

TOTAL CONTROL™

**Total Control
Manager/SNMP**

SOFTWARE GUIDE



© 1996 by U.S. Robotics Access Corp.
8100 North McCormick Blvd.
Skokie, IL 60076-2999
All Rights Reserved

U.S. Robotics and the USRobotics logo are registered trademarks of U.S. Robotics Access Corp. Total Control and Total Control Enterprise Network Hub are trademarks of U.S. Robotics Access Corp. Any trademarks, tradenames, service marks or service names owned or registered by any other company and used in this manual are the property of their respective companies.

Table of Contents

What's New in this Release	vi
Chapter 1 About this Guide	1-1
Software Overview	1-1
Preliminary Considerations	1-1
Documentation Scope.....	1-2
Contents.....	1-2
Common Terms	1-3
Chapter 2 System Components	2-1
Hardware Requirements.....	2-1
Minimum.....	2-1
Recommended.....	2-1
Software Requirements	2-2
Chapter 3 Installing the Software	3-1
Preliminary Steps.....	3-1
DOS Preparation	3-2
Software Installation.....	3-2
To Install NetWare Management System	3-2
To Install <i>Total Control Manage/SNMP</i>	3-4
Installing Added-Cost Options	3-4
Security ODBC Installation	3-5
Installation Adjustments.....	3-6
Removing Novell Prompts.....	3-6
Editing SYSTEM.INI.....	3-6
Change Required for Accounting/Event Logging	3-8
Change Required for Security.....	3-8
Software Installation Tips and Troubleshooting.....	3-9
Uninstalling NMS and TCM.....	3-11
Customizing the NET.CFG File.....	3-12
Sample NET.CFG Files.....	3-13
SLIP_C1.CFG.....	3-13
SLIP_C2.CFG.....	3-14
Ethernet NET.CFG	3-15
Token Ring NET.CFG.....	3-16

Loading Network Drivers	3-16
SLIP Connection Example	3-17
Ethernet Connection Example	3-17
Token Ring Connection Example	3-17
Unloading Drivers	3-18
Testing Connectivity	3-18
Loading <i>Total Control Manager/SNMP</i>	3-19
Chapter 4 Conducting the First Session	4-1
Adding the Chassis to the Database	4-1
Viewing the Virtual Front Panel Display	4-6
Making a Selection	4-8
Feature Enable	4-9
Chapter 5 Saving a Chassis Definition/Configuration	5-1
Chassis Definition	5-1
Modify and Delete	5-2
Chassis Configuration	5-2
To Save the Configuration for all Objects in a Chassis	5-2
To Restore the Configuration for all Objects in a Chassis	5-4
Chapter 6 Configuring Installed Cards	6-1
Using the Configuration Window	6-2
Setting Parameters	6-5
Loading a Configuration	6-7
Downloading Card-Specific Software	6-8
Chapter 7 Viewing Statistics	7-1
Verifying Object Status	7-1
Monitoring Performance	7-2
Chapter 8 Configuring Traps/Alarms	8-1
Traps	8-1
Alarms	8-4
Chapter 9 Sending Commands to Installed Cards	9-1
To Execute a Command	9-1
Available Commands	9-3
Chapter 10 Using NMS Tools	10-1
Creating Network Maps	10-1
Configuring Alarms	10-3
Compiling MIB Files	10-7
Using the MIB Browser	10-7

Chapter 11 Testing	11-1
Tone Tests.....	11-1
Responder Tests.....	11-4
Loop Back/Self Test/Idle Phone Line Test	11-5
Chapter 12 DS0 Configuration	12-1
Time Slot Assignment	12-1
DS0 Configuration	12-3
Fractional T1 Support	12-4
Chapter 13 Chassis Inventory	13-1
Chapter 14 Accounting/Event Logging	14-1
Feature Description.....	14-1
Overview	14-1
Installation Adjustments.....	14-2
Client Configuration.....	14-3
NMC Logging Group.....	14-3
Event Logging Server	14-3
Primary Log Server IP Address.....	14-4
Secondary Log Server IP Address	14-4
Log Server's UDP Port Number	14-4
Logging Client TX Retry	14-4
Log Group Selection	14-5
NMC Logging Traps	14-6
Logging Server Has Been Lost Trap.....	14-6
Other Devices Faults/Groups	14-6
Server Configuration	14-7
Editing the Output Definition (OUTDEF.DAT) File	14-8
Keyword Descriptions.....	14-9
FILE	14-9
TIME	14-9
PATH	14-9
DISK_LOW	14-10
DISK_FULL	14-10
NEW_LOG_FILE.....	14-11
Format Specifiers	14-11
Programming Attributes.....	14-13
Editing the Dictionary (ACCTDICT.DAT) File.....	14-15
Log Generation.....	14-16
Native RADIUS Call Log (.rad)	14-17
Event Log (.nmc).....	14-17
Call Termination Log (.con)	14-20

Using the Prototype Database.....	14-22
Launching the Accounting Report Sample Application.....	14-23
Automated Log File Importing.....	14-23
Total Control Call Accounting Charts.....	14-24
Total Control Event Filtering and Reporting.....	14-25
Native RADIUS Call Filtering and Reporting	14-25
Attribute/Data Type Descriptions.....	14-26
Appendix A Menu/Toolbar Descriptions	A-1
Appendix B LED Status Descriptions	B-1
Appendix C Hub Security	C-1
Feature Overview	C-1
Hub Security Feature Installation	C-5
Configuring Hub Security	C-8
Modem Programmed Settings.....	C-8
NMC Programmed Settings.....	C-9
NMC Faults	C-16
The Security Manager	C-19
Planning the User List	C-19
Using the Security Manager.....	C-19
Main Menu	C-20
File Menu	C-20
Record Menu.....	C-20
Configuration Menu.....	C-20
View Menu.....	C-21
Window Menu.....	C-21
Help Menu	C-21
Security Manager Toolbar	C-21
Navigating the Security Manager.....	C-22
Server Configuration Window	C-22
Dial Back Group Window.....	C-24
User Group Window.....	C-26
User Window	C-33
Call Restriction List.....	C-36
Using Wildcards in a Call Restriction List	C-37
Troubleshooting.....	C-37
Adding/deleting users takes too long.....	C-37
The <i>Security Manager</i> slows down.....	C-37
The <i>Security Manager</i> no longer launches.....	C-38
User browsing is too slow.....	C-38

Appendix D Auto Response	D-1
Product Overview	D-1
Auto Response Configuration	D-2
Before Configuring Auto Response	D-3
Configuring Auto Response	D-4
Events and Responses	D-7
Overview	D-7
Chassis-Level Events and Responses.....	D-7
Module-Level Events and Responses	D-8
Channel-Level Events and Responses	D-8
Event Options	D-11
Response Options	D-25
Appendix E Cellular Modem Support	E-1
Cellular Support as an Added Cost Option	E-1
Functional Description	E-1
MNP10.....	E-2
ETC	E-2
Activating ETC and MNP10	E-3
MNP10 Cellular Template.....	E-4
ETC Fixed Site Cellular Template.....	E-5
ETC Mobile Cellular Template	E-6
Cellular Configuration Group	E-7
ETC Parameters	E-7
MNP10 Parameters.....	E-12

Index

What's New in this Release

Total Control Manager/SNMP Release 4.1 supports the following new features:

- ◆ **New Chassis-Wide Software Download**
An enhancement to the Total Control Manager software now allows users to perform multiple software downloads to all card types by launching a single window.
- ◆ **New Auto Response Events**
Two new events have been added to the Auto Response feature. These events are registered on a channel level and are reported when the appropriate traps are enabled.
- ◆ **New Modem Disconnect and Connect Fail Reasons**
Three new modem disconnect and connect fail reasons will be reported by the modem.
- ◆ **VN4 Switch Support**
A new option, priSwVn4, is now available for the Primary Switch Type Set parameter in the PRI Cards' (E1 and T1) PRI Trunk Settings configuration group. This new option allows you to set the primary switch type for the PRI ISDN NAC. The setting takes effect after the card has been reset.
- ◆ **New NMC Commands**
Two new commands were added for the NMC. You may now restore NMC settings from the factory default or from the settings saved in the NMC's NVRAM. These commands allow you to load the NMC configuration independent of the chassis configuration.
- ◆ **Additional Configurable Parameters**
Six new NMC, six new Modem, and six new T1 parameters were added to provide more configurable functionality.
- ◆ **Accounting Enhancements**
Where previously there was only an option to enable/disable a trap, many traps now include options so you may specify enable/disable for both trap and log record generation.
- ◆ **Additional Information in the Inventory Feature**
Additional information (Installed RAM/FLASH and DIP Switch Settings) is now reported when the Inventory feature is invoked.

Chapter 1

About this Guide

Software Overview

The Total Control Enterprise Network Hub is a sophisticated modem management system that includes direct input of digital T1 phone service and LAN connectivity options. *Total Control Manager/SNMP* is the Windows-based application software component. It operates within the framework of the Novell NetWare Management System to provide access to all cards installed in a Total Control chassis. With Virtual Front Panel Display (VFPD) and other powerful features, *Total Control Manager/SNMP* streamlines the setup, management, and monitoring of a LAN/WAN communications network and improves system performance.

Preliminary Considerations

Check that the following milestones have been accomplished before using this manual:

- Install the necessary hardware (unless the system has been shipped assembled): the Total Control chassis (full 17-slot version or smaller 7-slot version), and the appropriate Network Application Cards (NACs) and Network Interface Cards (NICs). If you have questions relating to installation, refer to the hardware guides for each component.
- If you are using a MP/16 with SNMP management, refer to its *Operator's Guide*.
- Establish IP addressing for the port(s) on the rear panel of the NMC NIC. This addressing should be consistent with your local internetworking scheme. More information can be found in the *Network Management Card Reference Manual*.

- Connect the NMC NIC to the PC that will be running the *Total Control Manager/SNMP* software (the Management Station) by one of three methods: a LAN connection, a direct RS-232/SLIP connection, or a remote modem connection.

Documentation Scope

Hardware installation guides are shipped along with every chassis. The optional Technical Reference Library is a group of manuals that describe the concepts and procedures for configuring the firmware of all Total Control cards.

Contents

This manual covers the following topics:

- Chapter 2—An overview of system components. This includes minimum and recommended hardware and software configurations.
- Chapter 3—How to install, load and uninstall the software.
- Chapter 4—An overview of the steps required to conduct your first session.
- Chapter 5—How to save and restore a chassis definition and configuration.
- Chapter 6—How to configure installed cards.
- Chapter 7—How to monitor the performance of installed cards.
- Chapter 8—How to set SNMP traps and generate alarms.
- Chapter 9—How to send commands directly to installed cards.
- Chapter 10—How to use relevant NMS tools.
- Chapter 11—How to run various system tests.
- Chapter 12—How to configure T1 Card DS0 channels.
- Chapter 13—How to obtain chassis inventory information on all installed cards.
- Chapter 14—How to configure and launch the accounting/event logging feature.

- **Appendices**—Detailed reference material for Toolbar and menu options, LED status descriptions, and a description of the added-cost options that may be enabled via a Feature Enable operation: Security, Auto Response and Cellular.
- **Index**—An alphabetical cross-reference of manual topics.

Common Terms

A general Glossary is provided in the *System Overview Manual* and in online help. However, the following terms are more particular to this manual, and will prove useful as you start to review this material.

Device. Often used in the software and throughout this manual to refer to a Total Control chassis or MP/16.

Drop-down list box. An option box with an arrow pointing down at the right side of the box. Clicking on this arrow displays additional options that may be selected.

Management Station (MS). The PC that is running SNMP host software and *Total Control Manager/SNMP*.

MIB. Management Information Base. An important concept in SNMP, the MIB is a set of defined properties for a piece of equipment that is to be managed on a network. The MIB describes objects, relations, and operations that pertain to each particular piece of equipment.

Object. In terms of SNMP, an object is a quantifiable parameter within a MIB that defines one of the characteristics of a piece of network equipment.

SNMP. Simple Network Management Protocol. An application protocol, widely supported, that offers network management. SNMP is part of the Internet suite of protocols.

Spin button. For a parameter that requires a numeric setting, this box has arrows pointing up and down at the right side of the box. Clicking on these arrows raises or lowers the numeric setting.

TCP/IP. Transmission Control Protocol/Internet Protocol. A suite of protocols that handles data packets in the Transport Layer (TCP) and Network Layer (IP) of the Open Systems Interconnection (OSI) model defined by the International Standards Organization (ISO). TCP/IP was first designed to meet the needs of the U.S. Department of Defense.

Chapter 2

System Components

Hardware Requirements

Minimum

- 80486-based IBM PC or compatible, 33 MHz
- 16 Mbytes RAM
- VGA graphics adapter and monitor
- 3.5-inch, 1.44-Mbyte floppy drive
- Mouse supported by Windows 3.1
- 40-Mbyte hard drive, with 20 Mbytes free
- Serial Communications Adapter with 16550 UART (required for port speeds above 19.2K bps)

Recommended

- 80486-based IBM PC or compatible, 66 MHz
- Super VGA graphics adapter and monitor
- Resolution setting of 800 x 600 256 colors

NOTE: As with all other Windows programs, lower screen resolutions and certain screen fonts may slightly alter the appearance of the *Total Control Manager/SNMP* window, but the menu items remain completely functional.

- 120-Mbyte hard drive, with 60 Mbytes free
- 16-bit Network Adapter (Token Ring only)
- RS-232 Serial Communications Port with 16550 UART

Software Requirements

- DOS 5.0 or higher
- Windows 3.1
- SNMP Host software, such as the Novell NetWare Management System (NMS)

NOTE: USR provides NMS 1.15B along with the *TCM* software and does not guarantee operation with any other version of NMS.

- ODI Device Driver

Chapter 3

Installing the Software

Before you install Total Control Manager/SNMP software, you must complete the hardware installation. In order for the software to communicate with the chassis, management data must pass to the Network Management Card (NMC). The data is routed to the NMC through a Network Interface Card (NIC), via an RS-232 connection or a LAN connection (Ethernet or Token Ring). Both methods depend on TCP/IP addressing for the data to be routed to the appropriate NMC NIC port. Detailed instructions for assigning IP addresses are contained in the *NMC Reference Manual*.

The Novell NetWare Management System must be installed before *Total Control Manager/SNMP*. Installation procedures are described in the following section. If you already have NetWare Management System software installed on your PC, skip ahead to the section that describes the installation of *Total Control Manager/SNMP*.

NOTE: For more detailed information about the NetWare Management System software, including tips for troubleshooting, refer to the Novell NetWare documentation that was included with this product.

Preliminary Steps

Be prepared with the following information.

- The location of the NET.CFG file on your PC
- The network adapter installed in your system
- The IP address for your workstation
- The IP subnet mask

- The IP address of an IP router (if any)

DOS Preparation

- 1 The DOS program SHARE.EXE must be running on the PC that you intend to use as your Management Station. Either add it to your AUTOEXEC.BAT or, from the DOS prompt, type **SHARE** and press Enter.
2. Start Windows.

Software Installation

To Install NetWare Management System

1. Insert the NetWare Management System Setup Disk in the floppy drive.
2. From the File menu of the Windows Program Manager, select the Run option.
3. Substituting the name of the drive in which you placed the floppy, type **drive:\SETUP** and press Enter to start the installation process.
4. You are initially prompted to indicate which NetWare components you want to install. Click on the box to indicate NetWare Management Map *only*.

IMPORTANT: If you are connected to a NetWare server and are installing NMS for the first time, this prompt will also include three other installation options: TCP/IP, NetExplorer, NetExplorer Plus, and NetWare 3.11 SNMP update software. These four install options appear with a checked box in front of them in the prompt window.

You **must** click on these three boxes to *remove* the “X” before you proceed. If you leave these options checked, you will be prompted at the end of the installation for a Disk 5 that is not included with your software, and the installation will fail.

5. You are then prompted for network registration information. Enter the administrator name and company name.

6. If connected to a network, the next prompt is for the size of the network. Specify whether there are under 100 nodes, between 100 and 1000, or over 1000.
7. Continue the installation, replacing Disks 1–4 in the floppy drive as requested. The Install program displays information about the NetWare Management System as the installation progresses.
8. After you insert Disk 4, you are prompted for a Network Adapter name. Select the **Other** option at the bottom of the window. This is especially important if you intend to make a SLIP connection between the PC and the chassis.
9. The Install program then asks for the location of certain network files. You do not need to complete this information. Click on the **OK** button at the bottom of the window.
10. The Install program may encounter incompatible network files. Click on **OK** to continue past these messages.
11. You are prompted to select a time zone, and to indicate whether or not daylight savings time is in effect.
12. The Install program asks to modify your system files (SHELL.CFG, CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI and WIN.INI). Allow the program to make these changes as you are prompted.
13. A window appears asking if you have IP address information. Click on **No**, and then click on **OK** on the next screen where the program informs you that the load of TCP/IP was unsuccessful. This is a normal result.
14. You are then prompted for a server name. Leave the field blank and click on **OK**.
15. The Install program then prompts for Disk 4. This disk should already be in the floppy drive. However, a bug in the Install program proposes the directory name where the files are being installed instead of the floppy drive name. Delete the directory name and replace it with the floppy drive name where the disk is loaded, then press Enter.

This completes the Novell portion of the Install. Review the Novell readme file, and then close it to proceed with the USR installation.

To Install Total Control Manager/SNMP

IMPORTANT: Before starting the installation of the USR software, be sure that all NMM components are closed.

1. Load the *Total Control Manager/SNMC* Setup Disk in the drive.
2. From the Program Manager File Menu, select Run. Type **drive:\SETUP** (substitute the correct drive letter) and press Enter to start the Install.
3. You are asked if you are running any other NMM components. Click on **No**.
4. When prompted, insert the second disk.
5. The Install program finishes, placing *TCM* executable and readme icons in the NMS program group. Review the readme file.

Installing Added-Cost Options

Two added-cost options require installation along with *Total Control Manager/SNMP*: Auto Response and Security. Both of these extra options consist of two upgrade components: one for the NMC and one for *TCM*.

- Each NMC intended to support the extra option must have the feature enabled on it. If you are installing a new NMC with an added-cost feature, it should have been enabled for you at the factory. If you wish to upgrade an existing NMC, see instructions for this under *Feature Enable* later on.
- Each installation of *TCM* must also be upgraded. After finishing the *TCM* installation, insert any disks for extra options and run the Setup program to enable them.

The Security feature requires Microsoft Open Database Connectivity (ODBC) software. A second disk is provided with this software.

Security ODBC Installation

The second disk that comes with the Security feature contains Microsoft Open Database Connectivity (ODBC) software, needed to maintain the security database.

1. Insert the floppy into the drive and type **drive:\SETUP** (substituting the letter of the drive). The ODBC Setup utility title screen appears.
2. Click on **Continue**. The Install Drivers window appears.



Figure 3-1. Install Drivers Window

As shown above, there should be only one option in the list of Available ODBC Drivers: Access Data (*.mdb).

3. Select the Access Data option from the list of Available ODBC Drivers and click on **OK**. Files are copied to your \windows\system directory. Then the Data Sources window appears.
4. Click on **Add**. From the list of Installed ODBC Drivers, select the **Access Data (*.mdb)** option, then click on **OK**. You are returned to the Data Sources window, and the Setup window appears.
5. Click on **Cancel**, then click on **Close** in the Data Sources window. The utility will report a successful installation.

Installation Adjustments

Removing Novell Prompts

NMS installation initializes WIN.INI so that certain messages appear each time you start Windows: a prompt to start NetExplorer Manager, and a NetWare error if you are not connected to a server. You do not need NetExplorer to run TCM and both messages may become irritating if they occur each time you start Windows. Follow these steps to turn them off.

1. Open WIN.INI and find the LOAD= statement.
2. Leaving intact the LOAD= portion of the statement, delete the filenames NMSCRON.EXE and NWPOPUP.EXE.
3. Save the changes to the WIN.INI file.
4. Restart Windows. The messages will no longer appear.

Editing SYSTEM.INI

There are two adjustments to make to SYSTEM.INI.

Port Reinitialization

To prevent Windows from reinitializing ports, we recommend editing the SYSTEM.INI file. All references to COM ports in the [386Enh] section should be remarked out using a semicolon, as shown below:

```
[386ENH]
;COM1BASE=03F8
;COM1IRQ=4
;COM1AUTOASSIGN=2
```

NOTE: Do not access the Advanced Settings in the Windows 3.1 Control Panel Ports application. Exiting the window automatically adds COMxBase= and COMxIrq= lines back into your SYSTEM.INI.

Novell Server Connection

If you do not plan to connect to a Novell server, remark out the Network=VIPX.386 statement from the [386Enh] section of the SYSTEM.INI file.

Compiling MIBs/Integrating Alarms You must perform the following steps to compile the MIBs if you intend to use a MIB Browser.

NOTE: If you have updated your *TCM*, you need only complete steps 1, 6, 7, and 8 below. *TCM* installation copies all the MIBs into the appropriate directories.

1. Perform a Software Download operation on the NMC, either via the pcsdl procedure or through *TCM*, as described in the *Software Download Summary* accompanying the disks.
2. Copy all the files on the second NMC diskette (Enterprise MIB Extensions) **except for CHS_TRAP.MIB** into C:\NMS\SNMPMIBS\ALLMIBS.
3. Review the USRMIBS.TXT file. This file contains descriptions of the MIBs provided by U.S. Robotics.
4. Copy only those MIBs you require into C:\NMS\SNMPMIBS\CURRENT.
5. Copy CHS_TRAP.MIB into C:\NMS\SNMPMIBS\TRAPMIBS.
6. Open the Novell NMS. From the Tools menu, select **SNMP MIB Compiler**. A warning box will indicate that all the MIBs in the C:\NMS\SNMPMIBS\CURRENT directory are about to be compiled. Click **OK**. A DOS program runs. When complete, type **Q** to quit. You will now be able to use the NMS MIB Browser.
7. When the compile is done, select SNMP Alarm Integrator from the Tools menu. Change to the C:\NMS\SNMPMIBS\TRAPMIBS directory.
8. Select **CHS_TRAP.MIB**, and click **OK**. A prompt appears asking if you want to continue. Click on **Yes**. After performing integration, a message appears indicating that the trap definitions were integrated successfully.

NOTE: There are a limited number of MIBs that can be compiled in NMS at one time. If you encounter an error when compiling MIBs or loading the browser, delete all but the necessary MIBs from the C:\NMS...CURRENT directory and try again.

Change Required for Accounting/Event Logging

The Accounting/Event Logging feature is based on RADIUS, a public domain client-server protocol. The NMC runs the RADIUS client and forwards customizable data to a server whose location you specify. To function correctly, register this feature as a TCP/IP Service after the installation is complete.

- If you already have a TCP/IP SERVICES file, add the following line to the file.

RADACCT 1646/UDP

Exit Windows and reboot your computer so that your system recognizes the new TCP/IP service. Remember to reload your protocol stack before starting Windows.

- If you do not already have a SERVICES file, we have provided a sample for you to use:

`\NMS\BIN\NET\SERVICES.SMP`.

1. Create a directory to hold the TCP configuration files, such as `C:\NET\TCP`.
2. Using the name of the directory you created, add the following line to your `NET.CFG` file:

PATH TCP_CFG C:\NET\TCP

3. Copy `\NMS\BIN\NET\SERVICES.SMP` to your TCP directory, giving it the name `SERVICES` (no extension).
4. Exit Windows and reboot your computer so that your system recognizes the new TCP/IP service. Remember to reload your protocol stack before starting Windows.

Change Required for Security

Security also uses a RADIUS-based client-server structure to store data. As with the Accounting/Event Logging feature, you must register the Security server in the TCP/IP SERVICES file. Follow the steps in the previous procedure, adding the following line to the SERVICES file:

RADIUS 1645/UDP

In addition, the Security feature restricts server access to certain *Clients*, which are allowed to use the authentication services. These clients may be set in the *Security Manager* application, and are typically USR NMCs and/or NETServers. You may

specify an authorized set of Clients, by either specific IP address or common name, as follows:

- If you already have a TCP/IP HOSTS file, add the following line to the file, using values that you have specified in the *Security Manager*:

[IP ADDRESS] [COMMON NAME]

Ensure the HOSTS file includes all USR NMC and NETServer IP addresses, and associated Common Names, for all Clients that will be authorized to use the authentication service.

Exit Windows and reboot so that your system recognizes the new TCP/IP SERVICES and HOSTS files. Remember to reload your protocol stack before starting Windows.

- If you do not already have a HOSTS file, we have provided a sample for you to use: \NMS\BIN\NET\HOSTS.SMP.
 1. Create a directory to hold the TCP configuration files, such as C:\NET\TCP.
 2. Copy \NMS\BIN\NET\HOSTS.SMP to your TCP directory, giving it the name HOSTS (no extension).
 3. Edit the sample file to reflect IP addresses and names.
 4. Exit Windows and reboot so that your system recognizes the new TCP/IP SERVICES and HOSTS files. Remember to reload your protocol stack before starting Windows

Software Installation Tips and Troubleshooting

<i>Problem</i>	You are prompted for disk 5 during installation and there is no disk 5.
<i>Solution</i>	During step 4 of the NMS Installation you left an X in the check boxes for NetExplorer, NetExplorer Plus, and NetWare 3.11 SNMP. Follow the Uninstall procedure in the next section and then reinstall, making sure all X's have been removed from these boxes before proceeding.

<i>Problem</i>	After the NMS is installed successfully, the USR installation fails.
<i>Solution</i>	Be sure that all NetWare components are closed before proceeding with the USR installation.
<i>Problem</i>	There is no “NEW USR DEVICE” option within the NMS File Menu after installation.
<i>Solution</i>	SHARE was not loaded when you installed <i>Total Control Manager/SNMP</i> . Load SHARE and reinstall the software.
<i>Problem</i>	You receive an error message when entering Windows: VTCP/IP NO TCPIP PROTOCOLS LOADED
<i>Solution</i>	Exit Windows and load the drivers later per the examples provided in the <i>Loading Network Drivers</i> section.
<i>Problem</i>	You receive an NWPOPUP error on starting Windows.
<i>Solution</i>	Edit the WIN.INI file and remove the filename NWPOPUP.EXE from the LOAD= line.
<i>Problem</i>	You receive a VIPX error on starting Windows.
<i>Solution</i>	This is generated when the IPXODI driver is not loaded and you try to connect to a Novell server. If you do not connect to a Novell server, remove VIPX.386 from SYSTEM.INI.
<i>Problem</i>	You want to re-install NMS and <i>TCM</i> .
<i>Solution</i>	First, follow the Uninstall procedure described in the next section; then re-install NMS and <i>TCM</i> using the instructions in this guide.

Uninstalling NMS and TCM

You have several opportunities during software installation to abort. If you complete the installation, recognize a problem, and decide to start over, you should uninstall the software before attempting to re-install it.

1. Go to the Windows File Manager and locate the NMS directory on the C:\ drive. If you accepted the directory suggested during installation, the files are in C:\NMS\.
2. During installation, you allowed the software to overwrite system files (SHELL.CFG, CONFIG.SYS, AUTOEXEC.BAT, SYSTEM.INI, and WIN.INI). The system saved the old files with the .NMS extension. Rename the .NMS system files so they overwrite the files loaded by NMS (e.g., rename CONFIG.NMS as CONFIG.SYS, etc.).
3. Delete the NMS directory and all its contents.
4. Delete the NMS group from Program Manager.
5. Exit your Windows session.
6. At the C:\ prompt, type the following command to locate any remaining NMS files:

DIR /S NMS <ENTER>

7. Delete any NMS files located and reboot your computer.
8. You may now return to the NMS installation procedure described earlier and begin again.

Customizing the NET.CFG File

In order for a PC to send management data to the NMC in the Total Control chassis, a NET.CFG file must be customized to set link parameters for the PC port that will communicate with the chassis. This connection may be via direct cabling, over a LAN, or by remote connection through a modem.

When *Total Control Manager/SNMP* is installed, two sample NET.CFG files are placed into the C:\NMS\BIN\NET directory. These files provide a sample structure for setting SLIP_PPP, link support and TCP/IP protocol parameters.

The sample SLIP_C1.CFG file is for a connection made through COM1 of the Management Station, and SLIP_C2.CFG shows a COM2 connection. You may use either one of these files as a model and edit your own NET.CFG file, customizing it for your IP addressing strategy.

Regardless of which method you plan to use for connecting to the chassis, follow these instructions for editing the file.

1. Under the Link Driver section, be sure to insert the correct Management Station port information (baud rate, port address, interrupt).
2. Under the Protocol TCPIP section, edit the IP address, subnet mask, and router address (if applicable) to reflect the addressing at your installation.
3. Rename the file to NET.CFG. Either leave the file in C:\NMS\BIN\NET, or copy it to another \NET directory you have created on the PC.

If you move the NET.CFG file to another directory, remember also to copy all the other files that are located in the C:\NMS\BIN\NET directory along with NET.CFG.

Sample NET.CFG Files

SLIP_C1.CFG

Link Driver SLIP_PPP

DIRECT	YES
BAUD	9600
OPEN	ACTIVE
TCIPCOMP	VJ
PCOMP	YES
ACCOMP	YES
PORT	3F8
INT	4
FRAME	SLIP

Link Support

Buffers 8 1500
MemPool 4096

Protocol TCPIP

#	ip_router	192.77.203.?
	ip_netmask	255.255.255.0
	ip_address	192.77.203.66
	tcp_sockets	8
	udp_sockets	8
	raw_sockets	1
	nb_sessions	0
	nb_commands	0
	nb_adapter	0
	nb_domain	

SLIP_C2.CFG

Link Driver SLIP_PPP

DIRECT	YES
BAUD	9600
OPEN	ACTIVE
TCPIPCOMP	VJ
PCOMP	YES
ACCOMP	YES
PORT	2F8
INT	3
FRAME	SLIP

Link Support

Buffers 8 1500
MemPool 4096

Protocol TCPIP

#	ip_router	192.77.203.?
	ip_netmask	255.255.255.0
	ip_address	192.77.203.66
	tcp_sockets	8
	udp_sockets	8
	raw_sockets	1
	nb_sessions	0
	nb_commands	0
	nb_adapter	0
	nb_domain	

Ethernet NET.CFG

The following is an example of a NET.CFG file set up for Ethernet. You will need to customize this according to your installation.

```
Link Driver          SMC8000
                     FRAME    ETHERNET_II

Link Support
  Buffers 8 1500
  MemPool 4096

Preferred Server=DQA

Protocol TCPIP
  ip_router          192.77.204.61
  ip_netmask          255.255.255.0
  ip_address          192.77.204.65
  tcp_sockets         8
  udp_sockets         8
  raw_sockets         1
  nb_sessions         0
  nb_commands         0
  nb_adapter          0
  nb_domain
```

Token Ring NET.CFG

The following is an example of a NET.CFG file set up for Token Ring. You will need to customize this according to your installation.

```
Link Driver          TOKEN
      PORT          A20
      FRAME         TOKEN-RING MSB
      FRAME         TOKEN-RING_SNAP

Link Support
      Buffers 8 4094
      MemPool 4096

Protocol TCPIP
#      ip_router      192.77.203.
      ip_netmask      255.255.255.192
      ip_address      192.77.203.21
      tcp_sockets      8
      udp_sockets      8
      raw_sockets      1
      nb_sessions      0
      nb_commands      0
      nb_adapter      0
      nb_domain
```

Loading Network Drivers

The appropriate network drivers must be loaded in the correct sequence in order for *Total Control Manager/SNMP* to send SNMP data to the chassis. TCP/IP may be loaded with either SLIP, Ethernet, or Token Ring drivers. These drivers can be loaded manually or, more conveniently, through AUTOEXEC.BAT.

All drivers are provided in the C:\NMS\BIN\NET directory with the exception of the Ethernet and Token Ring drivers. Be sure to copy these drivers to whichever \NET directory you use.

SLIP Connection Example

Drivers must be loaded in the following order for a SLIP connection:

LSL
SLIP_PPP
TCPIP
DOSDIALR

Ethernet Connection Example

Drivers must be loaded in the following order for an Ethernet connection:

LSL
SMC8000
IPXODI*
TCPIP
NETX*

*Only required on a Novell network.

Token Ring Connection Example

Drivers must be loaded in the following order for a Token Ring connection:

LSL
TOKEN.COM
IPXODI*
TCPIP
NETX*

*Only required on a Novell network.

Unloading Drivers

It may be convenient to create a batch file that will allow you to unload all the drivers. Drivers must be unloaded in the exact reverse order from how they were loaded. The command line switch “-u” can be used to unload the drivers. For example, to unload the drivers for a SLIP connection, you might create a batch file named KILLSLIP.BAT as follows:

```
DOSDIALR -u
TCPIP -u
SLIP_PPP -u
LSL -u
```

Testing Connectivity

1. Installation of the software creates an NMS Program Group in Windows. Open this group and double click on the NetWare Management System icon. The NMS screen appears.
2. From the Fault Menu, select the **Test Connectivity** option. The Connectivity Test window appears.

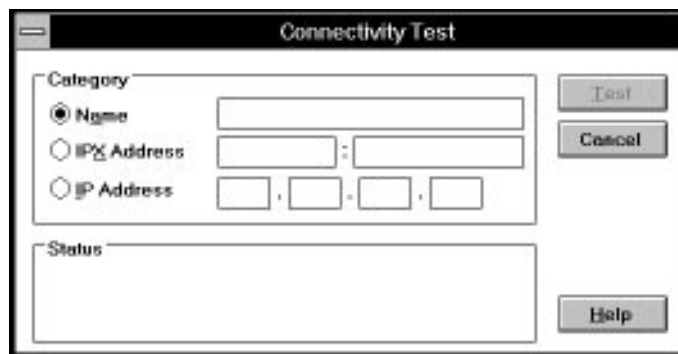


Figure 3-2. Connectivity Test Window

3. Type in the IP Address that you have assigned to the NMC NIC port you are using.
4. Click on the **Test** button. This test is equivalent to performing a ping on a network device. If the software can communicate with the chassis, a confirmation message appears in the Status box

Loading Total Control Manager/SNMP

1. From the NMS View menu, select the **Total Control Manager** option. This will launch *Total Control Manager/SNMP*.
2. Start the process of adding your chassis to the software database. Instructions for this procedure can be found in Chapter 4, *Conducting the First Session*.

Chapter 4

Conducting the First Session

This chapter describes the preliminary steps for setting up the *Total Control Manager/SNMP* software. The first step is to add a definition of the Total Control chassis to the management database.

Adding the Chassis to the Database

1. From Windows, open the NMS Program Group, and then double click on the NetWare Management System icon.
2. From the View menu of the NMS, select the **Total Control Manager** option. Select **New** from the TCM File menu. The following window appears.



Figure 4-1. New Device Window

3. The first field in the New Device window is Device Name. For your first entry, the Device Name field defaults to USRDevice1; replace this with any ascii character combination that suits your network naming scheme. This

name will be displayed under the device icon when the chassis is added to an NMS map (NMS mapping is discussed in Chapter 10.)

4. In the IP Address field, enter the specific Internet Protocol address that will be used to route SNMP management data to the chassis. This is the address that you previously assigned to the NMC NIC port you intend to use: either the WAN port (cabled to your PC or connected by remote modem link) or the LAN port (cabled to your LAN). These addresses are assigned using the NMC RS-232 User Interface (see Chapter 2 of the *Network Management Card Reference Manual*).
5. The default in the Device Type field is set to a U.S. Robotics chassis. You can skip past this field and ignore the AutoDiscovery button.
6. Under SNMP Community Strings, define the passwords in the database that will allow access to the device.
 - The Read-Only field is the password string in the database used to grant an operator the ability to view the status of the chassis. The default string in the Read-Only field is “public”.
 - The Read-Write field allows you to set a password string in the database is used to grant an operator the ability both to view the status of the chassis and to make configuration changes. The default string in the Read-Write field is “private”. Change this string to match the string you previously set with the RS-232 User Interface at the NMC NIC user interface port.

NOTE: If you decide at a later time to change the SNMP Community String, you must change it in two places: in the NMC, by using the RS-232 User Interface, and in the *Total Control Manager/SNMP* software. Instructions for the RS-232 User Interface are contained in the *NMC Reference Manual*. To make the change from within *Total Control Manager/SNMP*, select **Modify** (rather than **New**) from the File menu.

7. The Notepad field is provided for any device-specific information that may be useful to an operator. This information can be viewed and edited when you display the device by selecting **Modify** from the File menu.
8. Once you are satisfied that all the information you have entered is correct, click on the **OK** button at the bottom of the screen. If you entered incorrect information or want to abandon this procedure, click on **Cancel**. For information on setting additional optional parameters, including parameters for communicating with the chassis by remote modem connection, see the next section

New Device— Optional Parameters

There is an additional level to the New Device screen that allows you to adjust less commonly changed parameters. To display this level, click on the **Options** button at the bottom of the screen. This expands the New Device window to the right, as in the following figure.

The screenshot shows a window titled "New" with a tabbed interface. The "Options" tab is selected, revealing several configuration sections on the right side of the window. The left side contains fields for "Device ID", "Device Name" (set to "USRDevice1"), "IP Address" (four empty boxes), "Device Type" (set to "WAN HUB" with a dropdown arrow), and "AutoDiscovery..." button. Below these are "SNMP Community Strings" for "Read Only" (set to "public") and "Read+Write" (set to "private"). A "Notepad" area is at the bottom left. The right side, under the "Options" tab, includes "Remote Serial Communications" with fields for "Phone Number", "Connect String", and "Modem Timeout (sec)" (set to 60). Below that is "Health Monitoring" with "Polling Rate (sec)" (set to 60). Then "LED Monitoring" with "Polling Rate (sec)" (set to 15). Finally, "General Monitoring Parameters" with "Polling Timeout (sec)" (set to 5) and "Polling Retries" (set to 3). At the bottom are "OK", "Cancel", and "Option <<" buttons.

**Figure 4-2. New Device Window
with Options Displayed**

The first category of parameters deals with Remote Serial Communications. This lets you define how a modem connected to your PC will access a remote modem connected to the NMC NIC.

For complete details about configuring modems to establish this connection, see instructions in the *Network Management Card Reference Manual* under Chapter 4, *Accessing a Remote NMC/NMC NIC*.

1. In the Phone Number field, enter the phone number that the modem connected to your PC must dial to access the remote modem connected to the NMC. The following initialization string is (Normal CD and DSR operations; echo off) automatically inserted and executed before the dial string is sent:

AT&C1&D2E0

Remember to include any dial modifiers (such as 9 to escape from an in-house PBX). There is a limit of 256 characters.

2. The Connect String field can be used to customize the dial string. If you have loaded X25DIALR.EXE instead of DOSDIALR.EXE, this field can be used to create a string that will write to and read from the COM port. See the next section, *Connect String Rules*.
3. In the Modem Timeout field, adjust the default of 15 seconds up or down to suit your requirements.
4. The Health Monitoring category displays the default Polling Rate of 60 seconds. This parameter defines how often the Management Station verifies the general health or status of the device.
5. In the LED Monitoring category, you can adjust the Polling Rate from its default of 60 seconds. This defines how often the Management Station verifies the status of the display lights on the device and adjusts its reporting of this data.
6. In the General Monitoring Parameters category, you can adjust the Polling Timeout from its default of 15 seconds, and adjust the Polling Retries from its default of 3.

Both of these parameters apply to the Health Monitoring and the LED Monitoring categories. The Polling Timeout defines the interval between attempts by the Management Station to retrieve data from the device, and Polling Retries defines how many attempts the Management Station will make to retrieve the data.

7. When you are satisfied with the parameters you have set in this window, click on the **OK** button at the bottom of the screen to establish communication with the device. Your modem will go off hook, call the remote modem, and connect to the NMC. Via polling, the NMC will send the Management Station a description of the devices in the chassis. When device discovery is complete, a graphical representation of the chassis appears on the screen at the Management Station.
8. Select the **Save** option from the File menu (or click on the floppy disk icon in the Toolbar) to add the chassis definition to the database. This means your Management Station will remember what the chassis looks like the next time you want to view it.

Connect String Rules

Rules for interpreting the connect string are based on the standard UNIX-to-UNIX Copy Protocol UUCP dial codes. There is a limit of 256 characters. Slightly different interpretation rules apply depending upon whether the DOSDIALR.EXE or X25DIALR.EXE TSR has been loaded.

DOSDIALR.EXE

The following interpretation rules apply to the DOSDIALR scenario, and are implemented before the string is passed to the COM port:

String Syntax	Interpretation	Comments
\p	/	Dial code pause for 120 msec.
\d	d,	Dial code pause for 2 sec.
\D	[phone number string]	Dial code insert phone number string (the value in the Phone Number field).
\c	Removed, no conversion of \n or \r.	Dial code doesn't interpret \n or \r.
\r	0x0B	Dial code carriage return.
\n	0x0C	Dial code new line.

Viewing the Virtual Front Panel Display

After you approve the parameters in the New Device window, connect to the chassis, and add the chassis to the database, the system displays a graphic representation of the chassis, referred to as the Virtual Front Panel Display (VFPD).

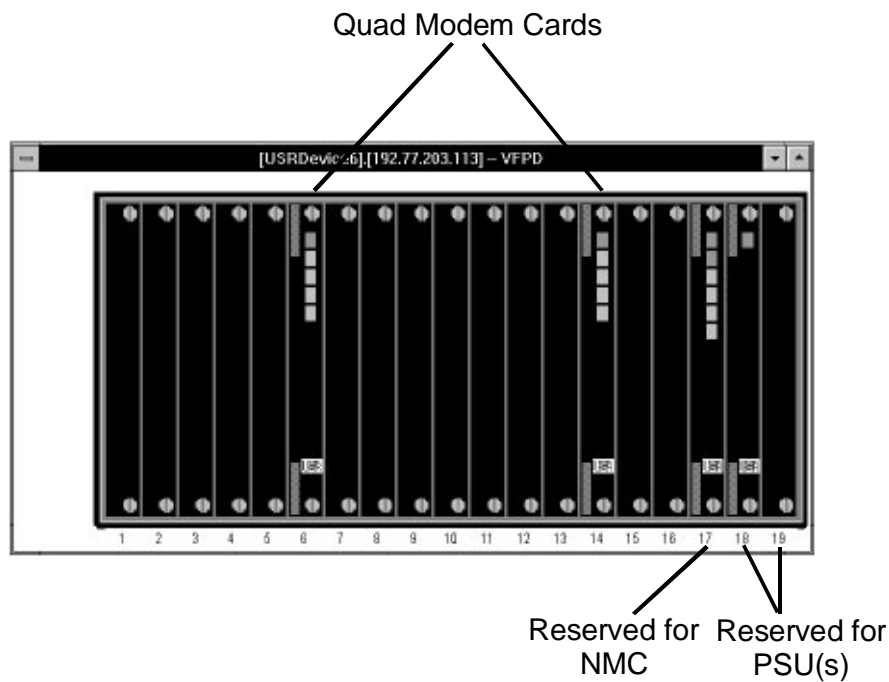


Figure 4-3. Sample Virtual Front Panel Display

When the VFPD is displayed, notice that the menu options displayed at the top of the screen change, and several more buttons on the Toolbar are enabled. For a description of the menu and Toolbar options, see Appendix A.

For the 17-slot, rack-mounted version of the Total Control chassis, the card slots in the chassis are numbered from 1 to 19 (slots 18 and 19 represent the PSUs). The smaller 7-slot chassis has slots numbered from 1 to 7, and the integral PSU is represented as 8 (see Figure 4-4).

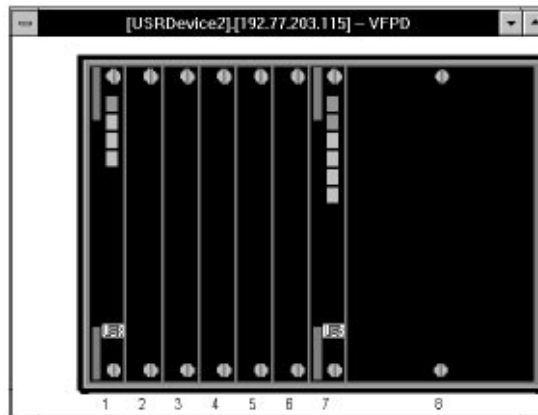


Figure 4-4. Virtual Front Panel Display for Small Chassis

If you are viewing an MP/16 chassis, the top two rows of LEDs represent modems, and the bottom row represents the MP/16 graphic Management Module.

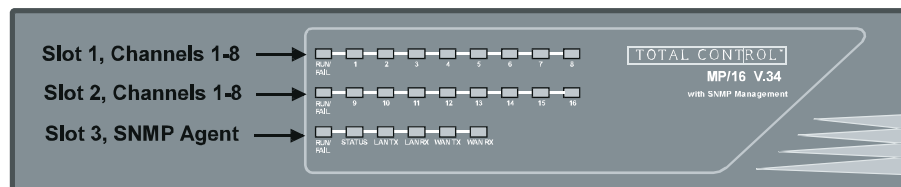


Figure 4-5. Virtual Front Panel Display for the MP/16

The LEDs represent the actual state of the LEDs on the cards; this information is refreshed according to the Polling Rate in the LED Monitoring section of the New Device window (see *Adding the Chassis to the Database* earlier in this chapter). The default is 60 seconds. If you want to change this, select Modify from the File menu.

The rear of the chassis, showing the NICs, may also be displayed and cards selected. Either select the Other Side option from the View Menu, or click on the corresponding Toolbar icon:

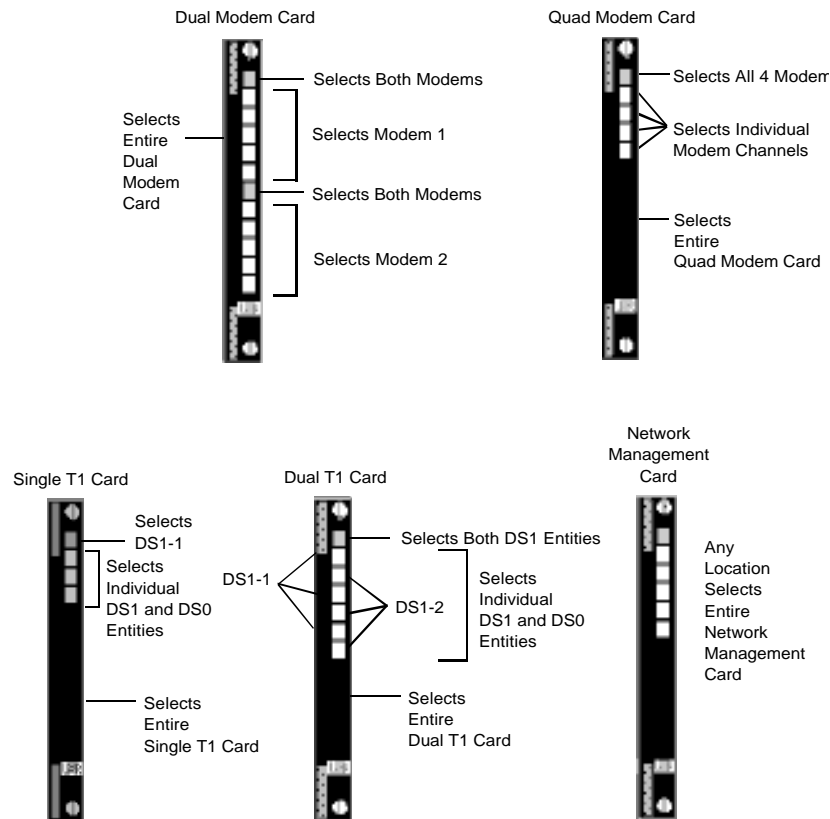


Making a Selection

Before viewing status, or applying any kind of configuration change, you must first select the card(s) or channel(s) on which you want to take action.

- To select a single channel on a card (for instance, one modem on a Quad Modem Card), click directly on the LED that represents the status of that channel with the left mouse button. The LED changes color to indicate selection.
- To select all channels on a card (for instance, all four modems on a Quad Modem Card), click with the left mouse button on the RN/FL LED (the top LED on all cards). All the LEDs change color to indicate that the channels are selected.
- To select an entire card, in order to perform an action on the card as a whole, click with the left mouse button anywhere on the black area of the card. The whole card (all the LEDs and the background in that slot) changes color.
- To select a range of objects across multiple cards, for example, Modem 2 on four adjacent Quad Modem Cards, hold down the CTRL button and click on each object with the left mouse button until you have selected all that you want to include.
- To select all objects of the same type as a currently selected object, choose the **Select All** option from the View Menu. For instance, if you currently have one channel of a Quad Modem Card selected and you then choose the Select All option, all modem channels in that chassis will be selected.

Figure 4-6 shows the “hot spots” on various cards for selecting individual channels, software entities, or the card as a whole.



**Figure 4-6. Selecting Cards/
Software Entities**

Feature Enable

TCM supports the ability to enable added-cost features in the Network Management Card (NMC). Release 3.1 of the Network Management Card allows enabling the Security, Auto Response, and Cellular features.

If you have purchased a new NMC with extra features, it should have been enabled for you at the factory. You may see which features are enabled in the NMC by viewing the new Added Cost Feature group in the NMC Programmed Settings.

If you wish to upgrade an NMC, complete the steps outlined in the following procedure.

Enabling a New Feature in the NMC

1. Contact U.S. Robotics Customer Support (1-800-231-8770). Have the NMC serial number ready. If you are not sure of the number, you can obtain it by using the Chassis Inventory feature described in Chapter 13 or by viewing the Identification Group in the NMC Programmed Settings.
2. Customer Support may perform a remote enable of your NMC, or they may ask you to perform a feature enable operation by providing you with either a character string or an enable disk. If they perform the enable remotely, it will be handled transparently to your site.
3. If they ask you to perform the enable, you must first select the NMC slot in the VFPD, and then select **Feature Enable** from the Configuration menu. The following window appears.



Figure 4-7: Feature Enable-Disable Window

4. If Customer Support has provided you with a character string, enter it in the Feature Key field. If they have provided you with an enable disk, click on the **File Open** button, and then select the appropriate *.key file to be loaded.
5. Click on the **Set** button.
6. Reboot the NMC. The new feature is immediately available.

Chapter 5

Saving a Chassis Definition/Configuration

There are two methods for saving chassis information. These two methods permit an operator to manage different ranges of information pertaining to the chassis.

Chassis Definition

The chassis definition includes all information that is entered when you complete the fields in a New Device window. This information is used for subsequent connections with the chassis. As detailed in Chapter 4, the chassis definition consists of the following information:

- Device Name
- IP Address
- SNMP Community Strings (Read-Only and Read-Write)
- Notepad (a text string containing information useful to the operator)
- Phone Number (for a remote modem connection)
- Connect String (for a DOSDIALR or X25DIALR string)
- Modem Timeout (default=60 seconds)
- Health Monitoring Polling Rate (default=60 seconds)
- LED Monitoring Polling Rate (default=60 seconds)
- General Monitoring Polling Timeout (default=15 seconds)
- General Monitoring Polling Retries (default=3 tries)

The chassis definition also includes snapshots of which cards are installed in the chassis. This only specifies card location, and does not include any configuration information for the installed cards. To save configuration information, follow the procedure outlined in the next section, *Chassis Configuration*.

Modify and Delete

After you have added a chassis definition to the database, you can change it by selecting the **Modify** option from the File Menu while you are viewing the device. The Modify Device window is identical to the New Device window, and allows you to edit all of your previously defined chassis parameters. To delete the definition, select Delete from the File Menu.

Chassis Configuration

The Save and Restore Configuration options apply to all of the parameters, or MIB objects, for the chassis and each of its installed cards. This is useful for backing up the configuration work you have performed on the cards installed in the chassis.

To Save the Configuration for all Objects in a Chassis

1. From the File Menu, select **Save Configuration**. The File Save As window appears.

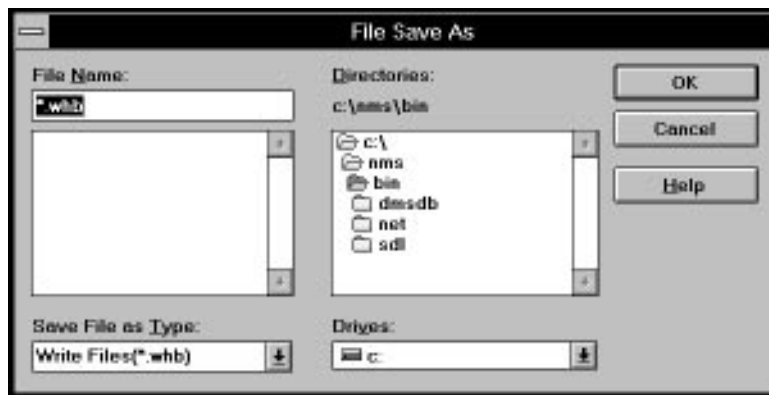


Figure 5-1. File Save As Window

2. Select a DOS path and filename for the configuration file. The default file extension is .whb.
3. Click **OK** to execute the operation. The following window appears.

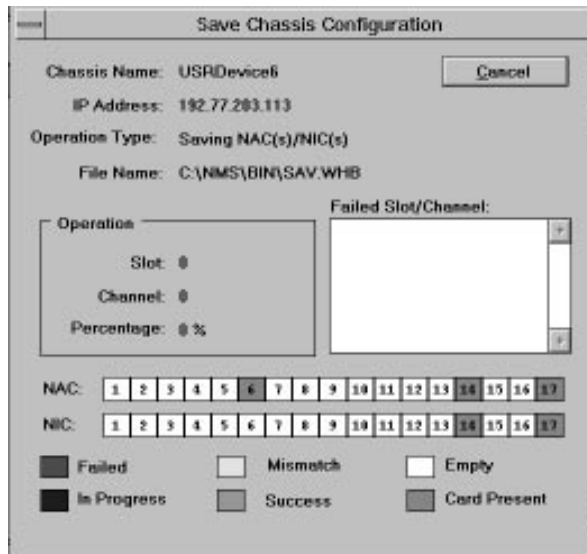


Figure 5-2. Save Chassis Configuration Window

The Save Chassis Configuration window shows you the status of all slots and the progress of the operation. The following color code is used:

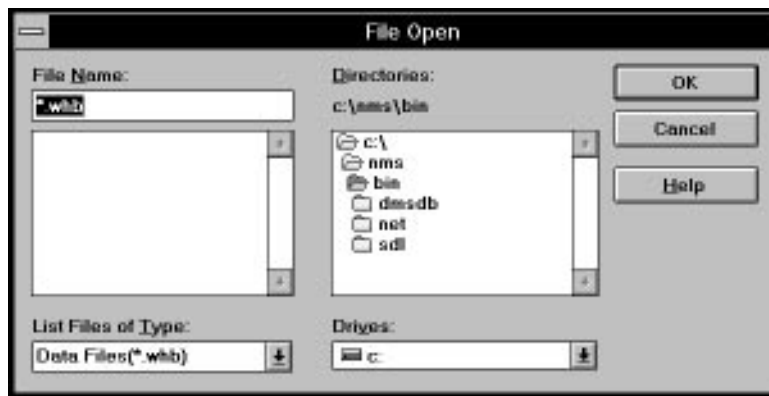
Color	Meaning
Red	Failed
Blue	In Progress
Yellow	Mismatch
White	Empty
Light Green	Success
Dark Green	Card Present

To Restore the Configuration for all Objects in a Chassis

If you configured all the cards and parameters in one chassis, and you have another identical chassis you need to configure, you can simply use the **Restore Configuration** option to configure the second chassis.

NOTE: The NMC IP address must be different on the second chassis:

1. From the File Menu, select Restore Configuration. The File Open window appears.



**Figure 5-2. Chassis Configuration
File Open Window**

2. Select the DOS path and filename for a previously saved configuration file.
3. Click **OK** to execute the operation.

Chapter 6

Configuring Installed Cards

Total Control Manager/SNMP communicates with the Network Management Card (NMC) via the Simple Network Management Protocol (SNMP). All management data sent to the NMC is framed in terms of SNMP. The NMC then uses a proprietary protocol to communicate with the cards installed in the chassis.

SNMP has five basic Protocol Data Units (PDUs) that it uses to manage devices.

Command	Operation
Get-Request	Retrieves current MIB values for a specified list of data types.
Get-Next-Request	Retrieves management information by moving sequentially through the MIB tree.
Set-Request	Sets the specified MIB items to the enclosed values.
Get-Response	Replies to any of the three commands above, with a response or error message.
Trap	Reports extraordinary events.

The NMC serves as an SNMP proxy agent for the NICs and NACs in the chassis. This means that the NMC has the ability to handle all SNMP requests from the Management Station (MS) for any of the cards in the chassis.

The NMC carries out these requests using the Management Bus Protocol. In addition, when the NMC detects that an extraordinary event has occurred on a device in the chassis, the NMC sends a trap to the appropriate Management Station (as configured in NMS). More information on traps can be found in Chapter 8.

Using the Configuration Window

The *Total Control Manager/SNMP* Configuration Window is the primary interface by which SNMP commands are sent to the devices installed in the chassis.

Selection of cards and channels is discussed at the end of Chapter 4. Once you have selected a card, you must open the Configuration Window to query or set parameters.

You can open the Configuration Window in one of three ways:

- ◆ Choose **Programmed Settings** or **Faults** from the Menu bar.
- ◆ Choose the appropriate button from the Toolbar (see Appendix A for a description of the Toolbar).
- ◆ Leave a parameter selected as you exit a Configuration Window session with one card, and double-click on another card or channel. The same Parameter Group topic for the newly selected card is displayed.

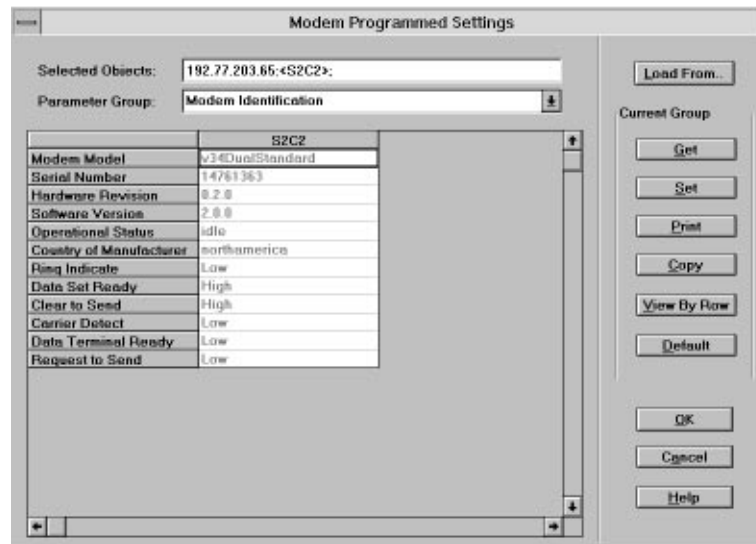


Figure 6-1. The Configuration Window

Title Bar

The title bar at the top of the Configuration window describes the function being performed (Programmed Settings or Fault Management) and the card selected from the chassis display.

For instance, if you select a Modem card from the chassis display, then select Programmed Settings from the Configuration menu, “Modem Programmed Settings” will be the title of the Configuration window.

Selected Objects

Displays the IP address of the selected chassis (NMC), and the slot numbers and channel numbers of the selected devices. For instance, “192.77.203.65:<S2C2>“ means that channel 2 of the device in slot 2 of a chassis with the address 192.77.203.65 has been selected. This field is read only.

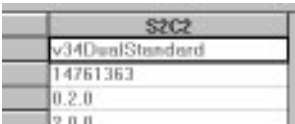
Parameter Group

This box provides a list of all configurable parameter groups that relate to the selected device and allows you to select a parameter group. The parameters for the group are displayed in the spreadsheet section described next.

Spreadsheet

Displays configurable parameters in the parameter group selected. Allows you to view and revise settings for the device(s)/channel(s) selected from the chassis display.

Column heading titles indicate which device/channel is configured with the values displayed in that column. For instance, if the column header reads “S2C2,” the configuration values for channel 2 of the device in slot 2 are displayed in the column.



S2C2		
v34DataStandard	14761363	0.2.0
9	n	n

Figure 6-2. Column Header

Any spreadsheet cell may be edited. If a value is read-only (RO), the value is grayed out and editing is not permitted. If a value is restricted to a particular range or set of options, a drop-down box lists the options available for selection.

The first column of the spreadsheet box is composed of the parameter names.

Load From Button

Allows you to copy parameter configurations from another device and load them on the currently selected device. Press this button to display the Load From dialog box. Enter the IP address, slot number, and channel number of the device with the desired settings. That device's settings will be copied to the currently selected device.

Get/Set Buttons

Triggers the SNMP Get or Set operation. The Get operation retrieves the last-saved values of the current parameter group from the MIB (Management Information Base) and updates the display. The Set operation writes the displayed values to the device MIB.

Print Button

Allows you to print the displayed parameter group's configuration values to your default Windows printer.

Copy Button

Allows you to copy any selected data to the Windows Clipboard so you can import the information into another program.

View by Row / View by Column

Allows you to alter the display of the parameters in the selected parameter group.

Default Button

Allows you to set the value in the selected parameter to the default defined in the MIB for that parameter.

OK Button

When OK is selected, the Configuration window closes. If any alterations have been made, but no Set command was issued, a dialog box will display asking you if the Set command should be issued before the window is closed.

Cancel Button

When Cancel is selected, the Configuration window closes without regard to any alterations made to the parameter values. Any changes you have made will be lost.

Help Button

When the Help button is selected, help related to the function of the Configuration window is displayed.

If you want help related to a specific parameter on the window, place your cursor in the parameter field and press your right mouse button.

Setting Parameters

Management of a device by SNMP requires the definition of a set of managed objects, or variables that can be written to and/or read from. The write operation (SET) is used for configuration or taking action, and the read action (GET) is used for obtaining status information about the object.

To Change a Parameter

1. From the Chassis display, select the card/channel to change.
2. Select **Programmed Settings** from the Configure menu.
The Configuration Window displays with a window briefly overlaying it that indicates the progress of the software in retrieving the current parameters.
3. Click on the **Parameter Group** box and change the group, if necessary, to display the parameter you wish to change in the Parameter box. (A complete list of groups and parameters is in the *Total Control Parameter Reference* and in the online Help.)

4. Highlight the parameter you want to change. The change can be made in one of the following ways:
 - ◆ To select your choice from a list, click on the drop-down list box.
 - ◆ To define the setting yourself, click on the currently displayed value and type the desired setting.

To Send a Change

1. To send your currently displayed changes in this Parameter group to the selected object (modem, T1 Card, etc.), click on the **Set** button. To send changes for all groups, click on the **OK** button. If you try to exit the Configuration Window without sending a Set command or clicking on OK to accept any changed parameters, you are prompted to accept or abandon your changes.
2. When you initiate a change (an SNMP Set operation), the following window appears.

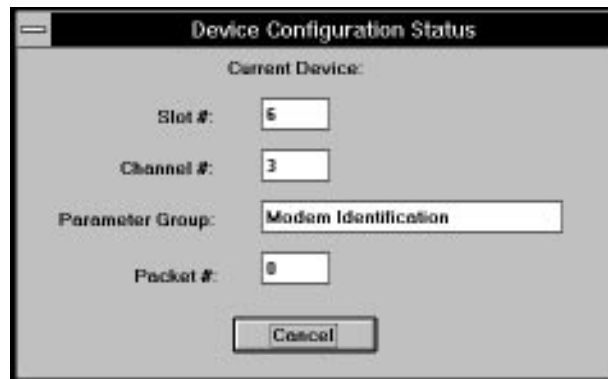


Figure 6-3. Device Configuration Status Window

This window demonstrates the progress of your change. It shows the destination slot and channel number, the Parameter group that is being changed, and the packet number of the data that is being sent.

Loading a Configuration

This option allows you to configure one card, then use that card to configure as many cards of the same type as you want.

To Load From a Device

1. Select one or more cards that require configuration, and then select **Programmed Settings** from the Configure menu (or Programmed Settings icon).
2. Click on the **Load From** button on the Configuration Window. The Load Configuration from Device window appears.



Figure 6-4. Load Configuration from Device Window

3. Fill in the following information to select another chassis object that contains settings you want to duplicate.
 - **IP address.** Type the IP address of another chassis (or leave the default of the current chassis in place).
 - **Slot #.** Type the slot number, from 1 to 17, of the card that contains the settings you want to copy.
 - **Channel #.** Type the channel number for the object that contains the settings you want to copy. For example, a Quad Modem contains channels 1 to 4.
 - **Community String.** Type the Read-Only SNMP Community String for the other chassis.

4. Click on **OK** at the bottom of the window to fill the Configuration Window with values from the selected object for all subgroups.
5. Click on **OK** at the bottom of the Configuration Window. The settings from the card you have specified in the Load From window are sent to all the cards you selected before opening the Configuration Window. A Device Configuration Status window (Figure 6-3) is displayed as these settings are sent.

Downloading Card-Specific Software

Software download reprograms the Flash ROM of a card. There are two main reasons to perform a software download.

- ♦ A critical failure is detected in the Flash ROM.
Each time a card is powered on, it performs various self-diagnostic tests. One of these tests is of the Flash ROM.
- ♦ An updated version of the card firmware is available.

CAUTION: If you are downloading to an NMC over the LAN or WAN connections and there is a loss of power, the card is pulled out from the chassis, or other similar interruption, you may not be able to continue the operation when power is restored. In this case, you will need to connect a cable directly to the user interface port of the NMC NIC and start the operation over again. Do not do anything to disturb the chassis (such as removing or inserting cards) while a software download operation is running.

To Access the Software

When you first install *Total Control Manager/SNMP*, software download files for the NACs in your system are loaded into c:\nms\bin\sdl. If you receive an upgrade for any NAC firmware, run the Setup program on the disk to place new NAC files into the same directory. *Total Control Manager/SNMP* automatically locates these files when you start the software download operation.

To Perform a Software Download

1. To perform software download from within the *Total Control Manager* software, first launch the application and establish a connection with a chassis.
2. From the Device Display on the *TCM* console window, select the card(s) to which you want to perform the download.

NOTE: Once you have entered the Software Download window, you will have the option of selecting or deselecting cards according to their slot number.

3. Select the **Software Download** option from the Configure Menu (see Figure 1), OR

Click on the Software Download icon (shown right) from the Toolbar. The Software Download window then appears (see Figure 6-5).

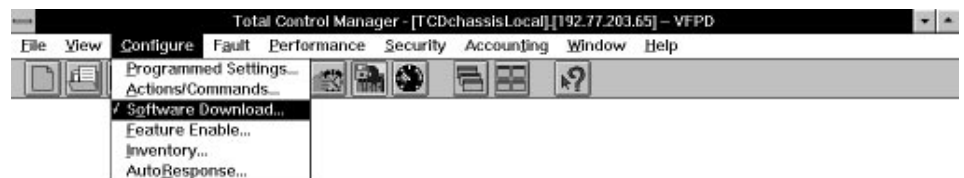
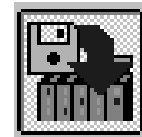


Figure 6-5. TCM Configure Menu's Software Download Option

This window contains five columns:

- ♦ The **Selection** column: Allows you to select multiple cards of various types on which to perform downloads. A check mark will appear for every selected card. If you selected a card on the Device Display, the card will have a checkmark in this column when the window is opened.
- ♦ The **Slot** column: Lists the slots of the chassis by number as well as the NACs (Network Application Cards) that occupy them.

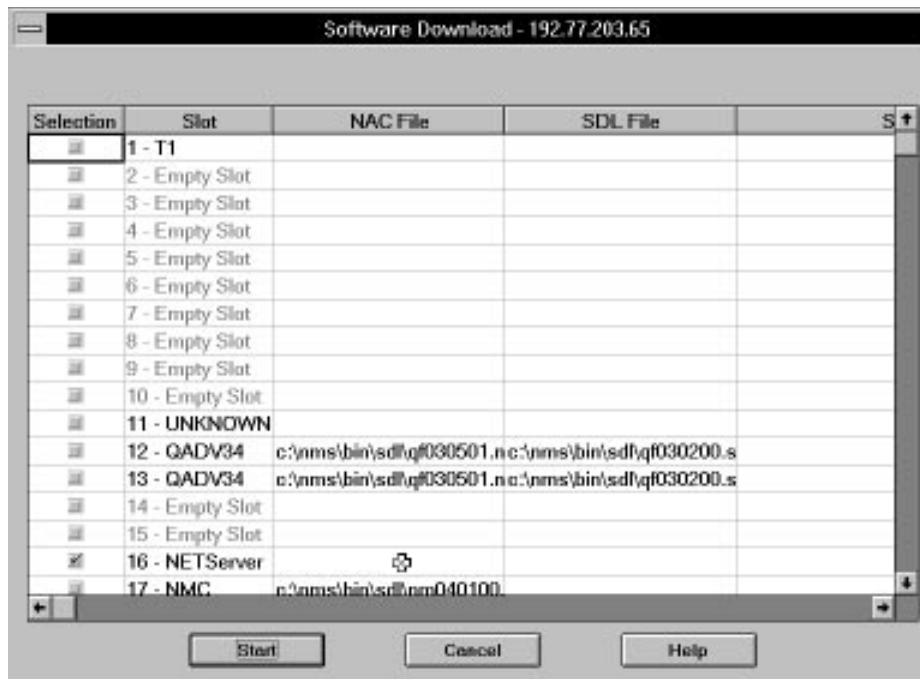


Figure 6-6. TCM's Software Download Window

- ♦ The **NAC File** column: Lists the most current .NAC file version in the \NMS\BIN\SDL directory. If this version is a more recent version of software than is on the NAC itself, it will be shown in red.
- ♦ The **SDL File** column: Lists the most current .SDL utility file version in the \NMS\BIN\SDL directory. If this version is a more recent version of software than was previously used, it will be shown in red.
- ♦ The **Status** column: Lists the status of each software download task on a card-by-card basis. Such messages as "In Progress" or "Complete" will appear in this column as the download progresses.

If you have loaded or moved the .NAC and/or .SDL files to a directory other than \NMS\BIN\SDL, you can access them by positioning the cursor in the **NAC File** and **SDL File** columns in the same row as the card you wish to perform a download to, then double-clicking the left mouse button. The Open

window shown in Figure 6-7 will appear. This window will allow you to select the directory where your files are, as well as the files you wish to download to this card.

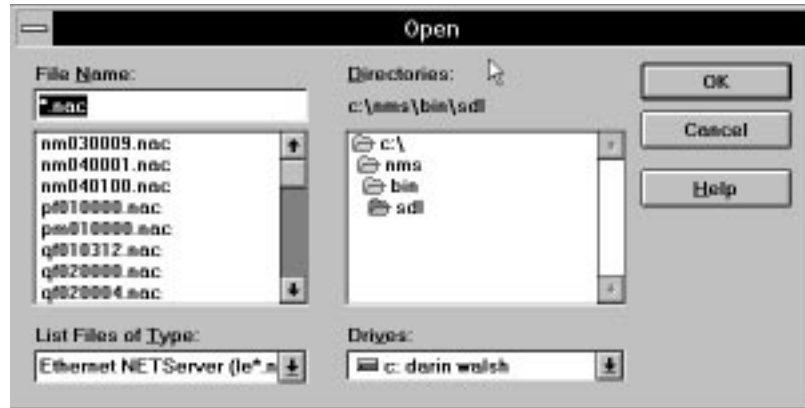


Figure 6-7. Software Download Open Window

4. Click **START** to begin the download.

NOTE: If you receive a Device Not Responding error message while trying to perform a software download, the cause may be too much other management traffic to the chassis. Reduce other operations (including multiple Management Station access) and try the operation again.

During the download, progress messages are displayed in the upper left corner of the Software Download window. A **Success** message indicates that the operation is complete.

NOTES:

- ◆ If you selected more than one card to download to and wish to cancel the operation while it is in progress, you can click on the **STOP** button in the bottom left side of the window. The SDL operation already in progress cannot be stopped, but the remaining operations will be canceled and the corresponding check marks will be removed.
- ◆ Some devices, such as the X.25 PAD, require you to reset the card after software download.

Chapter 7

Viewing Statistics

The techniques described in this chapter permit you to query the status and monitor the performance of cards installed in the chassis.

Verifying Object Status

Total Control Manager/SNMP allows you to query the status of cards installed in the chassis. This can be accomplished in two ways:

- By viewing the LEDs that represent the card on the chassis display. A full description of these LEDs and their significance is contained in Appendix B.

You can also obtain LED information by selecting the **LED Polling Information** option from the View Menu. The following window is displayed.



Figure 7-1. LED Polling Information Window

This window gives you an idea of the frequency of LED polling, as well as the number and nature of errors encountered.

- By performing an SNMP GET operation while viewing the parameters for a selected card on the Configuration Window. Configuration Window operations are described in Chapter 6.

Monitoring Performance

Total Control Manager/SNMP allows you to set up a systematic approach to monitoring the performance of cards installed in the chassis. Keep the following points in mind about performance monitoring:

- Although you can select more than one card from the chassis display to monitor, only one type of card may be viewed at a time.
- Up to ten parameters can be selected for any one monitoring session.

Once you have selected one or more cards from the chassis display, you can launch the session monitor in two ways:

- Click on the **Performance** icon at the far right of the Toolbar (represented as a gauge, like a tachometer). For a description of the Toolbar, see Appendix A.
- From the Performance Menu, select **Session Monitor**.

The Functional Group Monitor Setup window appears. Figure 7-2 shows a Functional Group Monitor Setup window for a V.32 *bis* Quad Modem.

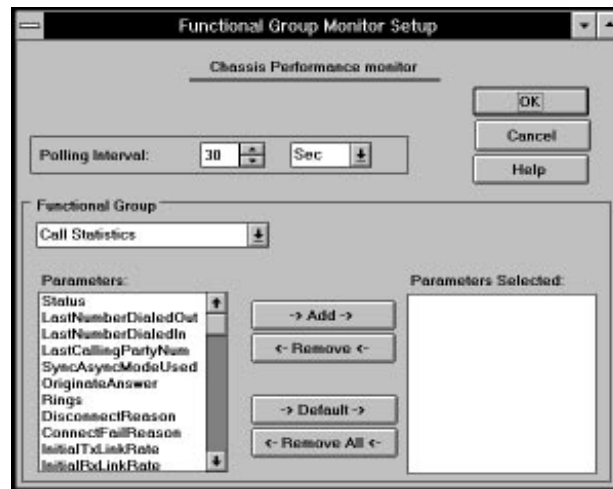


Figure 7-2. Functional Group Monitor Setup Window

This window lets you choose the parameters to be queried. For a full set of parameter definitions, see the *Total Control Parameter Reference* or the online Help.

1. For Polling Interval, you can adjust the 30-second default to provide you with updated status reports at specific time intervals. Click on the spin button to increase or decrease this figure.
2. In the Functional Group drop-down list box, select a parameter group (a full list is in the *Total Control Parameter Reference*). For instance, for a modem, select either **Call Statistics** or **Modem Events**.
3. Under Parameters, highlight the Parameter Choices options you wish to query, and then click on the **Add** button. Your choices will appear in the Parameter Selection box. You can also select parameters as follows:
 - Hold down the Ctrl key and click with the left mouse button to select multiple parameters.
 - Click on the **Default** button to select up to ten parameters from the group. If there are more than ten parameters, only the first ten are displayed.
 - Use the **Remove** and **Remove All** buttons to delete selection(s) from the Parameters Selected box.
4. Select **OK** to start the query operation. The Performance Table appears with the statistics you have requested.

NOTE: If you press OK before selecting any parameters to query, the first ten parameters in the first functional group will be queried.

Start Date	Synchro address	Modulation type	Error Control type	Accession type
06/01	asynchrocast(1)	rejection of all data	none	none
06/02	asynchrocast(1)	rejection of all data	none	none
06/02	asynchrocast(1)	rejection of all data	none	none
06/04	asynchrocast(1)	rejection of all data	none	none

Figure 7-3. Performance Table

Chapter 8

Configuring Traps/Alarms

Traps

Traps are unsolicited SNMP messages sent from a network device to a Management Station to signal that a specific event, or fault, has occurred on or within that network device. Traps allow the operator to detect, isolate, and correct problems or events that occur with an object. Alarm is a generic term that refers to how a Management Station reacts when it receives an SNMP trap.

Traps are configured (enabled/disabled) in *Total Control Manager/SNMP* through Fault management. For many traps, it is also possible to log the occurrence of an event using the Accounting/Event Logging feature (see Chapter 14).

To Set up a Trap

1. To set Fault parameters for one or more cards, select the card(s) or software entities on a card, as described in Chapter 4. Then either select **Trap Settings** from the Fault Menu or click on the **Fault** icon in the Toolbar (represented as a hand setting an alarm clock). The Configuration Window appears with the Faults displayed, and the selected card address is displayed in the Selected Objects field.
2. Some Fault parameters simply need to be enabled; one example of this type of parameter for a modem is an Incoming Call Terminated event. Other parameters require that you first select a threshold, and then enable the trap for the corresponding event.

The following example sets up a trap for a DTE Idle Timeout Limit:

- a. From the Parameter Group box, select the **Modem Event Thresholds** group.

- b. In the Parameter box, highlight the **DTE Idle Timeout Limit** parameter.
- c. In the spreadsheet parameter value box, either type in a number, or use the spin button at the right of the box to raise or lower the setting value. This number represents the number of minutes with no activity that the modem waits before reporting a DTE Transmit Data Idle event.
- d. Press the **Set** button.
- e. In the Parameter Group box, select **Trap Enables**. This is shown in Figure 8.1.
- f. In the Parameter box, highlight the **On Connection Timeout** parameter.
- g. In the Spreadsheet Parameter Value box, select the **Enable** setting.

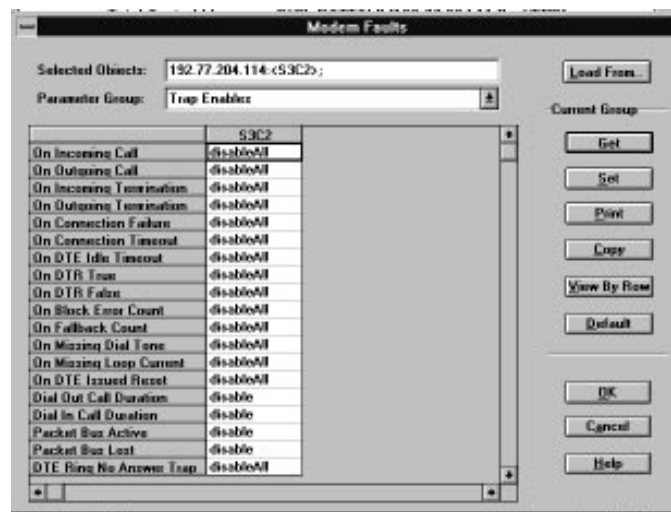


Figure 8-1. Trap Enables Group

- h. Click on the **OK** button at the right of the window to send this setting to the modem. The Device Configuration Status window shows the status of the operation while the settings are sent.

To Select a Trap Destination

After you have configured *Total Control Manager/SNMP* to generate traps, you can choose to send these traps to one or more Management Stations.

1. From the Fault Menu, select **Trap Destinations**. The Trap Destination Table window appears.

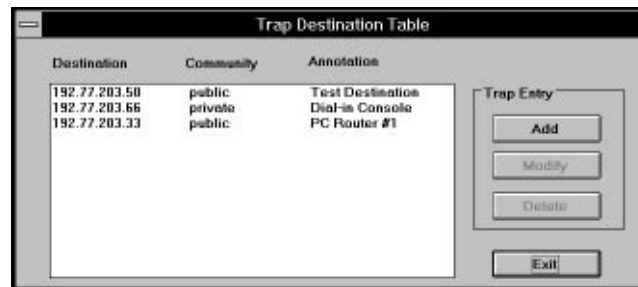


Figure 8-2. Trap Destination Table

2. Click on the **Add** button at the right side of the window. The Add Trap Destination window appears.



Figure 8-3. Add Trap Destination Window

3. Enter the following information:
 - IP address of the trap destination
 - SNMP Community String
 - Annotation (any additional informative text)
4. Click on **OK** to accept the trap destination information.

Alarms

Alarms are handled through the Novell NetWare Management System. Follow these steps to set up an alarm in the NMS:

1. Integrate MIB data with alarm data in the NMS. (See Chapter 3.)
2. Decide on disposition of alarms (how the system provides notification in the event of an alarm).
3. View the Alarm Monitor.
4. Display the Alarm Report.

For more detailed instructions, see Chapter 10 of this manual or the Novell documentation provided with this product.

Chapter 9

Sending Commands to Installed Cards

This chapter describes how to send commands directly to cards installed in the chassis. Actions or Commands are those modifiable parameters that allow the operator to initiate a change immediately, including resetting, taking out of service, testing, etc. Depending on the card(s) or components (LEDs) you have selected from the chassis display, a different range of commands may be available.

To Execute a Command

1. Select one or more cards or software entities from the chassis display, as described in Chapter 4.
2. Either select **Actions/Commands** from the Configure Menu, or click on the Action icon on the Toolbar (represented as a bolt of lightning striking a card). The Total Control Manager Commands window appears.

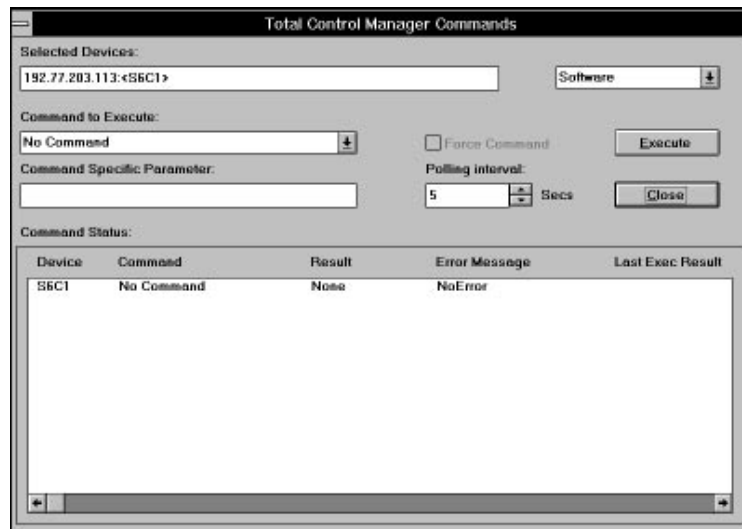


Figure 9-1. Total Control Manager Commands Window

3. The Total Control Manager Commands window contains the following fields:
 - **Selected Devices.** This field displays the IP address, and the slot and channel number, of the cards you have selected from the VFPD.
 - **Hardware/Software.** This drop-down list box either displays Hardware, Software, or both, depending on the card and how you have selected it. This allows you to choose whether to perform an action on the card itself or on a software entity on the card.
 - **Command to Execute.** This drop-down list box presents the options for the hardware or software command to be issued to the selected card(s). It displays No Command until you select an option.
 - **Command Specific Parameter.** This box presents any additional parameter that must be qualified for the command, if any exists.
 - **Force Command.** This check box allows you to specify that the command should be sent to the card regardless of its operational state. For some commands, this option is not allowed. For others, the box may be checked by default, but you may choose not to force the command by clicking on the box to remove the checkmark.
 - **Polling Interval.** This field displays the default 5-second interval for polling to obtain the status of an executed command; use the spin button at the right of the field to raise or lower this interval.
 - **Execute/Close.** Press the **Execute** button to carry out the command you have selected; press **Close** to exit from the window without executing a command.
4. When you have selected the appropriate command, press **Execute**. The command is sent to the selected card(s). The Command Status table at the bottom of the window displays the following information for each selected card:
 - **Device.** This column contains the slot and channel numbers for all of the cards selected.

- **Command.** This column displays commands that have just been chosen to be performed on the selected card(s).
- **Result.** This column returns the result of the executed command.
- **Error Message.** This column contains a message regarding any errors that were encountered in attempting to execute the command, if any.
- **Last Exec Result.** This column displays the result of the most recent command that was executed on the card.

Available Commands

Command Type	Command
Modem Hardware Commands (Card Level)	No Command Remove from Service Restore to Service Hardware Reset Software Download
Modem Software Commands (Channel Level)	No Command Software Reset Store to NVRAM Restore from Default Restore from NVRAM Off Hook On Hook Load HW Flow Control Defaults Load SW Flow Control Defaults Load MNP10 Cellular Defaults Load V42 Cellular Mobile Defaults Load V42 Cellular Fixed Defaults
Modem Analog NIC Hardware Commands (Card Level)	No Command Remove from Service Restore to Service Hardware Reset

Command Type	Command
Modem Analog NIC	No Command
Software Commands (Channel Level)	Non-disruptive Self Test Busy Out Phone Line Non-Busy Out Phone Line
	NOTE: The Quad Analog/Digital NIC has only one channel, so test results from channels 2-4 are invalid.
NMC Software Commands	No Command Save Chassis to NVRAM Restore Chassis from Default Restore Chassis from NVRAM Non-Disruptive Self-Test Software Reset Save UI to EEPROM Restore NMC from Default Restore MC from NVRAM
T1 Card Hardware Commands (Card Level)	Hardware No Command Remove from Service Restore to Service Hardware Reset Software Download
T1 Card Software Commands (Card Level)	DT1 No Command Save to NVRAM Restore from NVRAM Restore from Default Non-disruptive Self-Test Disruptive Self-Test Software Reset Reset -> Hi Pri. Timing Src
T1 Card Software Commands (DS1)	No Command Force Receiver Reframe

Command Type	Command
T1 Card Software	No Command
	Hard Busyout
Commands (DS0)	Soft Busyout
	Restore
	Disconnect
	Transparent Test
X.25 Gateway	No Command
Software Commands	Save to NVRAM
	Restore from Defaults
	Non-Disruptive Self Test
	Disruptive Test
	Software Reset
	Download Configuration
	Upload Configuration
X.25 Gateway	No Command
Hardware Commands	Remove from Service
	Restore to Service
	Hardware Reset
	Software Download
NETServer	No Command
Hardware Commands	Remove from Service
	Restore to Service
	Hardware Reset
	Software Download

Chapter 10

Using NMS Tools

This chapter describes features of the Novell NetWare Management System that are useful in helping to manage the Total Control chassis. This chapter is intended to provide overview information about these features only; for complete information, refer to the Novell documentation provided with this product.

This chapter covers the following topics:

- Creating Network Maps
- Configuring Alarms
- Compiling MIB Files
- Using the MIB Browser

NOTE: All of the following sections assume that you have launched the NetWare Management System, and are starting from the vantage point of the NMS Main Menu.

Creating Network Maps

The Novell NetWare Management Map software offers two types of network maps, which can be linked to form an effective network management tool.

- **Internet Map.** When you save the definition of a Total Control chassis (see Chapter 5), an image of the chassis is automatically generated in the NetWare Management Map. This Internet Map shows a logical representation of all defined chassis in the system.
- **Locational Map.** This is a manually created graphical representation of the physical layout of all the elements of your network. Using stored or created bitmap graphics, you can assemble a network view that spans a single facility located in one building, or a network that spans cities throughout a whole country. This map represents logical and physical networks in their geographic locations.

To Open the Internet Map

1. From the File Menu, select **Open**. From the submenu, select **Internet Map**. The map displays icons representing all the chassis definitions that have been saved in *Total Control Manager/SNMP*.
2. Double click on any chassis icon on the Internet Map to launch *Total Control Manager/SNMP* and display the VFPD for that chassis.

To Create a Locational Map

1. From the File Menu, select **New Locational Map**. The Locational Map Editor window appears.
2. From the Toolbar at the top of the Locational Map Editor, select the **Wallpaper** icon (represented as a roller applying a strip of wallpaper). A Browse dialog box appears.
3. Select one of the bitmap files provided in the NMS\WALLPAPR directory, or substitute a bitmap image of your own, to serve as the background graphic in which to situate your network representation.

Eight icons are provided to represent locations ranging from an office to an entire country. These icons should be viewed as building blocks that can be linked to each other to create a layered view of your network.
4. In the Locational Map Editor window, point and click where you want the center of the bitmap image to appear.
5. Click on the **Icon Palette** button on the Toolbar (to the right of the Wallpaper button). Select an icon to represent the next lower level in the hierarchy of the network installation.

For example, if your first choice was a country map, the next icon you choose may be a state map. You may want to represent a view of installations located in different cities at the top layer. Double-clicking on one of the city icons may bring up an icon that represents a campus in that city, and so on. Your hierarchy may be simple or complex.

6. Assign the map a name and save it.

To Place Total Control Icons onto a Locational Map

1. This operation does not require the Locational Map Editor, so close it if it is open. Open both the Locational Map and the Internet Map.
2. Highlight an icon representing a Total Control chassis on the Internet Map.
3. Hold down the left mouse button and drag the icon onto the Locational Map. Place the chassis where you want it to appear.

Configuring Alarms

In order for an SNMP trap to cause an alarm to appear in the NMS, the trap must be enabled within each chassis running *Total Control Manager/SNMP*. For instructions on trap configuration, and setting Management Station trap destinations, see Chapter 8.

Alarm functions require the Alarm Manager portion of the NMS to be running; this software is launched automatically when you start the NMS. Alarm configuration in the NMS is located in the Fault Menu, and alarm integration is located in the Tools Menu. Options here allow you to perform the following functions:

- Integrate Alarms
- Configure Alarm Disposition
- View an Alarm Monitor
- Generate Alarm Reports

Alarm Integration

Once you configure your traps, you must integrate the MIB data that describes these traps into the NMS Alarm Manager.

1. From the Tools Menu, select **Alarm Integration**. A Browse dialog box appears that allows you to select the CHS_TRAP.MIB.
2. Click on **OK** to begin the alarm integration.

Alarm Disposition

Once you have enabled a Total Control chassis to generate a trap within *Total Control Manager/SNMP* for an event, you can configure the type of notification(s) that will be generated for that trap within NMS.

1. From the Fault Menu, select **Alarm Disposition**. The Configure Alarm Disposition window appears.

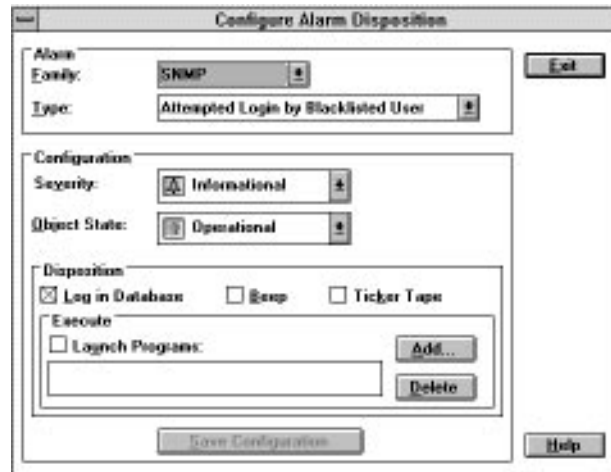


Figure 10-1. Alarm Disposition Window

2. For the Family of alarms, select **SNMP**. Then select the type of alarm from the drop-down list box.
3. Under Configuration, select from the drop-down list boxes for the alarm severity and the object state for the affected object (such as *Operational* or *Degraded*). The object state is the condition you anticipate for the object as a result of the alarm. This in turn affects the displayed icon for the device; for instance, if you have set the object state to Non-operational, the icon is “grayed out” to indicate a severe condition, but can still be selected.
4. Select an action for the alarm disposition. Upon the occurrence of an alarm, you may choose to log the alarm in the database, create an audible beep, display a “ticker tape” message across the status line of the NMS, or execute a program of your choice. When you have selected the appropriate disposition(s), click the **Save Configuration** button at the bottom of the window.

Alarm Monitor

The Alarm Monitor is a real-time display of all alarms that have occurred since you launched NMS, or since the last time the Alarm Manager was restarted.

1. From the Fault Menu, select **Alarm Monitor**. The Alarm Monitor fills the NMS screen.



Figure 10-2. Alarm Monitor Window

This window is divided into the following sections:

- The top pane contains pie charts representing the severity and family of alarms generated. All Total Control alarms are part of the SNMP family. This pane is updated every two minutes.
- The bottom pane contains nine columns of alarm information; the most recent alarm is displayed in the top row of the table. These columns contain:
 - the time that the alarm was received
 - the type of alarm
 - the affected station
 - the alarm severity

- the operational state of the affected device
- the network address of the affected device
- the station type of the affected device
- the time that the alarm was sent to the NMS
- an alarm summary.

Use the scroll bar at the bottom of the table to view all of this information.

Alarm Reports

The Alarm Report displays information about alarms that are logged to the database. This option is enabled in the Alarm Disposition window, described earlier.

If no icons are selected in a map, the Alarm Report displays all alarms. If an icon is selected, the Alarm Report shows only those alarms that were generated by the chassis represented by that icon.

The Alarm Report contains all the information presented in the Alarm Monitor table, including the following fields: a note that you have entered about the alarm, an indication of whether or not the alarm has been acknowledged, and the date and time that the alarm was acknowledged.

The Alarm Report can be used for the following purposes:

- Acknowledge alarms
- Delete alarms from the database
- Print alarm information
- Add a note to an alarm for a co-worker
- Find and display a device specified by a selected alarm on the Internet Map

Compiling MIB Files

MIB files are not compiled automatically when you install *Total Control Manager/SNMP*. The MIB Compiler is a useful tool in the event that MIBs change or have been updated.

1. When TCM is installed, all MIBs are copied into the C:\NMS\SNMPMIBS\ALLMIBS directory. Copy those MIBs you want to compile into the C:\NMS\SNMPMIBS\CURRENT directory.
2. From the NMS Tools Menu, select **SNMP MIB Compiler**. The following prompt appears:

This compiles all the files in the C:\NMS\SNMPMIBS\CURRENT directory. It writes the binary output to the file C:\NMS\SNMPMIBS.BIN. Do you want to continue?
3. Click on **OK** to execute the compile.

Using the MIB Browser

The MIB Browser enables you to send SNMP commands directly to a device for a selected MIB object. This allows you to GET the current value of an object, as well as SET the object to a specified parameter.

1. From the Tools Menu, select **SNMP MIB Browser**.
2. Fill in the IP address and the SNMP community string.
3. When the chassis is selected, the Profiles box fills in with a list of SNMP profiles available for the chassis. Select a desired profile, or use the **Add** or **Edit** buttons to customize a profile of your own. The profile contains the following information:
 - IPX or IP address
 - The SNMP community string
 - The request mode (single request or polled)
 - The polling interval
 - The display method (table or graph)
 - One or more attributes to retrieve from the selected device

4. Select a profile and click **OK**. The requested information is displayed as a table or graph of attributes and values, depending on the display chosen. Tables allow you to perform GET and SET operations, while graphs are appropriate for charting polled data over time.

Chapter 11

Testing

The following kinds of tests can be run with compatible modems:

- Tone Tests
- 105/102 Responder Tests
- Loop Back Tests
- Self Tests
- Idle Phone Line Tests

Tone Tests

The tone test feature allows an operator to use the DSP (Digital Signal Processor) of a modem to test the quality of a T1 DS0 channel. When the test is initiated, the DS0 is automatically placed in transparent test mode to carry out the test. The T1 NAC connects individual DS0s to the modem and ignores any signaling on these DS0s. After the test is complete, the NMC sends a Restore DS0 command to the T1 NAC to take the DS0 out of the transparent state.

Tone Test Rules

- Except for a loopback test state, a request for transparent test mode overrides any other DS0 state, including an alarm or any state entered into by command, such as call ignore.
- A request for tone test disconnects any calls in progress on the DS0.
- If the span line is configured to respond to a loopback request, and one occurs while there is a tone test in progress, the span line will enter the loopback state. After the loopback, all DS0s will return to idle.
- When the DS0 is restored after the tone test is over, an alarm state will be restored and updated, but any DS0 that

had been in a connected state or in a state that was entered into by command will be returned to the idle state.

To Send a Tone Test

The following steps detail how to send a tone over a DS0.

1. Select a modem from the VFPD.
2. From the Fault Menu, select **Remote Testing**, and then select **Send a Tone**. The following window appears.

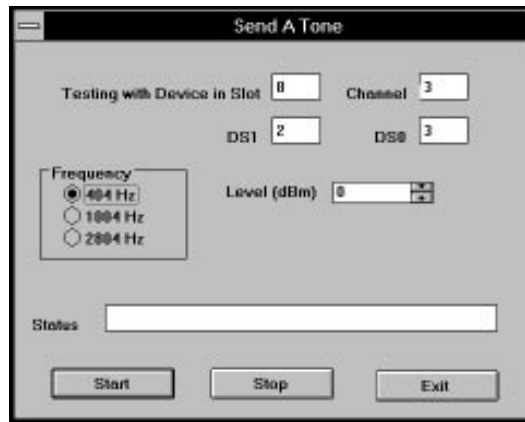


Figure 11-1. Send Tone Window

3. The top of the Send Tone window shows the slot and channel of the selected modem.
4. In the next two boxes, the DS1 and DS0 currently sharing the modem's time slot are displayed.
5. In the Frequency box, you may choose whether the test should be generated at 404, 1004, or 2804 Hz.
6. In the Level (dBm) field, you may set the amplitude of the test from 0 to -20 dBm.
7. If you want to cancel setting up the test (before you have clicked on the Start button), click on the **Exit** button. Click on the **Start** button to begin testing, and use the **Stop** button to end the test at any time.

NOTE: Do not exit the window without clicking on the Stop button.

8. Test results appear in the Status field.

To Receive a Tone Test

The following steps detail how to receive a tone over a DS0.

1. Select a modem from the VFPD.
2. From the Fault Menu, select **Remote Testing**, and then select **Receive a Tone**. The following window appears.

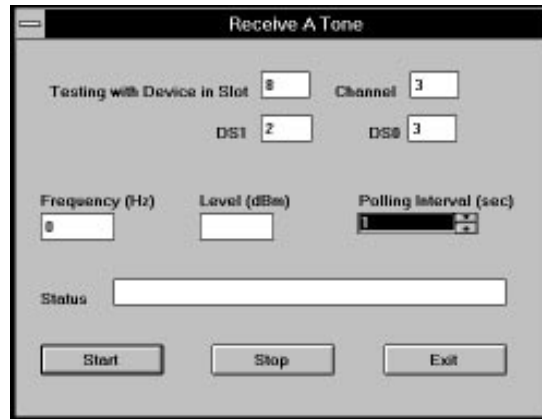


Figure 11-2. Receive Tone Window

3. The top of the Receive Tone window shows the slot and channel of the selected modem.
4. The next two boxes show the DS1 and DS0 currently sharing the modem's time slot.
5. The Frequency field shows whether the test is being generated at 404, 1004, or 2804 Hz.
6. The Level (dBm) field shows the amplitude at which the test is being generated, from 0 to -20 dBm.
7. The Polling interval field allows you to set how often the results of the test should be monitored, in seconds.
8. If you want to cancel setting up the test (before you have clicked on the Start button), click on the **Exit** button. Click on the **Start** button to begin testing, and use the **Stop** button to end the test at any time.

NOTE: Do not exit the window without clicking on the Stop button.

9. Test results appear in the Status field.

Responder Tests

Responder Test

Responder tests are used to evaluate the performance of point-to-point circuits. Traditionally, 105 Responder testing is associated with T1 trunks. In the Total Control chassis, the test is performed by the modem.

The 105 Responder test is performed in two directions: Near to Far and Far to Near. In accordance with *AT&T Compatibility Bulletin No. 106*, the test measures the following:

- Any 2-way loss of signal, measured at 404, 1004 and 2804 Hz in decibels
- C-Message Noise (in dBrnC, or decibels relative to reference noise with C-message weighting)
- C-Notched Noise (in dBrnC, or decibels relative to reference noise with C-message weighting)

The 105 Responder test also measures the Signal to Noise ratio, reported in decibels.

Responder Test

The 102 Responder test is a subset of the 105 Responder test. Of the available tests, it only uses the 1004 Hz tests.

Starting the Responder Test

To launch a 102 or 105 Responder test, select a modem, select **Remote Testing** from the Fault Menu, then choose **Responder Test**. The following window is displayed.

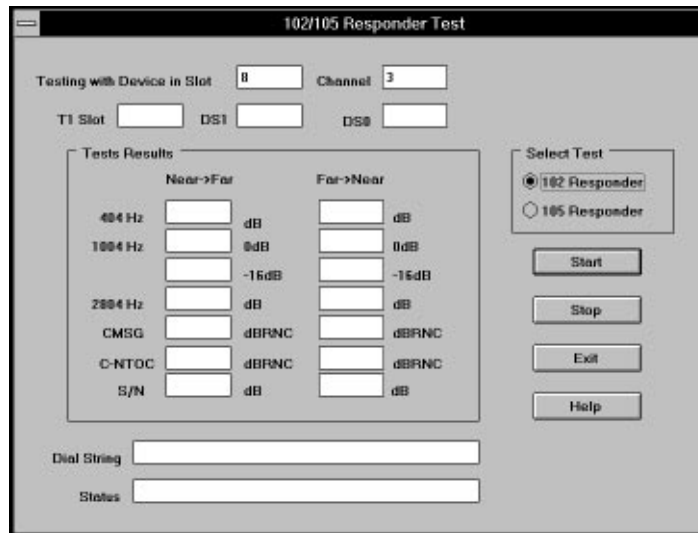


Figure 11-3. 102/105 Responder Test Window

- *Testing with Device in Slot*—displays the modem(s) selected.
- *T1 Slot/DS1/DS0*—permits selection of T1 channel.
- *Select Test*—offers either 102 or 105 Responder test.
- *Test Results*—displays test results for both directions.
- *Dial String*—permits customization of test string.
- *Status*—displays test result message.

After specifying parameters, click on the **Start** button to launch the test. Click on the **Stop** button to end the test before exiting the window.

Loop Back/Self Test/Idle Phone Line Test

Loop Back

Loop back tests check the operation of the modem's transmitter and receiver. A test pattern is looped locally or through a remote modem to verify proper operation. Any errors detected in the data stream are counted and reported. Once a loop back test is started, it will continue until you explicitly stop it. Available loop back tests are Local Analog Loop Back, Local Digital Loop Back, Remote Digital Loop Back, V.54 Local Analog Loop Back, and V.54 Remote Digital Loop Back.

NOTE: The Analog Loop Back tests cannot be performed on the Quad Digital modems, or on the Quad Analog/Digital modems when in digital mode. The Digital Loop Back tests cannot be performed by the Quad Analog modems, or the Quad Analog/Digital modems when in analog mode.

Self Tests

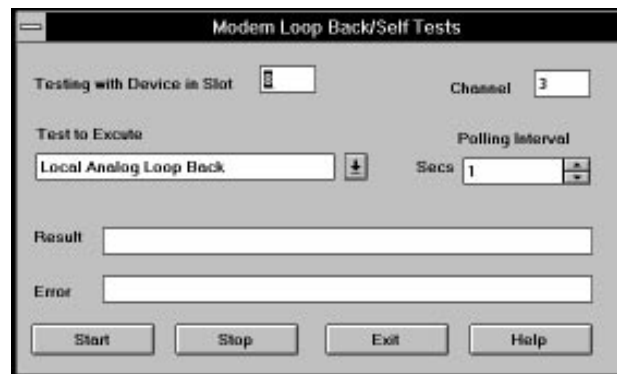
The modem has the ability to perform self tests on various parts of its hardware. These tests are performed on a pass-fail basis. Once started, these tests run to completion. Available self tests are Test RAM, Test ROM, Test NVRAM, and a comprehensive self test.

Idle Phone Line Test

When the modem is not connected, it can test to see if the phone line is functioning properly. If a modem is idle when this test is requested, it goes off hook and tests the phone line for loop current presence and dial tone presence. The modem returns information as to the condition of the phone line. If the modem is connected when this test is requested, it returns a result of unable.

Starting a Loop Back/Self Test/Idle Phone Line Test

Select a modem from the VFDP, and then select the **Modem Tests** option from the Fault Menu. The following window appears.



**Figure 11-4. Modem Loop Back/
Self Tests Window**

The Slot and Channel of the selected modem(s) appear at the top of the window. Under Tests to Execute, select the test you wish to perform, adjusting the Polling Interval as appropriate for the type of test. Click on **Start** to begin the test, and keep in mind that you must click on the **Stop** button to end a loop back test. Results and Errors are reported in the fields at the bottom of the window

Chapter 12

DS0 Configuration

Time Slot Assignment

With appropriate software release levels (at least 1.1.0 of *Total Control Manager/SNMP* and release 2.0.0 of the T1 Card), it is possible to allocate DS0 channels, enabling you to define the virtual connection from each DS0 to a modem.

The relationship between the TDM Bus and a modem is fixed, based on the modem slot and channel. The modem does not vary from its pre-defined time slot assignment. A specific DS0 may be assigned to a modem and share that time slot, enabling communication.

Configuration is performed by selecting the T1 Card from the chassis display, choosing the **Programmed Settings** option from the Configure menu or clicking on the icon, and then selecting the **DS0 <-> Modem Configuration Group**. The following window appears.

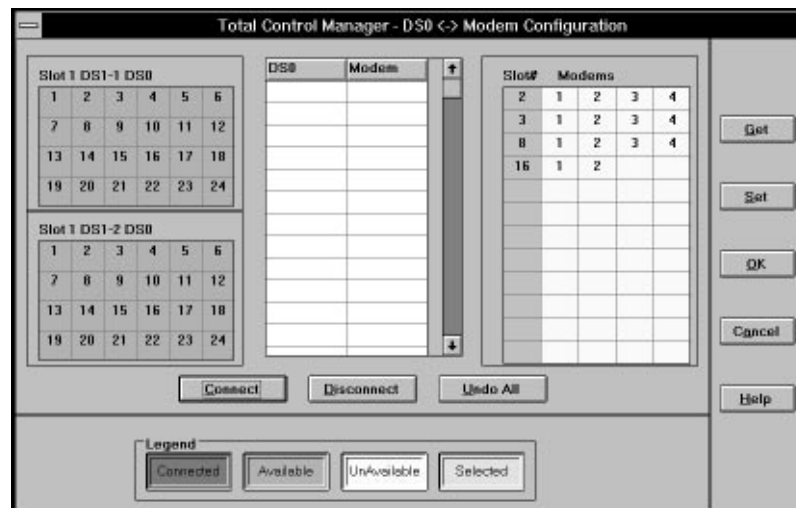


Figure 12-1. DS0 <-> Modem Configuration Window

As shown in the Legend at the bottom of the DS0 <-> Modem Configuration window, the status of time slots in this interface is represented by color, as follows:

Color	Status
Green	Connected
Orange	Available
Gray	Unavailable
Yellow	Selected

In order to connect a modem to a DS0:

1. Select an available or connected DS0 from either span line (represented in the two boxes at the left of the window) by clicking with the left mouse.
2. Select the modem slot and channel in the box at the right of the window.
3. Click on the **Connect** button at the bottom of the window.

Your connection choice appears in the box in the middle of the window.

CAUTION: Connecting a modem and DS0 through this screen will disrupt any other previously established connection involving these devices.

4. Click on the **Set** button at the right of the window to send your configurations to the chassis.

An established connection can be broken by selecting the two devices and clicking on the **Disconnect** button. The channel does not return to its original state, but instead is placed in the Unused state.

To delete a change that you have made (if you have not yet clicked on Set to send the change), click on the **Undo All** button.

DS0 Configuration

To set T1 Card parameters, select either a DS1 or the entire card from the chassis display, and then select the **Programmed Settings** icon or menu option.

Select DS1

DS1 Trunk Settings—specify that a stuffed byte should be sent to the TELCO for an inactive DS0. This is done to maintain a sufficient density of 1's in a fractional T1 application. Possible settings are 0–255; default is 254, or FE (Hex).

Select DS0

DS0 Time Slots—specify the TDM slot number used by the DS0. Possible settings are 0–64. A setting of 0 and a configuration state of Unused (see below) indicates a fractional T1 application. Any other configuration state with a time slot of 0 indicates a disconnected state.

DS0 Configuration Types—specify DS0 connection type. The only current option is the default, Connect to the TDM Bus.

DS0 Configuration States—specify the state of the DS0:

- *Normal*—the typical DS0-TDM Bus connection, and the only one that can be overridden by a Command.
- *Busy Out*—equivalent to the Hard Busy Out command. Implemented as a configuration state so that it may be saved to and restored from NVRAM.
- *Transparent*—sets a DS0 channel up so that no robbed bit signaling is performed for call set up and tear down, and data and signaling are kept separate. Requires modem compatibility. Implemented as a configuration state so that it may be saved to and restored from NVRAM.
- *Fractional/Unused*—disconnects a DS0 from the TDM Bus and sends a stuffed byte pattern to the TELCO. If a user has purchased a fractional T1 line, all DS0s that are not subscribed to should be placed in this state (see the next section, *Fractional T1 Support*).

Fractional T1 Support

Fractional T1 is a mode of T1 operation that uses only a portion of the 24 DS0s available in a DS1 span line. At the time a T1 line is ordered, the user subscribes from the TELCO for a specific number of DS0s; this is the number of channels that will be available for use by the Total Control chassis.

To set a DS1 for fractional support from within *Total Control Manager*, the DS0s that are not needed must be selected from the card on the chassis display and disabled using the Programmed Settings option. Changing the state of DS0s to and from fractional mode overrides previously made connections involving the DS0.

1. Select the T1 span line from the chassis display and select **Programmed Settings** from the Configure Menu or click on the icon.
2. Select the **DS0 Configuration States** group. A list of all 24 DS0 channels appears.
3. For each DS0 that is not to be used, select the status **Unused State**.

Chapter 13

Chassis Inventory

In order to provide a mechanism for collecting data about the chassis, *Total Control Manager/SNMP* provides an Inventory feature.

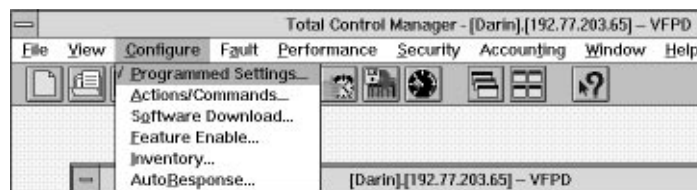


Figure 13-1. Configure Menu

As shown above, Inventory is selected from the Configure menu. The following inventory features are supported:

- Multiple Chassis inventory
- View Report
- Save to Disk
- Print Report
- Export to other application report via clipboard

The following MIB-II objects may be retrieved from any SNMP device.

Object	Example
System Description	U.S. Robotics 17-Slot Chassis
Vendor's Identification Object ID	1.3.6.1.4.1.429.2.2
IP Address	192.77.203.94

In addition to the information above, the following objects may be obtained from every NAC/NIC present in the chassis.

Object	Example
Description	USR Dual V.32 Bis Modem NAC
Hardware Version	1.0
Serial Number	30073609
Product Code	00021000
Software Version	2.2.0
DRAM	0
Flash RAM	0

To launch the feature, select **Inventory** from the Configure menu. The Device List window appears, based on the list of chassis IP addresses that have been saved for this installation of *Total Control Manager/SNMP*.



Figure 13-2. Device List Window

By default, the current chassis IP address has a red checkmark in a box to the right of the address. Customize the number of devices to be queried by clicking on the box corresponding to any additional chassis whose inventory information you want to retrieve. Then click on **OK** to start the inventory process. The Inventory window appears.

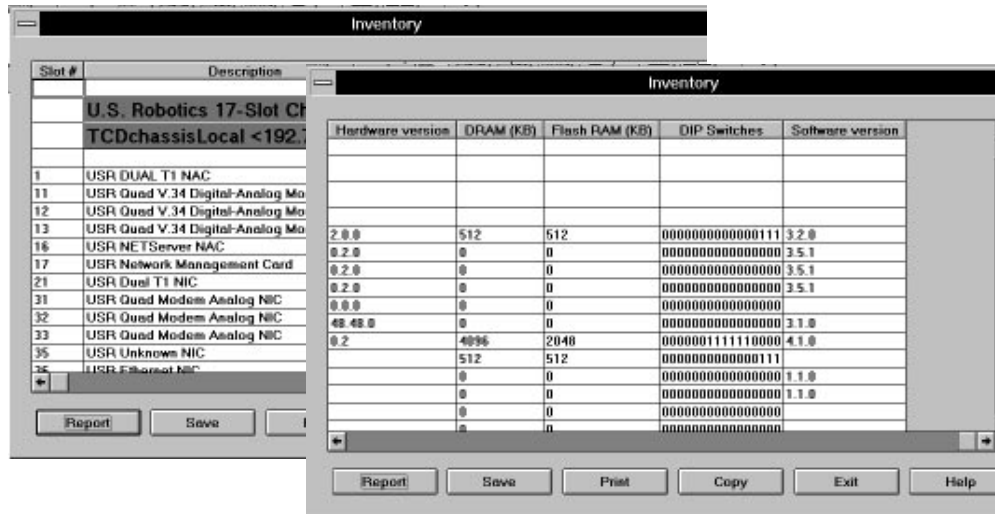


Figure 13-3. Inventory Window

Report View

When you click on the Report button in the Device Inventory window, a query is conducted of the selected device(s) to produce the inventory report. For chassis devices, the report has information for every slot containing a NAC/NIC. The slot number, description, hardware revision, serial number, product code, and software revision are reported for every slot.

Save to Disk

The Save button saves the currently displayed report to a text file. The standard File "Save As" dialog box prompts you for the file name.

Print Report

The Print button prints the currently displayed report. Printing may be performed using any printer that is supported in Windows. The report is printed to the default printer set up in the Windows Print Manager.

Export to Other Application Report via Clipboard

The Copy button transfers the report to the Windows clipboard. The Windows clipboard allows data to be transferred from one program to another. Many programs that deal with documents or other data include the Edit menu with the Paste option. When you select Paste from the menu, the program transfers the report from the Clipboard to the program.

Exit Window

Exit the Inventory window.

Help

Display a Help window with information on the Inventory feature.

Chapter 14

Accounting/Event Logging

Feature Description

Overview

By setting up Traps in the *Total Control Manager/SNMP* software to the *enableLog* setting, you ensure that certain information will be forwarded by the NMC to the Accounting Server. The *enableAll* setting will send out data both as a trap and as a log entry (see the note below). Depending on how you set up the server, it will format some or all the of data received from the NMC into logs you can view and analyze at a later time.

The NMC client communicates with the PC-based server via Ethernet or Token Ring IP LAN. Information such as call statistics and specific chassis events may be sent by NMC clients across a LAN connection to be logged. You may then use a post-processing application or database script to format the logged data.

NOTES:

- ◆ We recommend against sending log data to a server via a SLIP connection.
- ◆ We recommend the Accounting Server be on a dedicated PC and discourage locating it on the same PC to which traps are being sent.
- ◆ Use discretion when configuring Traps with the *enableAll* setting. If too much information is sent, the server PC may be overloaded. When you enable a trap *and* a log, information is sent twice from the NMC.

Installation Adjustments

The Accounting/Event Logging feature is based on RADIUS (Remote Authentication Dial In User Services), a public domain client-server protocol. The NMC runs the RADIUS client and forwards customizable data to a server whose location you specify. You must register RADIUS as a TCP/IP service after the automated installation is complete.

- ♦ If you already have a TCP/IP SERVICES file, add the following line to the file:

RADACCT 1646/UDP

Exit Windows and reboot your computer so that your system recognizes the new TCP/IP service.

- ♦ If you do not already have a SERVICES file, we have provided a sample for you to use: \NMS\BIN\NET\SERVICES.SMP.

1. Create a directory to hold the TCP configuration files, such as C:\NET\TCP.
2. Using the name of the directory you created, add the following line to your NET.CFG file:

PATH TCP_CFG C:\NET\TCP

3. Copy \NMS\BIN\NET\SERVICES.SMP to your TCP directory, giving it the name SERVICES (no extension).
4. Exit Windows and reboot your computer so that your system recognizes the new TCP/IP service.

Client Configuration

Once you have installed and loaded *TCM*, there are two aspects of the Accounting/Event Logging feature that must be configured. The best way to think of this is first to configure the NMC client, which sends the data; then configure the server, which creates logs. A full description of parameters is contained later in this chapter.

The NMC client is configured through the *Total Control Manager/SNMP* interface by selecting the NMC from the chassis display and setting specific Programmed Settings and Faults. Through *TCM*, you can configure the following objects.

NMC Logging Group

- ◆ Enable a primary and secondary server, and define the IP address of each
- ◆ Set the UDP port
- ◆ Set the number of retries the client may send to the server
- ◆ Specify the call statistics group(s) that will be sent to the server

The following parameters may be configured when you select the NMC from the chassis display, select **Programmed Settings** from the Configure Menu, and open the **Logging Group**.

Event Logging Server

Description: This parameter is used to select the RADIUS Accounting Server to be used for event logging. If you select the primary server, there will be a fallback position. That is, if the primary server were to stop accepting data for any reason, the data would be sent to a secondary server. If the secondary server were to stop accepting data, the data would no longer be sent. Information would then be lost unless you were able to get the primary server back up. If you select the secondary server and the server experienced a problem receiving data, the data would simply be lost.

Settings: primary
 secondary
 none

Default: none

Primary Log Server IP Address

Description: The IP address of the primary server.

Setting: IP Address

Secondary Log Server IP Address

Description: The IP address of the secondary server.

Setting: IP Address

Log Server's UDP Port Number

Description: This specifies the UDP port number of the RADIUS Accounting Server, and should never need to be changed. This port must be registered in your TCP/IP SERVICES file (see software installation instructions).

Default: 1646

Logging Client TX Retry

Description: This specifies how many times the NMC log client may attempt to retransmit messages to the server without an acknowledgment response.

Default: 3

Log Group Selection

Description: This parameter lets you specify which call statistics groups are included in logs. The groups are as follows:

Group 1 Usage Statistics

(always sent)

User Name
Call Start Date/Time
Call End Date/Time
Call Termination Reason
Number Dialed--OUTGOING ONLY
ANI--INCOMING ONLY
DNIS--INCOMING ONLY
Call Duration

Group 2 Data Transfer Statistics

Characters Sent
Characters Received
Octets Sent
Octets Received
Blocks Sent
Blocks Received
Blocks Resent
Characters Lost
Line Reversals

Group 3 Performance Statistics

Block CRC Errors
Link NAKs
Link Fallbacks
Link Upshifts
Link Timeouts
Initial Link TX Rate
Final Link TX Rate
Initial Link RX Rate
Final Link RX Rate
Retrans Requested
Retrans Granted

Group 4 Operating Mode Statistics

Sync/Async Mode
Modulation Type
Originate/Answer Mode
Error Control Type
Data Compression Type
HST Back Channel Rate
Default DTE Data Rate
High Freq Equali

<i>Settings:</i>	none	(only group 1 data sent)
	group2	(data from groups 1 and 2 sent)
	group3	(data from groups 1 and 3 sent)
	group4	(data from groups 1 and 4 sent)
	group23	(data from groups 1, 2 and 3 sent)
	group24	(data from groups 1, 2 and 4 sent)
	group34	(data from groups 1, 3 and 4 sent)
	all	(data from all groups sent)
<i>Default:</i>	none	

NMC Logging Traps

- ♦ Enable a trap to be generated on the loss of the server

Logging Server Has Been Lost Trap

This parameter may be configured when you select the NMC from the chassis display, select **Trap Settings** from the Faults Menu, and open the **Logging Group**.

Description: Enable/disable the trap generated when communication is lost with the logging server. This trap reports a trap sequence number, an event ID, the time the loss occurred (GMT), and whether the primary or secondary accounting server was lost.

Settings: enable
 disable

Default: disable

Other Devices Faults/Groups

Event log record generation for other chassis events is controlled by extending the trap enable/disable mechanism. Where previously there was only an option to enable/disable a trap, most traps now include options so that you may specify enable/disable for both trap and log record generation. The default trap setting is Disable All; you may also select Enable Trap, Enable Log, or Enable All.

NOTE: Not all traps have these options. View the available options for a specific trap object to determine which traps may be set in this fashion.

Server Configuration

Once the NMC has been programmed to send data to the server, additional configuration is required to format the data when it is logged. The RADIUS protocol allows the NMC to communicate its log data to generic RADIUS servers, making the NMC compatible with an open systems log facility. Wherever possible, the NMC log records use the standard RADIUS attributes in order to maximize the amount of data that can be interpreted by a generic RADIUS report generator. RADIUS provides a robust delivery mechanism for the log records by using an acknowledged UDP/IP protocol.

Two types of RADIUS accounting packets are used:

- ♦ *Accounting-Request*. To log an event, the NMC client sends an *Accounting-Request* packet containing the event log information to the IP address of the selected server.
- ♦ *Accounting-Response*. The server processes the packet and responds to the NMC with an *Accounting-Response* packet.

Within an *Accounting-Request* packet, there can be a number of attributes containing the information to be stored. Each attribute *Type* corresponds to a specific item defined by the RADIUS draft. The NMC client has over 40 pieces of information that do not fall under defined attribute *Types* and must use the *Vendor-Specific* attribute. The USR data is encapsulated within this attribute. Definitions are contained later in this chapter.

The Accounting/Event Logging application operates on one set of files for a 24-hour period. At midnight, the server closes the files and opens a new set of log files. The files are named using the format *yyymmdd.ext*, where *yy* = year, *mm* = month, *dd* = date, and *ext* is the three character extension defined for the file type (typically *.con*, *.rad*, or *.nmc*).

If the server runs out of available disk space, the application is closed and the clients are forced to switch to an alternate server. To prevent this from happening, an administrator should set up scripts to delete unnecessary log files when *NEW_LOG_FILE* and *DISK_LOW* messages are received.

Editing the Output Definition (OUTDEF.DAT) File

An external database definition file is used to define the format for each of the output tables. The file maps attributes (defined in the dictionary file—see the next section) to specific column (field) positions in the output file.

TCM installation places the OUTDEF.DAT file in the C:\NMS\BIN\ACCTING directory. See instructions for editing this file later in this chapter under *Server Configuration*.

The OUTDEF.DAT file is the mechanism that permits you to control the content of the three logs. By editing the OUTDEF.DAT file, you can exert a high level of control over the content of the logs as well as automate actions to be taken at different stages of log creation. You may use your preferred text editor to edit the OUTDEF.DAT file so it will generate and customize desired logs.

File Syntax

In order to generate logs, the OUTDEF.DAT file must be edited using the correct syntax. There are three components to this syntax that need to be understood: keywords, attributes, and format specifiers.

- ♦ The following are recognized keywords:

Keyword	Description
FILE	Which log file is to be created (should always be followed by a list of attributes to be included in the file)
TIME	Whether local or GMT time is to be used
PATH	Where the log file is to be stored
DISK_LOW	What action to take on low disk space
DISK_FULL	What action to take on full disk space
NEW_LOG_FILE	What action to take when log is closed

- ♦ If the first field of a line does not contain one of these keywords, it is parsed as an attribute. Attributes are contained in the dictionary file (ACCTDICT.DAT). The attributes that follow a line containing the keyword FILE indicate that the values for those attributes are to be stored in a log file (.con, .rad, or .nmc).
- ♦ The format specifier is an optional element of the attribute line that allows you to specify what format is used to store the attribute value in the log.

Keyword Descriptions

FILE

This indicates a log file to be defined, and has three fields:

- ♦ keyword FILE
- ♦ reference name of the log file (e.g., NMC_CONNECTIVITY)
- ♦ suffix of the log file (3 character limit), used to indicate the type of information stored (e.g., con, rad, or nmc)

The name of the log file is the date in the format yymmdd followed by “.” and the suffix (con, nmc, or rad).

Example

```
FILE          NMC_CONNECTIVITY      con
```

TIME

This indicates what time zone to use for any time that appears in the log file. It has two fields:

- ♦ keyword TIME
- ♦ time zone (must be GMT or LOCAL)

If TIME does not appear, the default is LOCAL.

Example

```
TIME                      GMT
```

PATH

This indicates the directory that the log files are written to. It has two fields:

- ♦ keyword PATH
- ♦ the directory path

If PATH does not appear, the default is the directory in which the accounting server executes, represented as a period.

Example

```
PATH                      .\files
```

NOTE: The directory must exist in order for the log file to be created. The example specifies a subdirectory (indicated by the “\”) named “files” that is under the directory from which the accounting server is

launched (indicated by the “.”). If the server were to be launched from a different directory (e.g., using Program Manager), the path indicated in the example may be invalid and the file may not be created.

DISK_LOW

This keyword indicates what to do when the free disk space is at a minimum. It has three fields:

- ♦ keyword DISK_LOW
- ♦ .exe/.bat file to be executed (optional)
- ♦ free disk space threshold in MBytes (optional)

Disk space is checked periodically, and if the free disk space threshold is reached, the defined .exe/.bat file is executed using the PATH of the log files as a parameter. This should be used to free up disk space, typically by purging the accounting log files. If the DISK_LOW keyword does not appear, a default of 10 Mbytes is assigned for the free disk space threshold.

Example

DISK_LOW	disklow.bat	12
----------	-------------	----

DISK_FULL

This keyword indicates what to do when the free disk space is at a fatal level. It has three fields:

- ♦ keyword DISK_FULL
- ♦ .exe/.bat file to be executed (optional)
- ♦ fatal free disk space threshold in MBytes (optional)

When the disk full threshold is reached, the defined .exe/.bat file is executed. This .exe/.bat may be used in the event that DISK_LOW fails to increase the free disk space; typically, this might be used to initiate an alarm of some kind, page an administrator, etc. If DISK_FULL does not appear in the file, a default of 5 MBytes is assigned for the fatal free disk space limit. If the .exe/.bat is omitted, the file USBEEP.EXE is run to provide alarm indication. After the file is executed the server application will terminate.

Example

DISK_FULL	diskfull.bat	6
-----------	--------------	---

NEW_LOG_FILE

This keyword indicates what to do when log files are closed at midnight. It has two fields:

- ♦ keyword NEW_LOG_FILE
- ♦ .exe/.bat file to be executed

At midnight, each log file is closed and new log files reflecting the new date are created. After the new log files are created, the .exe/.bat is executed using the PATH of the log files as a parameter. This .exe/.bat typically purges and/or imports the old log file into a database.

Example

NEW_LOG_FILE

newlog.bat

Format Specifiers

Each attribute definition has two fields:

- ♦ attribute name
- ♦ format specifier (optional)

The format specifier overrides the default specifier provided by the dictionary file. Each attribute has a type that has a number of format options.

All transactions are composed of Attribute/Value pairs. The value of each attribute is specified as one of four data types. Enumerated values are stored in the user file with dictionary VALUE translations for easy administration. See *Attribute/Data Type Descriptions* at end of this chapter for a list of all valid Attributes.

Valid data types are:

Data Type	Definition	Format Options
string	0–254 octets	no additional formatting available
ipaddr	4 octets in network byte order	Three different format options are available: IPdot, e.g., 192.203.77.91 IPhex, e.g., C0CB4D5B IPdec, e.g., 3234549083

Data Type	Definition	Format Options
integer	32 bit value in big endian order (high byte first)	Two different format options are available: [Text]% % replaced by the integer value value print out corresponding VALUE dictionary text
date	32 bit value in big endian order—seconds since 00:00:00 GMT, Jan. 1, 1970	Five different format options are available: date1 mm/dd/yy hh:mm:ss date2 dd-mm-yy hh:mm:ss date3 yymmddhhmmss date4 example: Wed Jan 02 02:03:55 1980 date5 seconds since 00:00:00 Jan. 1, 1970

Programming Attributes

After the keyword FILE, which begins defining an output file, you must list attributes whose values you want to be included in the file. Each attribute is represented by a column in the file. Beside each entry, an optional format string can be provided that will override the format string provided by the dictionary.

Example—Connection Log

These records provide call information from the NMC client, using two types of events: Event-Id = Incoming-Connection-Terminated or Event-Id = Outgoing-Connection-Terminated. The example below contains only selected attributes (many more are available).

FILE	NMC_CONNECTIVITY	.con	
	Client-Id	IPdot	
	Chassis-Slot	%	
	Channel	%	
	Event-Date-Time	Date1	
	Event-Id	%	
	Acct-Session-Id		
	User-Name	string	User:VALUE
	Call-Start-Date-Time	Date1	
	Call-End-Date-Time	Date1	
	Connect-Term-Reason	%	
	Acct-Session-Time	integer	
	Acct-Input-Octets	integer	
	Acct-Output-Octets	integer	
	Default-DTE-Data-Rate	%	
	Last-Number-Dialed-In-DNIS	string	
	Last-Number-Dialed-Out	string	
	Last-Callers-Number-ANI	string	

Example—Event Log

The event log table stores event information generated by an NMC client, but not recorded in the Call Termination Log. This includes such things as Module-Inserted, Connection-Attempt-Failed, etc.

FILE	NMC_EVENTLOG	.nmc
	Client-Id	IPdot
	Chassis-Slot	%
	Channel	%
	Event-Date-Time	Date1
	Event-Id	%
	Acct-Session-Id	
	Failure-to-Connect-Reason	%
	Server-Time	Date1
	Client-Port-Id	%

Example—Native RADIUS Log

The generic RADIUS table stores events that do not have the USR specific Event-Id attribute (i.e., non-NMC events). Any attributes of interest must be entered into this file definition or they will be discarded.

FILE	GENERIC_RADIUS	.rad
	Client-Id	IPdot
	Server-Time	Date1
	Acct-Status-Type	%
	Acct-Session-Id	
	Acct-Session-Time	%

Editing the Dictionary (ACCTDICT.DAT) File

The dictionary file matches attribute numbers to their type and a textual representation. TCM installation places the file ACCTDICT.DAT file in the C:\NMS\BIN\ACCTING directory. The ACCTDICT.DAT file should not be edited, but may be referred to for the names of attributes to be programmed into the OUTDEF.DAT file.

A dictionary file matches attribute numbers to their type and a text representation. The following line defines attribute 6 to represent User-Service-Type using an integer value.

ATTRIBUTE	User-Service-Type	6	integer
-----------	-------------------	---	---------

The integer value held by this attribute may be further described by a VALUE entry later in the file:

VALUE	User-Service-Type	Login-User	1
VALUE	User-Service-Type	Framed-User	2
VALUE	User-Service-Type	Dialback-Login-User	3

The USR implementation extends the dictionary specification to define USR-specific attributes and provide output formatting capability. An additional keyword, ATTRIB_NMC, is used to define USR attributes, for example:

ATTRIB_NMC	Attrib-Name	Attrib-Number	Datatype	Format
------------	-------------	---------------	----------	--------

Native RADIUS attributes and USR-specific attributes belong to the same name-space (i.e., there cannot be a USR attribute *User-Name*). The server application treats all attributes equally after they are extracted from the request packet. The Attrib-Number for USR attributes is a 16-bit value rather than the RADIUS 8-bit value. The datatype is limited to the original RADIUS specification (i.e., integer, string, IP address, date). Format specifies additional output formatting, for example:

ATTRIB_NMC	Slot-Index	0xBF39	integer	Slot-%
------------	------------	--------	---------	--------

If a value of 10 is returned in the USR Slot-Index attribute, it is written to the database as: "Slot-10".

Log Generation

The NMC client removes an event record from its input queue, formats it properly for the Accounting server, sends it, and waits for the reply before starting on the next event record. If communication is lost between the NMC and the primary server, data will be sent to the secondary server. If communication is lost with the secondary server before it is re-established with the primary server, the NMC client discards the event records.

The Accounting/Event Logging application operates on one set of files for a 24-hour period. At midnight, the server closes and re-initializes the files. This means that log files are not available for import on the same day they are generated. The files are named using the format *yymmdd.ext*, where *yy* = year, *mm* = month, *dd* = date, and *ext* is the three character extension defined for the file type (typically *.con*, *.rad*, or *.nmc*).

The NMC client can receive event records from 65 possible sources—one NMC and a possible 64 modems (16 Quad Modem cards). The NMC client also has an input queue capable of handling 65 event records. This allows for the maximum possible requesters to be issuing event records simultaneously. If the input queue of the NMC client becomes overloaded, the requester's attempt to issue an event record will be rejected. It is up to the requester to handle these rejections. Until the rejections are dealt with, the events are discarded.

If the server runs out of available disk space, the application is closed and the clients are forced to switch to an alternate server. To prevent this from happening, an administrator should set up scripts for *NEW_LOG_FILE* and *DISK_LOW* to delete log files when they are no longer required.

The Accounting/Event Logging server sorts input requests and writes them to three separate tab-delimited logs. RADIUS event information is written to the Native RADIUS Call Log. NMC event records are separated according to event type: call-related event records are written to the Call Termination Log and all other NMC/Chassis event records are written to the Event Log.

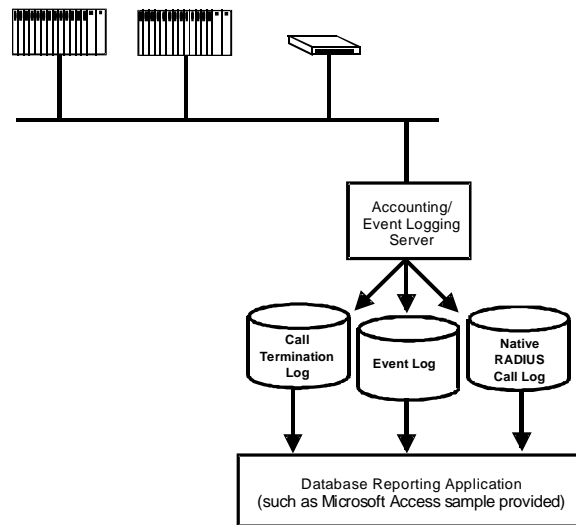


Figure 14-1. Log Files Generated

The log files generated by the server can be imported into any Windows-compatible database application, such as MS Access or Excel, to be used for specific reporting purposes.

Native RADIUS Call Log (.rad)

The Native RADIUS Call Log collects all native RADIUS standard attributes. This table is currently empty.

Event Log (.nmc)

Depending on your configuration of the NMC client, the Event Log collects all NMC event records sent to the server, except call termination records. This data is formatted in the log according to your customization of the output definition file. The mechanism for collecting and formatting Event Log records is basically the same as for the Call Termination Log, except that if an attribute is sent that does not have an associated column, it is formatted using the dictionary and appended to the table's final column (not listed in the output definition file). It is, therefore, important to have dedicated columns for all regularly sent attributes, otherwise they are placed in this default column.

This method allows all chassis event records to exist in a single table. If set up correctly, the last column will represent a textual description of the event and relevant values. For example, a Module-Inserted event might give the card description V.34_Dual_Modem.

The event record format may be extended to include the necessary event information. The following information is included with all event records.

- ◆ UDP Port Number
- ◆ Event Sequence Number
- ◆ Event Identifier
- ◆ Event Date/Time Stamp

The following table identifies the information sent in the log record for each event, in addition to the standard fields listed above. The Generic Slot Record consists of the Slot Number and Module Type. The Entity Index indicates a description beyond slot, e.g., modem channel.

Events	Additional Information In Event Record
Module Inserted (6)	Generic Slot Record
Module Removed (7)	Generic Slot Record
PSU Voltage out of Range (8)	Expected voltage Actual voltage
PSU Failed (9)	PSU Index
HUB Temperature out of Range (10)	Chassis temperature Temperature threshold
Fan Failed (11)	No additional information
Module Watchdog Time-out (12)	Generic Slot Record
Management Bus Failure (13)	Generic Slot Record Entity Index
Incoming Connection Established (14)	Generic Slot Record Call status Entity Index
Outgoing Connection Established (15)	Generic Slot Record Call status Entity Index
Incoming Connection Terminated (16)	See following description
Outgoing Connection Terminated (17)	See following description
Connection Attempt Failed (18)	Generic Slot Record Entity Index Failure to connect reason
Connection Time Limit Expired (19)	Generic Slot Record Entity Index Connect time limit
DTE Transmit Idle (20)	Generic Slot Record Entity Index DTE Data Idle Timeout

Events	Additional Information In Event Record
DTR True (21)	Generic Slot Record Entity Index DTR True Timeout
DTR False (22)	Generic Slot Record Entity Index DTR False Timeout
Block Error Count at Threshold (23)	Generic Slot Record Entity Index Block Error Count Limit
Fallback Count at Threshold (24)	Generic Slot Record Entity Index Fallback Count Limit
No Dial Tone Detected (25)	Generic Slot Record Entity Index
No Loop Current Detected (26)	Generic Slot Record Entity Index
Modem Reset by DTE (32)	Generic Slot Record Entity Index
Modem Ring No Answer (33)	Generic Slot Record Entity Index Ring No Answer Limit
DTE Ring No Answer (34)	Generic Slot Record Entity Index Ring No Answer Limit
Dial Out Login Failure (42)	Generic Slot Record Entity Index User Name
Dial In Login Failure (43)	Generic Slot Record Entity Index User Name
Dial Out Restricted Number (44)	Generic Slot Record Entity Index User Name
Dial Back Restricted Number (45)	Generic Slot Record Entity Index User Name
User Blacklisted (46)	Generic Slot Record Entity Index User Name
Attempted Login by Blacklisted User (47)	Generic Slot Record Entity Index User Name
Response Attempt Limit Exceeded (48)	Generic Slot Record Entity Index User Name Security Response Limit
Modem Login Attempt Limit Exceeded (49)	Generic Slot Record Entity Index User Name Security Login Limit

Call Termination Log (.con)

Depending on your configuration of the NMC client, the Call Termination Log collects call termination records generated by the chassis modems. This data is formatted in the log according to your customization of the output definition file. The table format may have a column assigned for each possible attribute (both RADIUS and USR) that can be sent for these events. An NMC can be configured to send additional information, depending on user requirements, based on four different groups of statistics. The current default configuration sends messages from the first group, Usage Statistics. These statistics are combined with the Generic Slot record and the Entity Index to yield the following fields:

- Client-Id
- Client-Port-Id
- Acct-Session-Id
- Event-Id
- Event-Date-Time
- Acct-Status-Type
- Chassis-Slot
- Channel
- User-Name
- Acct-Session-Time
- Call-Start-Date-Time
- Call-End-Date-Time
- Connect-Term-Reason
- Last-Number-Dialed-In-DNIS
- Last-Caller's-Number-ANI
- Dialback-No
- Server-Time

The mechanism for collecting and formatting these records is to place each attribute from the input packet into a column defined in the output definition file. If an attribute is located that does not have an associated column, it is silently discarded. Any "empty" columns are filled with the delimiting character (tab).

Event Records for Incoming Connection Terminated (16) and Outgoing Connection Terminated (17) are identical, except as noted in the table below (ANI, Number Dialed, and DNIS in Group 1).

Incoming Connection Terminated (16)	Generic Slot Record Entity Index
and	Usage Statistics (Group 1 - always sent): User Name (mdmCsSecurityUserName) Call Start Date/Time Call End Date/Time Call Termination Reason (mdmCsDisconnectReason) ANI (mdmCsLastCallingPartyNum)--INCOMING ONLY Number Dialed (mdmCsLastNumberDialedOut)--OUTGOING ONLY DNIS (mdmCsLastNumberDialedIn)--INCOMING ONLY Call Duration (mdmCsCallDuration)
Outgoing Connection Terminated (17)	Data Transfer Statistics (Group 2): Characters Sent (mdmCsCharsSent) Characters Received (mdmCsCharsReceived) Octets Sent (mdmCsOctetsSent) Octets Received (mdmCsOctetsReceived) Blocks Sent (mdmCsBlocksSent) Blocks Received (mdmCsBlocksReceived) Blocks Resent (mdmCsBlocksResent) Characters Lost (mdmCsCharsLost) Line Reversals (mdmCsLineReversalQty) Performance Statistics (Group 3): Block CRC Errors (mdmCsBlerQty) Link NAKs (mdmCsLinkNakQty) Link Fallbacks (mdmCsFallbackQty) Link Upshifts (mdmCsUpshiftQty) Link Timeouts (mdmCsLinkTimeoutQty) Initial Link TX Rate (mdmCsInitialTxLinkRate) Final Link TX Rate (mdmCsFinalTxLinkRate) Initial Link RX Rate (mdmCsInitialRxLinkRate) Final Link RX Rate (mdmCsFinalRxLinkRate) Retrains Requested (mdmCsRetrainsRequested) Retrains Granted (mdmCsRetrainsGranted) Operating Mode Statistics (Group 4): Sync/Async Mode (mdmCsSyncAsyncModeUsed) Modulation Type (mdmCsModulationType) Originate/Answer Mode (mdmCsOriginateAnswer) Error Control Type (mdmCsErrorControlType) Data Compression Type (mdmCsCompressionType) HST Back Channel Rate (mdmCsBackChannelRate) Default DTE Data Rate High Freq Equalization (mdmCsEqualizationType) On-Line Fallback (mdmCsFallbackEnabled)

Using the Prototype Database

We expect that each customer has unique requirements for call accounting history and reporting. A prototype MS Access v.2.0 database reporting application is supplied along with *Total Control Manager/SNMP*. This application uses sample data that is stored in a file named ACCTSAMP.MDB, which is placed in the C:\NMS\BIN\ACCTING directory.

This application is intended to serve as a starting point in assisting customers to generate their unique reports. We encourage the user to customize the type of information to capture and maintain in the log files.

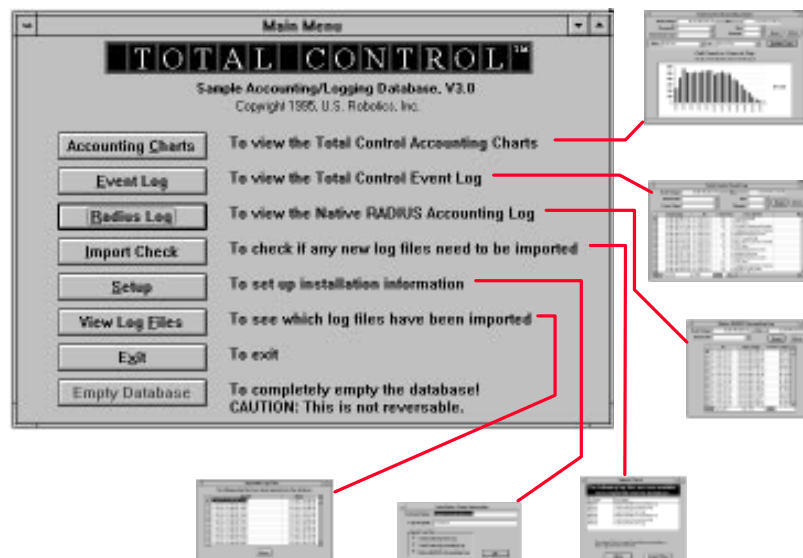


Figure 14-4. Total Control Accounting Application Main Menu

This prototype application provides samples of the following:

- ◆ Automated Log File Importing
- ◆ Total Control Call Accounting Charts
- ◆ Total Control Event Filtering and Reporting
- ◆ Native RADIUS Call Filtering and Reporting

Launching the Accounting Report Sample Application

When you install *TCM*, icons for the Accounting Server and the Accounting Report are placed in the Windows NMS group. Double click on the **Accounting Server** icon to launch the accounting server; double click on the **Accounting Report** icon to launch the prototype database application we have provided to serve as an example of how to manipulate log data.

Both the Accounting Server and the Accounting Report sample database application can also be launched from either the *TCM* Main Menu:



Figure 14-2. TCM Accounting Menu

or from the Novell NMS Main Menu:

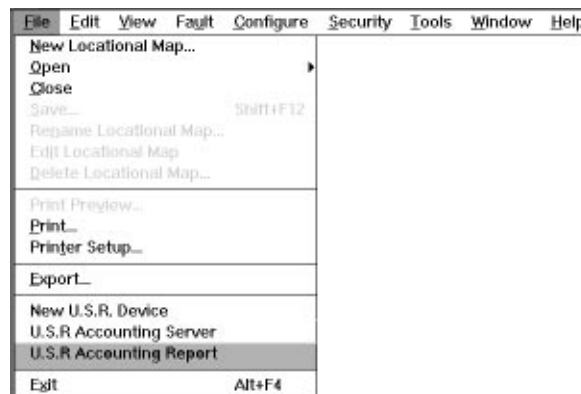


Figure 14-3. NMS File Menu

Automated Log File Importing

Log files are generated daily with the data you have configured. The prototype application provides a simple means to import the log files that have been generated by the system. From the Main Menu of the Accounting application, click on **Import Check** to see if new files have been generated. Then start the import to incorporate all the new data into the application, and then view the new log files.

NOTE: Log files are not available for import on the same day they are generated. They become available after midnight when the files are closed.

Log File Import Management

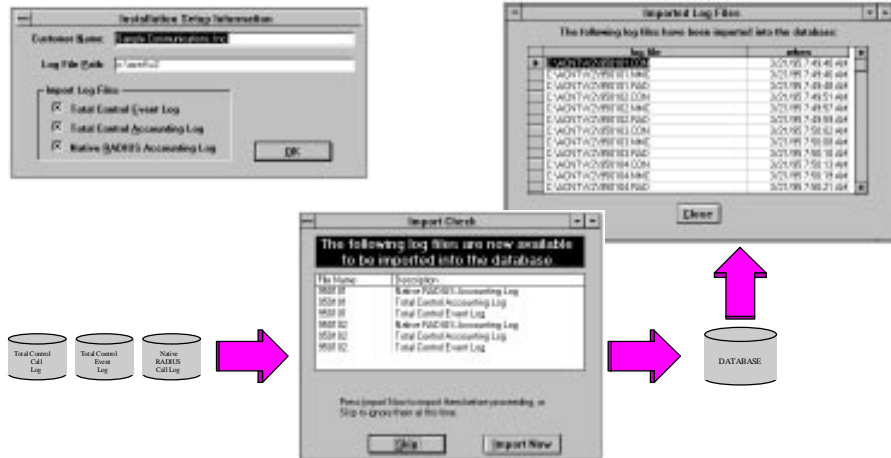


Figure 14-5. Total Control Log File Management

Total Control Call Accounting Charts

Click on **Accounting Charts** on the Main Menu to customize and display charts built from the log data. Statistics are pulled from the call termination events for chassis modems.

Call Accounting Statistics

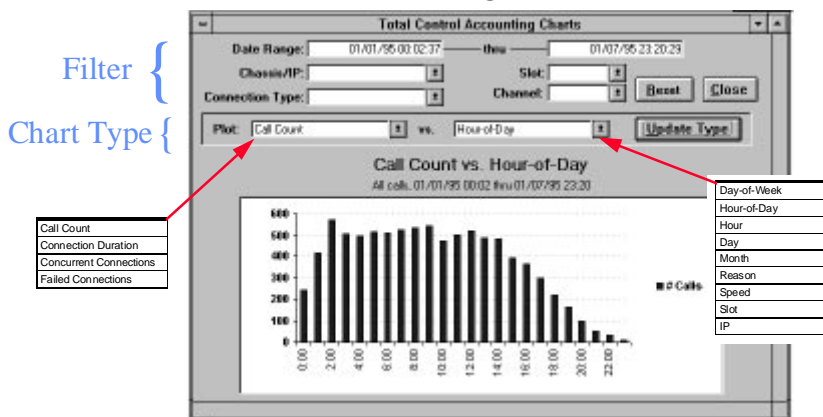


Figure 14-6. Total Control Call Accounting Statistics

Total Control Event Filtering and Reporting

Click on **Event Log** so system events can be programmed to generate log entries, and that data can then be filtered to meet your own reporting needs. This is an especially powerful feature when combined with the Auto Response and Security options.

Chassis Event Log

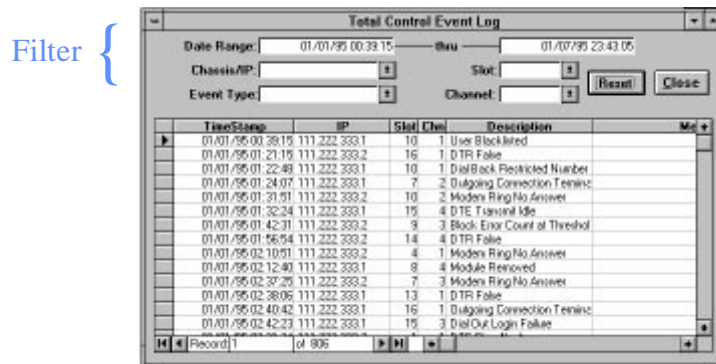


Figure 14-7. Total Control Event Reporting

Native RADIUS Call Filtering and Reporting

All native RADIUS data may also be captured and logged. Click on **RADIUS Log**.

Native RADIUS Call Log

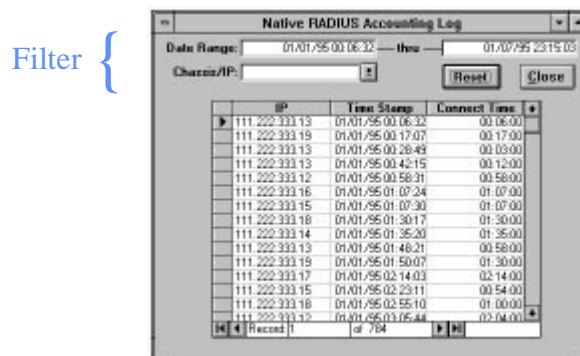


Figure 14-8. Native RADIUS Call Log

Attribute/Data Type Descriptions

The following pages contain these tables:

Table 1. Log Message RADIUS Attributes and Data Types

Table 2. USR Vendor Specific Attributes and Data Types per Event Type (Event IDs 06 through 21)

Table 3. USR Vendor Specific Attributes and Data Types per Event Type (Event IDs 22 through 49)

USR Event	Event ID	RADIUS Attributes (Value) and Data Types									
		User Name (1)	Client ID (4)	Client Port ID (5)	Dial Back No. (19)	Vendor Spec. (26)	Acct. Status Type (40)	Acct. Input Octets (42)	Acct. Output Octets (43)	Acct. Sess. ID (44)	Acct. Sess. Time (46)
Card Inserted	06		S,A	S,I		S,V				S,I	
Card Removed	07		S,A	S,I		S,V				S,I	
Power Supply Warning	08		S,A	S,I		S,V				S,I	
Power supply failed	09		S,A	S,I		S,V				S,I	
Temperature Warning	10		S,A	S,I		S,V				S,I	
Fan Failed	11		S,A	S,I		S,V				S,I	
Watchdog Timeout	12		S,A	S,I		S,V				S,I	
Management Bus Failure	13		S,A	S,I		S,V				S,I	
Incoming Connection Est.	14		S,A	S,I		S,V	S,I			S,I	
Outgoing Connection Est.	15		S,A	S,I		S,V	S,I			S,I	
Incoming Connection Term.	16	S,C	S,A	S,I	S,C	S,V	S,I	O2,I	O2,I	S,I	S,I
Outgoing Connection Term.	17	S,C	S,A	S,I		S,V	S,I	O2,I	O2,I	S,I	S,I
Connection Attempt Failure	18		S,A	S,I		S,V				S,I	
Connection Timer Expired	19		S,A	S,I		S,V				S,I	
DTE Transmit Data Idle	20		S,A	S,I		S,V				S,I	
DTR True	21		S,A	S,I		S,V				S,I	
DTR False	22		S,A	S,I		S,V				S,I	
BLER Count at Threshold	23		S,A	S,I		S,V				S,I	
Fallback Count at Threshold	24		S,A	S,I		S,V				S,I	
No Dial Tone	25		S,A	S,I		S,V				S,I	
No Loop Current	26		S,A	S,I		S,V				S,I	
Modem Reset By DTE	32		S,A	S,I		S,V				S,I	
Modem Ring No Answer	33		S,A	S,I		S,V				S,I	
DTE Ring No Answer	34		S,A	S,I		S,V				S,I	
Dial Out Login Failure	42	S,C	S,A	S,I		S,V				S,I	
Dial In Login Failure	43	S,C	S,A	S,I		S,V				S,I	
Dial Out Restricted No.	44	S,C	S,A	S,I		S,V				S,I	
Dial Back Restricted No.	45	S,C	S,A	S,I		S,V				S,I	
User Blacklisted	46	S,C	S,A	S,I		S,V				S,I	
Blacklisted User Login Att.	47	S,C	S,A	S,I		S,V				S,I	
Resp. Att. Limit Exceeded	48	S,C	S,A	S,I		S,V				S,I	
Login Att. Limit Exceeded	49	S,C	S,A	S,I		S,V				S,I	

S = Standard

O = Optional. Part of Call Termination statistics group n.

Data Types: A = IP Address, I = Integer, C = Character String, T = GMT date/time,

V = Variable (see Vendor Specific attribute table).

Table 1. Log Message RADIUS Attributes and Data Types

			USR Event IDs																	
USR Attribute	Attr. Value	Data Type	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21		
DTE-Data-Idle-Timeout	0x0048	I															S			
Default-DTE-Data-Rate	0x005E	I											O4	O4						
Last-Number-Dialed-Out	0x0066	C												S						
Sync-Async-Mode	0x0067	I											O4	O4						
Originate-Answer-Mode	0x0068	I											O4	O4						
Failure-to-Connect-Reason	0x0069	I													S					
Initial-Tx-Link-Data-Rate	0x006A	I											O3	O3						
Final-Tx-Link-Data-Rate	0x006B	I											O3	O3						
Modulation-Type	0x006C	I											O4	O4						
Equalization-Type	0x006F	I											O4	O4						
Fallback-Enabled	0x0070	I											O4	O4						
Characters-Sent	0x0071	I											O2	O2						
Characters-Received	0x0072	I											O2	O2						
Blocks-Sent	0x0075	I											O2	O2						
Blocks-Received	0x0076	I											O2	O2						
Blocks-Resent	0x0077	I											O2	O2						
Retrains-Requested	0x0078	I											O3	O3						
Retrains-Granted	0x0079	I											O3	O3						
Line-Reversals	0x007A	I											O2	O2						
Number-Of-Characters-Lost	0x007B	I											O2	O2						
Back-Channel-Data-Rate	0x007C	I											O4	O4						
Number-of-Blers	0x007D	I											O3	O3						
Number-of-Link-Timeouts	0x007E	I											O3	O3						
Number-of-Fallbacks	0x007F	I											O3	O3						
Number-of-Upshifts	0x0080	I											O3	O3						
Number-of-Link-NAKs	0x0081	I											O3	O3						
Simplified-MNP-Levels	0x0099	I											O4	O4						
Connect-Term-Reason	0x009B	I											S	S						
DTR-False-Timeout	0x00BE	I																		
Fallback-Limit	0x00BF	I																		
Block-Error-Count-Limit	0x00C0	I																		
Simplified-V42bis-Usage	0x00C7	I											O4	O4						

On = Optional. Part of Call Termination statistics group n.

S = Standard

Data Types: C = Character String, I = Integer, T = GMT date/time

Table 2. USR Vendor Specific Attributes and Data Types per Event Type (Event IDs 06 through 21)

			USR Event IDs																	
USR Attribute	Attr. Value	Data Type	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21		
DTR-True-Timeout	0x00DA	I																S		
Last-Number-Dialed-In-DNIS	0x00E8	C											S							
Last-Callers-Number-ANI	0x00E9	C											S							
Chassis-Temp-Threshold	0xBE84	I					S													
Card-Type	0xBE85	I	S	S																
Security-Login-Limit	0xBEDE	I																		
Security-Resp-Limit	0xBEFA	I																		
DTE-Ring-No-Answer-Limit	0xBF17	I																		
Final-Rx-Link-Data-Rate	0xBF2C	I											O3	O3						
Initial-Rx-Link-Data-Rate	0xBF2D	I											O3	O3						
Event-Date-Time	0xBF2F	T	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S		
Chassis-Temperature	0xBF31	I					S													
Actual-Voltage	0xBF32	I			S															
Expected-Voltage	0xBF33	I			S															
Power-Supply-Number	0xBF34	I				S														
Channel	0xBF38	I							S	S	S	S	S	S	S	S	S	S		
Chassis-Slot	0xBF39	I	S	S					S	S	S	S	S	S	S	S	S	S		
Event-Id	0xBFBE	I	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S		
Number-of-Rings-Limit	0xBFE6	I																		
Connect-Time-Limit	0xBFE7	I														S				
Call-End-Date-Time	0xBFF6	T											S	S						
Call-Start-Date-Time	0xBFF7	T											S	S						

On = Optional. Part of Call Termination statistics group n.

S = Standard

Data Types: C = Character String, I = Integer, T = GMT date/time

Table 2. (Continued)

			USR Event IDs																
USR Attribute	Attr. Value	Data Type	22	23	24	25	26	32	33	34	42	43	44	45	46	47	48	49	
DTE-Data-Idle-Timeout	0x0048	I																	
Default-DTE-Data-Rate	0x005E	I																	
Last-Number-Dialed-Out	0x0066	C																	
Sync-Async-Mode	0x0067	I																	
Originate-Answer-Mode	0x0068	I																	
Failure-to-Connect-Reason	0x0069	I																	
Initial-Tx-Link-Data-Rate	0x006A	I																	
Final-Tx-Link-Data-Rate	0x006B	I																	
Modulation-Type	0x006C	I																	
Equalization-Type	0x006F	I																	
Fallback-Enabled	0x0070	I																	
Characters-Sent	0x0071	I																	
Characters-Received	0x0072	I																	
Blocks-Sent	0x0075	I																	
Blocks-Received	0x0076	I																	
Blocks-Resent	0x0077	I																	
Retrains-Requested	0x0078	I																	
Retrains-Granted	0x0079	I																	
Line-Reversals	0x007A	I																	
Number-Of-Characters-Lost	0x007B	I																	
Back-Channel-Data-Rate	0x007C	I																	
Number-of-Blers	0x007D	I																	
Number-of-Link-Timeouts	0x007E	I																	
Number-of-Fallbacks	0x007F	I																	
Number-of-Upshifts	0x0080	I																	
Number-of-Link-NAKs	0x0081	I																	
Simplified-MNP-Levels	0x0099	I																	
Connect-Term-Reason	0x009B	I																	
DTR-False-Timeout	0x00BE	I	S																
Fallback-Limit	0x00BF	I			S														

On = Optional. Part of Call Termination statistics group n.

S = Standard

Data Types: C = Character String, I = Integer, T = GMT date/time

Table 3. USR Vendor Specific Attributes and Data Types per Event Type (Event IDs 22 through 49)

USR Attribute	Attr. Value	Data Type	USR Event IDs															
			22	23	24	25	26	32	33	34	42	43	44	45	46	47	48	49
Block-Error-Count-Limit	0x00C0	I		S														
Simplified-V42bis-Usage	0x00C7	I																
DTR-True-Timeout	0x00DA	I																
Last-Number-Dialed-In-DNIS	0x00E8	C																
Last-Callers-Number-ANI	0x00E9	C																
Chassis-Temp-Threshold	0xBE84	I																
Card-Type	0xBE85	I																
Security-Login-Limit	0xBED E	I																S
Security-Resp-Limit	0xBEF A	I															S	
DTE-Ring-No-Answer-Limit	0xBF17	I							S	S								
Final-Rx-Link-Data-Rate	0xBF2 C	I																
Initial-Rx-Link-Data-Rate	0xBF2 D	I																
Event-Date-Time	0xBF2F	T	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Chassis-Temperature	0xBF31	I																
Actual-Voltage	0xBF32	I																
Expected-Voltage	0xBF33	I																
Power-Supply-Number	0xBF34	I																
Channel	0xBF38	I	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Chassis-Slot	0xBF39	I	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Event-Id	0xBF B E	I	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S	S
Number-of-Rings-Limit	0xBFE6	I																
Connect-Time-Limit	0xBFE7	I																
Call-End-Date-Time	0xBFF6	T																
Call-Start-Date-Time	0xBFF7	T																

On = Optional. Part of Call Termination statistics group n.

S = Standard

Data Types: C = Character String, I = Integer, T = GMT date/time

Table 3. (Continued)

Appendix A

Menu/Toolbar Descriptions

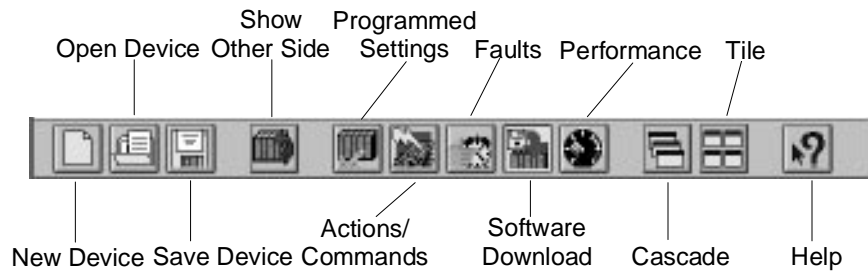



Figure A.1—Toolbar Options

Toolbar Icon	FILE Menu Option	Description
	New	Define the communication parameters for a new chassis. If a connection is successful with the new device, the communication parameters can be saved to the database.
	Open	Open a session with a previously defined chassis.
	Close	Close the currently viewed chassis.
	Save	Save the definition of the currently viewed chassis.
N/A	Save As	Assign a new name to the current chassis.
N/A	Modify	Modify the definition of the current chassis.
N/A	Delete	Delete the current chassis record from the database.
N/A	Save Configuration	Save the configuration of the currently viewed chassis and its installed cards to a file with a *.whb extension.
N/A	Restore Configuration	Restore a previously saved configuration file.




Toolbar Icon	FILE Menu Option	Description
--------------	------------------	-------------

N/A	Print	Send the currently viewed screen to the printer.
N/A	Print Preview	View a preview of a printed screen.
N/A	Print Setup	Redefine your default print parameters.
N/A	Exit	Exit <i>Total Control Manager/SNMP</i> .

Toolbar Icon	VIEW Menu Option	Description
--------------	------------------	-------------

N/A	NMS	Display the NetWare Management System window.
	Other Side	Toggle display between front and rear of the currently viewed chassis.
N/A	Select All	Select all objects of the same type as the object currently selected on the chassis display.
N/A	LED Polling Information	View the following statistics: Time of last valid LED poll, First error encountered, and Number of polling errors.
N/A	Toolbar	Toggle display of the Toolbar off and on.
N/A	Status Bar	Toggle display of the Status Bar off and on.

Toolbar Icon	CONFIGURE Menu Option	Description
--------------	-----------------------	-------------

	Programmed Settings	Display the Configuration window to select from a list of configurable parameters for the currently selected object on the chassis display.
	Actions/Commands	Display the <i>Total Control Manager</i> Commands window and specify a command to be carried out on the selected card(s).
	Software Download	Display a Download Files window to launch the appropriate SDL (software download utility) and NAC (operation code) files to be downloaded to the currently selected object.

Toolbar Icon	CONFIGURE Menu Option	Description
N/A	Feature Enable	Display a window from which you may enable added-cost options for your NMC. This can be done either by entering a special character string that has been generated for your NMC, or by loading a *.key file. Both options require you to contact USR Customer Support.
N/A	Inventory	Display a window from which you may query basic identification data for cards in the chassis, such as hardware/software versions, serial numbers, etc.
N/A	Auto Response	Display a window to program actions to be taken automatically in response to system events. (Requires that the Auto Response be enabled.)

Toolbar Icon	FAULT Menu Option	Description
N/A	Trap Settings	Display the Faults and Trap Settings on a Configuration window to specify a list of exception events and thresholds determining when SNMP traps for the currently selected card(s) should be sent to the Management Station(s).
N/A	Trap Destinations	Display the Trap Destination Table to specify how SNMP traps generated by objects in the chassis are to be routed.
N/A	Modem Tests	Initiate a loopback or self test on a modem, or conduct an idle phone line test.
N/A	Remote Testing	Specify that a modem should send or receive a tone to test a T1 DS0 channel, or initiate a 105 or 102 responder test on the specified DS0 channel.

Toolbar Icon	PERFORMANCE Menu Option	Description
--------------	-------------------------	-------------



Session Monitor

Display the Functional Group Monitor Setup window, to choose performance parameters that can be queried for the currently selected card(s).

Toolbar Icon	SECURITY Menu Option	Description
--------------	----------------------	-------------

N/A

Hub Security Server

Launch the added-cost option Hub Security server, a RADIUS-based authentication tool that establishes security clearance for incoming and outgoing calls.

N/A

Security Manager

Launch the database editor utility for the Hub Security server called the *Security Manager*.

N/A

Community Names

Set SNMP Community Strings (both read-only and read-write) for the currently displayed chassis. Strings may consist of up to 12 characters.

N/A

Authorized Stations

Add, delete, or modify IP addresses, network masks, and optional text annotation for management stations you want to permit to access the chassis. The list may hold as many as 10 entries. The default condition for this group is empty, which permits access to any station on the same subnet as the NMC.

Toolbar Icon	ACCOUNTING Menu Option	Description
--------------	------------------------	-------------

N/A



Accounting Server

Launch the Accounting/Event Logging server, a RADIUS-based tool that permits specified trap events to be sent by the NMC to one of three logs (Call Log, Event Log, Native RADIUS Log) generated as ASCII files.


N/A

Accounting Reports

Launch the prototype MS Access-based application developed by USR to demonstrate the possibilities for using data generated by the Accounting/Event Logging feature.

Toolbar Icon	WINDOW Menu Option	Description
	Cascade	Resizes and layers open windows so each title bar is visible.
	Tile	Resizes and arranges open windows side by side.
N/A	Arrange Icons	Arranges icons on the desktop so they are easy to see.

Help Options

Toolbar Icon	HELP Menu Option	Description
	N/A	Context sensitive Help. Click on this button, then choose the window element for which information is desired. Alternatively, select an object and press the F1 key or click on your left mouse button.
N/A	Index	Launches the <i>Total Control Manager/SNMP</i> Help program.
N/A	Using Help	Launches the Microsoft Windows Help program.
N/A	About Total Control Manager	Displays information about the current version of <i>Total Control Manager/SNMP</i> .

Appendix B

LED Status Descriptions

CARD TYPE	LED	STATUS	DEFINITION
Dual T1 Card (T1_NAC)	RN/FL	Solid Green	Normal operation
		Solid Red	Critical failure
		Flashing Red	Non-critical failure
		Flashing Green	Power-up self-test, software download in process (or software download required), or EEPROM reinitializing
	Carrier 1	Solid Green	Span Line 1 receive signal present and framed
		Solid Red	Span Line 1 receive signal present and unframed
		Off	Span Line 1 receive signal not present
	Carrier 2	Solid Green	Span Line 2 receive signal present and framed
		Solid Red	Span Line 2 receive signal present and unframed
		Off	Span Line 2 receive signal not present
	Alarm 1	Off	No alarm condition on Span Line 1
		Solid Red	Alarm condition on Span Line 1
	Alarm 2	Off	No alarm condition on Span Line 2
		Solid Red	Alarm condition on Span Line 2
	Loopback 1	Off	Span Line 1 not currently in loopback mode
		Green	Span Line 1 currently in loopback mode
	Loopback 2	Off	Span Line 1 not currently in loopback mode
		Green	Span Line 1 currently in loopback mode

CARD TYPE	LED	STATUS	DEFINITION
Single T1 Card (ST_NAC)	RN/FL	Solid Green	Normal operation
		Solid Red	Critical failure
		Flashing Red	Non-critical failure
		Flashing Green	Power-up self-test, software download in process (or software download required), or EEPROM reinitializing
	Carrier	Solid Green	Span Line 1 receive signal present and framed
		Solid Red	Span Line 1 receive signal present and unframed
		Off	Span Line 1 receive signal not present
	Alarm	Off	No alarm condition on Span Line 1
		Solid Red	Alarm condition on Span Line 1
	Loopback	Off	Span Line 1 not currently in loopback mode
		Green	Span Line 1 currently in loopback mode
Quad Modem (QM_NAC)	RN/FL	Solid Green	Normal operation (card level)
		Flashing Green	Software download required or in progress
		Solid Red	Critical failure (card level)
		Orange	Modem negotiating a call
	CHAN 1– CHAN 4	Off	Modem 1–4 idle
		Solid Green	Modem 1–4 online
		Flashing Green	Modem 1–4 testing
		Solid Red	Modem 1–4 critical failure
Dual Modem (DUAL_NAC)	RN/FL 0/1	Solid Green	Normal operation for Modem 0/1
		Solid Red	Critical failure for Modem 0/1
		Flashing Green	Modem 0/1 testing
		Off	Modem 0/1 out of service

CARD TYPE	LED	STATUS	DEFINITION
	OH 0/1	Solid Red	Modem 0/1 off hook
		Off	Modem 0/1 on hook
	CD 0/1	Solid Red	Modem 0/1 detects a carrier signal, or the CD override is on
		Off	Modem 0/1 detects no carrier
	DTR 0/1	Solid Red	Modem 0/1 receiving Data Terminal Ready signal from the DTE
		Off	Data Terminal Ready signal not present for Modem 0/1
	TX 0/1	Flashing Red	Data currently being transmitted by Modem 0/1
		Solid Red	Data Transmit signal in a Space condition for Modem 0/1
		Off	Data Transmit signal in a Mark condition for Modem 0/1
	RX 0/1	Flashing Red	Data currently being received by Modem 0/1
		Solid Red	Data Receive signal in a Space condition for Modem 0/1
		Off	Data Receive signal in a Mark condition for Modem 0/1
NMC Card (NMC_NAC)	RN/FL	Solid Green	Normal operation
		Solid Red	Critical failure
		Flashing Green	Testing, software download required or in progress
		Flashing Green/Red	Non-critical failure
	Hub Stat	Solid Green	Normal operation
		Flashing Red	Network Management Bus failure
		Solid Red	Critical failure
	LAN TX	Solid Green	NMC transmitting data on LAN port
		Off	NMC not transmitting data on LAN port
	LAN RX	Solid Green	NMC receiving data on LAN port

CARD TYPE	LED	STATUS	DEFINITION
		Off	NMC not receiving data on LAN port
	WAN TX	Solid Green	NMC transmitting data on WAN port
		Off	NMC not transmitting data on WAN port
	WAN RX	Solid Green	NMC receiving data on WAN port
		Off	NMC not receiving data on WAN port
Power Supply Unit (PWR_NAC)	RN/FL	Solid Green	Normal
		Solid Red	Failure
X.25 PAD (X.25.NAC)	RN/FL	Solid Green	Normal
		Flashing Green	Initialization/Software Download
		Solid Red	Critical Failure
	Port 1 TX	Solid Green	Transmitting Data
		Solid Red	Critical Failure
		Off	No Data Transmission
	Port 1 RX	Solid Green	Receiving Data
		Solid Red	Critical Failure
		Off	No Data Receipt
	Port 2 TX	Solid Green	Transmitting Data
		Solid Red	Critical Failure
		Off	No Data Transmission
	Port 2 RX	Solid Green	Receiving Data
		Solid Red	Critical Failure
		Off	No Data Receipt

Appendix C ***Hub Security***

Feature Overview

Hub Security is an added-cost option for *Total Control Manager/SNMP (TCM)* software. Hub Security requires version level 3.0 on both *Total Control Manager/SNMP* and the Network Management Card.

In order to add Hub Security to your system as a supported feature, it must first be enabled. If you purchased a new NMC, the additional feature should be enabled when you receive it. You can verify that a Feature Enable operation has been performed on your NMC by doing one of the following:

- ◆ Install the *Total Control Manager/SNMP* software on your management station, connect to a chassis, and view the Programmed Settings of the NMC. View the settings for the Added Cost group. The values will indicate which, if any, features have been enabled.
- ◆ Connect to the User Interface port on the NMC NIC, as described in Chapter 2 of the *NMC Reference Manual*. Type **3** (Feature Enable) from the Main Menu and if the Feature Enable screen displays something other than a series of 0's, a feature has been enabled.

If you must perform a Feature Enable operation, do the following:

1. If you have not yet upgraded the NMC to version 3.0, do so by performing a Software Download operation.
2. Obtain a Feature Enable Key from U.S. Robotics Customer Service. They will assist you in the Feature Enable operation.

3. If you are using *Total Control Manager/SNMP* software, be sure your *TCM* and *NMC* are upgraded to at least version 3.0. Install Hub Security from the extra diskette (supplied when you purchase the option) by running the Setup utility. Refer to Chapter 3 for detailed instructions.

Hub Security

Hub Security allows you to prevent unauthorized users from making outbound (dial out) calls using rack modems, and making inbound (dial-in) connections with these modems. Both dial-in and dial out calls generate events to which the system responds according to scripts that you configure using the *Security Manager* application.

Hub Security implements a User Database to store security configurations on a per-user or group basis, and a Security Log to record security-related events.

The Hub Security feature provides user authentication by using the RADIUS (Remote Authentication Dial-In User Service) client-server protocol. RADIUS is a public domain protocol that regulates access to a secure network through a centrally managed authentication server. U.S. Robotics has modified the RADIUS server so that it can run on a PC using Windows, and uses supersets of the standard RADIUS protocol and database file format.

A user may do the following:

- ◆ Use the authentication server for U.S. Robotics modems and NETServer.
- ◆ Use the authentication server for non-U.S. Robotics products.
- ◆ Use one authentication server for multiple Total Control chassis, as well as multiple non-U.S. Robotics products.
- ◆ Use previously created RADIUS database files.

No hardware changes are required, but this option does require compatible versions of the NMC or *Total Control Manager/SNMP 3.0*, and modem software. Dual Modems supported the initial release of Hub Security; Quad V.34 Modems will support Hub Security as of release 1.5 or higher.

The graphic below demonstrates how the different components of this feature operate together.

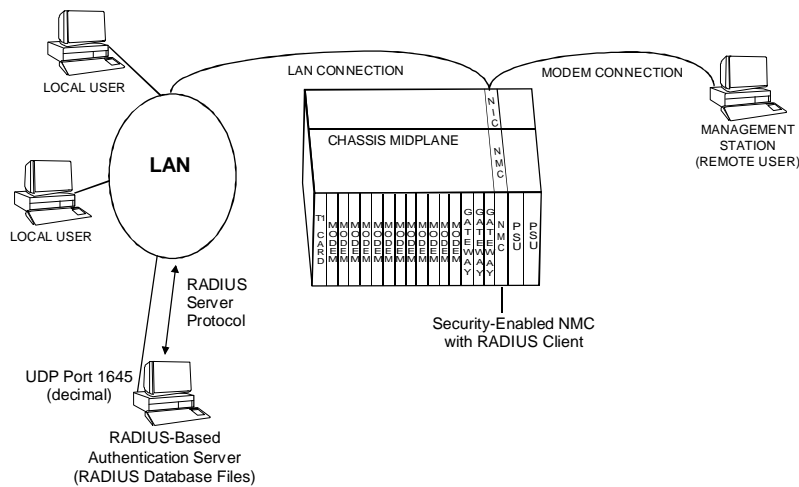


Figure C-1. Hub Security Operation

RADIUS Compatibility

RADIUS is defined in the Network Working Group Internet draft (DRAFT-IETF-NASREQ-RADIUS-02.TXT), and may be obtained from [ftp.livingston.com:/pub/livingston/radius](ftp://livingston.com:/pub/livingston/radius). Based on a model of distributed security previously defined by the Internet Engineering Task Force (IETF), RADIUS provides an open and scaleable client-server security system.

Internet Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or rendered obsolete by other documents at any time. It is inappropriate to use Internet DRAFTS as reference material or to cite them other than as “work in progress.”

To learn the current status of any Internet Draft, please check the “1id-abstracts.txt” listing contained in the Internet Drafts Shadow Directories on ds.internic.net (U.S. East Coast), nic.nordu.net (Europe), ftp.isi.edu (U.S. West Coast), or munnari.oz.au (Pacific Rim).

NETServer Security Feature

Using this feature, a network administrator can maintain one user table for all U.S. Robotics NETServers on the network, rather than individual tables for all cards. Each NETServer acts as a client of the RADIUS server.

When a user dials into the NETServer, the NETServer first checks its own Users Table. If it can’t find the user, and it is configured to do so, it sends an authentication request to the RADIUS server.

The NETServer encrypts the user name and password with an encryption key shared by the NETServer and the RADIUS server, then passes the encrypted user name and password on to the RADIUS server. The RADIUS server then checks the user name and password against its USERS file, accepts or rejects the user, then passes this information back to the NETServer client.

- ◆ If access is denied, the NETServer disconnects the call.
- ◆ If access is granted, the RADIUS server forwards the appropriate user table information to the NETServer. Configuration of this information is performed by the *Security Manager*, and is described later in this Appendix.

Hub Security Feature Installation

Hub Security requires two security-enabled U.S. Robotics components: Network Management Card (NMC) and *Total Control Manager (TCM)*.

The Hub Security feature also requires two additional steps:

- ◆ Installation of Microsoft Open Database Connectivity (ODBC) software
- ◆ Registration of the RADIUS server on the PC

Installation Procedure

The second disk that comes with the Hub Security feature contains Microsoft Open Database Connectivity (ODBC) software needed to maintain the security database.

1. Install the *Security Manager* program files by running the Setup utility contained on it.
2. Insert the Microsoft (ODBC) disk into the drive and type **drive:\SETUP** (substituting the letter of the drive). The ODBC Setup utility title window appears.
3. Click on **Continue**. The Install Drivers window appears:



Figure C-2. Install Drivers Window

As shown in the figure, there should be only one option in the list of Available ODBC Drivers: Access Data (*.mdb).

4. Select Access Data from the list of Available ODBC Drivers and click **OK**. Files are copied to your \windows\system directory. The Data Sources window appears.
5. Click on **Close**.

Installation Adjustment

Next, you must register the authentication server:

- ◆ If you already have a TCP/IP SERVICES file, add the following line to the file, then exit Windows and reboot your computer so that your system recognizes the new TCP/IP service.

RADIUS 1645/UDP

- ◆ If you do not already have a SERVICES file, there is a sample for you to use: \NMS\BIN\NET\SERVICES.SMP. Follow these procedures:

1. Create a directory, such as C:\NET\TCP.
2. Using the name of the directory you created, add the following line to your NET.CFG file:

PATH TCP_CFG c:\net\tcp

3. Copy \NMS\BIN\NET\SERVICES.SMP to your TCP directory, giving it the name SERVICES (no extension).
4. Exit Windows and reboot your computer so that your system recognizes the new TCP/IP service.

Hub Security also restricts server access to certain NMC or NETServer *Clients*. These Clients may be set in the *Security Manager* application. Specify an authorized set of Clients by either specific IP address or common name, as follows:

- ◆ If you already have a TCP/IP HOSTS , file, add the following line to the file, using values that you have specified in the *Security Manager*:

[IP ADDRESS] [COMMON NAME]

Ensure the HOSTS file includes all U.S. Robotics NMC and NETServer IP addresses, and any associated Common Names, for all Clients that will be authorized to use the authentication service. Exit Windows and reboot so that your computer recognizes the new TCP/IP SERVICES and HOSTS files.

- ◆ If you do not already have a HOSTS file here is a sample for you to use: \NMS\BIN\NET\HOSTS.SMP. Follow these procedures:
 1. Create a directory to hold the TCP configuration files, such as C:\NET\TCP.
 2. Copy \NMS\BIN\NET\HOSTS.SMP to your TCP directory, giving it the name HOSTS (no extension).
 3. Edit the sample file to reflect IP addresses and names.
 4. Exit Windows and reboot so that your computer recognizes the new TCP/IP SERVICES and HOSTS files.

Configuring Hub Security

The Hub Security feature configuration is enabled and initialized by setting modem and NMC programmed setting parameters in the *Total Control Manager/SNMP* Configuration window. Prior to launching the *Security Manager* to complete the configuration, these steps should be performed. Similar enabling steps may be taken with the NETServer using the *NETServer Manager* software or from the command line software.

NOTE: After setting Hub Security parameters, save to NVRAM on first the modem(s) and then the NMC. Be aware, however, that the NMC cache stores slot configuration values, and moving a modem from one slot to another risks configuration loss. If you move a modem, verify that the new slot default settings do not override the NMC-enabled Hub Security settings:

1. Save settings to NVRAM on the configured modem(s), then save to NVRAM on the NMC.
2. Insert the modem into the new slot.
3. Perform a GET on the modem parameters, then a SET.
4. Save the modem's settings to NVRAM, then the NMC.

Modem Programmed Settings

The Hub Security Group in the Modem Programmed Settings allows you to enable Dial In/Dial Out Security, and set related timer delays.

Dial In Enable

Description: Allows the modem to be configured for dial-in security. Enabling this disables the modem's built-in Link Security operation.

Settings: No dial-in security will be negotiated
 Connection allowed when no NMC present
 No calls answered when no NMC present
 Hold phone line busy when no NMC present

Default: No dial-in security will be negotiated

Dial Out Enable

Description: Allows the modem to be configured for dial-out security. Enabling this disables the modem's built-in Link Security operation.

Settings: No dial out security will be negotiated
No call attempted when no NMC present
Connection allowed when no NMC present

Default: No dial-in security will be negotiated

DTR DCD Delay

Description: Allows configuration of a time delay, in 100ths of a second, between receipt of DTR and assertion of DCD when the user on an incoming security call has successfully completed the security dialog. This parameter only applies to modems using an RS-232-like interface.

Settings: 0..255

Default: 1

DTR DSR Delay

Description: Allows configuration of a time delay, in 100ths of a second, between detection of DTR and assertion of DSR when an incoming security call has successfully completed security negotiation.

Settings: 0..255

Default: 1

NMC Programmed Settings

The Hub Security Group in the NMC Programmed Settings allows you to customize some or all of the login prompt text and define the user's prompt-response timeout.

You can enter up to 80 characters for each prompt, including control characters and ANSI Escape Sequences to effect cursor control (for example, ^J is used to indicate a line feed, and ^M indicates a carriage return).

The following is a list of the Message Names and a description of when the messages appear to users:

User Name Prompt

Description: First prompt that appears when users establish a connection with a Hub Security-enabled modem. It may consist of up to 80 characters, and identifies the system and prompts users to enter their names. (See *Dial In/Out Password Prompt*.)

Settings: Display String, such as ^J^MU.S. ROBOTICS
TOTAL CONTROL^J^MUSERNAME:

Default: 0

User Password Prompt

Description: Appears after a valid response has been received to a User Name Prompt. It may consist of up to 80 characters, and prompts users to enter their password. (See *User Name Prompt*.)

Settings: Display String, such as ^J^MPASSWORD:

Default: 0

Dial Back Name Prompt

Description: Only appears when users are configured for dial back security (dialing back to either a stored or an entered number), and may consist of up to 80 characters. In addition, the Request Login Validation on Dial Back field must be enabled for the user in the RADIUS user database. (See *Dial Back Password Prompt*.)

Settings: Display String, such as ^J^MU.S. ROBOTICS
TOTAL CONTROL DIAL BACK^J^ MU SER
NAME:

Default: 0

Dial Back Password Prompt

Description: Appears after a valid response has been supplied to the *Dial Back Name Prompt*. It may consist of up to 80 characters.

Settings: Display String, such as ^J^MPASSWORD:

Default: 0

Dial Back Number Prompt

Description: Only appears if a user has been configured for Dial Back Entered mode in the RADIUS user database. It may consist of up to 80 characters, and prompts users to enter a number at which the system can call them back.

Settings: Display String, such as ^J^MENTER YOUR DIAL BACK PHONE NUMBER:

Default: 0

Dial Back Pending Prompt

Description: Only appears if a user has been configured for Dial Back mode (to either a stored or an entered number) in the RADIUS user database. It may consist of up to 80 characters. This message confirms to users that they have logged in successfully, and lets them know that the system has reserved a modem to call them back.

Settings: Display String, such as ^J^MSUCCESSFUL LOGIN, DIAL BACK PENDING.

Default: 0

Modem Select Prompt

Description: Only appears if a user is configured for Dial Back mode in the RADIUS user database and has enabled the Request Dial Back Modem Selection field. The system displays a list of allowed dial back modems that have been entered for this user. Users must enter the number that appears on the menu next to the modem of their choice. This prompt may consist of up to 80 characters.

Settings: Display String, such as ^J^MENTER YOUR DIAL BACK MODEM:

Default: 0

Login Failed Message

Description: Appears when users fail to enter a valid name/password combination. It may consist of up to 80 characters.

Settings: Display String, such as ^J^MINVALID LOGIN ATTEMPT.

Default: 0

Restricted Number Prompt

Description: Appears when a user has been prompted to enter a dial back phone number, and the entered number violates the allowed numbers specified in the Call Restriction List. It may consist of up to 80 characters.

Settings: Display String, such as ^J^MRESTRICTED PHONE NUMBER.

Default: 0

Invalid Modem Select Message

Description: Appears when users that are configured for both Dial Back mode as well as Request Dial Back Modem Selection and select a modem to which they are not allowed access, as defined in the list of allowed Dial Back modems. This message may consist of up to 80 characters.

Settings: Display String, such as ^J^MINVALID MODEM.

Default: 0

No Modems Available Message

Description: Appears when the system is unable to reserve a modem for dial back that was either selected by the user or defined in the list of Allowed Dial Back Modems. It may consist of up to 80 characters.

Settings: Display String, such as ^J^MSELECTED MODEM UNAVAILABLE.

Default: 0

Connect Success Message

Description: Confirms that users have successfully completed their login and may proceed with either their dial-in or dial-out call. It may consist of up to 80 characters.

Settings: Display String, such as ^J^MSECURITY
CONNECTION SUCCESSFUL.

Default: 0

New Password Message

Description: Appears when a user's password has expired. It follows the Change Password Message, and is issued once for the new password and then again to confirm the new password. It may consist of up to 80 characters.

Settings: Display String, such as ^J^MNEW PASSWORD:

Default: 0

Change Password Message

Description: Appears during name/password authentication when the user's password has expired. It may consist of up to 80 characters. This message is immediately followed by the New Password Message.

Settings: Display String, such as ^J^MPASSWORD
EXPIRED

Default: 0

Response Timeout

Description: Represents the number of seconds that users have in which to respond to system prompts. Users failing to respond within the specified time are disconnected, and a Dial Security login failure trap is generated. Any login failures of this type also apply to the User Blacklist function if a valid user name has been entered. This field takes precedence over a modem's inactivity timer during a security login.

Settings: 10..255

Default: 30

Response Attempt Limit

Description: Represents the number of tries a user is allowed per prompt during any one security session. If this number is reached, the call is terminated. For purposes of this parameter, user name and password are treated as a single prompt. This means that if a valid name and an invalid password are entered, the failure is counted against both the Prompt Response Attempt Limit and the Failed Logins Before Blacklist.

Settings: 1..16

Default: 1

Response Echo Enable

Description: When enabled, this option tells the NMC to echo the user's typed responses back to the user's screen. Password responses are echoed as X's.

Settings: Disable
Enable

Default: Disable

Dial Back Delay

Description: Defines the number of seconds to wait between successive dial back attempts--that is, how long the NMC waits before attempting the next dial back when it is unable to connect.

Settings: 1..100

Default: 30

Dial Back Attempt Limit

Description: Defines the number of times that the NMC will attempt to dial back a user that is configured for dial back if an initial dial back attempt fails.

Settings: 1..100

Default: 1

Security Server IP Address

Description: Identifies the IP address of the RADIUS security server where the NMC RADIUS client sends requests.

Settings: IP address

Default: 0

Security Server UDP Port

Description: Identifies the UDP port where the NMC's RADIUS client issues requests to the RADIUS security server.

Default: 1645

Security Server Retries

Description: Defines the number of attempts that the NMC's RADIUS client will make when attempting to send requests to a RADIUS security server.

Settings: 1..100

Default: 1

Modem Attempt Limit

Description: Represents the number of times an attempt can be made to log in on any one modem without success. If this value is exceeded, the Login Attempt Limit Exceeded trap is generated if it has been enabled.

Settings: 1..16

Default: 3

NMC Faults

The Security Traps Enables Group in the NMC Faults allows you to enable SNMP traps upon security events.

Dial Out Login Failure Trap

Description: Enables/disables a trap when a dial out login security session has failed.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

Dial In Login Failure Trap

Description: Enables/disables a trap when a dial-in login security session has failed.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

Dial Out Restricted Number Trap

Description: Enables/disables a trap when a dial out security session has failed as a result of attempting to dial a restricted phone number.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

Dial Back Restricted Number Trap

Description: Enables/disables a trap when a dial back security session has failed as a result of attempting to dial a restricted phone number.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

User Blacklist Trap

Description: Enables/disables a trap when a security user reaches the final failed login attempt limit and is now being blacklisted.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

User Blacklist Login Trap

Description: Enables/disables a trap when a security login attempt by a currently blacklisted user occurs.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

Response Attempt Limit Exceeded Trap

Description: Enables/disables a trap when a security user has failed to issue a valid response to a particular security prompt before the configured limit.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

Login Attempt Limit Exceeded Trap

Description: Enables/disables a trap when a security session has failed because the indicated user does not appear in the security user database.

Settings: enableTrap
 disableAll
 enableLog
 enableAll

Default: enableTrap

The Security Manager

Planning the User List

Before creating a User List, you may want to give some thought to the following issues:

- ◆ You should have a complete list of user names and, if you intend to set them up as dial back users, the phone numbers at which they should be dialed back (if stored numbers are to be used). Make a table of user names that includes passwords and phone numbers.
- ◆ Be prepared with all relevant client information that you have set up for your NMC(s) and NETServer(s).
- ◆ Consider a strategy for assigning passwords. If you have a few thousand users dialing into your system, you will want a password strategy that is easy for you to use, but still preserves security.
- ◆ Consider a strategy for assigning user groups. Assigning users to user groups as they are added simplifies the process. One approach is to create user groups based on the access users need to the DTE. Sample user group names might be MIS, SALES, LAN_ACS, etc.

Using the Security Manager

Installing the Hub Security feature creates icons in the NMS group for both the Security Server and the *Security Manager*. You may also launch these applications from the Security menu in NMS.

When it is launched, the server must run at all times (the server remains in a minimized state). The editor is an offline application and does *not* update the server until you exit.

NOTE: If the PC running the server is powered down unexpectedly, the server loses its counter for keeping track of Failed Logins. This means that users who were blacklisted since the last time the server information was saved will be permitted to log in. You should periodically open and close *Security Manager* or the server itself to save the data stored on the server. This counter is unique in this respect.

Main Menu

When the Total Control *Security Manager* is launched, the following window appears:

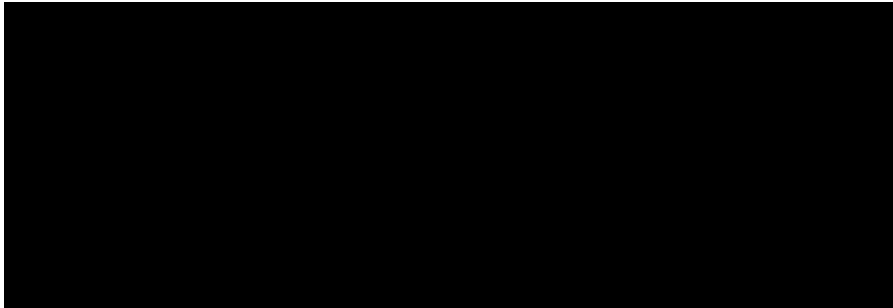


Figure C-3. *Security Manager* Main Menu

File Menu

Exit—Exit the application.

Record Menu

- ◆ *First Record*—Go back to the first record in the file.
- ◆ *Previous Record*—Go back to the previous record in the file.
- ◆ *Next Record*—Advance to the next record in the file.
- ◆ *Last Record*—Advance to the last record in the file.

Configuration Menu

- ◆ *Server Configuration*—Display the Server Configuration window to set options that will apply for all users.
- ◆ *Dial Back Configuration*—Display the Dial Back Configuration window to configure dial back groups.
- ◆ *User Group*—Display the User Group window to configure groups of users.
- ◆ *User*—Display the User window to configure individual users.

View Menu

- ◆ *Toolbar*—Toggle on and off the display of the Toolbar at the top of the window.
- ◆ *Status Bar*—Toggle on and off the display of the Status Bar at the bottom of the window.

Window Menu

- ◆ *Cascade*—Arrange open windows in a cascaded fashion.
- ◆ *Arrange Icons*—Arrange any closed icons in the window along the bottom.

Help Menu

- ◆ *Index*—Display an Index of the Help for the application.
- ◆ *Using Help*—Display Help for the Windows Help system.
- ◆ *About Security Manager*—Display version information about the application.

Security Manager Toolbar

The *Security Manager* Toolbar contains the following icons:

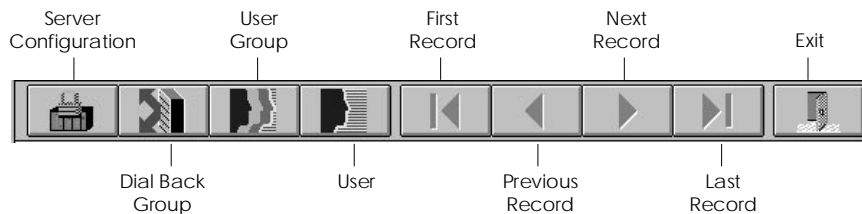


Figure C-4. Security Manager Toolbar

Navigating the Security Manager

Server Configuration Window

Click on the **Server Configuration** icon on the Toolbar. The following window appears:

The screenshot shows the 'Server Configuration' dialog box. It contains the following fields and controls:

- Server Filename:** A text box labeled 'Users File' with the value 'c:\etc\raddb\users' and a 'Browse...' button.
- Server Log:** A button labeled 'Events to Log...'.
- Clients:** A 'Client Name' text box with '192.77.203.65', a 'Secret Key' text box with asterisks, and 'New...', 'Delete', and 'Browse...' buttons.
- Server Statistics:** A section showing 'Users File Size: 20 bytes', 'Last Modified: May 25, 1995', 'Total Users: 0', and 'Users Blacklisted: 0'.
- Passwords:** A section with an unchecked checkbox 'Encrypt Passwords in Users File', 'Min Password Length' set to 5 characters, 'Password Warning' set to 25 days, and 'Password Duration' set to 30 days.
- Buttons:** 'Cancel' and 'Done' buttons at the bottom right.

Figure C-5. Server Configuration Window

NOTE: All of the parameters displayed in the Server Configuration window are system-wide. That is, they apply to ALL users, not to specific users or groups of users.

Server Filename

The Users File field permits you to select the file on which the *Security Manager* is to operate. The sample file that is shipped with the software is installed as c:\etc\raddb\users. Use **Browse** to locate a file that you may have placed in a different directory.

The *Security Manager* and the authentication server operate on three files: a *users* file, a *clients* file and a *dictnary* file. Once you select the *users* file, it is assumed that the *clients* and *dictnary* files reside in the same directory. If those corresponding files are not found, the *Security Manager* displays an error.

Server Log

The Server Log option specifies which events to log. The server saves this information to c:\etc\raddb\logfile.

NOTE: This log file is not in any way related to security traps you may have configured in the *Total Control Manager*.

To configure the type of information that is saved to the log file, press **Events To Log**. The Events to Log dialog box appears. The default is to log all four of the following options:

- ◆ Failed Login Attempts
- ◆ Successful Login Attempts
- ◆ User Blacklisting
- ◆ Password Changes

If you do not want one or all of these events to be logged, click on the checkbox in front of the option to remove the x.

NOTE: If you decide to generate a log file, monitor it periodically and delete it if it grows too large.

Clients

In the Client Name field, select from a list of valid clients (NMCs or NETServers) with their corresponding client secret keys (set up via the NMC RS 232 User Interface or the NETServer command line software). The *clients* file is stored in the same directory as the *users* file (by default, c:\etc\raddb).

The client name should be entered in either the standard dotted Internet notation (xxx.xxx.xxx.xxx) or as a name that can be resolved (via the HOSTS file) to a standard dotted notation of the IP address of an allowed client.

The secret key field is a text string that is paired with a single Client ID. The secret keys are known both to the RADIUS server and that particular RADIUS client. The key is then used to encrypt data sent between the client and the server.

Server Statistics

This area in the window is used to display the following statistics:

- ◆ *Users File Size*—the file size in bytes.
- ◆ *Last Modified*—the last date on which the file was changed.
- ◆ *Total Users*—total number of users included in the file.
- ◆ *Users Blacklisted*—number of users with blacklist status.

Passwords

Passwords are also saved in the Users database file. The following parameters, which apply to all passwords, may be set:

- ♦ A selected checkbox specifies that this file should be encrypted. Check the box to specify that passwords in the Users file should be encrypted. Checking this box also encrypts the Secret Keys in the Clients file. This process is reversible by clicking on the box again to remove the X.
- ♦ The Minimum Password Length is the smallest number of characters accepted for *input* into the RADIUS database. This applies to users who are entering passwords through the *Security Manager* as well as users who are prompted for new passwords via the authentication server. Users who choose to enter passwords by directly editing the database file will not be affected by this minimum.
- ♦ Password Duration and Password Warning are standard RADIUS database fields. They determine how long new passwords are valid, and how many days a user should be warned before a password is set to expire.

NOTE: If you manually set a Password Expiration for a user, this Password Duration does not apply.

Dial Back Group Window

Click on **Dial Back Groups**. The following window appears:

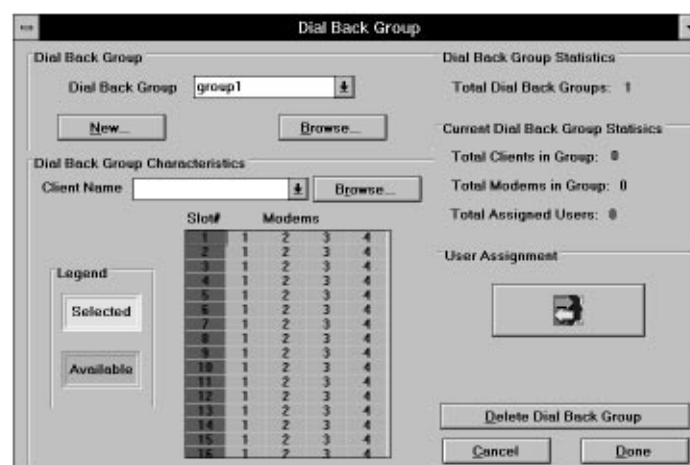


Figure C-6. Dial Back Group Window

Dial Back Group

The control group in the upper left of this window contains **New** and **Browse** to either name a new group or select from a list of existing groups.

Dial Back Group Characteristics

- ◆ The *Client Name* field allows you to set up and select from a list of chassis names or IP addresses to define the dial back group. Up to nine clients may be selected for a single dial back group.
- ◆ Below the Client Name field is the modem selection grid. Each IP address has a list of modems that are valid for this dial back group. The first column in the grid represents modem slots, and the other columns represent modem channels.

Click on **Modem channels** once to select them. The channel cell on the grid turns yellow.

NOTE: A single dial back group may span multiple IP addresses (chassis), but if a user selects a particular dial back group, only the modems on the chassis he or she is calling into are valid to be used for dial back. This means that if users enable dial back modem selection, they may only choose from a dial back groups that they both belong to *and* which contains dial back modems from the same IP address that they are calling into.

Dial Back Group Statistics

A counter displays the number of Total Dial Back Groups.

Current Dial Back Group Statistics

The following statistics are displayed for the current dial back group:

- ◆ Total Clients in Group
- ◆ Total Modems in Group
- ◆ Total Assigned Users

User Assignment

By pressing **User Assignment**, it is possible to browse the users who have included this dial back group in their list. The Dial Back Group Assignment window is displayed. You may also change the users assigned to this dial back group in this window.

File Control Buttons

- ♦ To erase the definition of this group, press **Delete Dial Back Group**.
- ♦ To exit from this window without saving any changes, press **Cancel**.
- ♦ To exit from this window with your changes saved, press **Done**.

User Group Window

From the main toolbar, click on the **User Groups** icon. The following window appears:

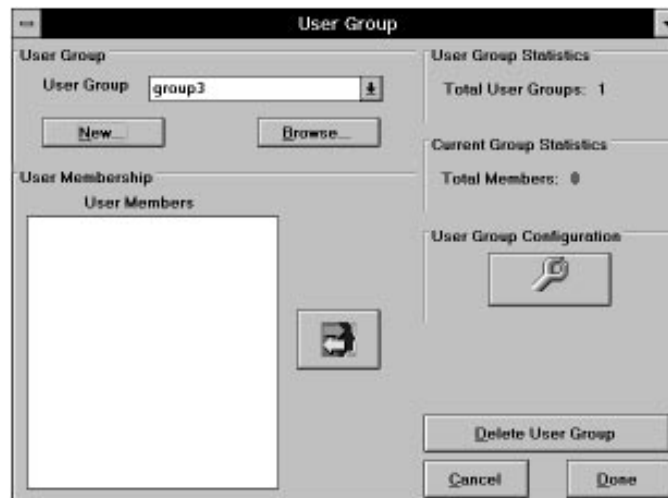


Figure C-7. User Group Window

In this window, you may review user group statistics, change the user membership list, or change the configuration parameters of this group.

User Group

In the User Group field, you may enter a new user group name or browse for an existing user group name.

User Membership

You may view which users are members of an existing user group by looking at the User Members list box. Users are assigned to a group by selecting the group in the User Configuration window (described later).

To add or delete a user from the group, click **Change Membership** at the right of the list box. The following window appears:

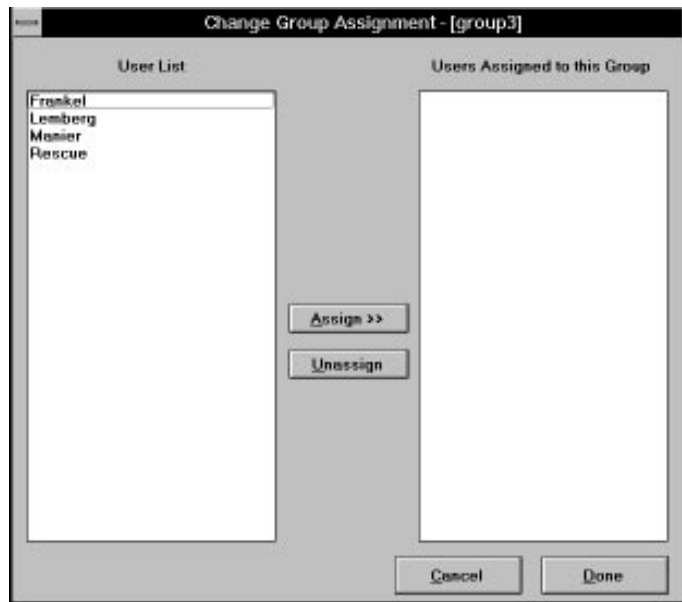


Figure C-8. Change Group Assignment Window

Select users from the list on the left, then click on **Assign** to add them to the Assigned Users list on the right. You can also unassign users from a group in this window. Click on **Done** to save your changes.

User Group Statistics

A counter displays the number of Total User Groups configured.

Current Group Statistics

A counter displays the number of Total Members in the currently displayed user group.

User Group Configuration

To set up parameters for the currently displayed user group, click on **User Group Configuration** (represented by a wrench). The following window appears:

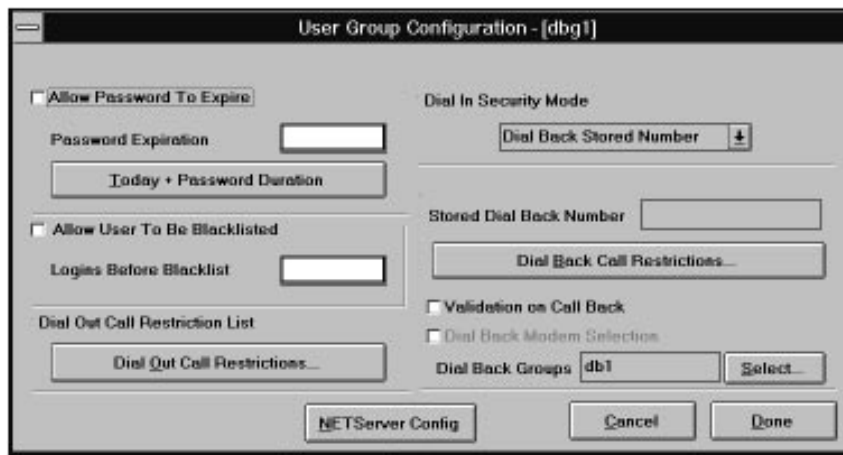


Figure C-9. User Group Configuration Window

This window is identical to the User Configuration window (described later), except that this one does **not** include a **User Group** field or a **Set to User Group** button.

The configuration variables for a user group are selected by clicking on the checkbox next to the desired control. This window contains the following parameters:

- ♦ *Allow Password to Expire*—Check this box to allow the passwords for members of the user group to age and expire based on the number of days specified in the Password Duration field in the Server Configuration window. You can change the date in the following ways:
 - Double click on the **Password Expiration** field. A blinking cursor appears in the field. At the right of the field is a spin button (a double-headed arrow, pointing up and down). Click on the up arrow once to display the current date.

When the cursor is located in the month field in the window, clicking once on the up arrow advances the date a month. Clicking on the down arrow moves the date back a month.

- Double click on the **Password Expiration** field again to display a calendar window that you can use to select an expiration date. See Figure C-10.



Figure C-10. Calendar Window

- Click on **Today + Password Duration** to display the next date the password is scheduled to expire. You can then manually edit the date.
- ♦ *Allow User to be Blacklisted*—Check this box to blacklist users in this group who consecutively fail login attempts. The Logins Before Blacklist box allows you to specify a number for consecutive login attempts.
- ♦ *Dial Out Call Restriction List*—Click on this button to display the following window:

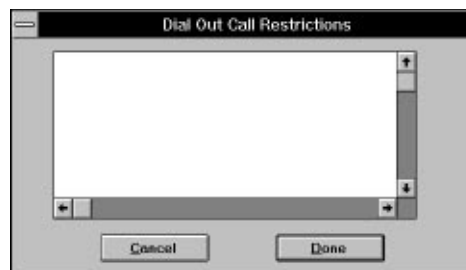


Figure C-11. Dial Out Call Restrictions Window

Use this window to enter a list that will be checked when users in this group dial out from the system. The syntax for this list is described later under *Call Restriction List* (described later). Call Restriction operates in the same way for both dial out and dial back users.

- ◆ *Dial In Security Mode*—Allows you to set three possible values that control how the dial-in user's call is handled after the initial name/password login sequence is successfully completed.
 - *Pass-Through*, where the user is connected to the DTE upon successful name/password validation.
 - *Dial Back Stored Number*, where the Total Control modem disconnects after the login sequence and dials the stored number of the remote modem.
 - *Dial Back Entered Number*, where the user is prompted to supply a number at which to be called back. Total Control checks the number against the Call Restriction list and dials.
- ◆ *Dial Back Configuration*—Allows you to set the following variables:
 - *Stored Dial Back Number*. Enter a number where the user is to be dialed back. This is used when the Dial In Security Mode is set to Dial Back Stored Number.
 - *Dial Back Call Restrictions*. Display a Call Restriction List to be checked when users enter a number at which they want to be called back. This window is identical to the Dial Out Call Restriction window described earlier. Syntax is described later under Call Restriction List.
 - *Validation on Call Back*. Check this box if you want a user to be prompted for name/password a second time when the system calls back.
 - *Dial Back Modem Selection*. Check this box if you want users to be presented with a menu from which to choose a dial back modem. The following rules apply:
 - If the modem that has been dialed is included in the dial back group, the system first tries to use that modem to dial back the caller.

- When dial-in users select an alternative dial back modem upon logging in, the system checks the specified dial back modem for availability and reserves it. If that modem is in use, the system advises the user and terminates the call.
- *Dial Back Groups.* Select a dial back group from the drop-down box, or click on **Select** to display the Select Dial Back Groups window. All dial back users must be a member of at least one dial back group.

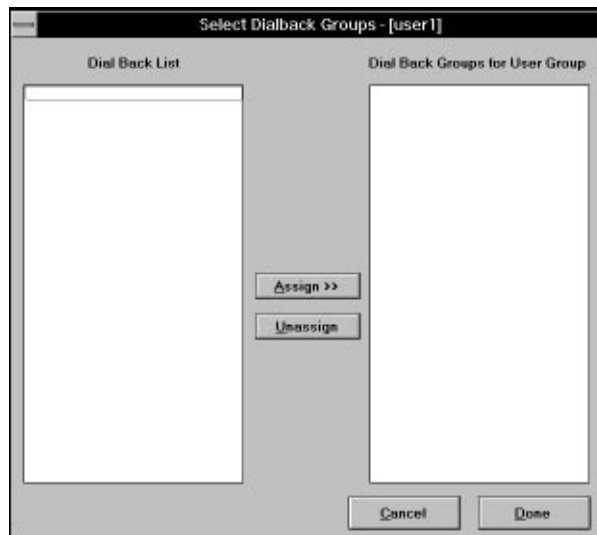


Figure C-12. Select Dial Back Groups Window

A list of all dial back groups is displayed in the box on the left. Select as many of these as you wish to assign to the current user group, and click on **Assign** to display these groups in the box on the right. To remove a dial back group from this user group, click on the group in the box on the right and then click on **Unassign**.

NETServer Configuration Window

Click on **NETServer Config** in the User Configuration or User Group Configuration window to set characteristics for the NETServer. The following window appears:

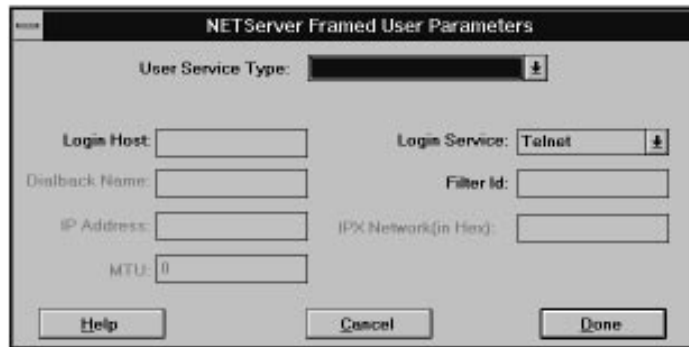
The image shows a Windows-style dialog box titled "NETServer Framed User Parameters". It contains several input fields and buttons. At the top is a dropdown menu for "User Service Type:". Below it are two columns of fields. The left column includes "Login Host:", "Dialback Name:", "IP Address:", and "MTU:". The right column includes "Login Service:" (with a dropdown menu showing "Telnet"), "Filter Id:", "IPX Network(In Hex):", and "IPX Network(In Hex):". At the bottom are three buttons: "Help", "Cancel", and "Done".

Figure C-13. NETServer Framed User Parameters

- ◆ *User Service Type*—Select Login User, Dialback Login User, Dialback Framed User or Framed User. Your choice will dictate which of the options in the rest of this window are available.
- ◆ *Login Host*—Enter the name or IP address of the host the user will log into.
- ◆ *Login Service*—Define what type of connection the user will make with the host:
 - Telnet (default port of 23)
 - Rlogin (default port of 513)
 - TCP-Clear (also called NetData, default port of 6000)
 - PortMaster (default port of 1642)
- ◆ *Dialback Name*—Enter the name of the host or system defined in the NETServer's Location Table.
- ◆ *Filter ID*—Enter the Filter ID to control the user's access to the host.
- ◆ *IP Address*—Enter the IP address of the NETServer.
- ◆ *IPX Network*—Enter the number of the IPX network the NETServer is on.

- ♦ **MTU**—Enter the Maximum Transmission Unit permitted across the serial port during a connection. PPP connections are set between 100 and 1500 (default=1500), and SLIP connections are set between 100 and 1006 (default=1006).
- ♦ **Help/Cancel/Done**—Select one of these buttons to display Help, cancel your changes, or accept your changes.

Control Buttons

When you are finished making changes in the User Groups window, click on **Done** to exit and save your changes. To exit without saving changes, click on **Cancel**. You may also use the **Delete User Group** button to remove a defined user group from the list.

User Window

From the main toolbar, click on **Users**. The following window appears:

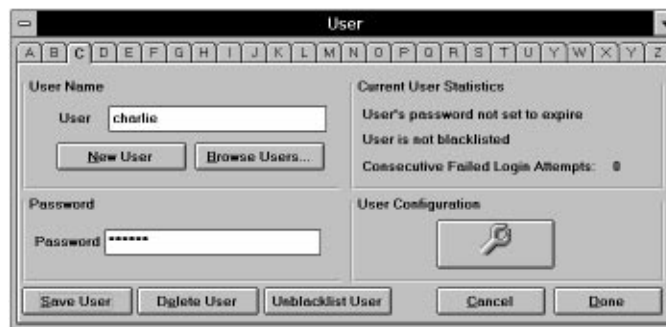


Figure C-14. User Window

User Name

Use the alphabetical tabs at the top of the window to jump quickly to a specific user. While this window is displayed, you may also use the arrow buttons in the main toolbar to advance or go back one user at a time, or jump to the first or last user.

To enter a new user, click on **New User**. Browsing large numbers of users is more conveniently performed in a spreadsheet format. The following window is displayed when you click on **Browse** in the User Name group box:

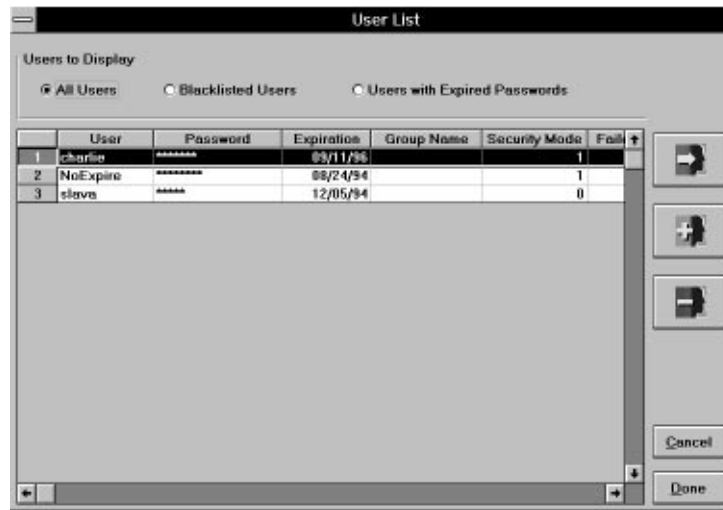


Figure C-15. User List Window

The User List grid displays a list of users (column on the left) followed by all the user's attributes (one user per row). Based on the option selected under Users to Display, the grid may display all users, just the users who have been blacklisted, or those who have expired passwords. The following parameters are listed in the grid (when configured) for each user:

- Password
- Expiration
- Group Name
- * Security Mode
- * Failed Logins
- * Logins Before Blacklist
- Dial Back Call Restrictions
- Dial Out Call Restrictions
- Stored Dial Back Number
- * Validation on Callback
- * Dial Back Modem Selection

*For these parameters, spin boxes may be scrolled to -1. This setting means that the default is always used. For instance, if Logins Before Blacklist is set to -1, the user will never be blacklisted.

You may sort the grid according to any user attribute by pressing on the appropriate grid square on the grid's top row. You may edit this directly or select a single user. Double click on any grid entry to change it.

There are buttons at the right of the screen. The top one, with an arrow (Go to User), brings up the User window for the currently selected user. This *loses any changes* you have made and cancels the User List window.

The next two buttons may be used to add or delete users (plus sign—Add User, minus sign—Delete User). **Cancel** and **Done** at the bottom of the window allow you to exit the window with or without saving any changes you may have made.

Password

Use this field to enter or change a password.

Current User Statistics

In this box the following statistics are displayed: whether or not a user's password is set to expire (and in how many days if it is set); whether or not a user is blacklisted; and how many consecutive failed login attempts this user has made.

User Configuration

From the User window, click on the wrench icon to display the following window:

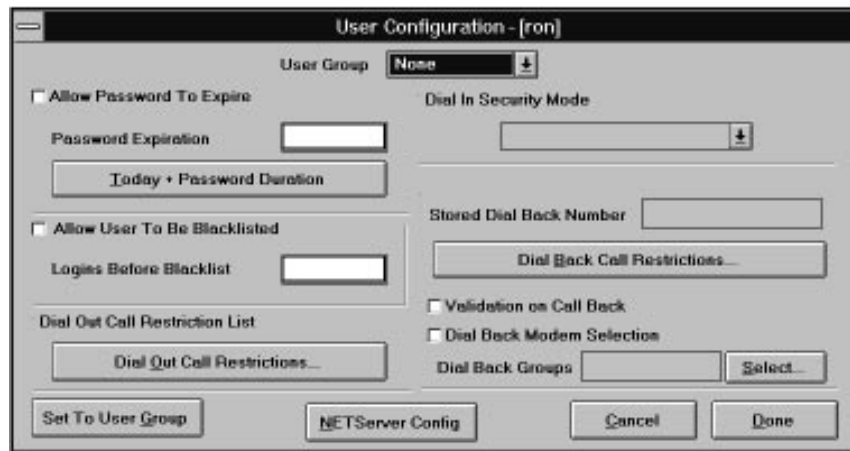


Figure C-16. User Configuration Window

This window has the same parameters set in the User Group Configuration window described earlier, plus two additional ones: the User Group field at the top of the window, and **Set to User Group** at the bottom left of the window. In the User Group field, you can scroll through a list of defined user

groups. When you have displayed the desired group, click on **Set to User Group** to make the parameters for this User match those of the displayed User Group.

Control Buttons

The following buttons are available at the bottom of the User window:

- ◆ *Save User*—Save the configuration of the currently displayed User.
- ◆ *Delete User*—Delete the currently displayed User from the system.
- ◆ *Unblacklist User*—Remove the blacklisting from the currently displayed User.
- ◆ *Cancel*—Exit without saving changes.
- ◆ *Done*—Exit and save changes.

Call Restriction List

You may restrict calls on dial out users and dial-in users who are configured for the system call back. When selected, a text entry window appears. The Call Restriction List may contain up to 20 entries to specify phone numbers that are explicitly allowed or disallowed. Each entry must begin with a plus sign (for an allowed number) or a minus sign (for a disallowed number).

When a user initiates a call, the list is processed. It attempts to match the requested phone number to the entries in the list, from top to bottom. Once a positive or negative match is found, list processing stops and the dial request gets Call Restriction status.

The following table provides a sample entry and explanation that might be seen in the Call Restriction List. For more information on wildcards, see the next section, *Using Wildcards in a Call Restriction List*.

Entry	Meaning
+1617\$	All calls within the 617 area code are permitted.
+1312\$	All calls within the 312 area code are permitted.
-1\$	No other long distance calls (outside of 617 and 312) are permitted.
-5551234\$	Local number 5551234 is not permitted. The ending dollar sign ensures the user does not try to break the match by adding extra digits. This kind of restriction is useful to disallow calls by some user groups to specified resources, while allowing access to other groups with a different template.
+\$	All other local calls are permitted.

Using Wildcards in a Call Restriction List

Wildcards simplify list entries. The single character wildcard is a question mark (?); the global character wildcard (to replace any number of characters) is a dollar sign (\$).

We recommend that you always end your list with either +\$ or -\$ to indicate how to handle numbers not specified in the list. You should also add the \$ wildcard after numbers you want to specifically disallow; otherwise, a user could get around the restriction by dialing more numbers to break the exact match.

Troubleshooting

Adding/deleting users takes too long.

- ◆ Try adding users by clicking on **New User** in the User window instead of using **Add** in the User List window.
- ◆ Use the **Delete User** in the User window for faster results. The **Delete** in the Browse Users window tends to be slower.

The *Security Manager* slows down.

If many users dialing in are changing their passwords, initialization of the editor tends to slow down. The *Security Manager* must open and read the **users** file, then compare it to the **security.mdb** file.

The *Security Manager* no longer launches.

Back up the contents of the c:\etc\raddb directory on a regular basis. If you encounter a problem launching the server or editor, consider editing the **users** file and deleting all entries back to a date before your trouble started.

If that does not help, follow this procedure:

1. Perform one more backup of all the c:\etc\raddb\ files.
2. Exit Windows and change to your temporary directory. This directory is specified by the DOS environment variable "TEMP" (type "set" at the DOS command prompt and note the name of your "TEMP" directory). Delete all the *.tmp files that have been generated by the application. Run either **chkdsk /f** or **scandisk** on the hard drive, and then reboot. Check to see if your problem has been fixed.
3. Reinstall *TCM*, including the ODBC installation program. When prompted to overwrite the existing database files, answer **Yes**. Remember that you have backed up your database files in step 1.
4. Copy the backed up versions of the files **users**, **clients** and **dictnary** back to the c:\etc\raddb directory.
5. Launch the server. If the server still will not launch, repeat steps 2 and 3, and then copy the backed up version of the **security.mdb** file to c:\etc\raddb.
6. If the server launches, start the editor. The first time it comes back up, it will take longer than usual to launch with the restored files.

User browsing is too slow.

Try to maintain at least 50 Mb of free memory on the hard drive for the users database. If less than 20 Mb is available, the browse process will be slow.

Appendix D

Auto Response

Product Overview

Auto Response is an added-cost option for *Total Control Manager/SNMP (TCM)* software. Auto Response requires version level 3.0 on both *Total Control Manager/SNMP* and the Network Management Card.

In order to add Auto Response to your system as a supported feature, it must first be enabled. If you purchased a new NMC, the additional feature should be enabled when you receive it. You can verify that a Feature Enable operation has been performed on your NMC by doing one of the following:

- ♦ Install the *Total Control Manager/SNMP* software on your management station, connect to a chassis, and view the Programmed Settings of the NMC. View the settings for the Added Cost group. The values will indicate which, if any, features have been enabled.
- ♦ Connect to the User Interface port on the NMC NIC, as described in Chapter 2 of the *NMC Reference Manual*. Type **3** (Feature Enable) from the Main Menu and if the Feature Enable window displays something other than a series of 0's, a feature has been enabled.

If you must perform a Feature Enable operation, do the following:

1. If you have not yet upgraded the NMC to version 3.0, do so by performing a Software Download operation.
2. Obtain a Feature Enable Key from U.S. Robotics Customer Service. They will assist you in the Feature Enable operation.
3. If you are using *Total Control Manager/SNMP* software, be sure your *TCM* and NMC are upgraded to at least version 3.0. Install Auto Response from the extra diskette (supplied when you purchase the option) by running the Setup utility. Refer to Chapter 3 for detailed instructions.

Auto Response Configuration

Auto Response allows Network Managers to define a set of actions (Auto Response script) to be taken automatically when a specified event occurs in the chassis. The event may be chassis-wide, or specific to a particular module (NAC) in a given slot of the chassis, or specific to a particular entity (such as a single modem channel).

Total Control Manager (TCM) provides a convenient graphical user interface (GUI) through which the Network Manager can configure these automatic responses. To access the feature, select the **Configure** menu and then **Auto Response**.

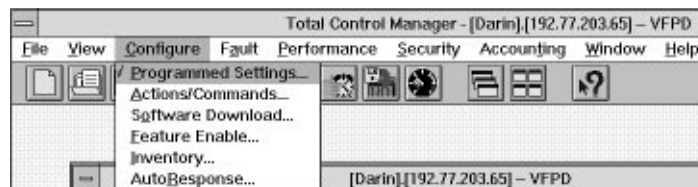


Figure E-1. Configure Menu

TCM does not need to be running when an event occurs in order for the NMC to invoke the appropriate response script, since these scripts are pre-programmed into the NMC and saved to NVRAM.

Before Configuring Auto Response

Before configuring Auto Response it is necessary to perform Alarm Integration through *Novell SNMP Alarm Integration*.

From the Novell NMS Fault menu, select:

Alarm Disposition

Configure Alarm Disposition

Family of Alarms

SNMP

Auto Response Trap

Refer to Chapter 10 for more information on alarm integration.

Auto Response events are SNMP traps and may require thresholds to be specified. When there are descriptors (thresholds) for an event, they must be programmed through the *TCM* Configuration window. See a list of events and responses latter in this appendix.

Example: The **Connection Time Limit Expired** event requires that you specify the **Connection Time Limit** threshold.

Configuring Auto Response

Select: **Slot(s)/Channel(s)** (from the chassis display)
 Configure (from the TCM Menu bar)
 Auto Response (from the Configure menu)

The following window is then displayed:

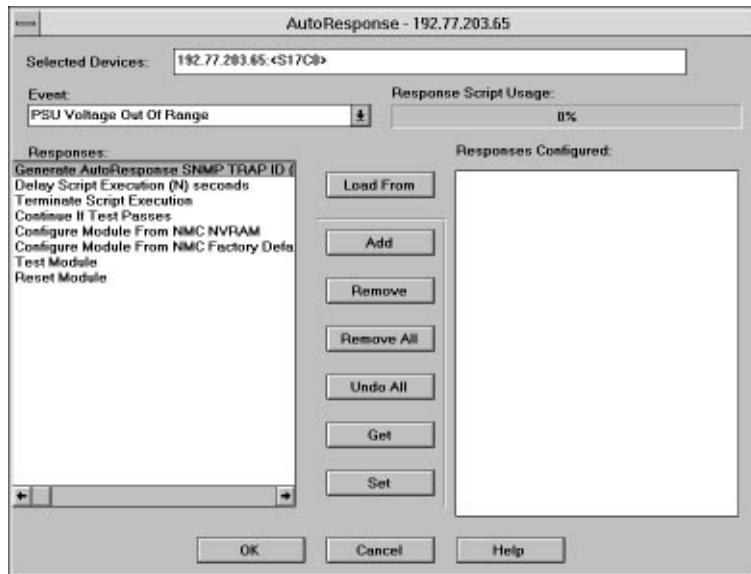


Figure E-2. Auto Response Window

Selected Devices (field)

This field shows the slot(s) or channel(s) selected from the chassis display.

Event (drop down box)

This box displays all the events that can be programmed for the device(s) selected. If you select an event that requires a descriptor (threshold), be sure that you have programmed the descriptor.

Response Script Usage (field)

This field shows the percentage of available script space you have programmed. Each response may take up a different amount of script space. Keep an eye on this gauge to avoid programming too many responses to a single event.

Responses/Responses Configured (selection box)

Use the following methods to configure a list of responses for each event. The responses *available* for the event are displayed on the left, and the responses *configured* for the event are displayed on the right.

NOTE: When you select a response that has descriptors, a window appears, presenting you with descriptor options.

Add (button)

To assign a response script to an event, select the response from the **Responses List** and then click on the **Add** button. The response is added to the Responses Configured list box. Responses can only be added one at a time. Some responses may require additional information (e.g., Delay N. Seconds). For responses that require additional input (a descriptor), the Auto Response Parameters window is displayed.

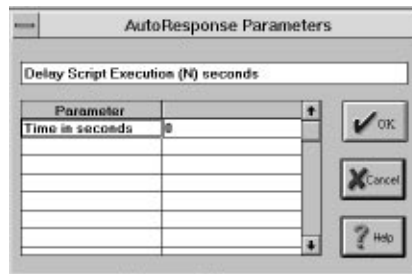


Figure E-3. Auto Response Parameters Window

Fill in your desired value and click **OK** to set the descriptor.

Also, through drag and drop, the responses in the Responses Configured list can be resequenced. To resequence a response, click on the response and hold down the left mouse button. Move the mouse until the cursor is over the desired position in the list and release the left mouse button.

Remove (button)

To remove a response, select the response from the Responses Configured list and then click the **Remove** button.

Remove All (button)

Click to remove all responses from the list.

Undo All (button)

Click to restore the event with the response script that was last retrieved from the NMC.

Get (button)

Query the NMC for the associated response script.

Set (button)

Assigns the response script to the event.

Load From (button)

This button brings up the **Load From Device** window. Enter the IP address, slot and/or channel of the device whose Auto Response settings you want to copy, and the response scripts are loaded from the device specified to the currently selected device(s).

OK/Cancel/Help (buttons)

Click on these buttons to accept changes you have made in this window, cancel them, or display a help window.

Events and Responses

Overview

Events are grouped into three categories: chassis/NMC events, module/slot events, and modem/channel events. Other event categories may be created in future releases for other devices. Presently, there are a few events that occur on one type of card, but cause action on another type of card. This capability will be expanded in the future for all events on all types of cards. The following sections provide a breakdown of events and responses allowed.

Chassis-Level Events and Responses

The chassis events/responses are brought up by selecting the NMC in the chassis display. They concern global conditions in the chassis and actions that might be taken from the NMC. The events and responses below are listed in the order in which they appear in the Auto Response window. Definitions are provided later in this appendix.

Chassis/NMC Events

- ** PSU Voltage Out of Range
- PSU Failed
- ** Fan Failed
- ** HUB Temperature Out of Range
- * Global Timer #1 Expired
- * Global Timer #2 Expired
- * Global Timer #3 Expired
- * Global Timer #4 Expired

-
- * Requires Configurable Descriptor
 - ** System-Defined Descriptor

Chassis/NMC Responses

- * Generate Auto Response SNMP Trap
- * Delay Script Execution N Seconds
- Terminate Script Execution
- Continue If Test Passes
- Configure Module from NMC NVRAM
- Test Module
- Reset Module

-
- * Requires Configurable Descriptor

Module-Level Events and Responses

Module events occur only on a per-slot basis. Consequently, the responses for these events always affect all devices in that slot. For example, assume that a Quad Modem Card has just been inserted into Slot 1. This triggers a Module Inserted event; consequently, a Configure Module from the NMC response list configures all four modems on that card with parameters stored in the NMC's NVRAM. The events and responses below are listed in the order in which they appear in the Auto Response window. Definitions are provided later in this appendix.

Module/Slot Events

- Module Inserted
- Module Re-Initialized
- Module Removed
- Module Non-Operational
- Module Watchdog Time-Out

Module/Slot Responses

- * Generate Auto Response SNMP Trap
- * Delay Script Execution N Seconds
- Terminate Script Execution
- Continue If Test Passes
- Configure Module from NMC NVRAM
- Configure Module from NMC Factory Defaults
- Remove Module from Service
- Restore Module to Service
- Test Module
- Reset Module
- Busy Out Module's Analog Phone Line
- Restore Module's Analog Phone Line

* Requires Configurable Descriptor

Channel-Level Events and Responses

The channel events occur only on a per-entity basis, so the responses for these events affect only those entities. Currently, up to four entities can reside on a given card, so up to four different response scripts can be constructed for a given slot. The events and responses below are listed in the order in which they appear in the Auto Response window. Definitions are provided later in this appendix.

Example: The NMC detects a blacklisted user attempting to log in to one of the modems on a Dual Analog Modem Card in Slot 1. Because the network administrator programmed a Busy Out Phone Line response on a per-channel basis for this event, this triggers a User Blacklisted event. The Busy Out Analog Phone Line response affects only that modem (channel) on the Dual Analog Modem Card where the event occurred. The other modem is not affected.

Modem Channel Events

Incoming Connection Established
 Outgoing Connection Established
 Incoming Connection Terminated
 Outgoing Connection Terminated
 Connection Attempt Failed
 * Connection Time Limit Expired
 Reset by DTE
 * DTE Transmit Idle
 * Block Error Count at Threshold
 * Fallback Count at Threshold
 Dial Out Login Failure
 Dial Out Restricted Number
 Dial In Login Failure
 Dial Back Restricted Number
 Dial Back Using Restricted Modem
 * Login Attempt Limit Exceeded
 User Blacklisted
 Attempted Login by Blacklisted User
 * Response Attempt Limit Exceeded
 Modem Watchdog Reset
 Management Bus Failure
 * DTR True
 * DTR False
 * Modem Ring-No-Answer
 * DTE Ring-No-Answer
 No Dial Tone
 No Loop Current Detected
 ** Global Timer #n Expired
 Packet Bus Active
 Packet Bus Lost

* Requires Configurable Descriptor

** System-Defined Description

Modem Channel Responses

- * Generate Auto Response SNMP Trap
 - * Delay Script Execution N Seconds
 - Terminate Script Execution
 - Continue If Test Passes
 - Reconfigure from NVRAM
 - Reconfigure from Modem Factory Defaults
 - Test Modem
 - Test Analog NIC
 - Test Analog Phone Line
 - Restore Analog Phone Line
 - * Busy Out DS0 - T1 Slot (N) Span (N) Channel (N)
 - * Restore DS0 - T1 Slot (N) Span (N) Channel (N)
 - Modem Software Reset
 - Terminate Connection
 - Busy Out Analog Phone Line
-

* Requires Configurable Descriptor

Event Options

The events listed in this section are provided in alphabetical order. Where applicable, event descriptors are listed.

NOTE: Some of the supported events interact with another added-cost option, Total Control Hub Security.

Attempted Login by Blacklisted User

Triggered—when a user who has been blacklisted by the Hub Security feature attempts to use a chassis modem.

Block Error Count at Threshold

Triggered—when a connected chassis modem receives the number of block errors specified by the event descriptor. Modems typically send data over the phone line using error-corrected packets or blocks. A block error (BLER) occurs when a modem receives a block that contains data errors.

Descriptor (user configured)

Card: Modem

Select: **Faults**
Modem Event Thresholds
Block Errors Limit

Definition: Number of block errors during a connection that will be used to qualify the event

Setting: 0–255 errors

Default: 0 (disables the event)

Connection Attempt Failed

Triggered—when a chassis modem fails to connect with a remote modem for an incoming or outgoing call.

Connection Time Limit Expired

Triggered—when a connection duration exceeds the user-defined connection time limit. (If connection termination is desired, the response list for this event should include that response.)

Descriptor (user configured)

Card: Modem

Select: **Faults**
Modem Event Thresholds
Connection Timeout Limit

Definition: Number of minutes a call may be connected before the event is triggered

Setting: 0–255 minutes

Default: 0 (no time limit observed)

Dial Back Modem Restriction Error

Triggered—when a dial-in user requests that the Total Control *Security Manager* dial back using a modem disallowed on a Dial Back Group list.

Dial Back Restricted Number

Triggered—when a dial-in user requests that the Total Control *Security Manager* dial back to a number that has been disallowed for them on a Call Restriction list.

Dial In Login Failure

Triggered—when a user dialing into a chassis modem enters an invalid response to a Total Control *Security Manager* prompt and exceeds the number of specified login attempts.

Triggered—if a user enters an invalid user name and/or password combination.

Triggered—if a user fails to respond to a login prompt within the set time limit.

Descriptors (user configured)

Card: NMC

Select: **Programmed Settings**
Hub Security
Response Attempt Limit

Definition: Number of tries a user is allowed per prompt during any one Security session

Setting: 1–16

Default: 1

Card: NMC

Select: **Programmed Settings**
Hub Security
Response Timeout

Definition: Number of seconds a users has in which to respond to system prompts

Setting: 10–255 seconds

Default: 30

Dial Out Login Failure

Triggered—when a user dialing out of a chassis modem enters an invalid response to a Total Control *Security Manager* prompt and exceeds the number of specified login attempts.

Triggered—if a user enters an invalid user name and/or password combination.

Triggered—if a user fails to respond to a login prompt within the set time limit.

Descriptors (user configured)

Card: NMC

Select: **Programmed Settings**
Hub Security
Response Attempt Limit

Definition: Number of tries a user is allowed per prompt during any one Security session

Setting: 1–16

Default: 1

Card: NMC

Select: **Programmed Settings**
Hub Security
Response Timeout

Definition: Number of seconds a users has in which to respond to system prompts

Setting: 10–255 seconds

Default: 30

Dial Out Restricted Number

Triggered—when a user dialing out of a chassis modem calls a number that has been disallowed on the Total Control *Security Manager* Call Restriction list.

DTE Ring-No-Answer

Triggered—when the DTE fails to raise DTR in response to an incoming call. The event descriptor specifies the maximum number of phone line rings by which the DTE should raise DTR to answer the incoming call.

This event is used to detect a "dead-air" or "ring-no-answer" situation. It is sent if one of the following conditions occur:

- ◆ The Quad modem receives a *digital* call, sends an incoming call message to the NETServer, but does not receive an answer call message within 60 seconds.
- ◆ The Quad modem receives a *digital* call, sends an incoming call message to the NETServer, but does not receive an answer call message before another call arrives.
- ◆ The Quad modem receives an *analog* call, sends an incoming call message to the NETServer, but does not receive an answer call message before it detects a specified number of rings. The number of rings can be selected by setting S-Register 0.

Descriptor (user configured)

Card: Modem Analog NIC

Select: **Faults**
NIC Event Thresholds
Ring No Answer Events

Definition: Number of rings allowed before this event is triggered

Setting: 0–255 rings

Default: 0 (disables the event)

DTE Transmit Idle

Triggered—when the connected modem's DTE remains idle (does not transmit data) for a number of minutes defined by the user.

Descriptor (user configured)

Card: Modem

Select: **Faults**
Modem Event Thresholds
DTE Idle Timeout Limit

Definition: Length of time the modem waits before reporting this event

Setting: 0 - 255 minutes

Default: 0 (disables the event)

DTR False

Triggered—when a modem's DTE changes its DTR line from high (true) to low (false) and holds it low for the number of seconds specified by the event descriptor.

Descriptor (user configured)

Card: Modem

Select: **Faults**
Modem Event Thresholds
DTR False Event Timeout

Definition: How long DTR must be low before triggering event

Setting: 0–255 seconds

Default: 0 (disables the event)

DTR True

Triggered—when a modem's DTE changes its DTR line from low (false) to high (true) and holds it high for the number of seconds specified by the event descriptor.

Descriptor (user configured)

Card: Modem

Select: **Faults**
Modem Event Thresholds
DTR True Time Limit

Definition: How long DTR must be high before triggering this event

Setting: 0–255 seconds

Default: 0 (disables the event)

Entity Watchdog Time-Out

Triggered—when one or more module entities (NACs) experience a watchdog time-out.

Fallback Count at Threshold

Triggered—when a chassis modem reaches the number of fallbacks specified in the event descriptor within a single call. If configured to do so, a chassis modem will automatically reduce its rate (fall back) to the next lower link rate if there are excessive data errors due to degraded signal quality. It will also automatically shift up to the next higher link rate when signal quality improves.

Descriptor(s)

Card: Modem

Select: **Faults**
Modem Event Thresholds
Fall Back Limit

Definition: Number of line fallbacks that will be used to qualify this event

Setting: 0–255 line fallbacks

Default: 0 (disables the event)

Fan Failed

Triggered—when the fan speed, monitored every three seconds for three successive samples by the NMC, becomes so slow as to risk damage due to inadequate cooling of the chassis. The fan used in the chassis supplies a square wave output signal with a frequency proportional to the rotational speed of the fan in RPM.

Measurements and multiple samples are used to ensure that this event does not occur too frequently, so Auto Response performance is not affected.

Descriptor (system configured)

- ◆ 17-slot chassis Fan Speed Thresholds (4500 RPM, 2000 RPM)
- ◆ 7-slot chassis Fan Speed Thresholds (1900 RPM, 1200 RPM)

Global Timer #n Expired

Triggered—when one of the four provided general purpose global timers expires. Each timer can be configured to expire periodically or only once.

Descriptor (user configured)

Card: NMC

Select: **Programmed Settings**
Auto Response Timer Groups
Global Timer #n Expired

Definition: See parameter options in the following chart.

Setting: See setting options in the following chart.

Each of the four timers can be configured to expire with the following parameters:

Descriptor	Definition
Start Date	Date (MM/DD/YY) the timer becomes active
Stop Date	Date (MM/DD/YY) the timer becomes passive (stops firing)
Start Time	Time (GMT) the timer becomes active
Stop Time	Time (GMT) the timer becomes passive (stops firing)
Timer Interval	Rate (in seconds) the timer fires between start/stop time/date

Hub Temperature Out of Range

Triggered—when chassis temperatures exceed the specified operating range (0C-50C), as measured at 20 second intervals by the NMC built-in temperature sensor.

Measurements and multiple samples are used to ensure that this event does not occur too frequently, so Auto Response performance is not affected.

Descriptor (system configured)

Temperature Thresholds (50C, 45C, 0C, 0C)

Incoming Connection Established

Triggered—when a remote modem successfully establishes a connection with a chassis modem.

Incoming Connection Terminated

Triggered—when a connection between a remote modem and a chassis modem is terminated for any reason.

Login Attempt Limit Exceeded

Triggered—when a user dialing into or out of a chassis modem fails to complete a successful Total Control *Security Manager* login session within the number of specified tries.

Descriptor (user configurable, but only on a chassis-wide basis)

Card: NMC

Select: **Programmed Settings**
Hub Security Group
Modem Attempt Limit

Definition: Number of successive failed login attempts on a single modem

Setting: 1–16 attempts

Default: 3

Management Bus Failure

Triggered—when the NMC loses contact with a modem. Each chassis modem communicates with the NMC via a dedicated management bus located on the midplane. When this event occurs, it is considered a symptom of a modem failure.

NOTE: If all modems on a multi-modem card are simultaneously in a Management Bus Protocol (MBP) fail state, a Module Non-Operational event is also triggered.

Modem Reset by DTE

Triggered—when a modem is reset by the DTE, either by an ATZ command or by dropping DTR to the modem. One powerful use for this event is to have *Total Control Manager* automatically reconfigure a modem to the settings in the NMC's NVRAM after it has been reset by the DTE.

Modem Ring-No-Answer

Triggered—when an *analog* modem that has been configured for auto answer fails to answer an incoming call. The event descriptor is an integer specifying the number of phone line rings by which the modem should have answered the incoming call.

Descriptor (user configured)

Card: Modem Analog NIC

Select: **Faults**
NIC Event Thresholds
Ring No Answer Events

Definition: Number of rings allowed before triggering this event

Setting: 0–255 rings

Default: 0 (disables the event)

Modem Watchdog Reset

Triggered—when a modem failure occurs. The watchdog is an independent hardware circuit on each modem entity that can detect software failures.

Module Inserted

(A module is defined as a NAC in the chassis.)

Triggered—when a module is inserted into the chassis. (The NMC never generates Inserted Events).

Not Triggered—when the chassis power transitions from off to on for modules already installed in the chassis.

Module Non-Operational

(A module is defined as a NAC in the chassis.)

Triggered—at the start of software download to a module.

Triggered—as a module is removed from service.

Triggered—if a module has failed (*i.e.*, all entities on a module have failed).

Module Re-initialized

(A module is defined as a NAC in the chassis.)

Triggered—when the chassis power transitions from off to on.

Triggered—when a module is inserted into the chassis.

Triggered—when software download is completed to a module.

Triggered—when a module is restored to service.

Triggered—when a module is hardware reset.

Module Removed

(A module is defined as a NAC in the chassis.)

Triggered—when a module is physically removed from the chassis.

No Dial Tone Detected

Triggered—when the modem goes off hook and detects an inadequate dial tone level on the *analog* phone line.

No Loop Current Detected

Triggered—when the modem goes off hook and does not detect the presence of loop current on the *analog* phone line.

Outgoing Connection Established

Triggered—when a chassis modem successfully establishes a connection with a remote modem.

Outgoing Connection Terminated

Triggered—when a connection between a chassis modem and a remote modem is terminated for any reason.

Packet Bus Active

Triggered—when a when a packet bus active event is detected by the modem.

Packet Bus Lost

Triggered—when a packet bus lost event is detected by the modem.

PSU Failed

Triggered—when the NMC detects a single fail signal of any PSU in the failed state upon the detection of an over-voltage or over-current condition. Signal samplings are taken by the NMC every five seconds.

PSU Voltage Out of Range

Triggered—when the NMC detects that voltage levels, for one or more of the power supplies on the midplane, are outside the normal operating range for three successive samples, taken at 20 second intervals.

After the event has triggered, a *single sample* within the *innermost* range specified by the event descriptors is needed before the event can be triggered again.

Measurements and multiple samples are used to ensure that this event does not occur too frequently, so Auto Response performance is not affected.

Thresholds are chosen to be compatible with all PSUs used in the 17-slot or the 7-slot chassis.

Descriptors (system configured)

- ◆ +5V Thresholds (+5.51V ,+5.35V ,+4.95V ,+4.75V)
- ◆ -5V Thresholds (-5.50V, -5.30V, -4.70V, -4.50V)
- ◆ +12V Thresholds (+13.1V, +12.8V, +11.4V, +11.0V)
- ◆ -12V Thresholds (-13.0V, -12.6V, -11.4V, -11.0V)

Response Attempt Limit Exceeded

Triggered—when a user dialing into or out exceeds the specified number of Total Control *Security Manager* prompt retries during a single Security session.

Descriptor (configured only on a chassis-wide basis)

Card: NMC

Select: **Programmed Settings**
Hub Security Group
Response Attempts

Definition: The number of tries a user is allowed per prompt during any one Total Control Security session

Setting: 1–16 tries

Default: 1

NOTE: This event usually occurs at the same time that the Dial Out Login Failure or Dial In Login Failure events occur.

User Blacklisted

Triggered—when a user dialing into or out of a chassis modem fails to enter the correct Total Control *Security Manager* password within the specified number of login attempts. To support this feature, the RADIUS security server provides a mechanism that informs the NMC when a user is blacklisted.

Response Options

The response options listed in this section are provided in alphabetical order. When you select a response that has descriptors, a window appears, presenting you with descriptor options.

NOTE: Some of the supported responses interact with another added-cost option, Total Control Hub Security.

Busy Out Analog Phone Line

Instructs the analog NIC to busy out the analog line for the modem generating the event.

Busy Out Module's Analog Phone Lines

Busies out all analog phone lines associated with the selected modem NAC.

Busy Out T1 DS0 Channel

Instructs the T1 Card to busy out the DS0 channel(s) for the modem generating the event.

Descriptor(s)

- ◆ Slot number where T1 Card is located (1-16)
- ◆ Number of DS1 entity on T1 Card (1-2)
- ◆ Number of the DS0 on this span (1-24)

NOTE: If you reallocate DS0s at any time, you must reconfigure this response.

Configure Module from Factory Defaults

(A module is defined as a NAC or NMC in the chassis.)

Configures all parameters for every entity on a module, including card- and channel-level entities. The values used are those established at the factory.

Configure Module from NMC NVRAM

(A module is defined as a NAC or NMC in the chassis.)

Configures all parameters for every entity on a module, including card- and channel-level entities. The values used are those last saved to the NMC's NVRAM through the Save To NVRAM command. This response performs the same level of configuration as is supported by the Auto-Configure feature of the NMC.

Continue If Test Passes

Used in conjunction with the Test response, this response affects the further execution of the script.

- ◆ If the test fails, the script execution continues with the response immediately following the test.
- ◆ If the test passes, the script parser searches through the script until it finds the Continue If Test Passes response. Once this response is found, the script execution continues with the response immediately following the Continue If Test Passes response. This provides the expert system (Auto Response engine) with some primitive decision-making capabilities without need for a full blown script language.

Delay Script Execution

Causes execution of a given script to suspend for the number of seconds specified in the response descriptor.

Descriptor(s)

Time Delay in seconds (0-127)

Generate Auto Response SNMP Trap

A single user-defined value (0-127) can be configured to be sent in this Trap. The management station or some other higher level Auto Response engine could use this feature to convey information when it detects a specific logic state (e.g., a specific point in the response script has been reached) for the purposes of performing additional responses to better handle the specific event that occurred.

Descriptor(s)

User Defined Auto Response Trap ID (0-127)

Modem Software Reset

Attempts to reset the processors associated with the modem entity through message exchange on the management bus. This relies on the given modem being at least partly functional, to the extent that it can communicate over the management bus. In an extreme situation, a modem may not be able to complete the request.

Reconfigure from Modem Factory Defaults

Resets all parameters for the modem entity to the factory defaults.

Reconfigure from NMC NVRAM

Configures all parameters for every entity on a module, including card- and channel-level entities. The values used are those last saved to the NMC's NVRAM through the Save To NVRAM command. This response performs the same level of configuration as is supported by the Auto-Configure feature of the NMC. If this request is denied, it is periodically retried until a modem accepts the request at some future time.

Remove Module from Service

(A module is defined as a NAC in the chassis.)

Holds all processors and circuits on the module in a reset state via the hardware reset circuit on the management bus interface.

NOTE: All modems on a multi-modem card are held in reset state via this response.

Reset Module

(A module is defined as a NAC or NMC in the chassis.)

Resets all processors and circuits on the module to a known state via the hardware reset circuit on the management bus interface.

NOTE: All modems on a multi-modem card are reset via this response.

Restore Analog Phone Line

Restores an analog line that has been busied out. This is the complement of the Busy Out Analog Phone Line response.

Restore Module to Service

(A module is defined as a NAC in the chassis.)

Removes all processors and circuits on the module from a reset state, via the hardware reset circuit on the management bus interface. This is the complement to the Remove Module from Service response.

NOTE: All modems on a multi-modem card are removed from the reset state via this response.

Restore Module's Analog Phone Lines

Restores all busied out analog phone lines associated with the selected modem NAC.

Restore T1 DS0 Channel

Restores a DS0 channel that has been busied out. This is the complement of the Busy Out T1 DS0 Channel response.

Descriptor(s)

- ◆ Slot number where T1 Card is located (1-16)
- ◆ Number of DS1 entity on T1 Card (1-2)
- ◆ Number of the DS0 on this span (1-24)

NOTE: If you reallocate DS0s at any time, you must reconfigure this response.

Terminate Connection

Hangs up the current call if one is in progress.

Terminate Script Execution

Provides a simple mechanism for disabling scripts without deleting their entire definition. When the script parsing engine comes across this response, script execution is stopped immediately.

There are no restrictions on where this response can be placed in the script.

Usage Tip: Inserting this response at the top of an existing script will cause the script not to execute. But, at some later date, the script could be re-enabled by removing this response.

Test Analog NIC

Performs a complete analog NIC self-test for a particular modem entity where an event has occurred. If any single test on the NIC fails, the entire test fails. Success or failure of this test affects which response in the script runs next (see the Continue if Test Passes response).

Usage Tip: Responses that perform tests are the mechanisms through which branching can be done in the response script execution. See the Continue if Test Passes response for a further description of this branching.

Test Analog Phone Line

Performs a complete analog phone line test for a particular modem entity where an event has occurred, including a test for dial tone and loop current. If any single test on the modem fails, the entire test fails. .

Usage Tip: Responses that perform tests are the mechanisms through which branching can be done in the response script execution. See the Continue If Test Passes response for a further description of this branching.

Test Modem

Performs a complete modem self test for a particular modem entity where an event has occurred. This is not a complete card-level test, but rather a complete test of one modem on a given card. If any single test on the modem fails, the entire test fails.

Usage Tip: Responses that perform tests are the mechanisms through which branching can be done in the response script execution. See the Continue If Test Passes response for a further description of this branching.

Test Module

(A module is defined as a NAC or NMC in the chassis.)

Tests all testable entities on the given module. In case of Dual or Quad modems, all modems on that card will be run through the self-test.

Usage Tip: Responses that perform tests are the mechanisms through which branching can be done in the response script execution. See the Continue If Test Passes response for a further description of this branching.

Appendix E

Cellular Modem Support

As of release 3.1, *TCM* supports Cellular modem applications by providing direct configuration of new cellular objects added to the modem MIB. These include objects for configuration of MNP10 and Enhanced Throughput Cellular (ETC).

Cellular Support as an Added Cost Option

Customers who require these options must pay an extra fee to have this feature enabled. In order to provide flexibility for our systems customers who may have a large installed base of product, the feature can be enabled in one of two ways:

- ◆ The modem may be shipped from the factory with Cellular support permanently enabled (Quad Modem versions 2.0 and higher).
- ◆ The NMC and the Quad Modem Card (versions 2.0 and higher) provide the ability to enable Cellular support on a chassis-wide basis through the NMC. This eliminates the need to obtain and perform individual feature enables for all of the modems in a network and ensures that if a modem is swapped, the replacement will also support cellular protocols. When this feature has been enabled, the NMC will inform the modems that they need to support the Cellular protocols any time a modem is installed, reset, or restored to service.

Functional Description

Modems with cellular support can negotiate for either of two cellular protocols: ETC and MNP10. These protocols are designed to combat a variety of link establishment and data transfer problems specific to cellular calls.

MNP10

MNP10 modifies data transfer techniques for increased reliability over cellular links. It uses three major strategies to do so:

- ♦ *Aggressive Adaptive Packet Assembly (AAPA)* adjusts the data packet size during data transfer in response to line conditions, ensuring the maximum allowable packet size at all times.
- ♦ *Link Management Idle (LMI)* is used to monitor line conditions when no data is being sent, and helps guard against lost connections.
- ♦ *Dynamic Transmit Level Adjustment (DTLA)* changes the transmit level “on the fly” to adapt to changing line conditions.

MNP10 can also be negotiated for non-cellular calls, but offers no advantage over other protocols for non-cellular calls.

DTLA is only necessary for calls across cellular links. Unless the modem is set for *MNP10 Cellular* (mdmCeOperDis/S60.3), it uses DTLA only when the originating modem is set for MNP10 Cellular. MNP10 can be negotiated for non-cellular calls, but offers no advantage over other protocols for those calls.

NOTE: *MNP Extended Services* (mdmCeMnpDis/S60.1) must be disabled to originate calls under V.34, V.FC, HST, or V.32 Terbo.

ETC

ETC represents U.S. Robotics' implementation of the Enhanced Throughput Cellular (ETC) protocol. ETC allows a modem to recognize calls from other modems using ETC and alter its settings for increased performance when transmitting data across cellular links.

ETC requires that the modems establish V.42 error control. ETC also requires a V.32 *bis*, V.32, or V.22-type connection. ETC does not function under V.34 modulation.

The modem implements ETC whenever it answers a call and receives the ETC calling tone from an originate modem. The modem must receive the ETC calling tone from the originate modem. It is the only way for the modem to know that it will be transmitting over a cellular link. If the modem does not receive the ETC calling tone, the call progresses normally without ETC.

The modem also implements ETC settings for *all* outgoing calls. This means that the modem forces a V.32- or V.22-type modulation and V.42 with a reduced packet size, and will not connect using V.34. It also transmits using de-emphasis and reduced transmit level, even if it is not connecting across a cellular link, which results in reduced throughput or even dropped calls. If the modem is going to be used for originating calls across non-cellular links, we recommend using the *Do not Originate with ETC* (mdmCeDbNoEtcDis/S66.7) setting.

Activating ETC and MNP10

Three cellular templates stored in the modem's ROM allow you to activate ETC or MNP10 with the modem settings that offer maximum performance. A template may be loaded in one of three ways:

- ◆ If you are using TCM, by using the *Modem Software Commands* (see Chapter 9 in the *Total Control Manager/SNMP Software Guide*).
- ◆ If you are using another SNMP management software, by using the Total Control Modem MIB modem command table.
- ◆ If you are using AT commands to configure the modems, by using the &Fn command.

WARNING: Do not load cellular templates if you have made special configuration changes to the modems. When you load a cellular template, it loads the hardware flow control defaults (&F1). Instead, configure cellular parameters individually with the settings listed under the appropriate template.

NOTE: Only one template may be loaded at a time. If you wish to activate *both* ETC and MNP10:

1. Load the MNP10 Cellular Template.
2. Configure the modem with the settings listed for the ETC fixed site (or mobile site) template.

MNP10 Cellular Template

TCM Modem Software Command: Load MNP10 Cellular Defaults

MIB Extension: loadMnp10CllulrDflt(25)

AT Command: &F4

This template loads the hardware flow control defaults (&F1) *and* the following settings:

♦ **MNP10 Negotiation**

The modem negotiates MNP10 for incoming and outgoing calls. If the connecting modem does not support MNP10, the call progresses without MNP10.

DTLA is only used if the originate modem negotiates MNP10 cellular, or if the modem is set for *Link Across a Cellular Network*.

♦ **MNP Extended Services**

Extended Services (MNPX) allows the modems to negotiate MNP10 as a part of the V.42 negotiation process. If the connecting modem supports MNPX, V.42 negotiation and V.42*bis* is used as the modulation and compression engine of choice. If the connecting modem does not support either V.42 or MNPX, MNP10 is negotiated under MNP, and MNP5 compression is used.

ETC Fixed Site Cellular Template

TCM Modem Software Command: Load V42 Cellular Fixed Defaults

MIB Extension: loadV42CllulrFxdDflt(27)

AT Command: &F6

This template loads the hardware flow control defaults (&F1) *and* the following settings:

- ◆ **ETC**

The modem implements ETC whenever it answers a call and receives the ETC calling tone from an originate modem. The modem must receive the ETC calling tone from the originate modem. It is the only way for the modem to know that it will be transmitting over a cellular link. If the modem does not receive the ETC calling tone, the call progresses normally without ETC.

The modem also implements ETC settings for *all* outgoing calls. This means that the modem forces a V.32- or V.22-type modulation and V.42 with a reduced packet size, and will not connect using V.34. It also transmits using de-emphasis and reduced transmit level, even if it is not connecting across a cellular link, which results in reduced throughput or even dropped calls. If the modem is going to be used for originating calls across non-cellular links, we recommend using the *Dialback without ETC* setting.

- ◆ **ETC Fixed Site Operations**

Modem sets transmit levels for fixed site cellular operations when ETC is used.

- ◆ **ETC Calling Tone Enabled**

The modem generates an ETC calling tone when it originates a call. The calling tone indicates to the answering modem that you wish to use the ETC cellular protocol.

- ◆ **9600 DCE Startup Rate**
Some cellular links may be so poor that calls are dropped even before the modems can initialize modulation and error control negotiation. To reduce the number of dropped calls, the modem is set to a 9600 bps startup rate. The modems negotiate at the lower and more stable link rate, and after ETC has been implemented, raise the link rate to the higher levels afforded by ETC.
- ◆ **Wait for Carrier 90 Seconds**
Over cellular links, modems often take longer to establish a carrier. This setting lengthens the time the modem waits for a carrier to 90 seconds.
- ◆ **Loss of Carrier Disconnect**
Cellular links frequently receive disturbances that cause extended loss of carrier. This setting lengthens the time before the modem hangs up upon loss of carrier to 10 seconds.

ETC Mobile Cellular Template

TCM Modem Software Command: Load V42 Cellular Mobile Defaults

MIB Extension: loadV42CllulrMblDflt(26)

AT Command: &F5

Use this template to enable ETC when the modem is answering or dialing from a cellular phone. Although Quad Modem Cards are usually not located on the mobile end (cell side) of a connection, you can advise callers to use these settings when placing calls from mobile locations.

The settings for this template are identical to those for the V.42 fixed site template (&F6), except for the following setting:

- ◆ **Enable ETC Mobile**
Modem sets transmit levels for mobile site (cell side) cellular operations when ETC is used.

Cellular Configuration Group

The parameters in this modem configuration group apply only to cellular calls. The settings do not affect normal connections.

ETC Parameters

The following settings only affect ETC calls.

ETC Max. Link Rate

MIB Object: mdmCeDceBitraLim

Command Setting Equivalent: S64

Description: Sets maximum DCE rate, preventing modems from connecting or falling forward to link rates higher than specified. Lowering the maximum link rate to 9600 bps can provide more stability for cellular calls under adverse conditions. However, higher throughput is sacrificed for calls over stronger cellular links that can support higher link rates.

Settings:

Max DCE Rate
4800 bps
7200 bps
9600 bps
12000 bps
14400 bps

Default: Max DCE Rate

ETC Transmit Level

MIB Object: mdmCeDceTxLev

Command Setting Equivalent: S65

Description: This setting allows a Cellular modem to control the DCE transmit level (default) or permits a specific decibel level to be imposed for a cellular operation.

A reduced transmit level is required for data transfer across cellular links. When ETC is established for a call, the modem automatically reduces its transmit (TX) level to the value specified by this parameter.

With the default setting, the modem sets the TX level according to ETC specifications based on whether it is transmitting over T1 or analog lines and whether the modem is set for fixed site or mobile. We do not recommend changing this setting.

Settings: Modem control TX level

10 dBm
11 dBm
12 dBm
13 dBm
14 dBm
15 dBm
16 dBm
17 dBm
18 dBm
19 dBm
20 dBm
21 dBm
22 dBm
23 dBm
24 dBm
25 dBm

Default: Modem control TX level

ETC Negotiation

MIB Object: mdmCeV42EtcDis

Command Setting Equivalent: S66.0

Description: This setting controls whether or not the modem will use ETC in response to the ETC calling tone.

Settings: Disable
 Enable

Default: Disable

ETC Fixed/Mobile Site

MIB Object: mdmCeV42CellSite

Command Setting Equivalent: S66.1

Description: Determines whether a Cellular modem will use a fixed site or mobile site cellular profile. The cellular profile sets transmit levels based on ETC specifications. With the exception of certain nautical and aerospace applications, most Total Control installations are fixed site.

Settings: Fixed site
 Mobile site

Default: Fixed Site

ETC Calling Tone

MIB Object: mdmCeV42EtcCallToneDis

Command Setting Equivalent: S66.2

Description: Determines whether or not the ETC calling tone is sent out by a Cellular modem during link establishment, telling the answering modem to use ETC settings.

Enable the ETC calling tone when originating calls from the mobile side (cell side) of a cellular link. Disable calling tone only if you experience problems when originating calls to non-cellular modems.

Settings: Disable
 Enable

Default: Disable

Force ETC Settings

MIB Object: mdmCeV42EtcTxLevConDis

Command Setting Equivalent: S66.3

Description: If ETC negotiation is enabled, this setting forces ETC transmit level control for all incoming calls.

Some callers may wish to negotiate ETC using the earlier 1.0 version, which does not generate the ETC calling tone used in version 1.1. In order for the modem to implement ETC when answering calls from modems with the earlier 1.0 version, it must be set to force ETC for every call it receives. (In this circumstance, the system administrator may wish to dedicate some modems for cellular calls only.)

Settings: Disable
 Enable

Default: Disable

ETC DCE Start-up Rate

MIB Object: mdmCeDceStartRate

Command Setting Equivalent: S66.4 and S66.5

Description: This permits selection of the DCE start-up rate for a Cellular modem.

Some cellular links may be so poor that calls are dropped even before the modems can initialize modulation and error control negotiation. To reduce the number of dropped calls, the modem should be set to a 9600 bps startup rate. The modems negotiate at the lower and more stable link rate, and after ETC has been implemented, raise the link rate to the higher levels afforded by ETC.

Settings: Auto
 4800 bps
 9600 bps

Default: Auto

ETC Transmit De-emphasis

MIB Object: mdmCeV42DceTxDemDis

Command Setting Equivalent: S66.6

Description: This permits selection of DCE transmit de-emphasis for a Cellular modem. Transmit de-emphasis is recommended when connecting over a cellular link, whether the modem is on the fixed site or mobile site. When enabled, transmit de-emphasis is automatically implemented whenever the modem receives an ETC call.

Settings: Disable
 Enable

Default: Disable

Do not Originate with ETC

MIB Object: mdmCeDbNoEtcDis

AT Command: S66.7=1

Description: Use the “disable” setting to disable ETC when originating calls to a non-cellular modem, yet allows ETC negotiation in answer mode. If the modem is used to place outgoing calls to non-cellular modems, use this setting to disable ETC during originate mode.

Settings: Disable
 Enable

Default: Disable

MNP10 Parameters

The following settings only affect MNP10 calls.

MNP10 Negotiation

MIB Object: mdmCeMnp10Dis

Command Setting Equivalent: S60.0

Description: Enabling this option for a Cellular modem allows a Cellular modem to connect using MNP10.

Settings: Disable
 Enable

Default: Disable

MNP Extended Services

MIB Object: mdmCeMnpXDis

Command Setting Equivalent: S60.1

Description: Extended Services (MNPX) allows the modems to negotiate MNP10 as a part of the V.42 negotiation process. If the connecting modem does not support either V.42 or MNPX, MNP10 is negotiated under MNP.

With MNPX disabled, modems can not negotiate MNP10 under V.42.

NOTE: If MNPX is disabled, calls from modems using MNPX and V.42 connect without MNP10.

Settings: Disable
 Enable

Default: Disable

MNP10 Compression Type

MIB Object: mdmCeComp

Command Setting Equivalent: S60.2

Description: This option applies to a Cellular modem for which data compression has been enabled. With the V.42 *bis* setting, the modem decides which type of compression engine to use on a case-by-case basis. Selecting MNP5 allows only that type of compression to be used on a cellular call.

Settings: MNP5
V.42 *bis*

Default: MNP5

MNP10 Cellulark

MIB Object: mdmCeOperDis

Command Setting Equivalent: S60.3

Description: Uses Dynamic Transmit Level Adjustment (DTLA). With the default, non-cellular setting, DTLA is only used if the remote modem originates an MNP10 cellular call. Enable only when originating from a cellular link.

Settings: Disable
Enable

Default: Disable

MNP10 Link Speed

MIB Object: mdmCeLinkSpeed

Command Setting Equivalent: S60.4

Description: Use the 1200 bps option to provide stability and reliability for extremely noisy MNP10 link conditions.

Settings: Link at High Speed
Link at 1200 bps (V.22)

Default: Link at High Speed

MNP10 Fallback

MIB Object: mdmCeMnp10FallbackDis

Command Setting Equivalent: S60.5

Description: When enabled, prevents the modem from falling back to lower speeds during MNP10 connections. Used for testing purposes only.

Settings: Enable
 Disable

Default: Disable

MNP10 Fall Forward

MIB Object: mdmCeMnp10FallforDis

Command Setting Equivalent: S60.6

Description: Prevents the modem from falling forward to higher speeds during MNP10 connections. Used for testing purposes only.

Settings: Enable
 Disable

Default: Disable

MNPX Detection Pattern

MIB Object: mdmCeMnpxDetPhaEna

Command Setting Equivalent: S60.7

Description: The MNPX pattern expedites MNP10 negotiation when connecting to other modems that support MNPX.

The MNPX detection pattern can cause problems when dialing to modems without MNPX—they connect, but without MNP10. Disable the MNPX detection pattern if you experience this problem when dialing to modems without MNPX. In answer mode, the MNPX detection pattern should always be enabled.

Settings: Enable
 Disable

Default: Enable

MNP10 V.42 *bis* Short Form Negotiation Rules

MIB Object: mdmCeShortFormRules

Command Setting Equivalent: S61

Description: Provides V.42*bis* compatibility when originating to some older MNP10 modems that do not have MNPX capabilities. The short form assumes that the maximum string length is 32 octets and the direction of compression is always bi-directional. When disabled, V.42 *bis* is negotiated with MNPX.

Settings: Disable
 Form 1 Code Words 512
 Form 2 Code Words 1024
 Form 3 Code Words 2048

Default: Disable

Index

—A—

A/E Logging
 Log Generation 14-16
AAPA E-2
Accounting 14-1
 Database Reporting 14-22
Accounting Menu
 Commands A-4
Accounting/Event Logging 14-1
 Change Required 3-8
 Charts 14-24
 Configuration 14-6
 Server 14-1
Accounting-Request Packet 14-7
Accounting-Response Packet 14-7
ACCTDICT.DAT 14-8, 14-15
Action See Commands
 Defined 9-1
 Execute 9-3
 Icon 9-1
Activating
 Both MNP10 and ETC E-4
 ETC E-3
 ETC and MNP10 E-4
 MNP10 E-3
Add Response D-5
Add Trap Destination Window 8-3
Added-Cost Options
 Auto-Response 3-4
 Security 3-4
Adding the Chassis to the Database 4-1-4-5
Alarm
 Configuration 10-3
 Disposition 10-4
 Window 10-4
 Integration 10-3
 Manager 10-3
 Monitor 10-5-10-6
 Window 10-5
 Reports 10-6
Alarms
 Defined 8-1
 Integration 3-7
 Set Up in NMS 8-4
Attempted Login by Blacklisted User D-11
Attributes 14-13, 14-26-14-31
Auto Response D-1
 Configuration D-2-D-6
 Copy Script D-6
 Enabling D-1

Event Options D-11-D-24
Events and Responses D-7
 Channel-Level Events and Responses D-8
 Chassis-Level D-7
 Module-Level D-8
 Overview D-7-D-10
Generate Trap D-27
Overview D-1-D-2
Parameters Window D-5
Pre-Configuration Requirements D-3
Resequencing Responses D-5
Response Options D-25, D-30
Window D-4
 Event D-4
 Response Script Usage D-5
Responses **D-5**
Selected Services D-4

—B—

Blacklisting C-29
Block Error Count at Threshold D-11
Busy Out
 Analog Phone Line D-25
 Module's Analog Phone Lines D-25
 T1 DS0 Channel D-25
Buttons
 Cancel 6-5
 Copy 6-4
 Default 6-4
 Get 6-4
 Help 6-5
 Load From 6-4
 OK 6-4
 Print 6-4
 Set 6-4
 User
 Configuration Window C-36
 Group Window C-33
 View by Column 6-4
 View by Row 6-4

—C—

Calendar Window C-29
Call
 Events 14-18
 Restriction List C-29, C-30, C-36-C-37
 Examples C-37
 Wildcards C-37
Termination Log 14-20

Calling Tone	
V.42ETC	E-9
Cancel	
Button	6-5
Card-	
Level Events and Responses	D-8
Card-Specific Software	6-8
Cellular	
Configuration Group	E-7–E-15
Enabling	E-1
ETC	
Parameters	E-11
Functional Description	E-3
MNP10	
Parameters	E-12–E-15
Modem Support	E-1
Protocols	E-1
Template	
ETCMobile	E-6
ETC Fixed Site	E-4–E-6
MNP10	E-4
Change Group Assignment Window	C-27
Change Password Message	C-13
Changing Parameter Settings	6-5
Channel-Level Events and Responses	D-8
Chassis	
17-Slot	4-6
7-slot	4-6
Adding to the Database	4-1–4-5
Configuring	5-2–5-3
Definition	5-1–5-2
Inventory	13-1–13-4
Management	10-1–10-8
MP/16	4-7
Restoring Configuration	5-4
Chassis-Level Events and Responses	D-7
Client Configuration	14-3
Client-Server Protocol	14-2
Commands	<i>See</i> Action
Available	9-3–9-5, 9-3–9-5
Defined	9-1
Execute	9-1–9-3
Installed Cards	9-1
Menu	A-1
Modem	
Analog NIC	
Hardware (Card Level)	9-3
Software (Channel Level)	9-4
Hardware (Card Level)	9-3
Software (Channel Level)	9-3
NMC Software	9-4
SNMP	6-1
T1 Card	
Hardware	9-4
Software	
Card Level	9-4
DS0	9-5
DS1	9-4
X.25 Gateway	
Hardware	9-5
Software	9-5
Common Terms	1-3
Community Strings	4-2, 5-1, 8-3
Compiling	
MIBs	10-7
Compiling MIBs	3-7
Components	
Required Hardware	2-1
Required Software	2-1
Conducting the First Session	4-1
Configuration	
Accounting Client	14-3–14-6
Chassis	5-2–5-3
Device	4-1
Loading	6-7–6-8
Object - Chapter 6	6-1
Restoring	5-4
User	
Group	C-28
Window	
Components	6-2–6-5
Using	6-2
Configure	
Menu	13-1
Commands	A-2
Module from Factory Defaults	D-25
Module from NMC NVRAM	D-26
Configuring	
Alarms	10-3
Hub Security	C-8
Traps/Alarms	8-1
Connect	
String Rules	4-5
Success Message	C-13
Connection	
Attempt Failed	D-11
Time Limit Expired	D-12
Connectivity Test	3-18
Continue If Test Passes	D-26
Copy Auto Response Script	D-6
Current	
Dial Back Group Statistics	C-25
Customizing	
Logs	14-8
NET.CFG	3-12

—D—	
Data Types	14-26–14-31
Database	
Accounting Prototype	14-22–14-25
Default	
Button	6-4
Delay	
Dial Back	C-14
DTR DCD	C-9
DTR DSR	C-9

Script Execution	D-26
Destination	
Trap.....	8-3
Device	4-1, 4-3, 4-6, 4-7, 5-1
Adding.....	4-1-4-5
Defined.....	1-3
Driver.....	4-3
List Window	13-2
Optional Parameters.....	4-3-4-5
Selection from the VFPD	4-8-4-9
Dial Back	
Attempt Limit.....	C-14
Delay	C-14
File Control Buttons.....	C-26
Group	C-25
Characteristics	C-25
Statistics	C-25
Window.....	C-24
Current Dial Back Group Statistics	C-25
Dial Back Group.....	C-25
Dial Back Group Characteristics	C-25
Dial Back Group Statistics.....	C-25
File Control Buttons	C-26
Modem Selection Grid.....	C-25
User Assignment	C-26
Modem Restriction Error	D-12
Name Prompt.....	C-10
Number	C-30
Number Prompt	C-11
Password Prompt	C-10
Pending Prompt	C-11
Restricted Number	D-12
Restricted Number Trap.....	C-17
User Assignment.....	C-26
Dial In	
Enable	C-8
Login Failure	D-13
Login Failure Trap	C-16
Dial Out	
Call Restrictions Window	C-29
Enable	C-9
Login Failure	D-14
Login Failure Trap	C-16
Restricted Number	D-15
Restricted Number Trap.....	C-16
Dialogue Punctuation	4-5
Dictionary File.....	14-15
Disable MNPX Detection Pattern.....	E-14
Do not Originate with ETC	E-11
DOSDIALR.EXE	4-5
Drivers	
Unloading	3-18
Drop-down list box	1-3
DS0	
Configuration.....	12-1, 12-3
DS0 Configuration Testing.....	11-1
DTE	
Ring-No-Answer	D-15
Transmit Idle	D-16

DTLA.....	E-2
DTR	
DCD Delay.....	C-9
DSR Delay	C-9
False	D-16
True	D-17

—E—

Editing the Dictionary File.....	14-15
Editing the Output Definition	14-8
Enabling the NMC.....	4-10
Encryption.....	C-24
Entity Watchdog Time-Out.....	D-17
Entity-Level Events and Responses.....	D-8
ETC	E-2
Activating.....	E-3
Calling Tone	E-9
DCE Start-up Rate.....	E-10
Fixed/Mobile Site.....	E-9
Max. Link Rate	E-7
Template	
Fixed Site.....	E-5
Mobile Site	E-6
Transmit De-emphasis.....	E-11
Transmit Level	E-8
ETC	
Ethernet	
Custom NET.CFG	3-15
Network Drivers.....	3-16, 3-17
Event	
Log.....	14-17
Logging	14-1
Server	14-3
Event Options.....	D-11

—F—

Fallback	
Count at Threshold.....	D-17
Fan Failed	D-18
Fault	
Menu	10-4
Fault Menu.....	8-1, 11-2
Commands	A-3
Faults	
Icon.....	6-2
Feature Enable	C-1, D-2, E-1
Auto Response	4-9
Cellular	4-9
for Added-Cost Options.....	4-9
Operation	4-10
Security.....	4-9
Verification	C-1
File	
Control Buttons.....	C-26
Menu	

Commands.....	A-1
Syntax	14-8
Flash ROM	6-8
Force ETC Settings	E-10
Format Specifiers	14-11
Fractional T1	12-4
Framed User	
Parameters.....	C-32
Functional Group Monitor Setup Window	7-2

—G—

Generate	
Auto Response SNMP Trap	D-27
Generic Slot Record	14-18
Get	
Button.....	6-4
Global Timer Expired	D-18

—H—

Hardware	
Requirements.....	2-1
Help	
Button.....	6-5
Help Menu	
Commands.....	A-5
HOSTS File	3-9, C-6
Hub Security	C-1
Configuration.....	C-8–C-18
Description	C-2
Enabling	C-1
Feature Installation	C-5–C-7
Installation.....	C-5
Management	C-19
NETServer.....	C-32
NMC Programmed Settings.....	C-9–C-15
Overview	C-1–C-4
Passwords.....	C-24
Requirements.....	C-3
Security Manager.....	C-19–C-38
Troubleshooting	C-37
User	
Group Window	C-26
Hub Temperature Out of Range.....	D-19

—I—

Icons	
Security Manager.....	C-21
Toolbar.....	A-1
Idle Phone Line Test	11-6
IETF	C-3
Incoming	
Connection Established.....	D-19
Connection Terminated.....	D-19

Install Drivers Window.....	3-5
Installation	
Added-Cost Options	3-4
Adjustments	3-6, 3-5–3-9
Hub Security	C-5
Novell NMS.....	3-2
ODBC	3-5
TCM	3-4
Integrating Alarms.....	3-7
Internet.....	1-3
Map	10-1, 10-2
Internet Drafts	C-4
Invalid Modem Select Message.....	C-12
Inventory	13-1–13-4
Inventory Window	13-3
IP (Internet Protocol)	
Addressing	3-1
Defined	1-4
IP Address	
Primary Log Server.....	14-4
Secondary Log Server.....	14-4
Security Server.....	C-15
ISO.....	1-4

—K—

Keyword Descriptions.....	14-9
Keywords	14-8

—L—

LED	
Polling Information.....	7-1
Polling Information Window.....	7-1
LEDs	
Defined	B-1
Dual Modem	B-2
Dual T1	B-1
NMC Card	B-3
Quad Modem	B-2
Single T1	B-2
X.25 Pad	B-4
Limit	
Dial Back Attempt.....	C-14
Modem Attempt	C-15
Response Attempt	C-14
LMI.....	E-2
Load From	
Button	6-4
Loading	
a Configuration.....	6-7
Network Drivers.....	3-16–3-18
Total Control Manager/SNMP	3-19
Log	
Examples	14-13
Dictionary File	14-15
Examples	

Event	14-14
Native RADIUS	14-14
Generating	14-16
Generation	14-16–14-21
Group Selection	14-5
Output Definition	14-8
Server's UDP Port Number	14-4
Logging	
Client TX Retry	14-4
Server Has Been Lost Trap	14-6
Login	
Attempt Limit Exceeded	D-19
Attempt Limit Exceeded Trap	C-18
Failed Message	C-12
Failure	
Dial In	D-13
Dial Out	D-14
Logs	
Importing	14-23
Loop Back Test	11-5
Loop Back/Self Test/Idle Phone Line Test ..	11-5–11-7

—M—

Management Bus	
Failure	D-20
Protocol	6-1
Slot	1-1
Management Information Base	
Browsing	10-7
Management Information Base (MIB)	
Browsing	10-8
Compiling	3-7, 10-8
Defined	1-3
Management Services (MS)	1-3
Management Station	
Defined	1-2
Map	<i>See</i> Command, Fault,
.....	Performance, Programmed Setting
Creating	10-2
Internet	10-1, 10-2
Locational	10-1, 10-2
Menu Definitions	A-1–A-5
Message	
Change Password	C-13
Connect Success	C-13
Invalid Modem Select	C-12
Login Failed	C-12
New Password	C-13
No Modems Available	C-12
Microsoft Open Database Connectivity (ODBC)	
Software	3-4
Minimum Password Length	C-24
MNP Extended Services	E-12
MNP10	E-1
Activating	E-3
Cellular	E-13
Compression Type	E-13

Fall Forward	E-14
Fallback	E-14
Link Speed	E-13
Negotiation	E-12
Template	E-4
V.42 <i>bis</i> Short Form Negotiation Rules	E-15
MNPX	E-12, E-14
Modem	
Attempt Limit	C-15
Cellular Support	E-1
Configuration Window	12-1
Loop Back/Self Tests Window	11-6
Programmed Settings	C-8–C-9
Reset by DTE	D-20
Ring-No-Answer	D-20
Select Prompt	C-11
Selection	C-30
Selection Grid	C-25
Software Reset	D-27
Watchdog Reset	D-20
Module	
Inserted	D-21
Non-Operational	D-21
Re-initialized	D-21
Removed	D-22
Module-	
Level Events and Responses	D-8
Level Responses and Events	D-8
Monitoring Performance	7-2
MTU	
Defined	C-33

—N—

Native RADIUS Call Log	14-17
Navigating the Security Manager	C-22
ETC	E-9
NET.CFG	3-11–3-16
NetExplorer Prompt	3-2
NETServer Configuration Window	C-32
NetWare Management System	3-2
Network	
Drivers	3-16–3-18
Map	10-1–10-3
Network Management Card (NMC) ... <i>See</i> Commands,	
.....	Faults, Performance, Programmed Settings
SNMP Proxy Agent	6-1
New Device Window	4-1
New Password Message	C-13
NMC	
Events and Responses	D-7
Logging Group	14-3
NMC Faults	C-15–C-18
NMC Logging Traps	14-6
NMS Tools, Using	10-1–10-8
No	
Dial Tone Detected	D-22
Loop Current Detected	D-22

No Modems Available Message	C-12
Novell NetWare Management System (NMS).1-1, 2-2	
Alarms.....	8-4, 10-3-10-6
Chassis	
Management.....	10-1-10-8
Icon	4-1
Installation.....	3-1, 3-2-3-3
Map.....	10-1
Maps	4-2
Prompts	3-6
Server Connection.....	3-2
Novell Server Connection.....	3-6

—O—

Object	
Configuration Restoration.....	5-4
Defined.....	1-3
Save.....	5-2-5-3
Send Changes to	6-6
Status	7-1
ODBC.....	C-5
Installation.....	C-5
ODI Device Driver.....	2-2
Open Systems Interconnection (OSI)	1-4
Options	
File Management.....	A-1
Toolbar.....	A-1
Window Control	A-5
Outdef.dat.....	14-8
Outgoing Connection	
Established	D-22
Terminated	D-22
Output Definition.....	14-8

—P—

Packet Bus	
Active.....	D-22
Lost	D-22
Parameters	
Changing	6-5-6-6, 9-1
Optional.....	4-5
Sending	6-6
Setting	6-5, 9-1-9-3
Password	
Duration	C-24
Expiration.....	C-29
Warning.....	C-24
Passwords	
Duration	C-24
Encryption	C-24
Hub Security.....	C-24
Minimum Length.....	C-24
User	
List Window.....	C-35
Warning.....	C-24

PDU.....	6-1
Performance	
Button	7-2
Modem.....	7-2
Monitoring	7-2-7-4
Table.....	7-4
Performance Menu	
Commands	A-4
Ping.....	3-18
Polling	
Information.....	7-1
Interval.....	7-3
LEDs.....	7-1
Port Reinitialization.....	3-6
Power Supply	
Unit.....	B-4
Preliminary Considerations.....	1-1
Primary Log Server IP Address	14-4
Print	
Button	6-4
Private Community String.....	4-2
Programmed Settings	
Icon	6-2
Programming Attributes.....	14-13
Prompt	
Dial Back	
Name	C-10
Number	C-11
Password.....	C-10
Pending.....	C-11
Modem Select	C-11
Restricted Number	C-12
User	
Name	C-10
Password.....	C-10
Protocol	
Data Units.....	6-1
Protocols	
ETC	E-2
MNP10	E-1
PSU	
Failed.....	D-22
Voltage Out of Range	D-23
Public Community String.....	4-2
Punctuation	4-5

—R—

RADIUS	
Accounting	14-1
Accounting Packets	14-7
Call Termination Log	14-20
Client Configuration.....	14-3
Compatibility	C-3
Defined	14-2
Dictionary File	14-15
Event Log.....	14-17
Generating Logs.....	14-15, 14-16

Native Log.....	14-17
Output Definition.....	14-8
Registration	14-2, C-6
Server Configuration.....	14-7
Reconfigure	
from Modem Factory Defaults.....	D-27
from NMC NVRAM.....	D-27
Remove	
All Responses.....	D-6
Module from Service.....	D-28
Response	D-6
Removing	
Novell Prompts	3-6
Requirements	
Hardware.....	2-1
Software	2-2
Reset	
Module.....	D-28
Responder Test	
Starting.....	11-4
Responder Tests.....	11-4
Window	11-5
Response	
Attempt Limit.....	C-14
Attempt Limit Exceeded	D-24
Attempt Limit Exceeded Trap	C-18
Echo Enable.....	C-14
Options.....	D-25
Script Usage	D-5
Timeout	C-13
Restore	
Analog Phone Line.....	D-28
Module's Analog Phone Lines.....	D-28
Module to Service.....	D-28
T1 DS0 Channel	D-29
Restricted Number Prompt.....	C-12
Ring-No-Answer	
DTE.....	D-15
Modem	D-20

—S—

Sample Call Restrictions	C-37
Save Chassis Configuration Window.....	5-3
Secondary Log Server IP Address.....	14-4
Secret Key	C-24
Security.....	C-1
Change Required	3-8–3-9
Mode.....	C-30
NETServer.....	C-4, C-32
ODBC	3-4, 3-5
Server	
IP Address	C-15
Retries.....	C-15
UDP Port.....	C-15
Security Menu	
Commands.....	A-4
Security Manager.....	C-19

Configuration Menu	C-20
File Menu	C-20
Help Menu	C-21
Main Menu	C-20
Navigating.....	C-21–C-36
Record Menu.....	C-20
Server Configuration Window	C-22
Toolbar	C-21
Troubleshooting	C-37–C-38
View Menu	C-21
Window Menu.....	C-21
Security Menu	
Commands	A-4
Self Tests	11-6
Send	
Tone Window.....	11-2
Server Configuration.....	14-7–14-15
Server Configuration Window.....	C-22
Clients	C-23
Passwords	C-24
Server	
Filename	C-22
Log	C-23
Server Statistics.....	C-23
SERVICES File.....	3-8, 3-9, 14-2, C-6
Session	
Monitor.....	7-2
Set	
Button	6-4
Setting	
<i>enableAll</i>	14-1
<i>enableLog</i>	14-1
Parameters	6-5
SHARE.EXE	3-2, 3-10
SLIP Connection	
Custom NET.CFG+.....	3-11–3-16
Network Drivers.....	3-16, 3-17
Slot-Level Events and Responses.....	D-8
SNMP	
Community String	4-2, 5-1
Community Strings.....	8-3
Defined	1-1
Get/Set.....	6-1, 6-4, 6-5
Host Software.....	2-2
Management Requirements	6-5
Traps.....	8-1–8-3
SNMP Proxy Agent	6-1
Software.....	<i>See</i> Total Control Manager/SNMP
..... and Novell NetWare Management	
Download.....	6-8–6-9
Download Window.....	6-10
Installation Tips	3-9–3-10
Requirements	2-2
Spin button	
Defined	1-3
Statistics	
User	
Group.....	C-27
Syntax	14-8

Attributes.....	14-13
Format Specifiers.....	14-11
Keywords.....	14-8

—T—

TCP/IP	
Defined.....	1-4
Origin.....	1-4
Terminal User Interface.....	4-2
Terminate	
Connection.....	D-29
Script Execution	D-29
Terminology.....	1-3
Test	
Analog NIC.....	D-29
Modem	D-30
Module.....	D-30
Testing.....	11-1
Tests	
Idle Phone Line.....	11-6
Loop Back	11-5
Responder.....	11-4
Self Tests.....	11-6
Starting Loop Back/Self Test/Idle Phone Line ..	11-6
Tone	11-1–11-3
Time	
Slot	
Status	12-2
Slot Assignment.....	12-1
Timeout	
Response	C-13
Tips	3-9
Token Ring	
NET.CFG	3-16
Network Drivers	3-16, 3-17
Tone	
Test	
Rules	11-1
Tests.....	11-1, 11-4
Receiving.....	11-3
Sending	11-2
Toolbar Options	A-1
Total Control	
Accounting Application Main Menu.....	14-22
Security	C-1
<i>Total Control Manager</i>	
Commands Window.....	9-1
Defined.....	1-1
Icons on a Locational Map.....	10-3
Requirements.....	2-1
<i>Total Control Manager/SNMP</i>	1-1
Framework	1-1
Installation.....	3-1, 3-4
Testing Connectivity	3-18
Trap	
Defined.....	8-1
Desination	8-3

Destination Table	8-3
Enabling.....	8-2
Lost Server.....	14-6
Select	8-3
Troubleshooting.....	3-9
Hub Security	C-37

—U—

U.S. Robotics Customer Support.....	4-10
UDP	
IP Protocol.....	14-7
Port Number.....	14-4
Security Server Port.....	C-15
Undo All Responses	D-6
Uninstalling NMS and TCM.....	3-11
Unloading Drivers	3-18
User	
Assignment	C-26
Blacklist Login Trap.....	C-17
Blacklist Trap.....	C-17
Configuration Window	C-35
Group.....	C-27
Configuration	C-28
Configuration Window	C-28
NETServer Configuration.....	C-32
Statistics	C-27
Window	C-26
Current Group Statistics.....	C-28
User	
Group	C-27
Group Statistics	C-27
Membership.....	C-27
List	
Planning	C-19
List Window.....	C-34
Current Statistics.....	C-35
Membership.....	C-27
Name	C-33
Name Prompt	C-10
Password Prompt.....	C-10
Window	C-33
User	
Name	C-33
User Blacklisted	D-24
Using the MIB Browser	10-7

—V—

Verifying Object Status.....	7-1
View by Column	
Button	6-4
View by Row	
Button	6-4
View Menu	
Commands	A-2
Viewing Statistics.....	7-1

Virtual Front Panel Display (VFPD)
Selecting from.....4-8-4-9
Viewing.....4-6

—W—

Wildcards C-37

Window Menu
Commands A-5

—X—

X25DIALR.EXE..... 4-4, 4-5