulating a DEC VT-100 terminal, select TTY. After you make your selection, press the Enter key. ***NOTE: Only Sysop sessions are affected.***
Sysop Idle Timer	The Sysop idle timer defines the maximum duration of inactivity time during a Sysop session before the call is terminated and the modem is reset.

Field	Function
	Press the space bar until the desired choice is displayed. When your choice appears in the field, press Enter key to make your selection. Available selections are 1 min, 5 min, 10 min, 20 min and none.
Host Session Idle Timer	The Host Session idle timer defines the maximum duration of inactivity time during a Host session before the call is terminated and the modem is reset. Press the space bar until the desired choice is displayed. When your choice appears in the field, press the Enter key to make your selection and advance to the next parameter. Available selections are 1 min, 5 min, 10 min, 20 min, none.
Host Session Disconnect on Ctrl + A	Initially Yes appears on the screen. Press the space bar to toggle to No.
Setup	Defines the AT command string used to set up the modem. You may edit this field, depending on your modem requirements. ***NOTE: The factory defaults shown on page 5-2 are specific for the installed modem. If the terminal server includes a modem of a different make or model, a different command string is required. Consult the modem manual to determine the appropriate command string.***
Answer	Defines the AT Command string used to answer calls. This should be either ATA

Field	Function
	(answer immediately) or left blank. ATS0=n (answer on the nth ring) can be included in the setup initialization, however, the default ATA is recommended.
Hangup	Defines the sequence for hanging up the line ~+++~AT|~ATS0=0 H0| where ~+++~ escape sequence ATS0=0 disables auto answer ATH forces modem on-hook hang up
Dial Strings *Modem*	The command string used to initiate a dial-out sequence with the modem. This is typically used as part of a Callback authentication process or to deliver an alarm. *Example:* **ATDT ### |** The default phone number will be substituted for the ### characters.
Dial Strings *Pager*	This command string specifies the dial string used by the modem to deliver a message to the pager. *Example:* **ATDT ### @ MSG ; |** The default pager number from the System Parameter table will be substituted for the ### characters and the default pager message will be substituted for MSG. Press **Enter** key to confirm your entry.

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

Verifying the Settings

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

- Dial into the terminal server to verify that you can access it. Log on as a Master user. If you cannot dial in, check the modem port settings.
- Check that the terminal server can dial out. Add an Action Item PHONHOME that is issued when a particular event is generated. Generate the event by using the GE command. (See Chapter 1 for more information on Action Tables and Action Items.) Have the terminal server dial a PC running a terminal emulation program. If the connection is successful, the date, time, site name, alarm and event comment is displayed on the screen.

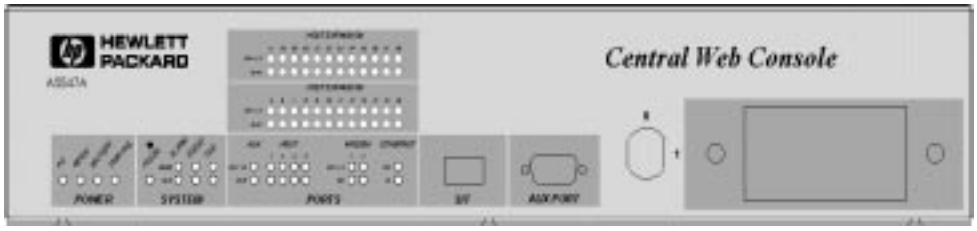
6. TROUBLESHOOTING

What this Chapter Contains

- Checking the Status of the LEDs
- Determining Network Status
- Querying Remote Devices
- Reboot the Terminal Server
- Reinitializing the Terminal Server
- Working with Configuration Files
- CONFIG Command Instructions
- DUMPF Command Instructions

Checking the Status of the LEDs

The following figure shows the status LEDs, all are visible from the front of the terminal server.



The following table lists the terminal server LEDs and explains the state or condition of the terminal server or its components when the LED is on or off. In addition to the conditions listed in the OFF column, all of the LEDs will be off when power to the terminal server is turned off.

LED	Term. Server condition, LED is on	Term. Server condition, LED is off
AC (green)	16V DC supply unit is operating.	Main power has failed; internal battery is supplying power to the unit. PWR FAIL LED is on.
48VDC	*Not in use with this version of the Central Web Console.*	
BATTERY (green)	Internal battery is charging.	Internal battery is charged.
PWR FAIL (red)	Main power has failed; internal battery is supplying power to the unit.	Main power supply unit is operating.

LED		Term. Server condition, LED is on	Term. Server condition, LED is off
PULSE (green)		Flashes to indicate unit is operating correctly.	Unit is running internal diagnostics (if AC or PWR FAIL LED is on)
ALARM	PEND (red)	Unit is processing an alarm.	Normal condition.
	CLR (green)	Normal operation.	Unit is running internal diagnostics
EVENT	PEND (red)	Unit queuing events (alarms) for processing.	Normal condition.
	CLR (green)	Normal operation.	Unit is running internal diagnostics
FILE	PEND (red)	Data stored on RAMdisk has reached the critical level.	Normal condition.
	CLR (green)	Normal operation.	
AUX	RX/TX (amber)	Unit receiving or transmitting data.	Idle.
	DTR (amber)	Serial device is connected to AUX port and DTR is asserted.	Port is not active or no serial device connected.
HOST n	RX/TX (amber)	Unit receiving or transmitting data.	Idle.
	DTR (amber)	Serial device is connected to Host port.	Host port is not connected to a serial device.
MODEM 1	RX/TX (amber)	Unit receiving or transmitting data.	Idle.
	CD (amber)	Unit is connected to a remote system.	Idle.

LED		Term. Server condition, LED is on	Term. Server condition, LED is off
ETHERNET	RX (amber)	Unit receiving data.	Idle.
	TX (amber)	Unit transmitting data.	Idle.

Determining Network Status

The **DNS** command displays the status of the network. If the network is running, the following message appears:

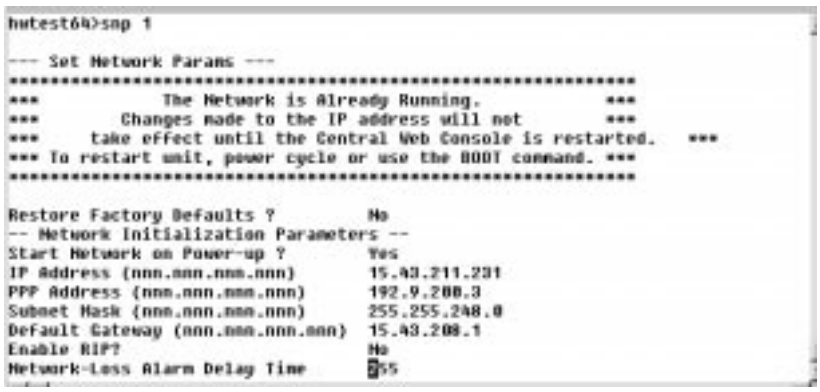
The terminal server determines network status by detecting traffic on the Ethernet link. The user sets the time interval for non-activity, which can range from 1 to 255 seconds. Two alarms indicate network status: if active the .NETUP alarm is issued, if inactive the .NETDOWN alarm is issued.

An attempt at a Telnet connection into the terminal server results in no response if the terminal server or network connection is down. A Sysop session through the AUX port is the only way to restart or communicate with the terminal server at this point.

NOTE: An Alarm/Event action routine must be created for these alarms. Otherwise the unit will receive the alarm but will not know what action to take.

To enter the time interval, type **SNP 1** at the prompt. At the Network-Loss Alarm Delay Time, enter the time interval for non-activity on the network.

An inactivity period longer than the Network-Loss Alarm Delay Time will trigger the alarm .NETDOWN.



Querying Remote Nodes

The Port and Session Control Functions menu includes the **PING** command. The **PING** command is issued to query another device (IP address) on a network.

Syntax: **PING** <Ipaddr>.

Where <Ipaddr> is the IP address of the device

If successful, the reply shows the length of time it took to reach the device. If the ping is unsuccessful, the message is “Device not Reachable.”

Rebooting the Terminal Server

You can restart the terminal server by either using the key switch on the front panel to power-cycle the unit (turn the key to Off then to On – "hard" boot) or by issuing the **BOOT** command from the command prompt – "soft" boot.

Reinitializing the Terminal Server

Use a PC or terminal connected to the AUX port to re-initialize the terminal server. The AUX port must be set at 9600 baud.

Note: This procedure requires that you re-establish your network parameters and rebuild your user database.

1. Reboot the unit.
2. Watch the LEDs carefully. When the Pulse LED lights, wait approximately one-half second and press Enter. The following System LEDs will light: Alarm, Event, and File.
3. Type **INIT**, do not press Enter! You will be asked to confirm system re-initialization, type **YES**. Begin this step within 10 seconds of completing step 2.
4. Re-establish your networking parameters (IP and Ethernet, and FTP addresses).
5. Download the HP.CFG and appropriate configuration files.
6. Configure the terminal server with the HP.CFG file and the appropriate configuration file. See the next section for further information about configuration files.

Working with Configuration Files

Each terminal server has a configuration file that specifies the parameters of the terminal server and determines how the unit operates. This file includes the Action Table, user Action Routines, System Parameters, and Parameters of the AUX, Modem, Host Ports and Text Pager Messages. Configuration files are created online or offline and are saved in ASCII file format with the extension **.cfg*. One file can be used to replicate parameters across multiple terminal servers. Configuration files can be saved to a storage device, saved to the RAMdisk, or printed to a screen.

Note: Issuing the Upgrade command or re-initializing the terminal server destroys all data stored to the RAMdisk.

Creating a Configuration File

Use an editing program such as Notepad or WordPad to edit or create configuration files; these programs can read and write simple ASCII formatted files. Word-processing programs such as Microsoft Word are not suitable for this function; they add formatting characters that destroy the structure of a configuration file.

Importing/Exporting a Configuration File

The File menu contains commands for transferring files between the terminal server and a storage or editing device. In addition, the terminal server supports two other commands: the DUMP command uploads a file to the screen or a storage device, DUMPF downloads a file to the RAMdisk.

CONFIG Command Instructions

Overview

A configuration file may be sent to the terminal server from a PC or to a PC from the terminal server. The **CONFIG** command imports a configuration file, and the **DUMP** command exports configuration data to a file. The CONFIG command allows a user to import a configuration into an terminal server with a direct connect via the AUX port, over phone lines, or via the network port.

1. Log onto the terminal server as a Master User.
2. Download the configuration file to the RAMdisk using XModem transfer.

3. To configure the terminal server, type **CONFIG *filename*** at the system prompt and press Enter.

```
Site123> RCV TEST.CFG

--- Receive File ---
Receiving XMODEM - File: \TEST.CFG
CCCC
-- Receive Complete --

03/01/99 11:51:16 E2E3 [AUX] File \TEST.CFG: Receive Complete
Ser123>CONFIG TEST.CFG

--- Upload Configuration Details ---
Begin SYSPARS
End   SYSPARS

; Disk Parameters

Begin SYSPARS
End   SYSPARS
Begin ACTROUT
End   ACTROUT

03/01/99 11:51:41 8601 [AUX] Upload Configuration Details - O.K.
Site123>
```

This section describes the different ways in which a terminal server's configuration can be "dumped" into a text file. The DUMP command allows the user to view or backup the configuration of an terminal server with a direct connection via the AUX port, over phone lines or via the network port.

Procedure for Viewing Configuration Data at the Terminal Screen

1. Log onto the terminal server as a Master User.
2. Type **DUMP** and press the ENTER key.

   The banner `Dump Configuration Details` appears, and a list of system tables and system parameters displays. View one or more of

the tables and parameters, press Crtl+x to clear the line and enter the characters for the parameters of choice and press 'ENTER'.

3. The banner "Press ENTER when ready to receive Configuration Dump (CTRL+A to Abort)" will appear. Pressing ENTER "DUMPs" the selected configuration to the screen for viewing.

Procedure for Saving the Configuration Data on the PC

1. Log onto the terminal server as a Master User.
2. Type **DUMP** and press the ENTER key.

   The banner `Dump Configuration Details` appears, and a list of system tables and system parameters displays. View one or more of the tables and parameters, press Crtl+x to clear the line and enter the characters for the parameters of choice and press 'ENTER'.

3. **The banner "Press ENTER when ready to receive Configuration Dump (CTRL+A to Abort)" will appear. *DO NOT PRESS THE ENTER KEY. Instead, use the communications program XModem transfer process to receive the configuration file from the terminal server. The 'ENTER' will be sent by the communication package and the CONFIG will be saved on the PC as the filename selected and in the specified directory.***
4. To verify that the file was saved correctly, open the file with a text editor such as "Notepad" or "Wordpad". The file should appear to have appropriate programming structure (Look for extraneous characters) and be terminated with the word "END".

DUMPF Command Instructions

Overview

The DUMPF command is identical to the DUMP command except DUMPF copies the configuration to the RAMdisk of a terminal server.

1. Log onto the terminal server as a Master User.
2. Type in the command **DUMPF** and press the ENTER key.

   At this point the banner `Dump Configuration Details to File` and the prompt `File name` will appear.
3. Enter a file name at the `File Name` prompt and press the ENTER key to see a list of the system tables and system parameters. Select all or part of the configuration and press ENTER key to save the file to the RAMdisk.
4. The transfer will take only a few seconds. To verify the transfer was successful, type '**VIEW** *filename*' at the system prompt.
5. To ensure the file was saved correctly on the "RAMdisk," enter the command **DIR** to display the directory and press the ENTER key.

```
Site123>DUMPF

---  Dump Config. Details to File ---

File name:    AAA.CFG
Dump List     ATAB
; Action Table
7 record(s) DUMPed to file ASG.CFG.

03/01/99 12:55:25 E9D8 [AUX] DUMP: ATAB
03/01/99 12:55:25 7C30 [AUX] DUMP: Complete
Site123>
```

Now it is possible to XMODEM or FTP the information to your PC by using the SEND command to transfer the configuration file.

Default Port Parameters

AUX Port Parameters

Baud Rate	9600
Char. Length / Parity	8 / None
Terminal Emulation	TTY
Default Access Class	Master
Output While Port Idle	Log Data
Sysop Idle Timer	None
Host Session Idle Timer	None
Host Session Disconnect on Ctrl+A	Yes

Modem Port Parameters

Modem Number	1
Baud Rate Settings:	
Modem Control Strings	19200
User Session	CONNECT n
Char. Length / Parity	8 / None
Terminal Emulation	TTY
Sysop Idle Timer	None
Host Session Idle Timer	None
Host Session Disconnect on Ctrl+A	Yes
Modem Control Strings (Use '|' for	ENTER; '~' for 1 second delay)
Setup	|~AT &F E0 &C1 &D2 S0=0|
Setup (continued)	
Answer	ATA|
Hang Up	~+++~AT|~ATS0=0 H0|
Dial Strings (Use '###' for Phone No.,	'MSG' for Pager Message)
Modem	ATDT ###|
Pager	ATDT ### @ MSG ;|

Host Port Parameters

Host Port Number	1
Restore Factory Defaults?	No
-- Host 1:	
Host Name	HOST1
Baud Rate Setting	9600
Character Length / Parity	8 / None
Alarm Filter	None
Force CD/DSR High	Yes
Flow Control	None
-- Automatic Buffering --	
Enable Automatic Buffering?	No
Compress closed buffer files?	No
Auto Switch: (Enter 0 to disable)	
When CURRENT File exceeds 'n' KB	50
Every 'n' Hours	24
Synchronize at what hour (0-23)	0

7. ACTION AND EVENT TABLES

What this Chapter Contains

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

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

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

Working with Action Tables

To send messages based on alarms generated by a HP Server or other serial device, an Action Table must be created in the terminal server. The terminal server compares all alarm messages against the alarm list in the Action Table. If a match is found, the associated action is taken.

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

1. The alarms to be monitored.
2. The actions to be taken when an alarm is received.

Structure of an Action Table

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

A typical Action Table is shown below.

```
>CD LA .

--- List Action Items ---

   Alarm:              Routine: Parameters:          Comments:

 1) .BYTESRCVD.1       CANCELAL .NOBYTES.1           Action for port activity
 2) .DAILY             CLKCHECK                      CHECK FOR DAYLIGHT SAVINGS
 3) .DTR1LOW           DOLIST  #NOTIFY               CABLE UNPLUGGED
 4) .FILESENT          TAPPAGE 5926932               NOTIFY JVC FILES GONE
 5) .HOURLY            DOLIST
 6) .HOURLY.1          RXCHECK 1                     CHECKS HOST PORT 1
 7) .HOURLY.2          APP_PC                        MOVE DATA TO POLLDATA.CDR
 8) .NOBYTES.1         LOG   240 DOLIST #NOTIFY      REPORT NO BYTRES IN 4 HOURS
 9) .POWERLOW          DOLIST  #NOTIFY               LOST POWER

-- End of List --
```

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

Alarm

There are three types of alarms/events.

1. Alarms produced by a host (HP Server, etc.) can be listed in the Action Table along with a specified action.
2. The terminal server can generate alarms (or events), by a host user or by a Sysop. Events generated by the terminal server are called internal events. All internal events start with a period (.). Internal events are listed in Chapter 8.
3. Events generated by user Action Routines. They are especially useful for further processing of alarms.

Action Routine

After the terminal server has determined that a match exists between the detected alarm and an entry in the Action Table, it executes the Action Routine listed. The *Action Routine* specifies what action should be taken when a particular event occurs. Each terminal server includes standard Action Routines (see Chapter 8).

Parameters

Action routines typically have parameters associated with them. A parameter may be a phone number, a pager number, or other information used by the Action Routine.

Comments

The comment may give more information about the alarm. With some Action Routines, when the terminal server processes an alarm, the comment is sent along with it.

Alarm Matching Criteria

When the terminal server receives an alarm, it follows a specific procedure when it searches the Action Table for a match to an alarm (event). Three passes are made.

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

2. If the first search fails to turn up a match, it searches for a record describing a range of alarms that includes the alarm it received. Such ranges can be entered into the Action Table to cover a multiple of alarm types.

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

Example:

Three pass lookup on Action Table:

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

Sample Action Table:

Alarm	**Action Routine**	**Parameters**	**Comments**
1.) ERR005	PHONHOME		
2.) ERR000-030	PHONHOME	2	
3.) ERR	PAGE		
4.) .AUTHFAIL	PAGE		
5.) .AUTHFAIL.1	PAGE		

Event:	
ERR000	matches (2)
ERR005	matches (1)
ERR040	matches (3)
.AUTHFAIL	matches (4)
.AUTHFAIL.1	matches (5)

Multiple Actions on a Single Alarm

In some instances you may want more than one action to occur when a single alarm is detected. For instance, a hacking attempt may be reported to two different people. In that case, the DOLIST command is used. The first line gives the general form of the alarm to be used as the trigger. The following lines have the same mnemonic but with an extension which denotes an order of action. In the example given below,

.1 and .2 are added to show two subsequent actions to be taken. When the .AUTHFAIL alarm is detected, the terminal server "phones home" and pages, sending the alarm and the comments.

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

ALARM	ACTION	PARAMETER	COMMENTS
.AUTHFAIL	DOLIST		HACKER ALERT
.AUTHFAIL.1	PHONHOME		
.AUTHFAIL.2	PAGE		

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

Planning the Action Table

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

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

NOTE: You must have at least Sysop 3 level access to add, delete or change Action Table items.

1. Determine which alarm conditions to monitor.

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

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

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

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

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

The reasoning behind this example is that a maintenance center, for instance, will probably want to be alerted to an unsuccessful system reload to check its status. By scheduling the report (PHONHOME) to take place 15 minutes after the event, an unsuccessful reload will be reported because a SYS0000 occurs. A successful reload will *not* be reported because an *INI000* occurs when the SYSLOAD is successful.

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

3. Test the Action Routine.

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

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

Sample: ACTION TABLE WORKSHEET

Alarm, Message, or Internal Event	Action Routine	Routine Parameters
.BATLOW	*DOLIST*	
.BATLOW-1	*PHONHOME*	*2*
.BATLOW-2	*PAGE*	*5551212,1234*
.DAILY	*DOLIST*	
.DAILY-1	*CLKCHECK*	
.DAILY-2	*SETHP*	*3*
.DTRLOW	*PHONHOME*	
.HOURLY	*LOGCHECK*	*50*
BSD090	*PHONHOME*	
INI000	*DOLIST*	
INI000-1	*CANCEL*	*SYS000*
INI000-2	*CLKSET*	
SYS000	*SCHEDULE*	*15 PHONHOME*
.DTRLOW	*PHONHOME*	

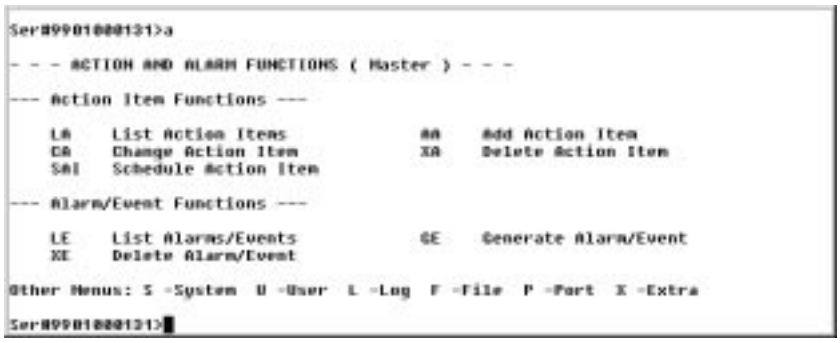
ACTION TABLE WORKSHEET

Alarm, Message, or Internal Event	Action Routine	Routine Parameters

Action Table Commands

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

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



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

Adding an item to the Action Table – AA Command

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

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

Field	Function
Alarm	Enter the alarm issued by the protected device or a terminal server internal event (internal events are listed at the end of this chapter) and press the Enter key.
Routine Parameters	Enter parameters associated with the Action Routine. Enter values for parameters associated with the specified Action Routine. Commas must separate parameters. A comma is not needed at the end of the field. If you want to skip a parameter, place a comma for the parameter and a second one to separate it from the next parameter. For example, to enter the first and third parameters (skip the second parameter), enter two commas in the middle: 1,,3.
Comments	Type any comments you want attached to the event. Then press the Enter key.

The system confirms that you have added an action item by displaying a confirming a log entry and displaying the system prompt.

List Action Items – LA Command

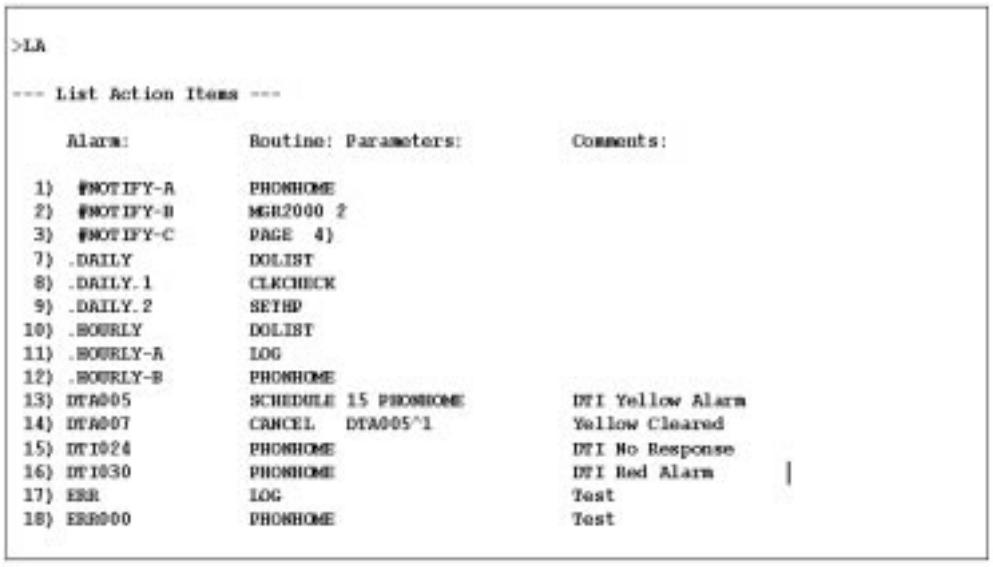
The List Action Items command displays the Action Table, which contains the following information:

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

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

Type **LA** at the system prompt and press the Enter key to display the List Action Items screen. To display only part of the Action Table, enter a modifier for example, **LA BSD** will display all alarms starting with the letters ‘BSD”.

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



```
>LA

--- List Action Items ---

    Alarm:          Routine: Parameters:          Comments:

 1)  #NOTIFY-A      PHONHOME
 2)  #NOTIFY-B      MGR2000 2
 3)  #NOTIFY-C      PAGE  4)
 7) .DAILY          DOLIST
 8) .DAILY.1        CLKCHECK
 9) .DAILY.2        SETHP
10) .HOURLY         DOLIST
11) .HOURLY-A       LOG
12) .HOURLY-B       PHONHOME
13) DTA005          SCHEDULE 15 PHONHOME          DTI Yellow Alarm
14) DTA007          CANCEL   DTA005^1             Yellow Cleared
15) DTI024          PHONHOME                      DTI No Response
16) DTI030          PHONHOME                      DTI Red Alarm
17) ERR             LOG                           Test
18) ERR000          PHONHOME                      Test
```

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

>LA .H

and press the Enter key. Only those action items starting with .H are then displayed.

Change Action Item Command – CA Command

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

```
Site123>CA

--- Change Action Item ---

     Alarm:          Routine: Parameters:          Comments:

  1) .DAILY          PHONHOME 2

Alarm                              .DAILY
Action Routine                     PHONHOME
Routine Parameters                 3
Comment

07/17/97 10:36:30 [A] .DAILY Action item added
07/17/97 10:36:30 [A] .DAILY Action item modified
```

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

>CA .D

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

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

Schedule Action Item – SAI Command

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

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

Continue through the fields by typing in your data and pressing the Enter key. Pressing the Enter key when the cursor is in the Comment field completes the process.

Field	Function
Parameters	Type the parameter, or parameters, that you want to associate with this Action Routine. Press the Enter key to advance the cursor to the next field.
Schedule Date	The day on which you want the Action Routine to activate, where:

today = The Action Routine is scheduled to occur today at the time specified (pressing the Enter key selects this date).

mm/dd/yy = Type the month, day, and year that you want the Action Routine to occur and then press the Enter key.

nn = Type the number of days from today that you want the Action Routine run and then press the Enter key.

Schedule Time — The time of day (using the 24-hour clock format) at which you want the Action Routine to activate, where:

now = The Action Routine will occur immediately (ASAP). Pressing the Enter key selects this time.

hh:mm = Type the time of day, in 24-hour clock format (for example,, 2:00 PM is given as 14:00) at which you want the routine run and then press the Enter key.

nn = Type the number of minutes from now that you want the routine run and then press the Enter key.

Event — If you are simulating a particular Event for testing, type the event here as it would have been received to trigger this action. For example, if you test PHONHOME, this field could be used to signify it is a test. The system defaults to "Sysop Generated".

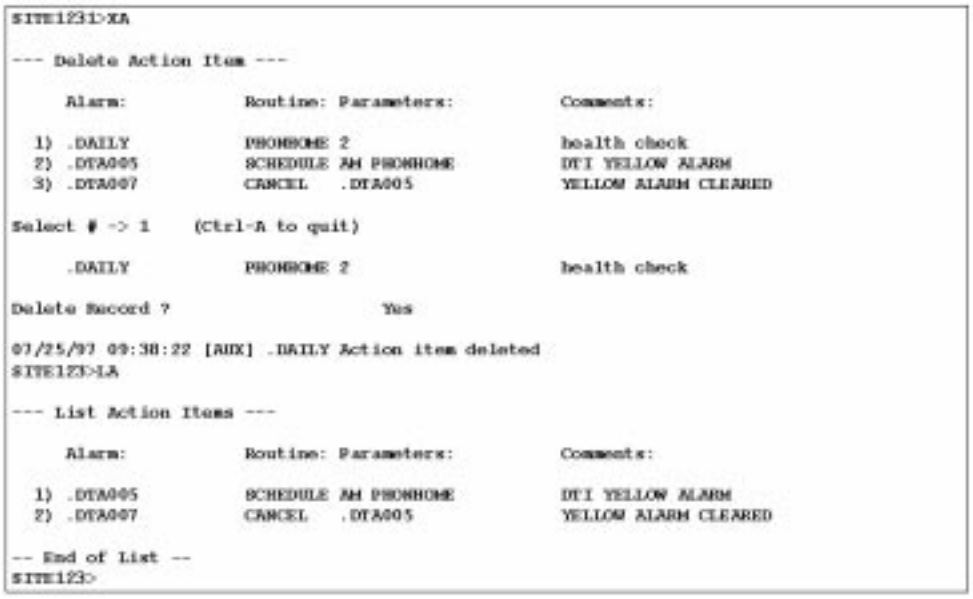
Comment — Type any comments that you want attached to the Event.

Delete Action Item – XA Command

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

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

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



```
SITE1231>XA

--- Delete Action Item ---

     Alarm:          Routine: Parameters:          Comments:

  1) .DAILY          PHONHOME 2                    health check
  2) .DTA005         SCHEDULE AM PHONHOME          DTI YELLOW ALARM
  3) .DTA007         CANCEL   .DTA005              YELLOW ALARM CLEARED

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

     .DAILY          PHONHOME 2                    health check

Delete Record ?                  Yes

07/25/97 09:38:22 [AUX] .DAILY Action item deleted
SITE123>LA

--- List Action Items ---

     Alarm:          Routine: Parameters:          Comments:

  1) .DTA005         SCHEDULE AM PHONHOME          DTI YELLOW ALARM
  2) .DTA007         CANCEL   .DTA005              YELLOW ALARM CLEARED

-- End of List --
SITE123>
```

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

Alarm/Event Functions Commands

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

List Alarms/Events – LE Command

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

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

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

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

>LE .H

and then press the Enter key.

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

Generate Alarm/Event – GE Command

Testing the Action Routine or an alarm is an important part of the process. The SAI command can be used to test an Action Routine. The Generate Alarm/Event command allows you to test any alarm defined in the Action Table. This command generates the Alarm or Event as if the data had been received on the host port or an internal Event had occurred. This command is useful for debugging or modifying Action Tables.

Type **GE** followed by the event that you want the Terminal server to generate. For example, type GE .AUTHFAIL. to generate the event .AUTHFAIL. You can also generate a “long” event-for example,, GE DTA005 1 0020 0031 7.

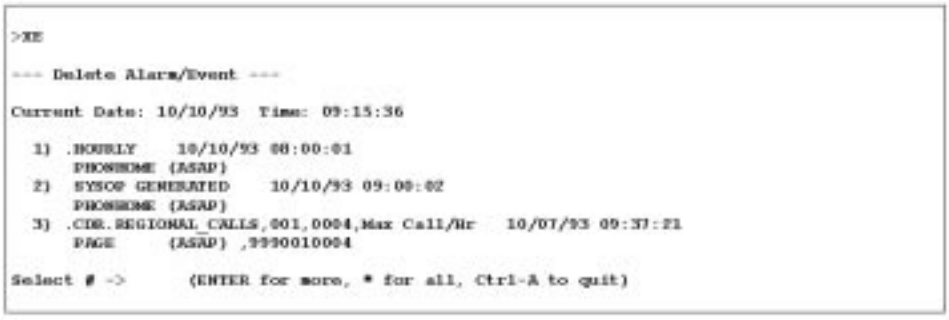
Alternatively, type GE and then enter the alarm/event to be generated at the prompt. Note that “Enter alarm/event” limits the number of characters. If you want to generate a “long” event, use the method described above.

Type the mnemonic for the alarm or event you want to have performed and press the Enter key. The system will confirm that the alarm/event was generated.

Delete Alarm/Event – XE Command

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

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



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

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

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

Internal Alarms and Events

In addition to the alarms generated by the Host or HP server system, the Terminal server supports several internal events. Chapter 8 contains a complete description of each internal event and standard Action Routines and required parameters.

Event	Description
.AUTHFAIL	Event occurs upon receipt of a failed authentication attempt.
.BAT48HIGH	Event occurs when battery voltage crosses over from an OK condition to a high voltage condition. Use the SSA command to specify the upper limit.
.BAT48LOW	Event occurs when battery voltage crosses over from an OK condition to a low voltage condition. Use the SSA command to specify the upper and lower limits.
.BAT48OK	Event occurs when battery changes from a high or low condition to an OK condition. Use the SSA command to specify the upper and lower limits.
.BUFREADY	Event occurs when a buffer file has been closed and is ready to be sent.
.CLKCHANGE	Event indicating that the internal clock of the Terminal server has changed.
.DISKCRIT	Event occurs when the RAMdisk reaches the critical level assigned by the Set Disk Parameters command.

Event	Description
.DISKFULL	Event occurs when the RAMdisk is full. All further attempts to write to the disk will be unsuccessful.
.DTRHIGH.n	Event occurs when the host or HP server asserts DTR (or host cable is connected); for example, DTRHIGH1(indicates the host or HP server on host port number 1 has asserted DTR or the host cable is connected (# indicates host port number).
.DTRLOW.n	Event occurs when the host or HP server stops asserting DTR or the physical connection is lost between Terminal server and the host or HP server (# indicates the host port number).
.HOURLY	Event occurs at the top of each hour.
.INTBATLOW	Event occurs when the internal battery status has been changed from OK to Low. A “low” battery status indicates that the voltage is less than 11 volts.
.INTBATOK	Event occurs when the internal battery status has been changed from Low to OK. For the .INTBATOK event to be generated, the voltage must go from <11 volts to above 11.5 volts.
.LOGFULL	Created by LOGCHECK. Event occurs automatically when the internal Log Buffer is full.
.MAXRETRY	Generated by PHONHOME, PHIRIS, PHSYSOP, or PAGE according to Max.Retries system parameter.
.MDMINITERR	Event indicating a modem initialization error.

Event	Description
.MEMLOW	Event occurs on the hour if less than 4 KB are available in the Terminal server variable area.
.MONTHLY	Event occurs once a month.
.NETDOWN	Event occurs after a preset length of time during which no network activity is detected.
.NETUP	Event occurs when network activity is detected following a period of inactivity.
.POWERUP	Event occurs when the system is powered up.
.PPPREQ	Event to trigger the dial-on-demand PPP link.
.POWERLOW	Event indicating that the external power supply has changed from OK to low.
.POWEROK	Event indicating that the external power supply has changed from low to OK.
.RTSHIGH.n	Event indicating that the RS-232 signal RTS has changed from Low to High. (# indicates host port number)
.RTSLOW.n	Event indicating that the RS-232 signal RTS has changed from High to Low. (# indicates host port number).
.S#HIGH	Event indicating that the 5 volt sensor has been changed from OK to High.
.S#LOW	Event indicating that the 5 volt sensor has been changed from OK to Low.

Event	Description
.S#OK	Event indicating that the 5 volt sensor has been changed from Low or High to OK.
.WEEKLY	Event occurs once a week, each Sunday at midnight.

Action Routines

The Terminal server is pre-programmed with a number of Action Routines that can be used when alarms or internal events occur.

Action Routine	Description
AUXCC	Not supported in this version of software.
CANCEL	Cancels a pending action.
CLKAHEAD\CLKBACK*	Advances (or sets back) the time setting in Terminal server by 1 hour and schedules CLKSET for immediate execution.
CLKCHECK	Checks if current date is the first Sunday in April or last Sunday in October. If it is, schedules either a CLKAHEAD or CLKBACK to occur at 2:00 am.
DOLIST	Causes a list of Action Routines to be performed.
LOG	Creates a log entry that describes the event.
LOGCHECK	Checks to see if the Log buffer has reached a specified threshold. If Log has exceeded the threshold, a .LOGFULL event is generated.
NOACTION	Creates "Event: " Log entry.
PAGE	Calls a pager number and delivers a message.
PHIRIS	Delivers an alarm message to IRIS[SM]. Not supported in this version of software.

Action Routine	Description
PHONHOME	Places a call to the maintenance-reporting center.
PHM2000	Not supported in this version of software.
PHPPP	Initiates a demand-dial PPP link
PHSYSOP	Places a call to the maintenance center and starts a Sysop session.
REMINIT	Performs the Remote Initialization function.
RUNM2000	Not supported in this version of software.
SCHEDULE	Schedules an action for a later time.
SETHP	Changes the setting of the Host Processing Flag. (see SHP system function command).
SNMPTRAP	Sends an SNMP trap to remote managers through the Ethernet or PPP link.

* Hidden routines (These routines are not offered by pressing the space bar, but is valid if entered manually)

8. ACTION AND EVENT ROUTINES

What This Chapter Contains

The Terminal server can be programmed to respond to a particular event or trigger. There are two types of events: Internal and External. An internal event is generated by the Terminal server automatically in response to a particular condition, such as a failed authentication attempt or a low battery. An external event is an alarm received from a device connected to the Terminal server. Internal events are listed in this chapter. The user defines all external events and the format must be as for internal events.

The action that the Terminal server initiates in response to an event is specified by the Action Routine associated with that event in the Action Table. A set of Action Routines is included with the Terminal server. A description and an example of each Action Routine are included in this chapter.

- Description of Events
- Description of Action Routines

NOTE: To see alarms whenever they occur (even if there is not match in the Action Table), type **LOGE ON** to select LOG Events ON. To revert to normal operation in which alarms are not logged unless they match an entry in the Action Table, type **LOGE OFF**.

Internal Events

.AUTHFAIL Internal Event

The .AUTHFAIL internal event occurs each time there is a failed attempt at authentication during a user logon. The format of this internal event is:

.AUTHFAIL Parameter 1 Parameter 2 Parameter 3

Where:

Parameter 1 **-** authentication failure code (typically used as a parameter associated with the PAGE Action Routine.) The codes for this parameter are listed in Table 10-1.

Parameter 2 **-** User ID

Parameter 3 **-** text description of the reason for the authentication failure.

Note: PassKey is not supported with this version of the Central Web Console.

Code	Description	Code	Description
0010	Invalid User ID	0050	Invalid password #1
0011	Blocked user	0053	Call Back unsuccessful
0012	Wrong time	0054	Invalid password #2
0032	Invalid PassKey response		

.BUFREADY

This alarm is sent when a buffer file is closed and is ready to be sent.

Alarm/Event	Action Routine	Parameters	Comments
.BUFREADY	PAGE	5551212,1234	File ready

.CCLERROR

The .CCLERROR event occurs automatically if the Terminal server detects an error in its internal program, or in a user-written Action Routine. Upon generation of a .CCLERROR event, an entry is made in the Error Log. This can be extracted later using the Display Error Log (**DER**) command.

Although this event is not expected to occur regularly (especially if Action Routines are properly tested), the occurrence of the .CCLERROR event might indicate that the Terminal server is not performing properly and should, therefore, be investigated. To insure proper processing of this event, associate it with a well-tested Action Routine.

Example:

Alarm/Event	Action Routine	Parameters	Comments
.CCLERROR	PHONHOME		

This example uses the default phone number to call the maintenance-reporting center.

.CLKCHANGE

The .CLKCHANGE alarm is generated when the internal clock of the Terminal server has been changed. This alarm could be the result of changing the clock for Daylight Saving Time using the Set Date and Time (**SDT**) command.

Alarm/Event	Action Routine	Parameters	Comments
.CLKCHANGE	SNMPTRAP	1	Clock Reset

.DAILY

This event occurs automatically each day at midnight. This event can also be used to schedule an action for some point later in the day.

Alarm/Event	Action Routine	Parameters	Comments
.DAILY	DOLIST		
.DAILY-1	SCHEDULE	08:00 PHONHOME	
.DAILY-2	CLKCHECK		

In this example, the routine associated with .DAILY-1 performs a daily "check-in" with the maintenance center at 8 AM. Units that do not "check-in" may have a problem that affects their ability to report alarms.

Additionally, the CLKCHECK routine associated with .DAILY-2 checks for a change from standard to daylight savings time at midnight, or vice-versa.

.DISKCRIT

The RAMDISK has reached a critical level assigned in the Set Disk Parameters (**SDP**) menu.

Alarm/Event	Action Routine	Parameters	Comments
.DISKCRIT	DOLIST		
.DISKCRIT-1	PHONHOME		
.DISKCRIT-2	SCHEDULE	30 PHONHOME	

In the example above, the .DISKCRIT alarm results in the a call to the default phone number specified in the system parameters. If the alarm is not canceled, the phone number will be called again in 30 minutes.

.DISKFULL

This alarm is generated when the RAMdisk is full. No additional information can be stored on the disk. If this occurs, data from host ports stored in buffer files will be lost.

Alarm/Event	Action Routine	Parameters	Comments
.DISKFULL	DOLIST		
.DISKFULL-1	PHONHOME		
.DISKFULL-2	SCHEDULE	30 PAGE	

In this example, the .DISKFULL alarm results in a call to the phone number set in the System Parameters (**SSP**) menu. If the alarm is not canceled with 30 minutes, a page is sent to the default pager number.

.DTRHIGH and .DTRLOW

or

.DTRHIGH.n and .DTRLOW.n internal events

where n = host port number

The .DTRLOW event occurs automatically on the high to low transition of the DTR signal on a Host port. The .n indicates the port number. This may be caused by a cable being removed from a port or by the attached equipment being switched off.

The .DTRHIGH event occurs automatically on the low to high transition of this same signal. This can be caused by attaching a cable to a port. These events can be used to detect if the HP server or host has lost power, or if the Terminal server has been disconnected from the maintenance port.

Alarm/Event	Action Routine	Parameters	Comments
.DTRLOW	SCHEDULE	2 PHONHOME	
.DTRHIGH	CANCEL	.DTRLOW	

This example schedules a PHONHOME to report the alarm two minutes after DTR is lost (transitions from high to low). If DTR is re-established (DTR goes high), the .DTRHIGH alarm occurs and cancels the action PHONHOME Action Routine. Since no port number is specified, this event will occur when DTR is lost on any port.

Alarm/Event	Action Routine	Parameters	Comments
.DTRLOW.1	PHONHOME		

This example initiates a PHONHOME if the Data Terminal Ready (DTR) signal is lost only on host port 1.

.HOURLY

This event occurs automatically at the beginning of each hour (for example, 1:00, 2:00, 3:00, etc.). Actions assigned to this event are performed every hour on the hour.

Alarm/Event	Action Routine	Parameters	Comments
.HOURLY	LOGCHECK		

This example checks if the log buffer is approaching its limit. If that is the case, the internal event .LOGFULL is generated.

.INTBATLOW

The status of the internal battery has changed from OK to low.

Alarm/Event	Action Routine	Parameters	Comments
.INTBATLOW	PHONHOME		

In this example, the PHONHOME Action Routine is initiated when the internal battery is low. After the alarm is received, a technician may be sent to the site.

.INTBATOK

The .INTBATOK alarm is generated when the status of the internal battery changes from low to OK. This indicates that the internal battery has been recharged or replaced.

Alarm/Event	Action Routine	Parameters	Comments
.INTBATOK	CANCEL	.INTBATLOW	

In the above example, the status of the internal battery has changed from low to OK, resulting in the canceling of the phone call to the maintenance center for the battery low alarm.

.LOGFULL

This event is a result of the LOGCHECK Action Routine when it detects that the LOG has passed a specified capacity threshold. In order for the .LOGFULL event to occur, the LOGCHECK routine must be associated with some regularly occurring event (such as .DAILY or .HOURLY).

Example:

Alarm/Event	Action Routine	Parameters	Comments
.LOGFULL	PHSYSOP	555-4321,3	

This example initiates a call to 555-4321 and then establishes an access class 3 Sysop session. The computer at 555-4321 could be programmed to receive the Site ID, extract the LOG from the Terminal server, and then issue the Clear Log History (**CLH**) command.

.MAXRETRY

This event is generated by PHONHOME, PHSYSOP, or PAGE. It will occur after the value entered for the Max. Retries system parameter is surpassed.

Example:

Alarm/Event	Action Routine	Parameters	Comments
.MAXRETRY	PHONHOME	2	

This example initiates a PHONHOME to Home Phone Number 2, as defined in the System Parameter table, when the maximum retry counter has been exceeded.

.MDMINITERR

This alarm is generated when a modem initialization error occurs.

Alarm/Event	Action Routine	Parameters	Comments
.MDMINITERR	SNMPTRAP	1	Modem error

.MEMLOW

The alarm .MEMLOW is generated on the hour if fewer than 4KB (4096 bytes) are available on the Terminal server variable area.

Example:

Alarm/Event	Action Routine	Parameters	Comments
.MEMLOW	PHONHOME		Memory low

In this example, the Terminal server will call the default number specified in the System Parameters screen when the remaining space on the Terminal server variable area is 4 KB or less.

NOTE: .MEMLOW does not detect low memory on the RAMDISK.

.MONTHLY

This event occurs automatically every month at the designated time.

Example:

Alarm/Event	Action Routine	Parameters	Comments
.MONTHLY	PHSYSOP	555-1234 1	

In the example the Terminal server will, once a month, phone the number specified in the parameters field and initiate an access class 1 Sysop session. The computer at 555-1234 could be programmed to receive the Site ID, request a host session and download the current configuration of the HP server to ensure that maintenance records are up to date.

.NETDOWN and .NETUP

The .NETDOWN alarm is issued after a preset length of time during which no network activity is detected. When network activity is detected, the .NETUP alarm is issued. The determination of network up and down is based on detected traffic on the Ethernet. The time interval for non-activity ranges from 1 to 255 seconds, and can be selected by the user. To do this, enter the **SNP** command and select **option**. At the Network Loss Alarm Delay Time, enter the length of time during which no network activity is detected.

Alarm/Event	Action Routine	Parameters	Comments
.NETDOWN	SCHEDULE	5 PHONHOME	
.NETUP	CANCEL	.NETDOWN	

In this example, the alarm .NETDOWN is generated, the default number specified by the PHONHOME parameter will be called 15 minutes after the .NETDOWN alarm is received. If a .NETUP alarm occurs, the .NETDOWN alarm will be canceled.

.POWERLOW

The .POWERLOW event is generated when the extern power connection has changed from OK to low. In the example below, the .POWERLOW event results in a call to the maintenance center.

Alarm/Event	Action Routine	Parameters	Comments
.POWERLOW	**PHONHOME**	**2**	

.POWEROK

The .POWEROK event is generated when the external power connection of the Terminal server has changed from low to OK. This event can be generated when the power cable to the Terminal server has been reconnected.

Alarm/Event	Action Routine	Parameters	Comments
.POWERLOW	**PHONHOME**	**2**	
.POWEROK-1	CANCEL	.POWERLOW	

In the example above, the .POWEROK event results in the canceling the call to the maintenance center.

.POWERUP

The .POWERUP event occurs automatically whenever the Terminal server is powered up. This might indicate a new installation, recovery from a power loss, or that the unit was moved to a new location.

Example:

Alarm/Event	Action Routine	Parameters	Comments
.POWERUP	PHONHOME		

This example causes the Terminal server to report to the maintenance center that the unit has been reset. If desired, someone can then investigate the reason for the .POWERUP event.

.PPPREQ

This event is triggered when a PPP link is needed to send an SNMP trap or to send a file via FTP. It is usually associated with the phone PPP (PHPPP) Action Routine.

Alarm/Event	Action Routine	Parameters	Comments
.PPPREQ	PHPPP	5551212	Create the PPP link.

The telephone number can be specified directly, or any of the default telephone numbers specified in the system parameters can be referenced. PHPPP assumes that there is no firewall or security on the remote access device. If this is not the case, contact your Hewlett-Packard Service Representative.

.RTSLOW.n
.RTSHIGH.n

The .RTSHIGH event is generated when the RS-232 RTS signal has changed from low to high. The .RTSLOW event occurs from the RS-232 RTS signal has changed from high to low. The .n indicates the port number.

Alarm/Event	Action Routine	Parameters	Comments
.RTSLOW	SCHEDULE	2 PHONHOME	
.RTSHIGH	CANCEL	.RTSLOW	

This example schedules a PHONHOME to report the alarm two minutes after RTS is lost (transitions from high to low). If RTS is re-established (RTS goes high), the .RTSHIGH alarm occurs and cancels the action PHONHOME Action Routine. Since no port number is specified, this event will occur when RTS is lost on any port.

Alarm/Event	Action Routine	Parameters	Comments
.RTSLOW.2	PHONHOME		

This example initiates a PHONHOME if the Ready to Transmit signal (RTS) is lost only on host port 2.

.WEEKLY

This event occurs automatically every week on Sunday evening at midnight.

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.WEEKLY	DOLIST		
.WEEKLY.2	SCHEDULE	1 08:00 PHONHOME	
.WEEKLY.3	SCHEDULE	5 08:00 PHONHOME	

This example schedules a "check-in" with the maintenance center on Monday, and Friday of each week at 8:00 AM.

Action Routines

CANCEL

This Action Routine cancels a scheduled action corresponding to a particular event containing particular parameters. When multiple pending events can be canceled, the one first into the queue is canceled.

Format: CANCEL

Resource Required: None

Parameters: *ASSOCIATED EVENT*, *1st Match Parameter, 2nd Match Parameter,…Nth Match parameter*

Associated Event: Event mnemonic of the event to be canceled.

Parameters to be matched against Event: As many parameters as necessary may be specified. The position of a parameter represents the position in the event to be matched. Blank parameters are "wild cards ". Parameters are separated by commas.

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.DTRLOW	CANCEL	.DTRHIGH	

This example will cancel the action associated with the event .DTRLOW.

Alarm/Event	Action Routine	Parameters	Comments
DTA007	CANCEL	DTA005, , ^2	

This example will cancel the action associated with event DTA005 if the second parameter in the DTA007 message is equal to the second parameter in the message associated with this action.

Alarm/Event	Action Routine	Parameters	Comments
DTA007	CANCEL	DTA005, , ,87	

This example will cancel the action associated with event "DTA007" if the third parameter in the DTA007 message equals 87.

CLKAHEAD and CLKBACK Action Routines

The CLKAHEAD Action Routine advances the Terminal server time by one hour.
The CLKBACK Action Routine sets the Terminal server time back by one hour.

CLKCHECK Action Routine

The CLKCHECK Action Routine checks to see if the current date is equal to the first Sunday in April or the last Sunday in October. If it is case, the Terminal server will schedule a CLKAHEAD or CLKBACK routine for 2 am.

Attaching this Action Routine to the event .DAILY will take care of standard-to-daylight and daylight-to-standard conversion.

Format: CLKCHECK

Resource Required: None

Parameters: None

Example:

Alarm/Event	Action Routine	Parameters	Comments
.DAILY	CLKCHECK		

DOLIST Action Routine

The DOLIST Action Routine causes a list of actions to be performed. The Terminal server scans the Action Table looking for event mnemonics that match or partially match parameter one.

Format: DOLIST *Name of list*

Parameters: *name of list*

The parameter is an alarm match string that is used as a criterion to search the action table for actions to be performed. If it is omitted, then the instigating event, itself, is used as the match criterion.

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.WEEKLY	DOLIST	.OOPS	

This example, on a weekly basis, performs all actions relating to events that begin with the event .OOPS.

Alarm/Event	Action Routine	Parameters	Comments
.DAILY	DOLIST		

This example performs all actions whose events match the instigating event. In the example, if the Action Table contains entries for .DAILY-1 .. .DAILY-XX, then the actions associated with those events will be performed.

LOG Action Routine

The LOG Action Routine creates a log entry describing the event. The Terminal server takes no further action.

Format: LOG

Resource Required: None

Parameters: None

Example:

Alarm/Event	Action Routine	Parameters	Comments
.CDR.AREA1	LOG		

This example logs the event .CDR.AREA1 into the terminal server log-history file.

LOGCHECK Action Routine

The LOGCHECK Action Routine checks to see if the log buffer has reached a specified threshold. If the log has exceeded this threshold then the event .LOGFULL is generated.

Format: LOGCHECK

Parameters: Percent full threshold (Default is 80)

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.DAILY	LOGCHECK		

In this example, the log buffer is checked to see if its threshold of 80% has been exceeded.

Alarm/Event	Action Routine	Parameters	Comments
.DAILY	LOGCHECK	50	

This example checks if the log buffer has exceeded a threshold of 50%.

NOTE: The event itself (.DAILY in this example) will generate log data, thereby tending to fill the log.

NOACTION Action Routine

The NOACTION Action Routine creates an "Event: " log entry, but otherwise does nothing.

Example:

Alarm/Event	Action Routine	Parameters	Comments
.LOGI	NOACTION		

PAGE Action Routine

The PAGE Action Routine calls a numeric pager (beeper) and delivers a numeric message.

Format: PAGE *PAGER PHONE NUMBER, Message*

Resource Required: Modem

Parameters: *phone number, message*

- **Pager Phone Number -** Phone number of pager (optional)
- **Message -** Message to be delivered (optional)

If either parameter is omitted, the default value (system parameter) will be used. Pager dialing and message delivery are controlled via the Pager Dial String (modem parameter). Refer to the Set Modem Port Parameters (SM) Command ("Modem Port Parameters" in Chapter 5).

NOTE: "@" waits for 5 seconds of silence before transmitting. If your pager system will not support this, modify the string to use

commas (fixed delay period) instead. When setting up for the "PAGE" action routine or setting up a user for pager authentication, the Terminal server uses the modem pager template in the modem parameters section. Issue a "SM command" and change the Pager command. The correct settings depend on the pager type and the delays from that particular site. Some specific examples:

Straight numeric pager
ATDT ### @ MSG ;|
or
ATDT ###,,,,, MSG ;|

Skytel pager with direct 1800 number access:
ATDT ### ,,,,,1#,MSG##;|

Skytel digital pager without direct 1800 access:
ATDT 18007597243,,,,,###,#MSG## ;|

Skytel text pager with direct 1800 access, but need a 9 to get an outside line:
ATDT 9,###,,,,,1#,MSG## ;|

> *The way to determine the correct number of commas needed is to dial the number manually. Count how many seconds it takes for the pager service to answer, and how many seconds until the pager system drops the call if nothing is entered. Split the difference and figure the correct number of commas when the comma is set to 2-second intervals. For example, if the counts are 7 seconds, and 12 seconds respectively, set the commas for 9.5 seconds, round up to 10 seconds, and divide by 2 seconds/comma = 5 (five commas).*

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.AUTHFAIL	PAGE		

This example calls a pager at the default number, when an authorization failure occurs, and delivers the default message to the pager.

Alarm/Event	Action Routine	Parameters	Comments
.BAT48LOW	PAGE	5551324,9990001	

This example calls a pager at the number 555-1324 and delivers the message "9990001" when the battery voltage falls below the set limit.

PHONHOME Action Routine

The PHONHOME Action Routine places a call to a specified number and delivers a Terminal server alarm message when the call is complete.

Format: PHONHOME

Resource Required: Modem

Parameters: *phone number*

1 to 3 - For home phone number 1, 2, or 3 (from system parameters**)**
or
Phone Number to call - Phone number to call. If omitted, Home Phone Number 1 is used.

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.HOURLY-2	PHONHOME		

This example calls Home Phone Number 1 (default) when the .HOURLY-2 internal event occurs.

Alarm/Event	Action Routine	Parameters	Comments
DTI030	PHONHOME	7324944440	TRUNK DOWN

This example places a call to phone number (732) 494-4440 when the external event DTI030 occurs.

PHPPP Action Routine

The PHPPP Action Routine initiates a demand-dial PPP link.

Format: PHPPP

Resource required: Modem

Parameters: *phone number*

1 - Phone number to dial (1, 2, or 3 are home numbers).

Example:

Alarm/Event	Action Routine	Parameters	Comments
.PPPREQ	PHPPP	5551212	

The PHPPP establishes a PPP link to a remote network. The TCP/IP applications can then be executed.

PHSYSOP Action Routine

The PHSYSOP Action Routine is the same as PHONHOME except at the end of the report, the remote terminal is placed in a Sysop session as user MDM_Default.

Format: PHYSOP *PHONE NUMBER TO CALL*

Resource Required: Modem

Parameters: *phone number, access class*

1 to 3 - For home phone number 1, 2, or 3 (from system parameters)
or
Phone Number to call - Phone number to call. If omitted, Home Phone Number 1 is used.
Access class of Sysop session - Defaults to 3 (Sysop3). May be specified as 1 (Sysop 1), 2 (Sysop 2), 3 (Sysop 3), or 4 (Master).

Examples:

Alarm/Event	Action Routine	Parameters	Comments
.MAXRETRY	PHSYSOP	5551212, 2	

This example telephones the Sysop at 555-1212 and places the terminal in a Level 2 Sysop session when the .MAXRETRY internal event occurs.

Alarm/Event	Action Routine	Parameters	Comments
DTI030	PHSYSOP	3,1	

This example phones the Sysop at Phone Home Number 3 and places the terminal in a Level 1 Sysop session when the DTI030 external event occurs.

SCHEDULE Action Routine

The SCHEDULE Action Routine schedules another Action Routine to be performed now, or at some later date or time.

Format: SCHEDULE

Resource Required: None

Parameters: Date or Time:

- **Date or "AM"** (optional) - Either a date in the format mm/dd/yy, or a number of days from today. If specified as a number of days, the Time parameter must also be included.

  If "AM" is specified, and the current time is greater than the "Start of Overnight Period" in the system parameters, the call is scheduled for the "AM Report Time." If the current time is between the AM Report Time and the Start of Overnight Period, then the action is scheduled for now.

  If "AM" is specified, omit the Time parameter.

  If Date is omitted, action is scheduled for this day.

- **Time** (optional)

  Either a time in the format hh:mm, or a number of minutes from the current time.

Event associated with action to be scheduled: - Name of Action Routine to be scheduled.

Action Routine Parameters: - Parameters to be passed to scheduled Action Routine.

Examples:

Alarm/Event	Action Routine	Parameters	Comments
CED063	SCHEDULE	AM PHONHOME	

This example schedules a PHONHOME for now or the next AM report when the external event CED063 occurs.

Alarm/Event	Action Routine	Parameters	Comments
CED063	SCHEDULE	15 PHONHOME 5551212	

This example schedules a PHONHOME to telephone number 555-1212 for 15 minutes from now.

Alarm/Event	Action Routine	Parameters	Comments
CED063	SCHEDULE	23:00 SETHP 3	

This example sets the Host Processing Flag to 3 at 11 PM tonight.

Alarm/Event	Action Routine	Parameters	Comments
CED063	SCHEDULE	2 0 PHYSYSOP 2,3	

This example schedules a PHONHOME for this time two days from now using Phone Home Number 2, and then establishes a Level 3 Sysop session.

Alarm/Event	Action Routine	Parameters	Comments
CED063	SCHEDULE	07/01/96 12:00 PHONHOME	

This example schedules a PHONHOME for 12:00 on July 1, 1996.

Alarm/Event	Action Routine	Parameters	Comments
CED063	SCHEDULE	1 18:00 DOLIST.SPECIAL	

This example schedules a DOLIST for 6 PM tomorrow.

SETHP Action Routine

The SETHP Action Routine changes the setting of the Host Processing Flag.

Format: SETHP *PROCESSING FLAG VALUE*

Resource Required: None

Parameters: **Host Processing Flag Value -** 1, 2, 3, or 5

Example:

Alarm/Event	Action Routine	Parameters	Comments
.CCLERROR	SETHP	**3**	

This example disables all Action Routines, including those of the Terminal server.

SNMPTRAP

Sends an SNMP trap to remote managers through the Ethernet or PPP link.

Parameters

1 - Sets trap level (1-10) This parameter is the enterprise specific trap ID and depends on the trap format (Nortel or Standard).

Example:

Alarm/Event	Action Routine	Parameters	Comments
ERRORA21	SNMPTRAP	3	

GLOSSARY OF COMMAND REFERENCES

Action And Alarm Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
AA	Add action item	Master, Sysop 3
CA	Change action item	Master, Sysop3
GE	Generate event	Master, Sysop 3
LA	List action items	All Sysop levels
LE	List events	All Sysop levels
SAI	Schedule action item	Master, Sysop 3, Sysop 2
XA	Delete action item	Master, Sysop 3
XE	Delete event	Master, Sysop 3, Sysop 2

System Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
DCC	Display contact inputs	All Sysop levels
DCCA/DCCB/ DCCC	Display contact inputs for extended banks	Master, Sysop 3
DSA	Display sensor alarms	All Sysop levels
DSI	Display sensor inputs	All Sysop levels
DSP	Display system parameters	All Sysop levels
RRLY	Reset relays	Master, Sysop 3
SDT	Set date and time	Master, Sysop 3

SHP	Set host processing flag	Master, Sysop 3
SRLY	Set relays	Master, Sysop 3
SSA	Set sensor alarms	All Sysop levels
SSP	Set system parameters	Master, Sysop 3

User Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
AU	Add users	Master
CU	Change users	Master, Sysop 3, Sysop 2
DU	Display users	Master, Sysop 3, Sysop 2
LU	List users	Master, Sysop 3, Sysop 2
XU	Delete users	Master

Log Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
AH	Access history	All Sysop levels
CER	Clear error log	Master
CLH	Clear log history	Master
DER	Display error log	All Sysop levels
FH	Display failure history	All Sysop levels
LH	Display log history	All Sysop levels

File Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
CD	Change directory	Master, Sysop 3
COMP	Compress a file	Master
COPY	Copy a file	Master
DDP	Display disk parameters	Master, Sysop 3
DEL	Delete a file	Master
DIR	List files in directory	Master
MD	Make a directory	Master
MOVE	Move a file	Master
RCV	Receive a file	Master
RD	Remove a directory	Master, Sysop 3
REN	Rename a file	Master
SDP	Set disk parameters	Master
SEND	Sends a file to another device	Master
UCOMP	Uncompress a file	Master
VIEW	View a file	Master

Buffer Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
BST	Display host buffer details	Master, Sysop 3
CLBUF	Close buffer file	Master
OBST	Open buffer status	Master
OPBUF	Open host buffer file	Master
SEBUF	Send all buffer files to another device	Master
SWBUF	Switch buffer files	Master

Session Control Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
CON	Connect to port	All Sysop levels
DIS	Disconnect from S2K	All Sysop levels
JS	Join host session	All Sysop levels
VS	View host session	All Sysop levels
VT	VT100 on and off`	All Sysop levels

Port Control Functions

COMMAND	DESCRIPTION	ACCESS LEVELS
DA/DM/DH/DT	Display AUX/Modem/Host/Telnet port parameters	
DNP	Display network parameters	All Sysop levels
DNS	Display network status	All Sysop levels
DPS	Display port signals	All Sysop levels
PING	Query remote device	Master
PPP	Start PPP session	All Sysop levels
PST	Port status	All Sysop levels
RES	Reset port	All Sysop levels
SA/SM/SH/ST	Set AUX/Modem/Host/Telnet port parameters	
SNP	Set network parameters	Master
STARTNET	Start up the network	Master

INDEX

A

B

C

D

E

F

G

I

L

M

N

P

R

S

U

V

X