ChannelWorks

digital™

Management

Part Number: EK-DECTV-MG. B01

ChannelWorks

Management

February 1994

This manual, in conjunction with the *ChannelWorks Network Installer's Guide* and the *ChannelWorks Cable TV Installer's Guide*, describes how to install the ChannelWorks bridge. This manual is intended for the network manager.

Supersession/Update Information: This is a revised manual.

digital™

Part Number EK-DECTV-MG B01

EK-DECTV-MG. B01
February 1994

The information in this document is subject to change without notice and should not be construed as a commitment by Digital Equipment Corporation. Digital Equipment Corporation assumes no responsibility for any errors that may appear in this document.

Contents

Contents

Contents

Figures

Tables

Preface

About This Book

The *ChannelWorks Management* manual guides you through:

- Understanding The ChannelWorks Bridge enterprise specific Management Information Base (MIB)
- Using the LANcity® Management Utility via the console port
- Using an SNMP manager to manage the ChannelWorks Bridge
- Configuring the ChannelWorks Bridge using the PC based utility and the bridge's enterprise specific SNMP MIB variables
- Troubleshooting a ChannelWorks Bridge based Metropolitan Area Network

The *ChannelWorks Management* manual also provides brief descriptions of the bridge's Spanning Tree Protocol, product features, SNMP manageability, the standard Management Information Base - MIB-II, and the Bridge MIB.

Who Should Use This Manual

The *ChannelWorks Management* manual is for network managers, certified cable TV technicians and installation technicians certified to perform troubleshooting of a ChannelWorks Bridge-based metropolitan area network.

Document Organization

The *ChannelWorks Management* manual contains the following sections:

- Chapter 1, "General Description," describes the ChannelWorks Bridge with brief descriptions of its Spanning Tree Protocol, performance, SNMP manageability. Chapter 1 also includes a brief description of the standard MIB - MIB-II and the Bridge MIB.

- Chapter 2, "The ChannelWorks Bridge Enterprise Specific MIB," describes how to access the ChannelWorks Bridge enterprise specific MIB variable text file to get additional descriptions of the MIB variables.

- Chapter 3, "Using The Management Utility," explains how to use the utility through the bridge's serial port for configuring operational parameters, adding and removing users, and providing user levels and passwords.

- Chapter 4, "Interpreting The ChannelWorks Bridge Statistics," provides information on interpreting the bridge's operational statistics.

- Chapter 5, "Configuring The ChannelWorks Bridge," describes how to set the bridge's remaining operating parameters, not covered in Chapter 3, using the management utility and the bridge's SNMP enterprise specific MIB variables. Also included are directions to set up the bridge for Serial Line Interface Protocol (SLIP) operation for serial port access to network management.

- Chapter 6, "Troubleshooting a ChannelWorks Bridge Based MAN," describes how to use the bridge's enterprise specific MIB variables to diagnose and resolve network problems.

- Appendix A, "Error and System Messages," describes how to access and interpret the SNMP enterprise specific MIB Support History file.

Conventions Used In This Guide

Convention	Meaning
Italic Font	Italic Font is used for titles of books or to give special emphasis. For example: For more information refer to the *ChannelWorks Network Installer's Guide*.
`Special Type`	Special Type (Courier Font) indicates messages or prompts from the system that appear on your screen. For example: `Configuration successfully installed.`
`Special Bold Type`	Special Bold Type (Courier Bold Font) is used within text instructions and in screen examples to show characters or words that you type. for example: `At the prompt, type` **`AA000400AB04.`** `prompt>` **`passwd`**
A Capitalized Word	A Capitalized Word within text indicates a key that you press. For example: Press Return. When you see two key names, press and hold the first key, and then type the second character. For example: To press Control-C, press and hold the Control key, and then type an uppercase **C**.

Associated Documents

Refer to the following documents for further information:

- *ChannelWorks Network Installer's Guide* - Describes connecting ChannelWorks to cable TV network and Ethernet/802.3 network cables and using the PC based Subscriber Utility to verify the ChannelWorks Bridge operating parameters.

- *ChannelWorks Cable TV Installer's Guide* - Describes setting up the cable TV headend trranslator, preparing the cable TV network for data communications, configuring and installing the ChannelWorks Bridge, and TransMaster frequency switch settings.

Known Problems

The following items are under investigation:

1. The ChannelWorks Bridge operation has been verified at frequencies corresponding to standard NCTA channel assignments. For optimal receiver operation avoid using the following forward (RX) frequencies:
   - 79.000 MHz
   - 85.000
   - 93.000
   - 105.000
   - 141.000
   - 429.000
   - 465.000 MHz

2. The management utility prevents the user from entering illegal and non-optimized Max Round Trip Delay values. However, the ChannelWorks Bridge software does not prevent the user from entering less than optimal Max Round Trip Delay value when performing SNMP "sets" on the enterprise specific MIB variable lcmaxrndtripdel in the ASIC Parameters group.

3. The Support History Log does not consider an error code at two different error levels as unique, which could be misleading as in the following example:

   If error 0x35 is logged as a level 2 and at a later time error id 0x35 is logged at a level 4, when displaying the Support History Log the second error as shows as a level 2 crash.

4. The Subscriber Utility and the Management Utility do not operate properly on a 66 MHz PC.

5. The PROM Monitor's printcfg command displays an incorrect software version value under the "Vers" heading. The "Description" heading displays the correct software version. You can also use the SNMP enterprise specific MIB variable lcsoftware in the Revision Levels group to view the correct software version.

6. Counters from the interface group of the MIB-II are not implemented correctly for the serial port.

7. The IPNetToMediaTable and the atTable of MIB-II cannot be modified via SNMP. The enterprise specific MIB variables lcmcastrx and lcbcastrx from the Sonic Stats group are not implemented.

1

General Description

Introduction

This manual explains how to manage a ChannelWorks Bridge, a 10-Mb/s, Ethernet to cable TV, transparent, spanning tree bridge. This chapter covers the following topics:

- ChannelWorks Bridge general description
- Spanning Tree Protocol overview
- Simple Network Management Protocol (SNMP) overview
- Management Information Base (MIB) descriptions

General Description

The ChannelWorks Bridge interconnects IEEE 802.3/Ethernet networks over a standard cable TV network. Each ChannelWorks Bridge on the backbone can access the network independently via its unique access method, UniLINK.

UniLINK provides the benefits of both contention based (CSMA/CD) and reservation-based access methods.

On a general cable operator's cable TV network, the ChannelWorks Bridge can provide a 10-Mb/s Ethernet data service in any two of 83 available standard 6 MHz channels (10 MHz to 550 MHz), at distances up to 70 miles. If required, the installer or network manager can change the initial channel allocation at any time.

Typical operation is as follows:

- A user sends out a data packet to a remote address.
- A locally attached ChannelWorks Bridge forwards the packet onto the cable TV network.
- A ChannelWorks Bridge at the remote site, forwards it onto the attached Ethernet segment and onto its final destination.

The bridge is capable of connecting to any standard 802.3 or Ethernet network that complies with the IEEE 802.3 10Base5 (thickwire), 10Base2 (ThinWire) or 10BaseT standards. The bridge is capable of connecting to any 802.7 compliant cable TV system, using a pair of standard 6 MHz channels and two "F" connectors.

The bridge can be installed in a desktop, rackmount or wallmount configuration. The heart of the bridge consists of two printed circuit boards: a CPU module and an RF modem module. The CPU module includes an R3000-based RISC processor and an application specific integrated circuit (ASIC) that implements the UniLINK protocol. In addition, the CPU module contains the Ethernet and console interfaces, as well as dynamic and non volatile memory. The RF modem board contains analog RF circuitry which modulates and demodulates the cable TV signal using QPSK modulation.

In addition to the two modules, the bridge contains a power supply and fan. The power supply provides the approximately 40 watts of power shared almost equally by the CPU and RF modules, and has three outputs: +5, +12 and -12 VDC. The bridge comes with seven LEDs to indicate its status.

The ChannelWorks Bridge comes with software programmed into Flash ROM. The software can be upgraded using the TFTP protocol. The bridge also comes with system and exerciser diagnostics. The bridge is manageable via SNMP, and uses standard MIBs as well as enterprise specific MIBs. The bridge can be managed in-band, over the network, or from a local RS-232 console port. Built in security features prevent tampering with the cable TV receive and transmit frequencies.

The ChannelWorks Bridge features include the following:

- The bridge can be used on any cable TV network that is up to 70 miles round-trip.
- The bridge is frequency agile. The transmitter operates in any one of 28 standard NCTA channels, and can be tuned to any frequency between 10 and 174 MHz in 250-KHz increments. The receiver operates in any one of 83 standard NCTA channels, and is capable of being tuned to any frequency between 54 and 550 MHz in 250-KHz increments.

- The ChannelWorks Bridge is flexible. The bridge can support single-rail or dual-rail plants, and sub-split, mid-split or high-split systems.

Spanning Tree Protocol Overview

The ChannelWorks Bridge implements the Spanning Tree Protocol according to the IEEE 802.1(d) standard.

A spanning tree is the logical configuration in which an extended local area network (LAN) or metropolitan area network (MAN) establishes itself just after a bridge is powered on. In a spanning tree

- There are no loops.
- There is only one path between any two bridges.
- All LANs/MANs are connected.

The spanning tree configuration process begins when the bridges are powered on or reset through an SNMP manager. Each bridge assumes it is the root of the spanning tree and declares itself so by sending out Hello messages, which are multicast to all other bridges connected to the same MAN.

When it receives a Hello message, a bridge compares the root information and designated bridge information in the message to its own. When the bridge hears a Hello message with a lower bridge ID value than its own, it ceases to declare itself as the root. The process eventually leads to the election of a single root bridge for the extended LAN or MAN and a single designated bridge for each individual LAN/MAN.

In the Hello message, the root and designated bridge information fields are simply the Media Access Control (MAC) address of the root and designated bridge with a root priority prefix. This prefix can be set using the Management Utility.

Use of the Spanning Tree Protocol allows bridges to provide redundant paths between critical LAN segments. The protocol ensures that only one path is operational at any given time.

Simple Network Management Protocol Overview

The Simple Network Management Protocol is a member of the TCP/IP protocol suite. The ChannelWorks Bridge SNMP uses the User Datagram Protocol (UDP) to exchange messages between a station manager, such as SNMPc™ or Digital's POLYCENTER SNMP Manager, and its SNMP Agent.

SNMP encompasses three main areas:

- A small set of management operations
- Definitions of manageable variables
- Data representations

The operations allowed are: Get, GetNext, and Set. These functions operate on variables that exist in the ChannelWorks Bridge. Examples of variables include static counters (Achieved Pacer Counter - lcachievedpacer), and the ChannelWorks Bridge port status (IfEntry - OperStatus).

All of the SNMP management functions are carried out through these simple operations. No action operations are available, but these can be simulated by the setting of flag variables. For example, to reset the ChannelWorks Bridge, an integer variable named "lcresetnow" is set to a specific value to reset the ChannelWorks Bridge.

SNMP variables are defined using the Abstract Syntax Notation One (ASN.1). ASN.1 specifies how a variable is encoded in a transmitted data frame; it is very powerful because the encoded data is self-defining. For example, the encoding of a text string includes an indication that the data unit is a string, along with its length and value. ASN.1 is a flexible way of defining protocols, especially for network management protocols where nodes may support different sets of manageable variables.

Management Information Base (MIB) Descriptions

The set of SNMP variables that the ChannelWorks Bridge supports is called the Management Information Base (MIB). The MIB is made up of several parts. The ChannelWorks Bridge provides support for the following data via SNMP:

- MIB-II as defined in RFC 1213
- Bridge MIB as defined in RFC 1286
- Enterprise Specific MIB, as defined in Chapter 2, "The ChannelWorks Bridge Enterprise Specific MIB"

2

The ChannelWorks Bridge Enterprise-Specific MIB

Introduction

This chapter provides information on how to access and review the ChannelWorks Bridge enterprise-specific SNMP Management Information Base (MIB).

The ChannelWorks Bridge Enterprise Specific MIB is a source file that complies with RFC 1212, Concise MIB Definitions. The ChannelWorks Bridge MIB can be compiled by an SNMP manager such as SNMPc™ or Digital's POLYCENTER SNMP Manager.

The ChannelWorks Bridge MIB source file is an ASCII text file that can be read by any popular word processor or editor. The ChannelWorks Bridge MIB is supplied with the Management Utility. Refer to Chapter 3, "General Description" for description of the utility.

Note: Do not modify the ChannelWorks Bridge MIB file, because it may not compile or recompile after modification.

Reading The ChannelWorks Bridge MIB File

To get a description of a ChannelWorks Bridge MIB variable, open the bridge MIB file using any word processor.

An example of a specific MIB variable follows:

```
lcstatstime OBJECT-TYPE
   SYNTAX   INTEGER
   ACCESS   read-write
   STATUS   mandatory
   DESCRIPTION
   "The number of seconds that defines the interval for
    the statistics collector."
     ::= { lctimertask 1 }
```

Use the description for information to describe the specific MIB variable.

3

Using The Management Utility

Introduction

This chapter covers the following topics:

- Setting up a PC to verify and modify the ChannelWorks Bridge operating parameters via its RS-232 serial port
- Using the Management Utility to configure the ChannelWorks Bridge security features, including user levels, user names and passwords
- Applying the functions of the utility and the management tools

To perform the functions described in this section, you need:

- A PC with a 3.5-in high-density diskette drive, mouse and RS-232 serial port
- Microsoft Windows® Version 3.1
- A nine-pin null modem cable
- The Management Utility and the Management Tools diskettes
- Windows Terminal terminal emulator
- A PC Simple Network Management Protocol (SNMP) network management tool such as SNMPc™
- The TCP/IP protocol suite from a major Windows vendor, such as NetManage™

Note: The SNMP manager and TCP/IP suite must be interoperable.

General Description

The Management Utility is a PC-based installation/configuration program consisting of multiple levels of menu structures with password entry protection. The utility provides a user-friendly Windows interface that leads the user through the installation/configuration process.

The functionality the utility provides depends on the entered level of the user accessing the utility. Refer to the "Management Utility Security Features" section for more information.

The utility is bundled with the Management Tools and the ChannelWorks Bridge Operating Software on three separate 3.5-in diskettes under the title of Cable TV Management Tools (LCC).

The Management Tools diskette contains:

- The bridge's SNMP enterprise specific MIB variables
- An SNMP security application
- The PC user interface for SNMPc's management system

Refer to Chapter 5, "Configuring The ChannelWorks Bridge," for more information on the Management Tools.

Setting Up User Accounts

You use the utility to perform verification and modification of ChannelWorks Bridge operating parameters. To access the utility, you must have a user name, password and level stored in the utility's database.

Perform the following procedure to add a user. This procedure assumes that you have installed the utility on your PC's hard drive and you have opened the utility's Bridge Manager program group window. If you have not installed the utility on your PC's hard drive, refer to the "Installing The Management Utility On A PC" section.

1. Click on the utility's icon. The utility displays the login window.
2. Type the initial Admin user name printed on the utility's floppy and press Tab.
3. Type the initial Admin user password printed on the utility floppy and click on OK.

Note: The initial Admin user name and password provides only Admin Level access. Other utility functions can not be implemented using the initial Admin user name and password. To insure security, use the initial Admin user name and password to create a unique user name and password for yourself. Use the utility's Delete User function to remove the initial Admin user name and password.

4. Click on Admin. The utility displays the utility Add User/Delete User pull down menu as shown in Figure 3-1.

5. Click on Add User from the Admin Pull Down menu.

   The Utility displays the Add User entry window with a default User Name, User Password and User Level entered as shown in Figure 3-2.

6. Use the mouse or keyboard to highlight the User Name. Delete it using the DEL key or type in a new user name right over the highlighted user name.

7. Use the mouse or keyboard to highlight the User Password. Delete it using the DEL key or type in a new user password right over the highlighted one.

8. Click on the desired User Level, and click OK. The Utility displays the Add User to Database window.

Note: Refer to the "User Levels" section for a description of the Utility's access levels.

9. Click on Yes.

   If there is a duplicate user name in the Utility's database, the Utility displays the User Status window indicating that there is a duplicate name and requests that you choose another name. Otherwise, the User Status window indicates that the new user was added successfully.

10. In either case, click on OK. The Utility returns you to the Main Menu.

User Levels

There are four levels of access for the management utility. The following is a description of the utility's access levels and range of access a user has to the bridge's operating parameters. utility's levels one and two have the same access capability as the Subscriber Utility. Refer to the "User Levels" section of the *ChannelWorks Network Installer's Guide* for a detailed description of User Levels One and Two. Summary descriptions of the Mangement Utility's levels are listed below.

Level One

This level allows the user to:

- Read the bridge's NVRAM
- View the current operating parameters of the bridge
- Start the terminal emulator
- Choose and initialize the PC's serial port

Figure 3-1 Admin Pull Down Menu

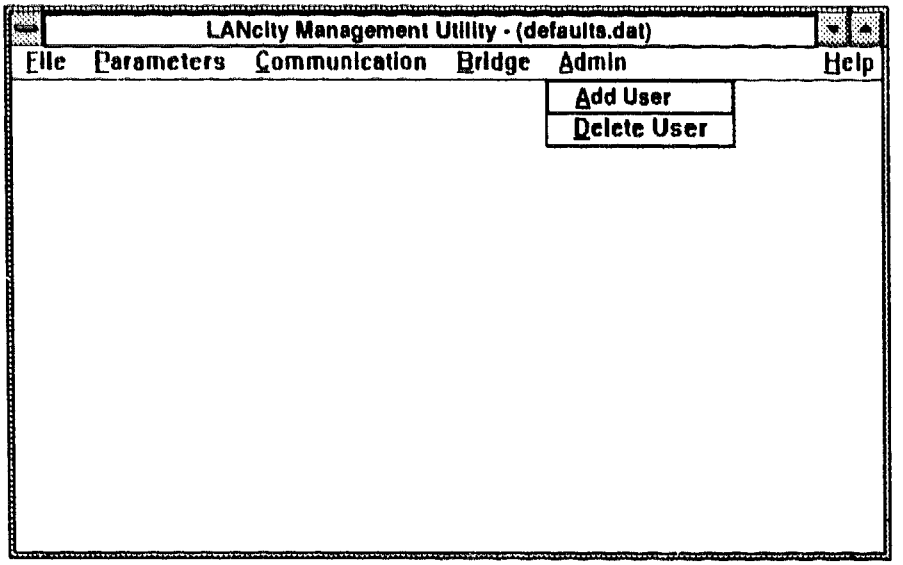
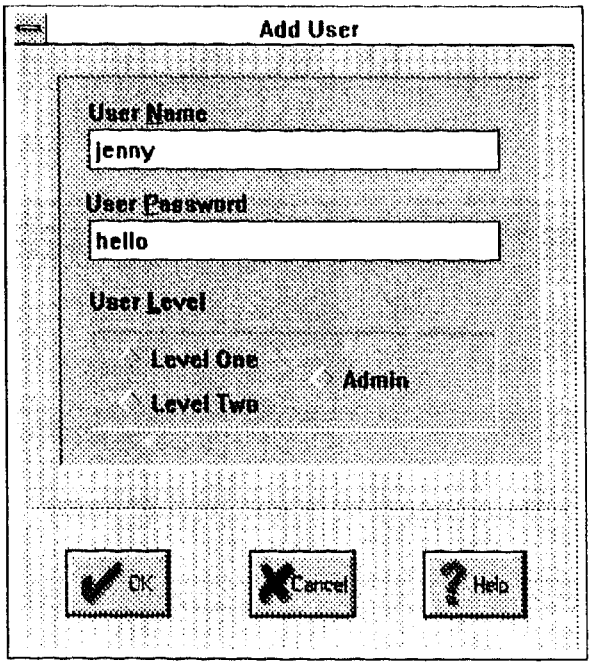


Figure 3-2 Add User Entry Window



Level Two

This level allows the user to perform all of Level One's functions and:

- Modify the following parameters from the Parame· ·rs pull down menu:
  - Bridge Control Group
  - Download Group
  - Dump Server Group
  - Filter Control Group
  - Network Management Control Group
  - System Group
  - Unique IP Addresses Group
- Load the above listed parameters from the individual group windows or from the Bridge Load Parameters window
- Open and save parameter files

Level Three

This level allows the user to perform all of Level One's and Two's functions and:

- Modify all of the bridge's operating parameters from the Parameters pull down menu
- Load all of the bridge's operating parameters from the individual group windows or from the Bridge Load Parameters window

Level Four

This level allows the user to add and delete users for levels of access described above.

Setting Up A PC To Verify And Modify The Bridge Via The Serial Port

The following sections describe how to:

- Install the Management Utility on a PC to access the bridge's NVRAM and verify or modify the bridge's operating parameters
- Connect a PC to the ChannelWorks Bridge's serial port and display the bridge's power on diagnostics using a terminal emulator

Installing The Management Utility On A PC

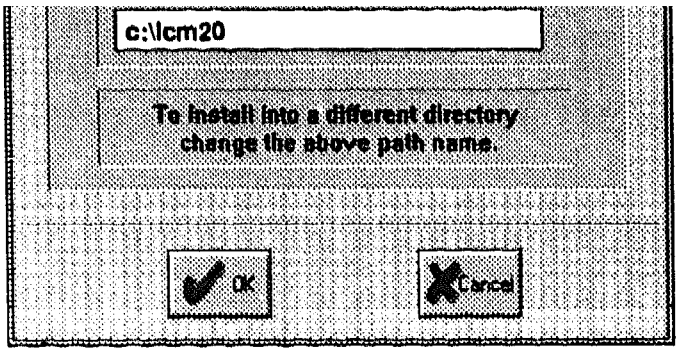
Perform the following procedure to install the Management Utility on your PC's hard drive:

1. Insert the utility's diskette in the PC's 3.5-in drive.
2. From the Window's Program Manager choose FILE, RUN.
3. At the command line type in the letter of your PC's 3.5-in drive followed by

   ```
   :\setuplcm.exe
   ```

   The PC displays the LC Install Utility dialog box, as shown in Figure 3-3.
4. To install the utility in a directory other than the one in the utility's dialog box, change the default path and choose OK. The utility creates the directory chosen, copies the program files to the directory, and displays the LC Install Utility program group creation dialog box.
5. Click on OK. LC Install Utility creates the utility Bridge Manager program group window. The utility places the following icons in the utility's Bridge Manager window:
   - The utility's executable
   - A Readme file
   - The utility's Release Notes.

You are now ready to run the utility from Windows.


c:\lcm20
To install into a different directory
change the above path name.
OK
Cancel

Connecting A PC To The ChannelWorks Bridge Serial Port

Perform the following procedure to connect a PC to the ChannelWorks Bridge serial port: This procedure assumes that you have installed the utility on your PC. If you have not installed the utility on your PC, refer to the "Installing The Management Utility On A PC" section.

1. Plug the unit into its power outlet.

Note: Do not connect the network cables at this time and do not turn the ChannelWorks Bridge on yet.

2. Plug in the PC and attach the nine-pin null modem cable between the PC and the ChannelWorks Bridge.

3. Power up the PC; start Windows.

4. Click on the utility's icon. The utility displays the login window.

5. Type your user name and password and click OK. The utility displays the terminal emulator launch window.

Note: Refer to the "Setting Up A User Account" in the *ChannelWorks Cable TV Installer's Guide* for the procedure to add a user with a valid password.

6. Click on YES. The utility displays Microsoft Windows' Terminal program.

Note: Microsoft Windows Terminal must be installed in your windows directory for this feature to work. Otherwise, you must start a terminal emulation program at this step.

7. Set the terminal emulator's communications parameters to:

   - Connector: PC port from step 2 (COM1, COM2, etc.)
   - Baud Rate: 9600
   - Data Bit : 8
   - Stop Bits: 1
   - Parity: None

Note: Refer to the "Selecting The Communications Port" section of the *ChannelWorks Network Installer's Guide* for directions to select your PC's COM port from the utility.

8. Power up ChannelWorks.

Note: When you turn the unit on, you should observe a delay of approximately 3 seconds in the power light coming on. If not, refer to Chapter 5. Figure 3-4 is an example of a terminal emulator as it displays the ChannelWorks Bridge power-on diagnostics.

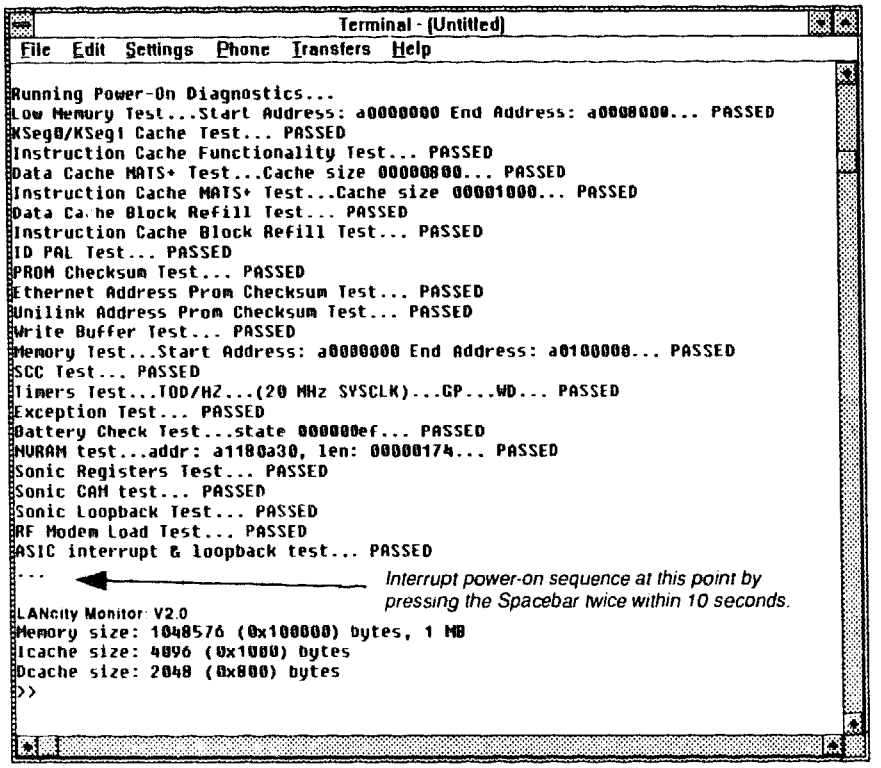
9. Verify that the ChannelWorks Bridge passes its "ASIC Interrupt and Loopback Test." This is the last test of the ChannelWorks Bridge power-on diagnostics.

10. Press the Spacebar twice, within 10 seconds after the ChannelWorks Bridge power-on diagnostics passes the ASIC Interrupt and Loopback Test and displays three periods in the left margin.

    This action prevents the ChannelWorks Bridge from performing its application boot at the end of its power up process. Approximately 30 seconds after you press the Spacebar, the ChannelWorks Bridge lists its memory sizes and displays its PROM monitor prompt of two greater than signs (>>). This allows access to the Channelworks Bridge NVRAM.

11. Close the terminal emulator application. This releases the PC's serial port for use by other programs such as the utility. Use the utility to perform the remaining procedures in this chapter.

Figure 3-4 ChannelWorks Bridge Power On Diagnostics



Management Utility Security Features

Before you start the application you must know about the bridge's security features. Refer to the *ChannelWorks Cable TV Installer's Guide* for more information on user levels, user names and passwords.

Note: The network manager is responsible for unauthorized access to the bridge's operating parameters.

Using The Management Utility

Main Menu Overview

Use the Main Menu to perform the following functions:

- Selecting the PC's serial communications port
- Opening and saving configuration data files
- Reading NVRAM to verify current parameters
- Selecting parameter groups to verify or modify
- Setting the SNMP frequency access password
- Clearing the History Log
- Loading the bridge with saved parameters
- Adding and deleting users and setting their user levels

The Main Menu's active title bar displays either:

- The IP Address of the unit that has just had its NVRAM's current parameters read
- The file name that has just been opened
- The default file name

Default Configuration File

The Main Menu's active title bar initially includes the default configuration file name "defaults.dat." This file is loaded every time you log on with a valid user name and password. All parameters are initialized with a default setting, except the Unique IP Addresses.

The Unique IP Addresses Group parameters come up blank upon initial login. You initialize the group's parameters by reading the bridge's NVRAM in order to perform parameter verification; the Unique IP Addresses Group can never be saved to a file to prevent you from accidentally duplicating the same IP Address in another unit.

Opening And Saving Configuration Data Files

The utility includes one configuration data file, defaults.dat. This file loads automatically upon login. You cannot overwrite the contents of this file by clicking on Save in the File pull down menu, but you can make changes and save the changed file using the "Save as..." function in the File pull down menu.

Opening A Saved Configuration Data File

To open a saved configuration data file perform the following procedure.

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. From the Main Menu, click on File.
2. Click on Open. The utility displays the File Open window.
3. Click on a directory or drive where your configuration data files are located. The utility displays a list of configuration data files.
4. Double click on the filename that you want to open. The utility displays the Open File window.
5. Click on OK. The utility initializes the group dialogues with the data from the saved file and returns to the Main Menu.

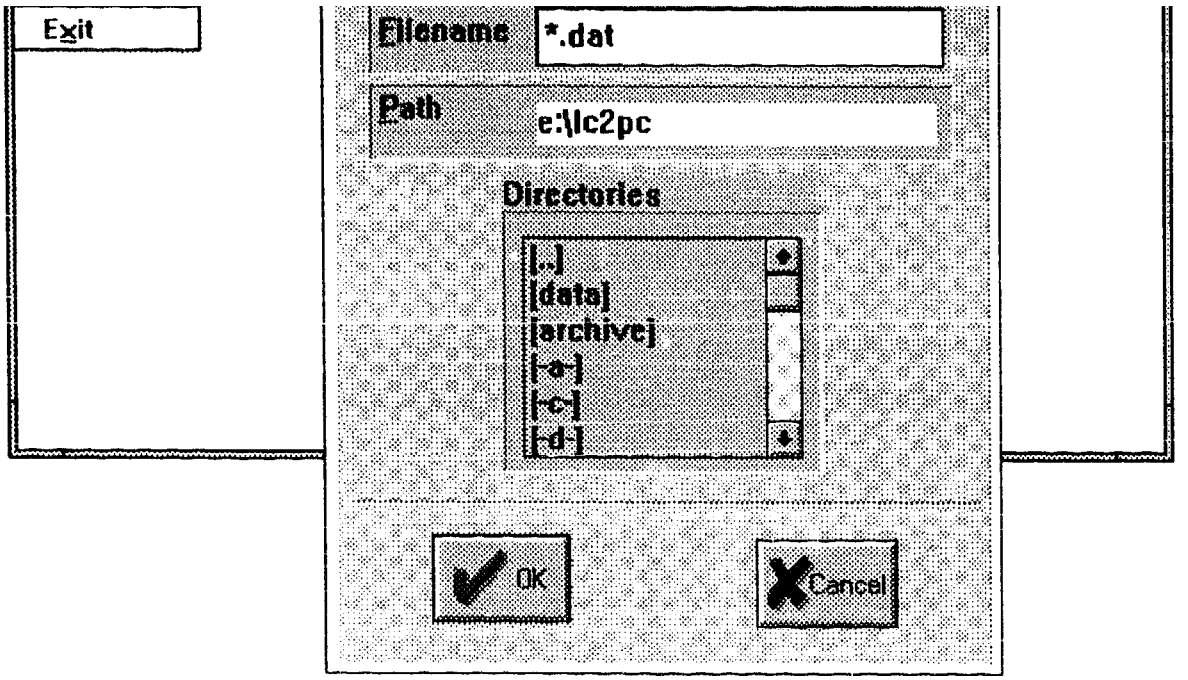
Saving A Configuration Data File To Access Again

To save a configuration data file that you may want to access again perform the following procedure.

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port." This procedure also assumes that you have modified bridge operating parameters that you want to save.

1. From the Main Menu, click on File.
2. Click on Save As. The utility displays the File Save As window as shown in Figure 3-5.
3. Use the mouse to select a directory or drive in which you want to save the file.
4. Double click the mouse on the current filename. The utility highlights the filename.
5. Type a new filename over the highlighted filename and click on OK. The utility saves the file as the new filename and closes the File Save As window.

Note: IP Addresses are not saved.


Exit
Filename
*.dat
Path
e:\lc2pc
Directories
[..]
[data]
[archivc]
[-a-]
[-c-]
[-d-]
OK
Cancel

Reading The ChannelWorks Bridge NVRAM

The utility allows you to read the contents of the bridge's NVRAM. The bridge stores its operating parameters in NVRAM. This process enables you to determine the status of each of the bridge's parameters.

Perform the following procedure to select parameters to verify.

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

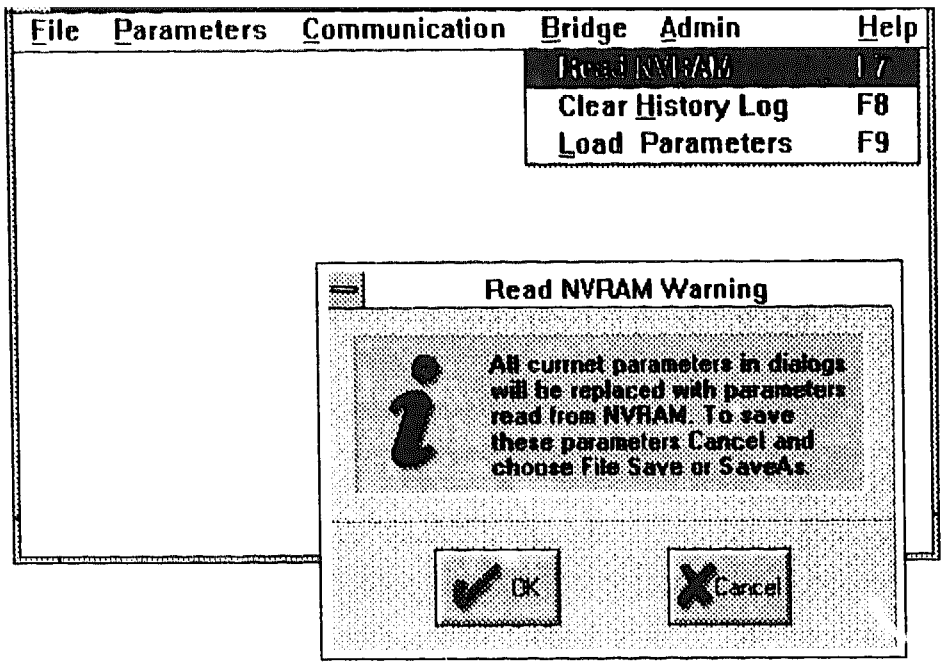
1. Select Bridge from the Main Menu and click on Read NVRAM. The PC displays the Read NVRAM Warning window as shown in Figure 3-6.

2. Click on OK.

   Reading NVRAM parameters takes about 4 minutes. While the utility reads the bridge's NVRAM, it displays the parameter groups being read in the utility's menu active title bar. After the utility reads the unit's NVRAM, the Main Menu's active title bar displays the IP Address of the unit and the title NVRAM Parameters. The utility also displays the Read NVRAM Initialized Group Dialogs window.

3. Click on OK.

You can save this information in a file using the File Save As function. Refer to the section on "Opening And Saving Configuration Data Files" and "Saving A Configuration Data File To Access Again" for more information.


File Parameters Communication Bridge Admin Help
Read NVRAM F7
Clear History Log F8
Load Parameters F9
Read NVRAM Warning
All current parameters in dialogs will be replaced with parameters read from NVRAM. To save these parameters Cancel and choose File Save or SaveAs.
OK
Cancel

Verifying A Selected Parameter Group

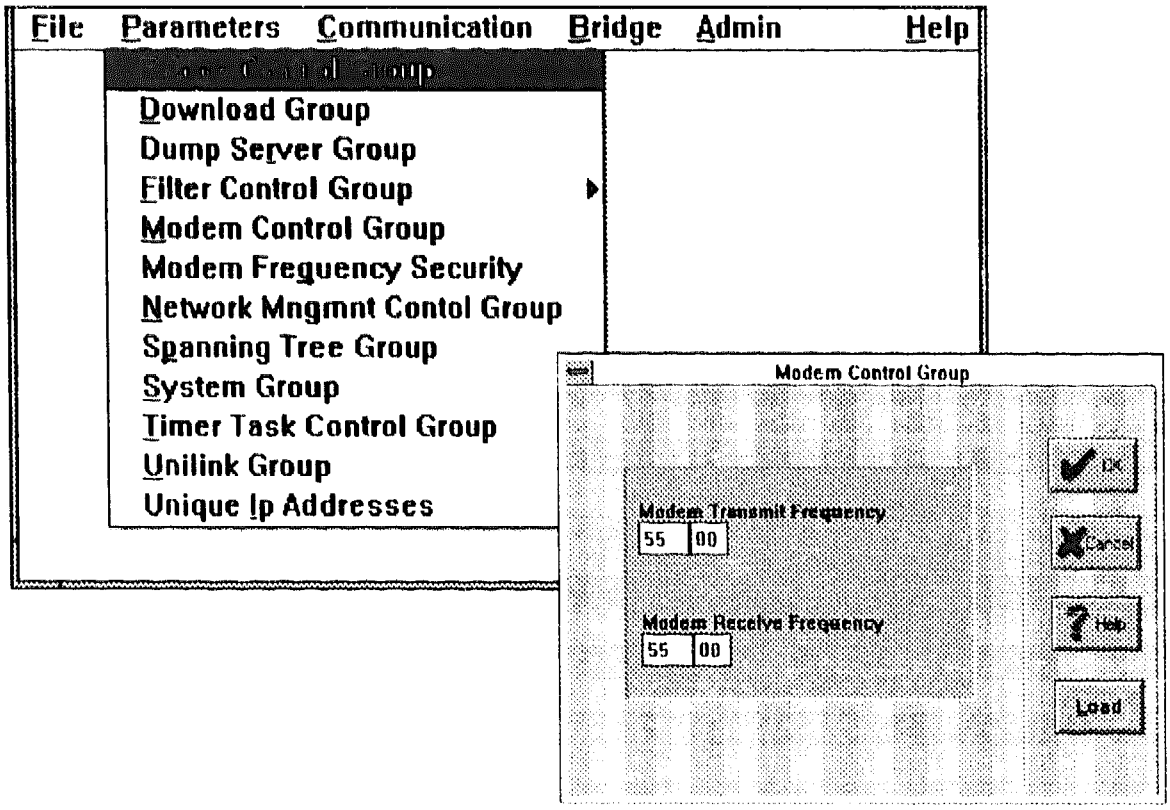
Perform the following procedure to verify a parameter group.

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Read the bridge's NVRAM. Use the procedure from the section "Reading The ChannelWorks Bridge NVRAM."
2. Confirm the unit's IP Address is in the Main Menu's active title bar.
3. Click on Parameters from the utility's Main Menu.
4. To see how this procedure works, click on the Modem Control Group selection. The utility displays the Modem Control Group parameters window as shown in Figure 3-7.

Note: The parameters that are not accessible are grayed out. Even when some parameters are accessible via the Pull Down list the parameter itself may be grayed out, depending on the user level. This is done to avoid unauthorized modification of the bridge's parameters. Refer to the section "Management Security Features" for more information.

5. Click on Cancel to close the window and return to the Main Menu.


File
Parameters
Communication
Bridge
Admin
Help
Download Group
Dump Server Group
Filter Control Group
Modem Control Group
Modem Frequency Security
Network Mngmnt Contol Group
Spanning Tree Group
System Group
Timer Task Control Group
Unilink Group
Unique Ip Addresses
Modem Control Group
Modem Transmit Frequency
55
00
Modem Receive Frequency
55
00
OK
Cancel
Help
Load

Modifying A Parameter Using The Default Configuration Data File

Perform the following procedure to modify a parameter using the default configuration data file:

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Confirm the utility's default configuration data filename "defaults.dat" is in the Main Menu's active title bar.
2. Click on Parameters from the utility's Main Menu.
3. Click on the Control Group you wish to modify. The utility displays the selected Control Group's parameters.
4. Using the mouse or keyboard, click on or highlight the parameter information you wish to change and type the new parameter in the highlighted field.
5. Verify that the information entered is correct, then click on OK to save the information for loading at a later time. Or, click on Load to load the parameter in the unit's NVRAM now. In either case, the utility displays the Save parameter or Load parameter confirmation window.
6. Click on YES if you wish to save or load the parameter. The utility performs the function and returns you to the Main Menu.

Modifying A Parameter Using A Saved Configuration Data File

Perform the following procedure to modify a parameter using a saved configuration data file:

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Open a saved configuration data file. Use the procedure from the section "Opening A Saved Configuration Data File."
2. Confirm the desired configuration data filename is in the Main Menu's active title bar.
3. Click on Parameters from the utility's Main Menu.
4. Click on the Control Group you wish to modify. The utility displays the selected Control Group's parameters.
5. Using the mouse or keyboard, click on or highlight the parameter information you wish to change and type the new parameter in the highlighted field.
6. Verify that the information entered is correct, then click on OK to save the information for loading at a later time. Or, click on Load to load the parameter in the unit's NVRAM now. In either case, the utility displays the Save parameter or Load parameter confirmation window.
7. Click on YES if you wish to save or load the parameter. The utility performs the function and returns you to the Main Menu.

SNMP Frequency Access Security MIB

The ChannelWorks Bridge allows authorized users to modify the cable TV's transmit and receive frequencies remotely using an SNMP manager. An SNMP set of the special frequency access password string is required to perform SNMP sets of both cable TV transmit and receive frequencies to new values. Refer to Chapter 5, "Configuring The ChannelWorks Bridge," for detailed instructions on how to use this feature.

Use the utility to set the SNMP frequency access password during the configuration of the bridge's parameters by the utility's Modem Frequency Security Group. Refer to the next section, "Setting the SNMP Frequency Access Password," for detailed instructions on how to set the SNMP frequency access password.

Setting The SNMP Frequency Access Password

The SNMP frequency access password is set during the configuration of the bridge's parameters through the utility's Modem Frequency Security Group.

Perform the following procedure to enable changing the cable TV transmit and receive frequencies of an operational unit using an SNMP manager.

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

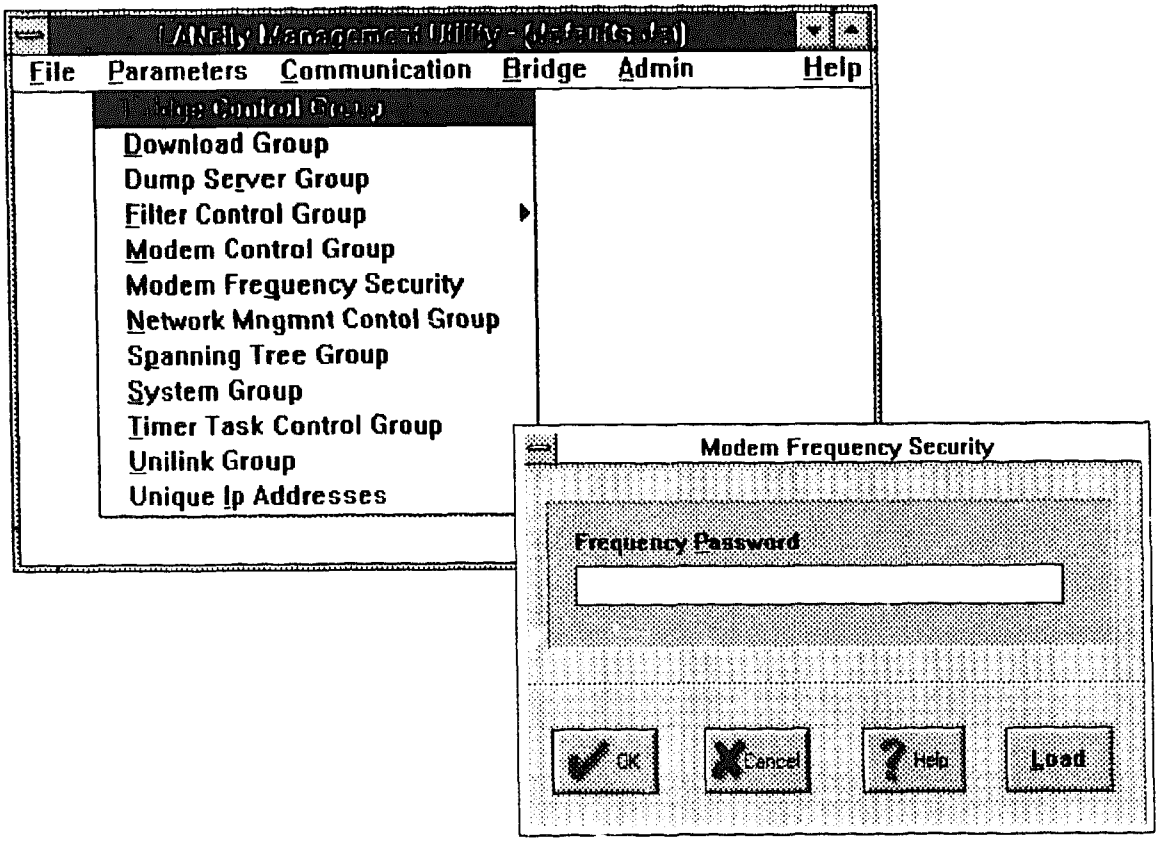
1. From the utility's Main Menu, click on Parameters.
2. Click on Modem Frequency Security from the Parameters Pull Down menu. The utility displays the Modem Frequency Security window, as shown in Figure 3-8.
3. Type in a password string, from 1 to 32 characters, and click on either OK to save the parameter for loading at a later time or Load to load the password string in the unit's NVRAM now.

   This is the string that must be matched by any user wishing to use an SNMP manager to modify modem frequencies in an operational unit.

   Refer to Chapter 5, "Configuring The ChannelWorks Bridge," for procedures to change the cable TV transmit and receive frequencies using the frequency access password and the Modem Control Group/Modem Security MIBs.

Note: The password can only be set or changed using the utility. If the password is lost or forgotten, you cannot change frequencies until the utility is rerun and a new password is entered.

Figure 3-8 Setting The SNMP Frequency Access Password



Loading The ChannelWorks Bridge With Specific Saved Parameters

As discussed in the sections "Opening and Saving Configuration Data Files," "Reading The ChannelWorks Bridge NVRAM," and "Modifying A Selected Group's Parameter," the parameters that have been saved can be loaded at a more convenient time. The Utility allows you to load a select number of parameters or all parameters at once.

The following procedure describes how to load the bridge's NVRAM with specific saved parameters.

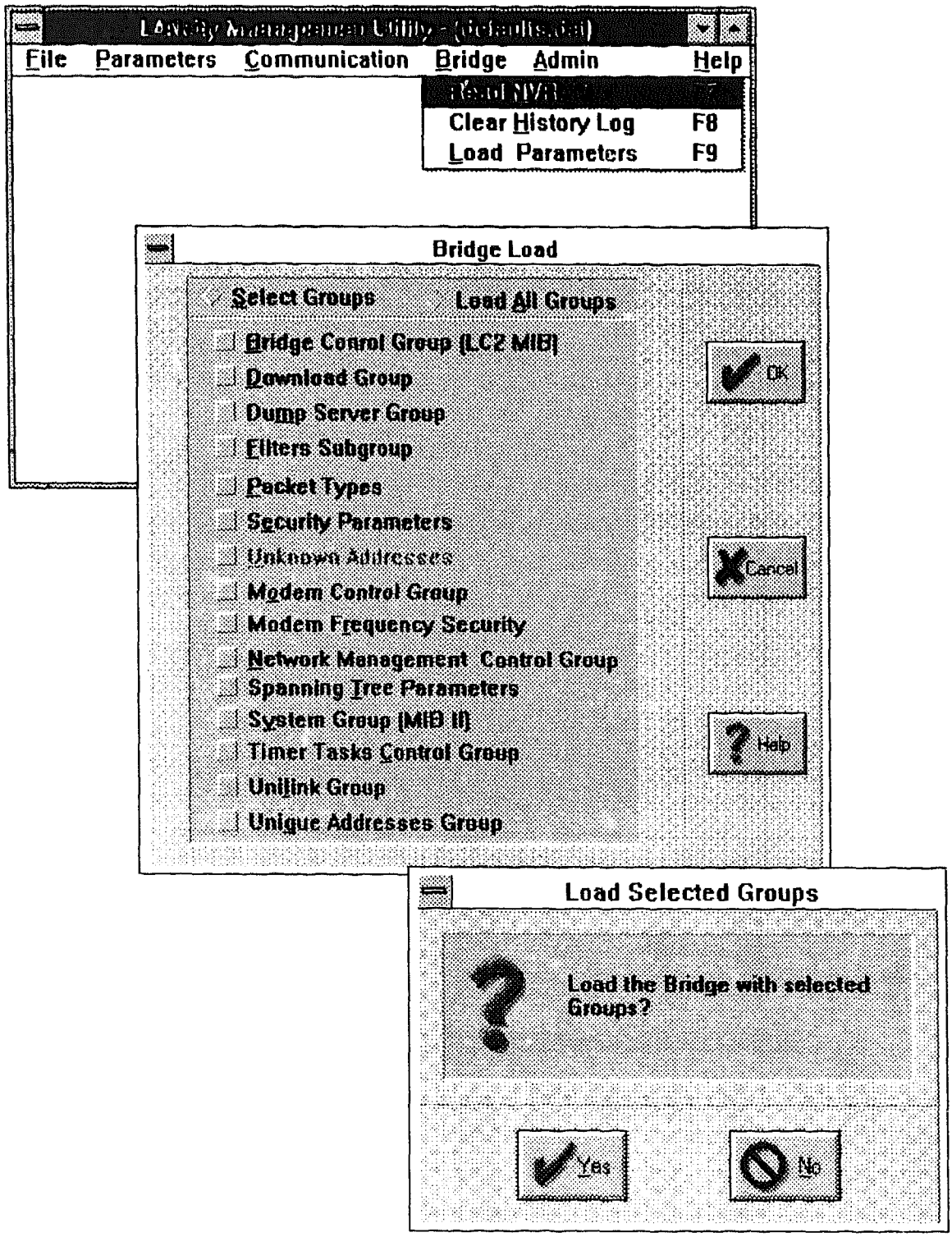
Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Click on Bridge from the utility's Main Menu.
2. Click on Load Parameters from the Bridge Pull Down menu.

   The utility displays the Bridge Load selection window, as shown in Figure 3-9.
3. Click on Select Groups.
4. Click on the parameter groups that you wish to load into the bridge's NVRAM.
5. Click on OK. The utility displays the Load Selected Groups window.
6. Click on YES to load the selected parameter groups. The utility displays the Verify Bridge Load window.
7. Click on YES to verify that the unit's selected parameters were loaded successfully.

   The utility verifies that the parameters were loaded successfully by performing a read and compare of the parameters' locations in NVRAM. Upon a successful load of the selected parameters, the utility displays the Load Status window.
8. Click on OK. The utility returns you to the Main Menu.

Figure 3-9 Loading The ChannelWorks Bridge With Specific Saved Parameters



Loading The ChannelWorks Bridge With All Saved Parameters

The following procedure describes how to load the bridge's NVRAM with all parameters, both saved and default.

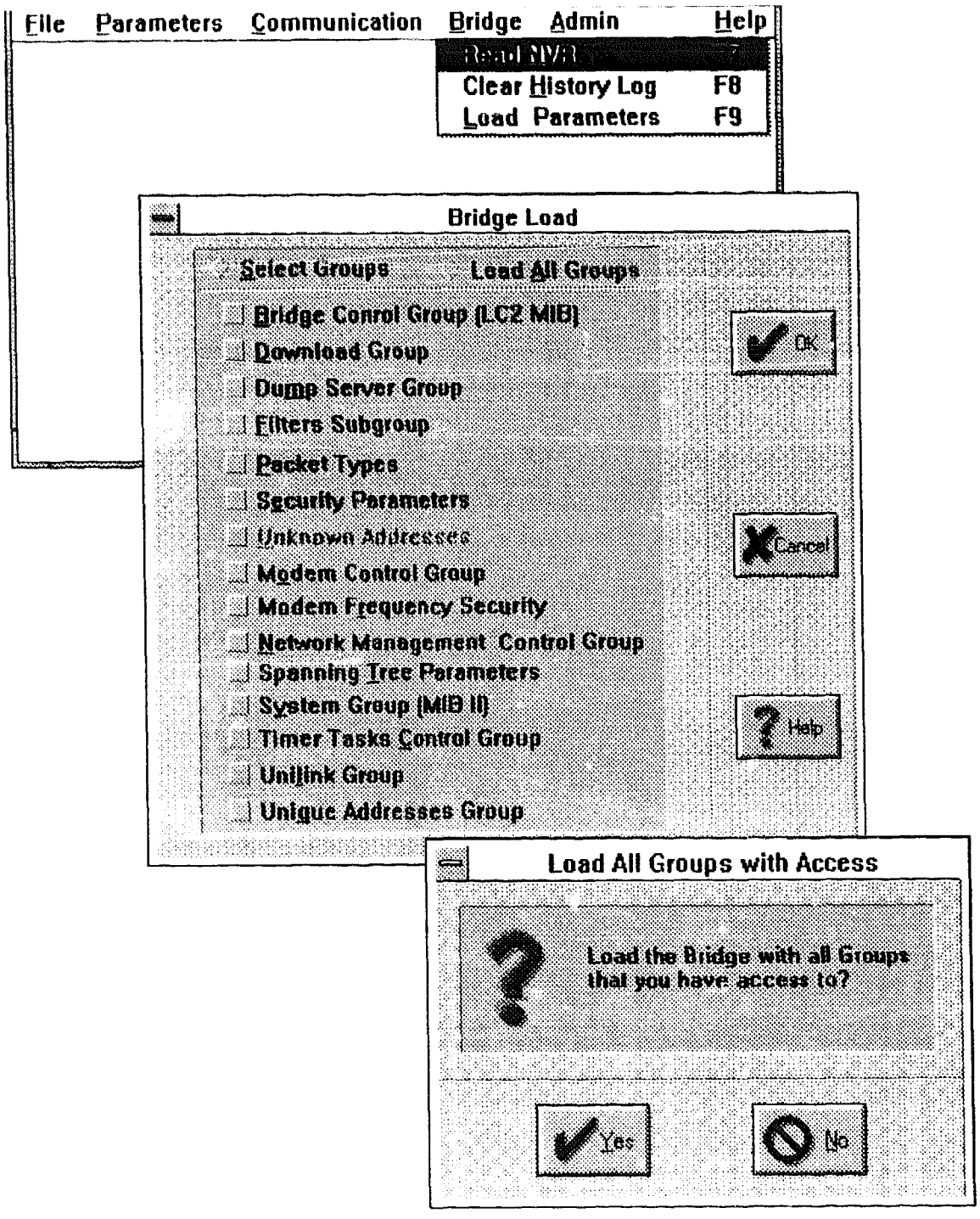
Note: All IP addresses and frequencies are set to 0s in the default configuration data file. You must modify these parameters with valid frequencies and addresses before loading the bridge.

Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Click on Bridge from the utility's Main Menu.
2. Click on Load Parameters from the Bridge Pull Down menu. The utility displays the Bridge Load selection window, as shown in Figure 3-10.
3. Click on Load All Groups. The utility redisplays the Bridge Load window "graying" out the parameter group selections.
4. Click on OK. The utility displays the Load All Groups with Access window, also shown in Figure 3-10.
5. Click on YES to load all parameter groups. The utility displays the Verify Bridge Load window.
6. Click on YES to verify that the unit's parameters were loaded successfully.

   The utility verifies that the parameters were loaded successfully by performing a read and compare of the parameters' locations in NVRAM. Upon successfully loading the parameters, the utility displays the Load Status window.
7. Click on OK. The utility returns you to the Main Menu.

Loading all group parameters takes approximately 3 minutes.


File Parameters Communication Bridge Admin Help
Read NVR
Clear History Log F8
Load Parameters F9
Bridge Load
Select Groups
Load All Groups
Bridge Conrol Group (LC2 MIB)
Download Group
Dump Server Group
Filters Subgroup
Packet Types
Security Parameters
Unknown Addresses
Modem Control Group
Modem Frequency Security
Network Management Control Group
Spanning Tree Parameters
System Group (MIB II)
Timer Tasks Control Group
Unilink Group
Unique Addresses Group
OK
Cancel
Help
Load All Groups with Access
Load the Bridge with all Groups that you have access to?
Yes
No

Clearing The Support History Log

The Support History Log is maintained in the bridge's NVRAM and is accessible through an SNMP manager. All events in ChannelWorks history which are considered significant are recorded in the log. These events and a detailed description of the Support History Log are discussed in Chapter 6, "Troubleshooting A ChannelWorks Bridge Based MAN".

This section discusses how to clear the Support History Log using the utility.

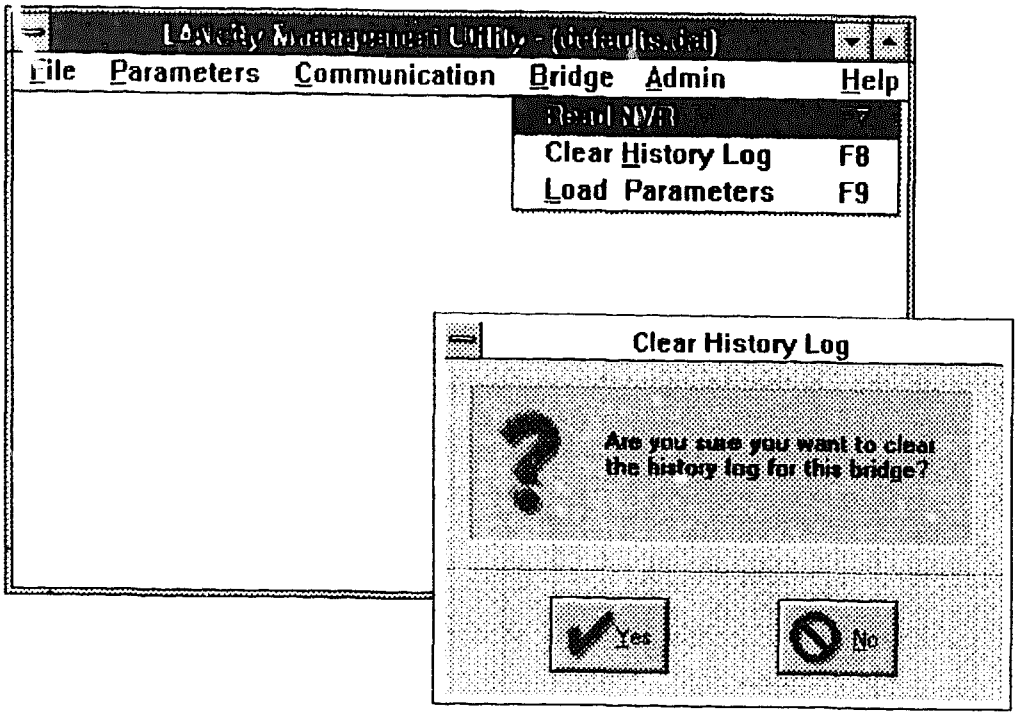
Note: This procedure assumes that you have performed the procedures in the section "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. From the utility's Main Menu, click on Bridge.
2. Click on Clear History Log from the Bridge Pull Down menu. The utility displays the Clear History Log confirmation window, as shown in Figure 3-11.
3. Click on YES to clear.

   Click on NO to return to the utility's Main Menu.

   After clearing the Support History Log, the utility displays a confirmation that it cleared the log successfully.
4. Click on OK. The utility returns you to the Main Menu.

Figure 3-11 Clear Support History Log



Setting Up The Security Group Filtering Parameters

Security Groups

The ChannelWorks Bridge Security Group feature allows users who share the same channel on the cable TV network to send data to other users in the same group without allowing users in other groups to have access to the data. This is especially important because it allows multiple customers to share the same channel but operate as though they were on different networks.

Simple Versus Shared Security Groups

The ChannelWorks Bridge supports two security group types, Simple and Shared. A given ChannelWorks Bridge may be a member of one security group of the Simple type or a member of one or more security groups of the Shared type, but may not be a member of a Simple security group and an Shared security group.

There are 2^{31} different security groups of the Simple type and 31 security groups of the Shared type. While a bridge that uses Simple security groups can belong to only one of them, a bridge that uses Shared security groups can belong to up to 31 different Shared groups.

Bridges are considered to be in the same Simple Security Group if their Security Group type is configured to be Simple and their values for the Security Group are configured to be equal. Figure 3-12 shows an example of the Security Group Filter window configured for Simple groups.

Two bridges are considered to be in the same Shared Security Group if their Security Group type is configured to be Shared and one or more of their Security Groups selected from the utility's Filter Control Group menu matches. Figure 3-13 shows an example of the Security Group Filter window configured for Shared groups.

Notice that if a bridge is configured to use Shared Security Groups and all of the Security Groups from the menu are selected, this bridge can pass user data with any other bridge configured to use Shared Security Groups, regardless of the Security Groups selected from the menu from that bridge.

Bridges that are members of each of these types may coexist on the same cable TV channel; however, they cannot pass data packets if they are members of different type groups.

Figure 3-12 Simple Security Group Settings

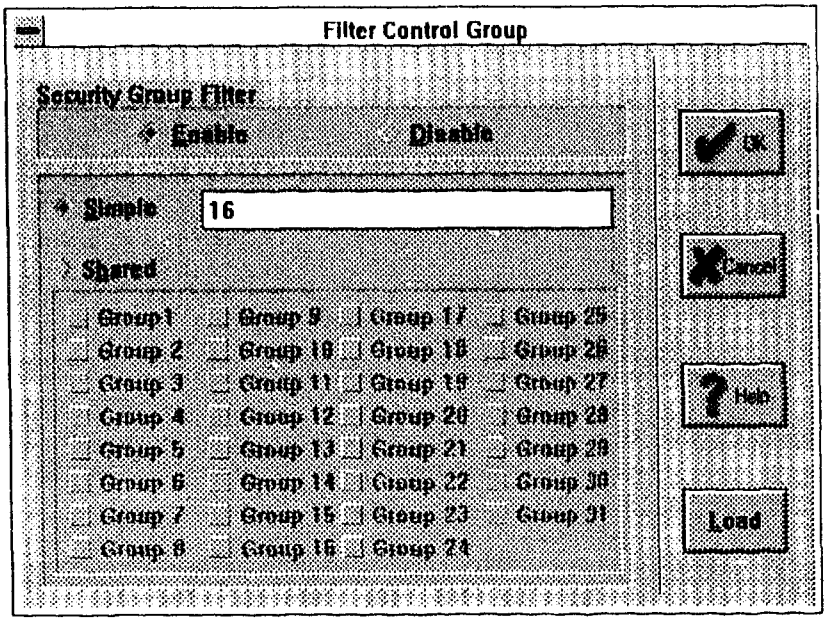
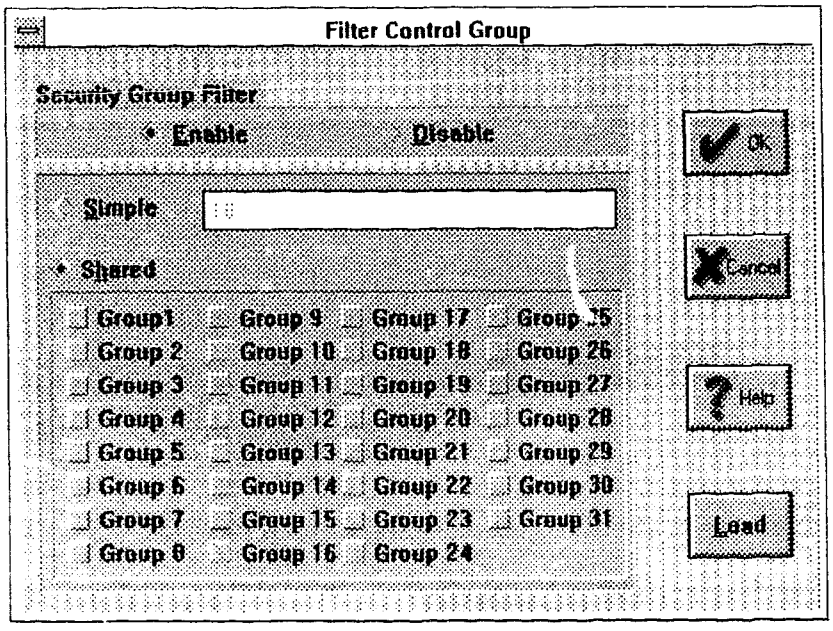


Figure 3-13 Shared Security Group Settings



Filtering Based On Security Group

When a packet is transmitted to the cable TV network, it includes the security group identification. When a bridge receives a packet from the cable TV network, it will be filtered if it is not in the same security group as the transmitting bridge.

User data packets, SNMP, and MOP packets are filtered based on Security Groups. Spanning Tree Protocol packets will not be filtered as a result of being from a bridge that is not in the same security group as the receiving bridge.

Note: Be careful when configuring Security Groups, so that management works as desired.

Setting Up Packet Type Filtering Parameters

Using the utility the network manager or cable TV installer can configure up to eight different packet types to be filtered by the ChannelWorks Bridge. An example of the utility's Filter Control Group Packet Filtering window is shown in Figure 3-14.

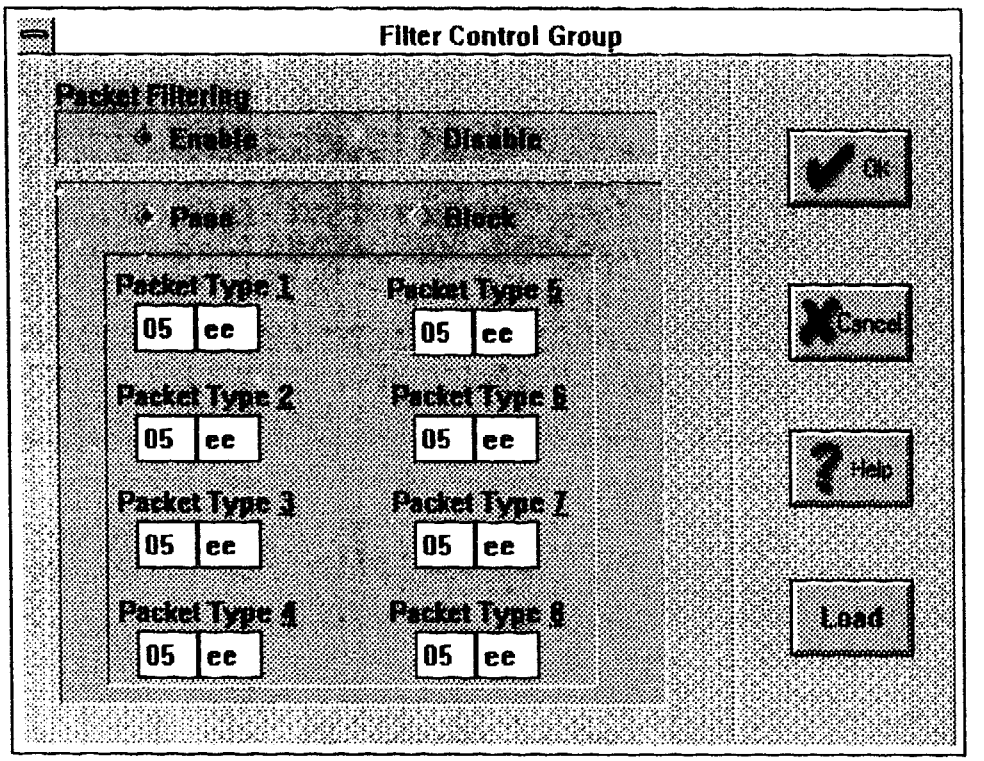
Any packet received on either the Ethernet or cable TV interfaces will be filtered if it matches one of these packet types.

All Ethernet frames contain a two byte field that identifies the packet type. The packet type is a number indicating the particular communications protocol that generated the frame. In IEEE/802.3 frames, this field indicates the length of the data contained in the frame. All packet types have a value greater than 1500 decimal, while the length of all IEEE/802.3 frames is less than or equal to 1500.

You can use this feature to selectively filter traffic on the basis of the packet type in the frame. For example, you may filter certain protocols such as XNS, DECnet, or LAT. Contact the particular vendors for the value of their protocol packet types.

Packet type filtering enables you to maximize network utilization by eliminating unnecessary traffic.

Figure 3-14 Packet Type Filtering Settings



4

Interpreting The ChannelWorks Bridge Statistics

Introduction

The ChannelWorks enterprise specific Bridge MIB includes counters and statistics that allow for diagnosis of network problems on the cable TV network. This chapter describes those counters, and explains how to interpret them.

The MIB also provides counters for diagnosis of network problems on the Ethernet port. These counters are in the enterprise specific MIB under the SONIC Errors Group. Note that ChannelWorks uses a standard Ethernet controller device (SONIC) to implement the Ethernet MAC Layer These counters are fairly standard and will not be described further.

Counters and statistics relating to the cable TV network are in the enterprise specific MIB under five groups. The first four groups are maintained directly by the ASIC hardware that implements the MAC Layer on the cable TV network. Bridge software maintains the third group.

- ASIC TX Statistics Group — Related to packets transmitted onto the cable TV network
- ASIC RX Statistics Group — Related to packets received from the cable TV network
- ASIC Summary Statistics Group — Related to summarizing various packet types, both transmitted and received
- ASIC Control Group — Related to resetting all ASIC statistics
- ASIC Software Statistics Group — Statistics maintained by upper-level software

The following sections describe these groups further.

ASIC Statistics Classes

ASIC statistics on the cable TV network are divided into classes based on type of information and transmission mode, as described in the following paragraphs.

Type of information

The queue identifies on which the packet is transmitted identifies whether the packet contains user data or MAC control information. These queues are described as follows:

- LO queue — used for data packets
- HI queue — used for MAC Layer control packets (UniLINK Packets)
- MAC queue — used for other MAC Layer control packets sent using reservation mechanism

Note: Transmit statistics are not maintained at a hardware level for the MAC queue, so it will not be discussed further in this section.

Access Mode

The cable TV MAC Layer can use either contention-based (CSMA/CD) or reservation-based access methods to transmit a packet on the cable TV network. This is identified as:

- Contention — packet sent using CSMA/CD access, only used for LO queue packets
- Dedicated — packet sent using reservation mechanism, LO or HI queue packets

Transmit Mode

The cable TV MAC Layer can either transmit a packet individually or concatenate it with others. This is identified as:

- Single — packet sent individually, LO or HI queue packets
- Concatenated — packet sent concatenated with others, only used for LO queue packets

ASIC TX Statistics Group

This group contains the detailed statistics relating to transmissions from the ChannelWorks Bridge to the cable TV network. The ASIC transmit statistics sub-groups are:

- txnormalinfo — Counters that are expected to increment during normal operation.
- txloerrorinfo — Counters indicating error conditions on the lo (data) queue.
- txhierrorinfo — Counters indicating errors on the HI and MAC queues used by UniLINK protocol.

Note: Error counts will increment. The network manager must establish a rate that is normal for his or her network and check for deviations from that rate.

ASIC Transmit Statistics Classes

Thus, there are a total of six transmission classes which a packet transmitted on the cable TV network can fall into. These six classed are listed below:

- lcloconsingle — data, contention mode, single packet
- lcloconconcat — data, contention mode, packets concatenated
- lclodedsingle — data, reservation mode, single packet
- lclodedconcat — data, reservation mode, packets concatenated
- lchicon — not used, all counters should always be zero
- lchided — non-data (UniLINK control), reservation mode, single packet

Note: Non-data packets are not concatenated.

For each transmission class, a separate set of counters is kept. The set of counters for a single class is enumerated below. Note there are six counters in the set for one class.

- Packet Counter — number of packets sent
- Frame Counter — number of concatenated frames sent
- Retry Counter — total retry count (can increment n times per packet)
- Deferred Counters — deferral count
- Retry Once Counter — number of packets sent after exactly one retry
- Retry Multiple Counter — number of packets sent after more than one retry
- Pending — number of packets pending

Note: On every network, there is always one unit that becomes the "Pacer." Thus its lchided packet count will differ significantly from other units.

ASIC RX Statistics Group

This group contains counters relating to the reception of data by the ChannelWorks Bridge from the cable TV network. The ASIC receive statistics subgroups are:

- rxnormalinfo — Counters that are expected to increment during normal operation
- rxerrornormalinfo — Error condition counters that are expected to increment during normal operation, such as CRC errors in contention mode
- rxoverloadinfo — Error condition counters relating to system/media overload
- rxabnormalinfo — Error condition counters not normally expected to increment

ASIC Receive Statistics Classes

Receive statistics for packets received from the cable TV network are again divided into classes. The classes are somewhat different than the ones used for transmitted packets, because the distinction between single and concatenated packets is not maintained by the receiver. Classes are differentiated by access method — contention or dedicated — and information type — data (LO queue) and non-data (HI and MAC queues). Non-data includes UniLINK Control as discussed in the section "ASIC Transmit Statistics Classes." The four receive classes are:

- lclocon — data, contention mode
- lcloded — data, reservation mode
- lchimaccon — non-data, contention mode
- lchimacded — non-data, reservation mode

For each class, a set of counters is kept. A set is listed below, in decreasing priority:

	LCB MIB Sub Group
• concat filter	abnorm
• hcs (header checksum) error	err
• crc error	err
• postamble	err
• eom (end of message) error	err
• packet too big	abnorm
• rda missing (out of memory)	overload
• rba missing (out of memory)	overload
• rx overflow	overload
• rx underrun	overload
• ext reject (special MAC-control filtering)	abnorm
• cam filter (filtered due to type/address)	abnorm
• trie filter (filtered due to type/address)	norm
• good packets received	norm

When a packet is received, it is classified according to the contents of a control field. If the receiver detects an error in the packet, the error is logged and the packet is discarded. If more than one error is detected, only the highest priority error is logged. When an error occurs, it is possible that the control field used to classify the packet is corrupt as well, and the error may be misclassified.

ASIC Summary Statistics Group

This summary statistics group presents a processed view of the ASIC TX and RX statistics. The ASIC Summary Statistics Group shows the basic operation of the UniLINK protocol.

The following enterprise specific MIB variables provide summaries of TX and RX packet statistics. The network manager must use the summaries to determine a baseline from which to diagnose network problems.

Total Data Packets Transmitted

You use the lcnonunilinktx MIB of the Summary Statistics Group to determine the total number of data packets transmitted by a bridge from HI queue. The lcnonunilinktx MIB is a summary of the following MIB variables:

	(lcloconsinglepkts)	single data packets transmitted in contention mode
	(lcloconconcatpkts)	concatenated data packets transmitted in contention mode
	(lclodedsinglepkts)	single data packets transmitted in dedicated mode
+	(lclodedconcatpkts)	concatenated data packets transmitted in dedicated mode
=	(lcnonunilinktx)	the total number of data packets transmitted

Total MAC Layer (HI-Queue) Packets Transmitted

You use the lcunilinktx MIB of the Summary Statistics Group to determine the total number of MAC Layer control packets transmitted by a bridge. The lcunilinktx MIB is a summary of the following MIB variables:

	(lchiconsinglepkts)	single MAC Layer packets transmitted in contention mode
+	(lchidedsinglepkts)	single MAC Layer packets transmitted in dedicated mode
=	(lcunilinktx)	the total number of MAC Layer packets transmitted

Percentage Of Retried Data Packets

You use the lcnonunilinkretry MIB of the Summary Statistics Group to determine the percentage of data packets retransmitted by a bridge. The lcnonunilinkretry MIB is a summary of the following MIB variables:

	(lcloconsingleretrycnt)	single data packet retries in contention mode
	(lcloconconcatretrycnt)	concatenated data packet retries in contention mode
	(lclodedsingleretrycnt)	single data packet retries in dedicated mode
+	(lclodedconcatretrycnt)	concatenated data packet retries in dedicated mode
=		the total number of data packets retried
×		100
=		100 times the total number of data packets retried
÷	(lcnonunilinktx)	the total number of data packets transmitted
=	(lcnonunilinkretry)	the percentage of data packets retransmitted

Total Data Packets Received From Other Nodes

You use the lcnonunilinkrx MIB of the Summary Statistics Group to determine the total number of data packets received by a bridge from other nodes. The lcnonunilinkrx MIB is a summary of the following MIB variables:

	(lcloconpkts)	single data packets received in contention mode
+	(lclodedpkts)	single data packets received in dedicated mode
=		the total number of data packets received
−	(lcnonunilinktx)	the total number of data packets transmitted
=	(lcnonunilinkrx)	the total number of data packets received from other nodes

Total MAC Layer Packets Received From Other Nodes

You use the lcunilinkrx MIB of the Summary Statistics Group to determine the total number of MAC Layer packets received by a bridge from other nodes. The lcunilinkrx MIB is a summary of the following MIB variables:

	(lchimacconpkts)	single MAC Layer packets received in contention mode
+	(lchimacdedpkts)	single MAC Layer received in dedicated mode
=		the total number of MAC Layer packets received
−	(lcunilinktx)	the total number of MAC Layer packets transmitted
=	(lcunilinkrx)	the total number of MAC Layer packets received from other nodes

Total Data Queue CRC Errors

You use the lclocrcerrors MIB of the Summary Statistics Group to determine the total number of data queue crc errors. The lclocrcerrors MIB is a summary of the following MIB variables:

	(lcloconcrc)	single data queue crc errors in contention mode
+	(lclodedcrc)	single data queue crc errors in dedicated mode
=	(lclocrcerrors)	the total number of data queue crc errors

Total MAC Layer Queue CRC Errors

You use the lchimaccrcerrors MIB of the Summary Statistics Group to determine the total number of MAC Layer queue crc errors. The lchimaccrcerrors MIB is a summary of the following MIB variables:

	(lchimacconcrc)	single MAC Layer queue crc errors in contention mode
+	(lchimacdedcrc)	single MAC Layer queue crc errors in dedicated mode
=	(lchimaccrcerrors)	the total number of data queue crc errors

Estimated Total Collisions

You use the lccollisionsrx MIB of the Summary Statistics Group to determine an estimated total number of collisions. The lccollisionsrx MIB is a summary of the following MIB variables:

	(lcloconcrc)	single data queue crc errors in contention mode
	(lclodedcrc)	single data queue crc errors in dedicated mode
	(lchimacconcrc)	single MAC Layer queue crc errors in contention mode
	(lchimacdedcrc)	single MAC Layer queue crc errors in dedicated mode
	(lcloconeom)	single data queue eom errors in contention mode
	(lclodedeom)	single data queue eom errors in dedicated mode
	(lchimacconeom)	single MAC Layer queue eom errors in contention mode
+	(lchimacdedeom)	single MAC Layer queue eom errors in dedicated mode
=	(lccollisionsrx)	the estimated total number of collisions

ASIC Control Statistics Group

This group provides the MIB variable lcresetstats. You can reset all ASIC statistics by performing an SNMP Set on lcresetstats.

Collisions

UniLINK does not support an explicit collision enforcement channel. Thus, a collision is detected by some form of packet error on the receive side. Typically, the FC field is corrupted and the errors logged in one of the four RX groups.

A corrupted frame control (FC) may appear as a contention or dedicated packet and may appear in either LO or HIMAC queues for RX statistic logging purposes. Most collisions cause either an hcs or eom error to be logged. If the collision causes the start of frame to be lost, nothing will be logged. If the collision causes the ChannelWorks Bridge modem's carrier detect to drop in and out, then multiple events may be logged for a single collision. As mentioned above, if the 16-bit Header Checksum happens to pass (no hcs_err) and the length field is less than the duration of carrier detect (no eom_err), then a crc error will be logged. Finally, a collision may be seen slightly differently by each ChannelWorks Bridge. Thus, a single collision may get logged as different events in different nodes.

Initial observations indicate that 90+% of collisions get logged as an hcs or eom error. Therefore, to get an estimate of the total number of collisions on the network, sum up the hcs and eom errors across all four RX groups. In a two node network, this number should approximately match the total retry count and the numbers between the two nodes should be approximately equal. In a larger network, this is no longer true, because some collisions may involve more than two nodes. Also, not every node is involved with each collision.

If the pkt_too_big or rba_missing counts are excessively high, then this is an indication of extremely high network activity with which the node cannot keep up. Or, the node has stopped forwarding traffic and may need to be rebooted.

All other RX statistics should only be interpreted by a trained service engineer. Certain bridge errata (lclocon_trie_filter) may cause some statistics to look out of the ordinary.

Bridge Software Statistics

The ChannelWorks Bridge software keeps track of TX statistics. The bridge's SNMP MIB variables for software statistics are listed here with brief descriptions. These are in the ChannelWorks Bridge SNMP MIB: "lancity.lcasicswstats."

- lctxbadlo — TX Bad LO Q
- lcdetldpkts — Determine Loop Delay packets attempted
- lchitxpkts — HI TX packets attempted
- lctxgoodhi — TX good HI Q
- lctxbadhi — TX bad HI Q
- lcrxgoodhi — RX good HI Q
- lcrsendbspkts — Block Sync packets attempted
- lcmactxpkts — MAC TX packets attempted
- lctxgoodmac — TX good MAC Q
- lctxbadmac — TX bad MAC Q
- lcrxgoodmac — RX Good MAC Q
- lcrxld — RX Determine Loop Delay packets
- lcrxbsts — RX Block Sync packets with timestamp
- lcrxbstsdrop — RX Block Sync packets with timestamp, ASIC not willing to SNAP
- lcrxbstssnap — RX Block Sync packets with timestamp, ASIC willing to SNAP
- lcrxexcepcount — RX Exception Error
- lctxexcepcount — TX Exception Error
- lcbsbexpiredcount — Block Sync Boundary Expired
- lcbasictimercount — ASIC Timer Expired

Bridge Software Statistics

The ChannelWorks Bridge software keeps track of TX statistics. The bridge's SNMP MIB variables for software statistics are listed here with brief descriptions. These are in the ChannelWorks Bridge SNMP MIB: "lancity.lcasicswstats."

- lctxbadlo — TX Bad LO Q
- lcdetldpkts — Determine Loop Delay packets attempted
- lchitxpkts — HI TX packets attempted
- lctxgoodhi — TX good HI Q
- lctxbadhi — TX bad HI Q
- lcrxgoodhi — RX good HI Q
- lcrsendbspkts — Block Sync packets attempted
- lcmactxpkts — MAC TX packets attempted
- lctxgoodmac — TX good MAC Q
- lctxbadmac — TX bad MAC Q
- lcrxgoodmac — RX Good MAC Q
- lcrxld — RX Determine Loop Delay packets
- lcrxbsts — RX Block Sync packets with timestamp
- lcrxbstsdrop — RX Block Sync packets with timestamp, ASIC not willing to SNAP
- lcrxbstssnap — RX Block Sync packets with timestamp, ASIC willing to SNAP
- lcrxexcepcount — RX Exception Error
- lctxexcepcount — TX Exception Error
- lcbsbexpiredcount — Block Sync Boundary Expired
- lcbasictimercount — ASIC Timer Expired

5

Configuring The ChannelWorks Bridge

Introduction

This chapter describes how to set specific ChannelWorks Bridge operating parameters using the Management Utility and the bridge's SNMP enterprise specific MIB variables. This chapter covers the following topics:

- Setting up for Serial Line Interface Protocol (SLIP) Operation
- Changing transmit and receive frequencies using an SNMP manager
- Using the Trivial File Transfer Protocol (TFTP) to perform a software upgrade
- Setting the Maximum Loop Delay Common Parameter

Setting Up For Serial Line Interface Protocol (SLIP) Operation

The ChannelWorks Bridge serial port provides support for the Serial Line Interface Protocol (SLIP). You use the bridge's serial port for SNMP management if your SNMP manager doesn't have a connection to or you don't wish to use the local Ethernet. The bridge to which the serial line is connected acts as a gateway for the rest of the network and is called the gateway unit.

Note: Ensure that your SNMP management station application is configured to operate through the Serial Line Interface Protocol according to its manufacturer's recommended settings. The management station port's communication characteristics must be compatible with the values used on the bridge's serial port. The ChannelWorks Bridge serial port's communication characteristics are:

- Baud Rate - 9600
- Character Size (Data) - 8
- Stop Bits - 1
- Parity - None

The bridge to which the PC manager is directly connected via the serial line is known as the gateway bridge.

At least two IP networks are involved:

- The SLIP network based on the serial line with two hosts
  - Manager and gateway bridge
- The cable TV Ethernet networks with the following hosts
  - Gateway bridge
  - All other bridges

The gateway bridge operates as an IP router between the two networks. Any other bridge could also be connected to a serial line. This would require another IP network.

Configuration Of Gateway Bridge

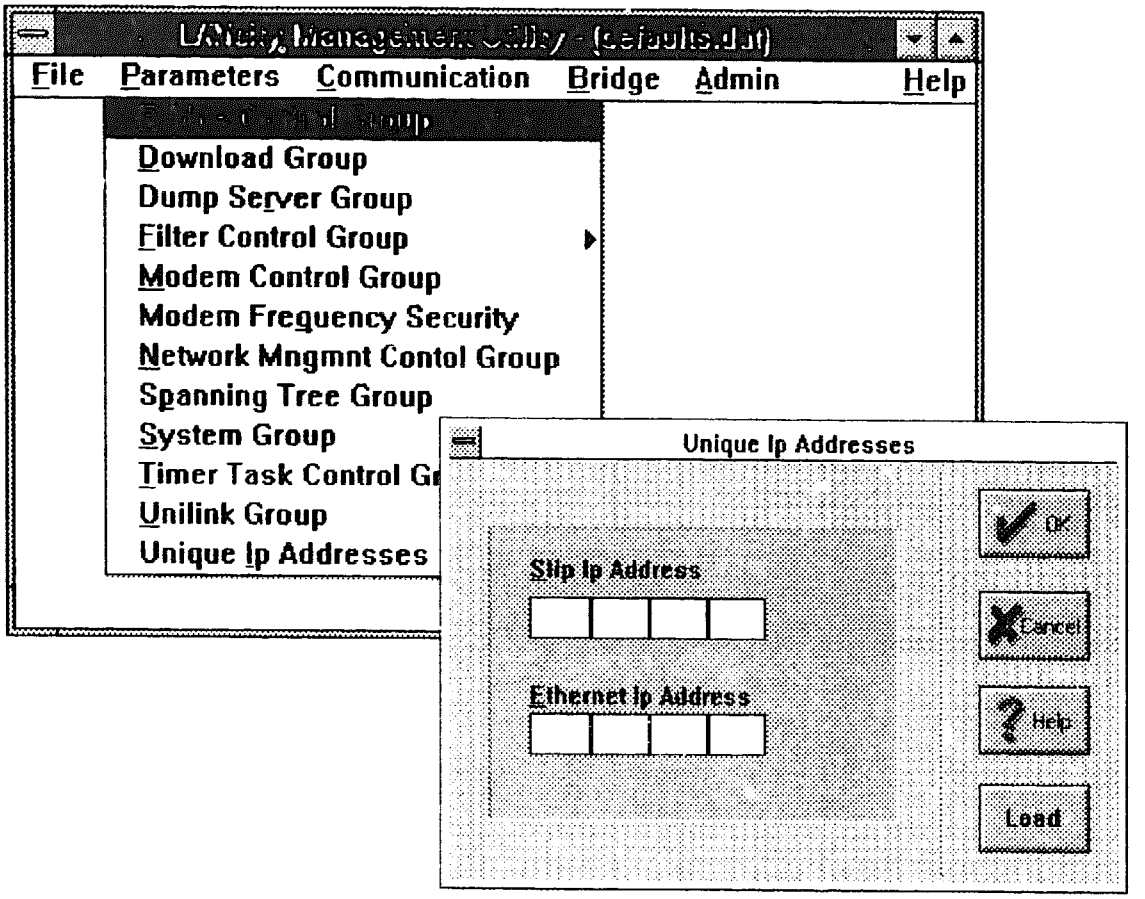
Perform the following procedure to configure the bridge for SLIP operation to perform SNMP management.

Note: This procedure assumes that you have performed the procedures in Chapter 3's section, "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Click on PARAMETERS from the utility's Main Menu.
2. Click on the UNIQUE IP ADDRESSES from the Parameters Pull Down Menu.

   The utility displays the Unique IP Addresses window, as shown in Figure 5-1.
3. Enter the Ethernet IP address of the bridge (note 1).
   - Network = Cable TV Ethernet Network
   - Host = This node
4. Enter the SLIP IP address of the bridge.
   - Network = SLIP serial line network
   - Host = This node

Figure 5-1 Unique IP Addresses



5. Verify that the information entered is correct and click on OK to save the information for loading at a later time. Or, click on LOAD to load the parameter in the unit's NVRAM now.

   The utility displays the Save parameter or Load parameter confirmation window.

6. Click on YES if you wish to Save or Load the parameter. The utility returns you to the Main Menu.

7. Click on the NETWORK MNGMENT CONTROL GROUP from the Parameters Pull Down Menu.

   The utility displays the Network Management Control Group window, as shown in Figure 5-2.

8. Enter the network managers SLIP IP address as the NM SLIP IP address.

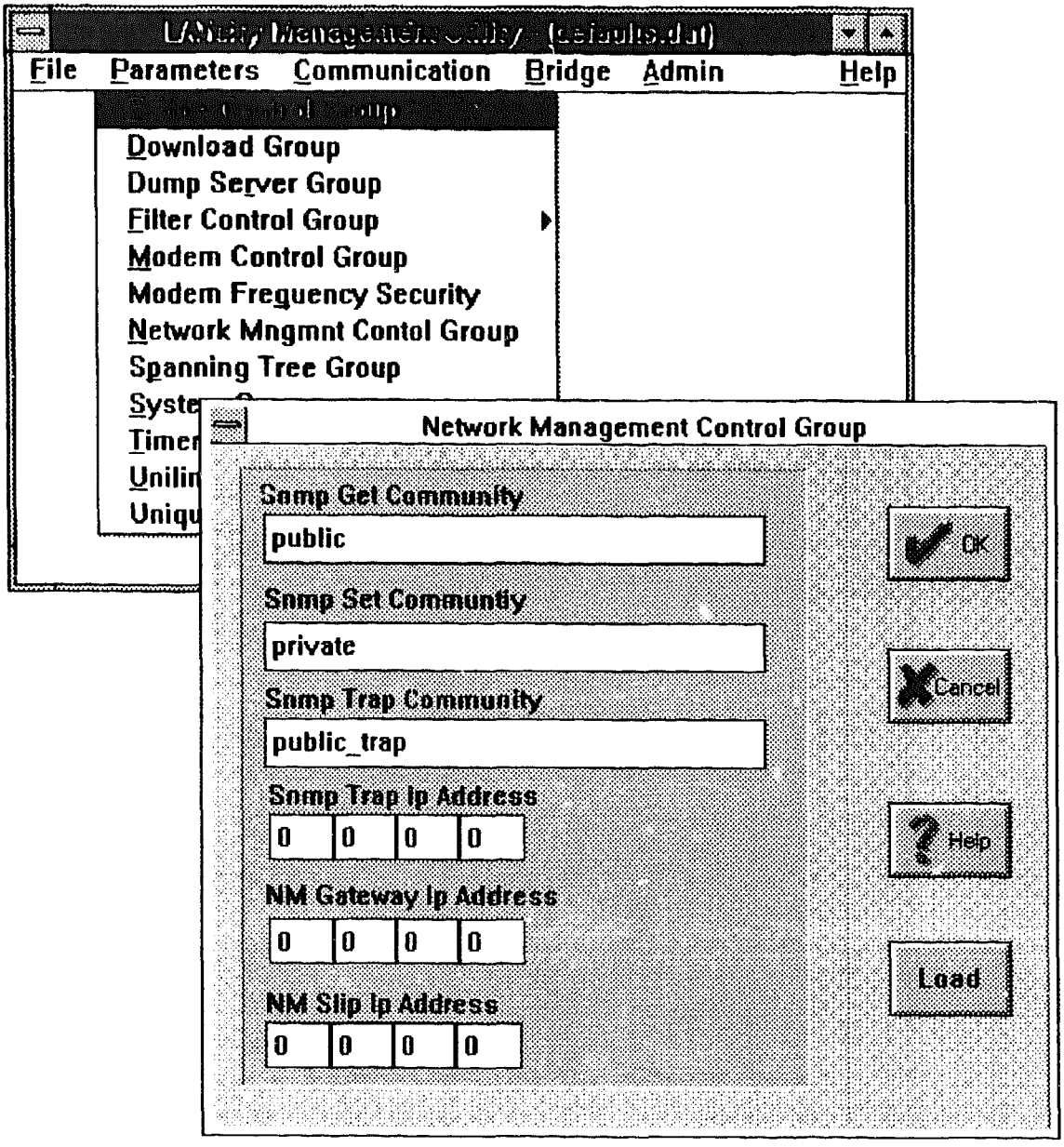
9. Enter the gateway bridge (this bridge) Ethernet IP Address as the NM Gateway IP Address.

10. Verify that the information entered is correct and click on OK to save the information for loading at a later time. Or, click on LOAD to load the parameter in the unit's NVRAM now.

    The utility displays the Save parameter or Load parameter confirmation window.

11. Click on YES if you wish to save or load the parameter. The utility returns you to the Main Menu.

Figure 5-2 Network Management Control Group



Configuration Of ALL Other Bridges

Perform the following procedure to configure the other bridges on the network that will be managed through the gateway bridge.

Note: This procedure assumes that you have performed the procedures in Chapter 3's section, "Connecting A PC To The ChannelWorks Bridge Serial Port."

1. Click on PARAMETERS from the utility's Main Menu.
2. Click on the UNIQUE IP ADDRESSES from the Parameters Pull Down Menu. The utility displays the Unique IP Addresses window, as shown in Figure 5-1.
3. Enter the Ethernet IP address of the bridge (note 1).
   - Network = Cable TV/Ethernet network
   - Host = This node
4. Enter the SLIP IP address of the bridge.
   - Network = A network that may be reached via the serial port of this bridge. In most cases there will be no physical connection and hence no network so that a fictitious IP network should be used. This network MUST be different than the SLIP IP network routed to by the gateway bridge for the routing to work correctly.
   - Host = This node.
5. Enter the network managers SLIP IP address as the NM SLIP IP Address.
6. Enter the gateway bridge Ethernet IP address as the NM Gateway IP Address.
7. Verify that the information entered is correct and click on OK to save the information for loading at a later time. Or, click on Load to load the parameter in the unit's NVRAM now.

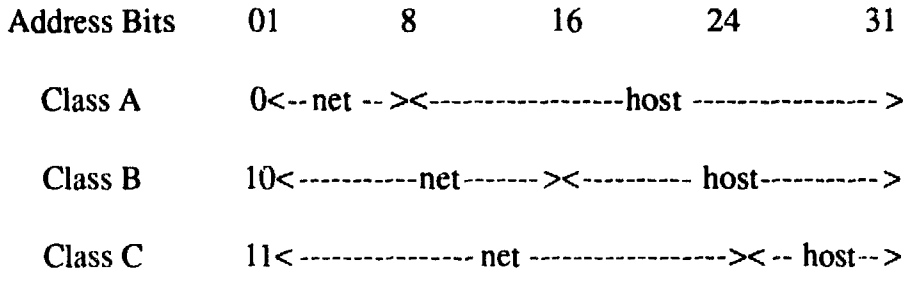
   The utility displays the Save parameter or LOAD parameter confirmation window.
8. Click on YES if you wish to save or load the parameter. The utility returns you to the Main Menu.

Once a SLIP connection has been established, it appears as a LAN interface to all network applications. Note that the network addressing rules apply for LAN interfaces must also apply to SLIP interfaces.

For example, the two systems on the SLIP network (your management station and the ChannelWorks Bridge it is connected to) must exist on the same subnet and each have a unique SLIP IP Address (for example, 192.190.4.1 and 192.190.4.43).

Note 1: An IP network address is a unique, 32-bit number made up of a network identifier and a host identifier, where the network identifier specifies a network and the host ID specifies a host on that network.

The division between network ID and host ID follows simple rules based on the network class. The network class is determined from the 3 high order bits of the address. Examples for the 3 common classes of address are shown below.



Changing Transmit And Receive Frequencies Using SNMP

The ChannelWorks Bridge provides authorized users the ability to modify the cable TV's transmit and receive frequencies remotely using an SNMP manager. An SNMP "set" of the special frequency access password string is required to perform SNMP sets of both cable TV transmit and receive frequencies to new values.

The SNMP frequency access password must be set during the configuration of the bridge's parameters by the utility's Modem Frequency Security Group. Refer to the Chapter 3's section, "Setting The SNMP Frequency Access Password," for detailed instructions on how to set the SNMP frequency access password.

Perform the following procedure to change the cable TV transmit and receive frequencies of an operational unit using an SNMP manager.

Note: This procedure uses the SNMP manager SNMPc to describe the frequency change procedure. A different SNMP manager may employ a different set of steps to accomplish the same result. The procedure assumes that you have compiled the SNMP enterprise specific MIB and have installed the set_freq.exe application on your PC according to your SNMP manager's instruction. The set_freq.exe application allows you to let the SNMP manager perform the "sets" on your password and the frequency changes in one step instead of you having to perform the SNMP sets individually.

This procedure also assumes that you have performed the procedures in the section "Setting up for Serial Line Interface Protocol (SLIP) Operation" and have opened the SNMPc manager. Figure 5-3 i an example of an SNMPc network map window.

Note: Your PC may also connect with the bridge through an Ethernet connection.

1. Using the mouse, double click on the icon of the bridge you wish to change frequencies.

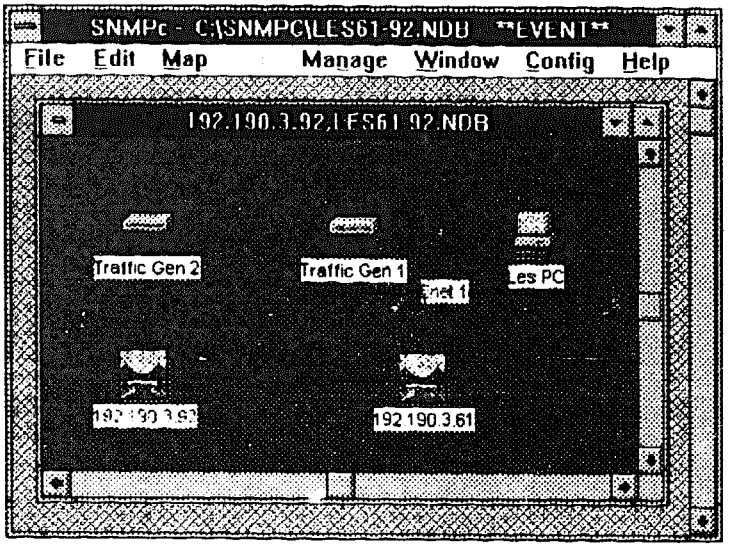
   The SNMP manager displays the Modem Frequency Security window, as shown in Figure 5-3.

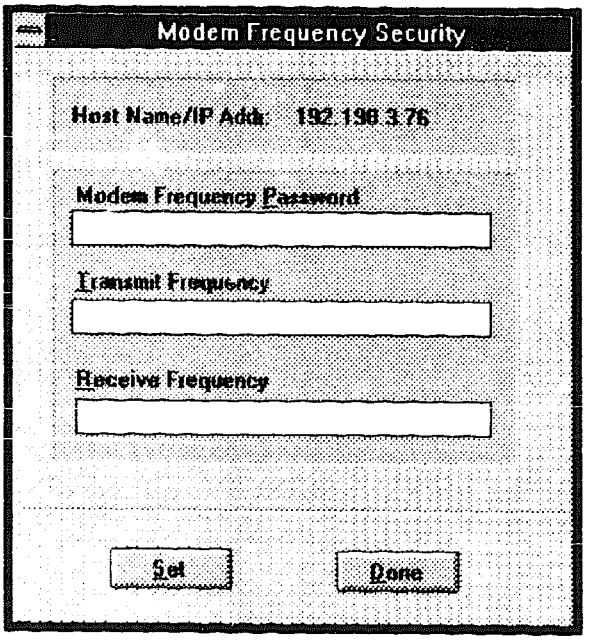
2. Type your Modem Frequency Security password in the space provided.

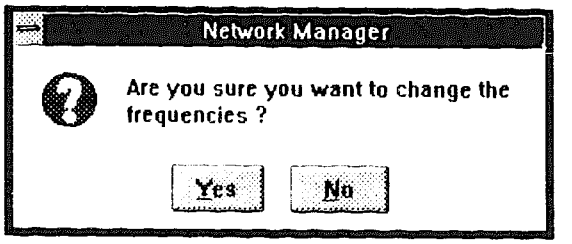
3. Tab or use the mouse to position the cursor in the space provided for the transmit frequency and type a four to five digit decimal number denoting the desired transmit frequency.

Note: Valid transmit frequencies are 10.00 MHz to 174.00 MHz in intervals of 0.25. Enter frequencies in KHz. 10 MHz is entered 10000. Decimal points are not used. The transmit frequency identifies the center of the return channel.

Figure 5-3 Changing Transmit And Receive Frequencies







4. Tab or use the mouse to position the cursor in the space provided for the receive frequency and type a four to five digit decimal number denoting the desired receive frequency.

Note: Valid receive frequencies are 54.00 MHz to 550.00 MHz in intervals of 0.25. Enter frequencies in KHz. 10 MHz is entered 10000. Decimal points are not used. The receive frequency identifies the center of the forward channel.

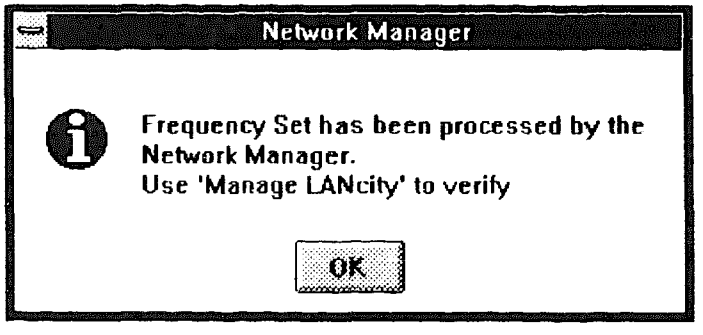
5. Click on the SET button. The SNMP manager displays the Frequency Set confirmation window, as shown in Figure 5-4.

6. Click on the OK button. The SNMP manager returns you to the Modem Frequency Security window.

7. Click on the DONE button.

The bridge's frequencies are set in NVRAM. You need to reset the bridge to activate the new frequencies.

Figure 5-4 Frequency Set Confirmation



Upgrading The ChannelWorks Bridge Software

The ChannelWorks Bridge uses the Trivial File Transfer Protocol (TFTP) to perform software upgrades. The following sections describe how to upgrade ChannelWorks Bridge software for a bridge that is operational.

This procedure does not apply to loading software into nonoperational bridges. The ChannelWorks Bridge Flash Prom must have an operational version of software running for the upgrade to be performed.

This procedure assumes that you are managing the ChannelWorks Bridge using an SNMP station manager and have network access to a TFTP server. The SNMP station manager and TFTP File Sever may or may not be located on the same PC. But, they both must be available over a network to ChannelWorks Bridges being upgraded.

Requirements

To perform a ChannelWorks Bridge software upgrade, you must have the following items:

1. TFTP File Server - This may be a PC or UNIX system

   PC running the Chameleon TCP/IP stack.
   SUN running SUNOS 4.1.22.

2. Operational SNMP Network Manager

   PC running SNMPc over TCP/IP stack.

3. The Cable TV Management Tools package

   Bridge's SNMP MIBs, Ver 1.6 and Ver 2.0
   Management Utility
   ChannelWorks Software Ver 2.0

Note: During the Software Upgrade process nodes running Ver 1.6 Software will not respond correctly to some SNMP requests made using the enterprise specific MIB compiled for Ver 2.0 Software. You should install and compile the LANcity enterprise specific MIB Version 2.0 after the software upgrade is complete.

4. Operational Networked ChannelWorks Bridge in Loopback Mode

   ChannelWorks Bridge connected to local Ethernet.
   You cannot perform the upgrade using TFTP over the serial port.
   Loopback Cable with 50-dB Attenuation.

ChannelWorks Bridge Upgrade Procedure

Perform the following procedure to complete the ChannelWorks Bridge software upgrade.

1. Use the utility to place the ChannelWorks Bridge in PROM Monitor Mode, read and save the bridge's NVRAM parameters.
2. Use the utility to load in stand-alone/loopback mode frequencies of 55 MHz TX and 55 MHz RX.
3. Connect the ChannelWorks Bridge's TX and RX F connectors together with the 50-dB attenuated loopback cable.
4. Boot the ChannelWorks Bridge in stand-alone RF loopback mode and connect it to the local Ethernet.
5. Open the TFTP server. Use the TFTP server's Settings pull down menu to determine the Server's public directory.
6. Install the loadable file from the 3.5-in diskette (LCB Software - LCB V2.0) to the public directory of the TFTP server.

   The filename is lcb.ftp. It is bundled with a readme file and a release notice. Loading the file in the TFTP server's public directory makes the file available over the network for LCBs being upgraded. Refer to your server's TFTP documentation for directory information.
7. Start the TFTP server.

Use the SNMP network manager to set the following variables from the Download Group:

Note: Verify that you have the correct version of the LCB MIB. The LCB MIB for the SNMPc network manager is called lc2.mib, is 68,129 bytes, and is located in the mibfiles directory.

8. Set the Load Server IP Address (lclsipaddress) to the IP address of TFTP server.
9. Set the Load Protocol to — tftp.
10. Set the Load File to the filename of the loadable file. The loadable filename from your 3.5-in upgrade diskette is lcb.ftp. Do not use full pathname.

Note: If your TFTP server is UNIX based, the Load File filename is case sensitive.

All parameters must be set exactly as stated. Verify that all previous steps are complete and accurate, especially filenames and IP Addresses. Verify that the TFTP server is on and the loadable file is in the TFTP server's public directory. Verify that you have still have connectivity and the ChannelWorks Bridge's LEDs are displaying the operational sequence of: Power On - steady, Status - quickly flashing, and Block Sync - steady.

11. Set the startdownload variable of the Download Group to 1 to initiate the operation. The bridge does the following:
    - resets
    - restarts in "download mode"
    - requests the TFTP file to be transferred
    - performs the transfer
    - copies the file into flash PROM
    - performs a checksum on the new image
    - logs the results of the upgrade to NVRAM
    - resets
    - restarts in "bridge mode" using the upgraded software
12. Use the SNMP network manager to check that the software version is set to 2.0. The MIB variable is lcsoftware in the Revision Levels Group.
13. Load and recompile the 2.0 LCB MIB.
14. Place the Field Upgrade Label on the bottom of the unit.

The ChannelWorks Bridge upgrade is complete and the unit is now ready for operation.

Note: If the ChannelWorks Bridge fails the upgrade procedure, it will not reboot. If this should occur, you may have to return the ChannelWorks Bridge using its original shipping container.

Potential Problems

This section identifies some potential problems that may occur while performing an ChannelWorks Bridge software upgrade using a TFTP File Server.

If the TFTP file transfer fails during the upgrade the bridge is left with no usable code image. In this case the bridge will need to be reloaded as if it were a nonoperational bridge.

Note: The software makes multiple attempts to perform the transfer. A failed transfer implies a catastrophic failure of the network or the file server.

During the Software Upgrade process nodes running the Ver 1.6 Software will not respond correctly to some SNMP requests made using the enterprise specific MIB compiled for Ver 2.0 Software. You should install and compile the LCB MIB Version 2.0 after the software upgrade is complete.

Although Version 2.0 Software is compatible with Ver 1.6 Software, mixed environments exhibit serious performance degradations. Due to performance considerations, it is not recommended to run a mixture of nodes with Ver 1.6 and Ver 2.0 on the same network at the same time, except during the field upgrade.

During the Upgrade process the ChannelWorks Bridge Version 2.0 Software will reprogram the NVRAM while maintaining the original parameters. However, it is recommended that all units' NVRAM be reprogrammed with the Management Utility Ver 2.0.

When the Ver 2.0 Software reprograms some of the new parameters they are set to defaults values. These defaults may be changed either through Ver 2.0 utility or through SNMP.

Remote Upgrades

Perform the following procedure to upgrade ChannelWorks Bridge software remotely:

1. Connect to the remote management system using FTP over SLIP.
2. Transfer the ChannelWorks Bridge loadable file.
3. Use the local PC to upgrade the software as described above.

Calculating The Loop Delay

Because of large delays in the network, a ChannelWorks Bridge must start its transmission earlier than its assigned transmit opportunity. Loop Delay is the round-trip propagation delay, to the headend and back, that a bridge sees. Thus, two ChannelWorks Bridges transmitting in the same transmit opportunity will have their data reach the headend at the same time.

A bridge must calculate its Loop Delay before it transmits any packets. The bridge accomplishes this by transmitting a Determine Loop Delay Packet. The bridge then times how long it takes to receive its packet back. If it does not return within the maximum latency of the network, the bridge assumes there was a collision, backs off and tries the Determine Loop Delay Packet later.

The ChannelWorks Bridge NVRAM parameter Maximum Loop Delay must be set equal to or greater than the Loop Delay of the bridge that is furthest from the headend. Table 5-1 may be used as a guideline to set the Maximum Loop Delay parameter. Refer to Chapter 3's section, "Modifying A Parameter Using The Default Configuration Data File" for the procedure to use to set the Maximum Loop Delay.

After the furthest bridge is operational, the ChannelWorks Bridge SNMP enterprise specific MIB variable "loop delay in bytes" (lcldinbytes) may be examined to fine tune this parameter.

Table 5-1 Maximum Loop Delay Guide

Max Delay	Km @ .92c	Mi @ .92c	Km @ .87c	Mi @ .87c	Km @ .70c	Mi @ .70c
96	14	9	13	8	11	7
128	21	13	20	12	16	10
192	35	22	33	21	27	17
256	49	31	47	29	37	23
288	56	35	53	33	43	27
384	78	48	73	46	59	37
512	106	66	100	62	80	50
576	120	74	113	70	91	57
768	162	101	153	95	123	77

6

Troubleshooting A ChannelWorks Bridge-Based MAN

Introduction

This chapter describes the ChannelWorks Bridge enterprise specific SNMP MIB variable Support History Log (lcsupporthistoryloginfo and LcHistoryEntry). The Support History Log description is provided to help understand how to diagnose and resolve ChannelWorks Bridge network problems.

The ChannelWorks Bridge Support History Log

The Support History Log is a table of 100 entries written sequentially. When the log reaches the final entry (99) it will wrap around.

Each entry in the log represents a significant event which has occurred to the ChannelWorks Bridge.

The current position of the write pointer to the log is maintained in the variable lcnextentry. You can access the variable from the Support History Log Group (lcsupporthistorylog) of the ChannelWorks Bridge enterprise specific MIB.

The write pointer may be reset to the start of the log by using SNMP to set lcnextentry to 0.

You can use SNMP MIB variable lcresetlog to reset the entire log.

Support History Log Format

Each entry in the log is described as follows:

- index — The position of this entry within the log.
- first time — The date and time at which this event first occurred.
- last time — The date and time at which this event last occurred.
- count — The number of consecutive occurrences of this event.
- error level — An indication of the severity of the event which occurred and of the events which will have occurred following this error.
- error id — An identifier representing the specific event which was logged. This corresponds to a software error code. Appendix A provides descriptions of each error ID in the Support History Log.
- module id — An identifier which indicates the specific module reporting the error. Appendix A provides descriptions of each module ID in the Support History Log.
- number of parameters — The number of valid parameters which were stored in the log for this entry (up to a maximum of 5).
- parameters 1 to 5 — The value of the parameter stored.

Note: To conserve space and allow a larger error log, parameters are only stored for the first entry of a specific error id/module id pair. Later entries have the number of parameters set to 0. Similarly when consecutive events are counted in a single entry, the parameters are those from the first occurrence.

Support History Log Entries

The detailed contents of each log entry have been programmed to represent a potential problem with the unit. Entries seen in the Support History Log should be reported to your support organization.

The error level provides good insight into the severity of an entry. The lower the number, the more severe the problem. Information and warning errors represent events which may be expected to occur periodically. They should be reported if they become frequent. Crash level errors are not normally expected.

Support History Log Definition of Terms

SNMP Trap Generation

Initiated by the network manager, SNMP operations can generate get, getnext or set requests to the SNMP agent resident in the bridge.

An SNMP trap is a mechanism by which the bridge can notify an SNMP manager of an event asynchronously (without waiting for the manager to send a request to the bridge). This mechanism is used to generate traps to the manager on such significant events as reset of the bridge, certain errors occurring, and completion of a memory dump.

Memory Dump

The ChannelWorks Bridge can dump the contents of its memory to a file server over the Ethernet or cable TV networks. In order for this to operate, the Dump Server IP Address and dump filename must be configured in the bridge.

The system designated as the dump server must be running a TFTP server at the time the dump is requested. The mechanism to cause a dump to occur is as follows:

1. An error occurs at a level for which a memory dump is specified.
2. The bridge generates a TFTP write request to the TFTP server
3. The server acknowledges the write request
4. The memory is transferred to the TFTP server and stored in the filename specified.

Appendix A

Support History Log Error And Module IDs

Introduction

This Appendix provides descriptions of the Support History Log's Error and Module IDs. Tables A-1 through A-6 describe each Error ID recorded by the Support History Log. Table A-7 describes each Module ID recorded by the Support History Log.

For descriptions of the Error and Module IDs' purposes, refer to Chapter 6, "Troubleshooting A ChannelWorks Bridge Based MAN."

Table A-1 Support History Log Error IDs

Error ID	Description
retrieve	an error occurred while trying to retrieve an item from a queue
Bpdu	bad "bridge protocol data unit" received by the spanning tree task
ITM	an invalid item type was retrieved from a queue
no Tx Buff	no transmit system buffer was available
no Rx Buff	no receive system buffer was available
dealloc	an error occurred when trying to deallocate a transmit system buffer
no sonic TDA	no transmit descriptor was available to transmit a system packet
alloc	an error occurred when trying to allocate a transmit system buffer
dealloc part	an error occurred when trying to allocate a receive system buffer
resource wait	an error occurred when trying to get a shared resource
resource release	an error occurred when trying to release a share resource
TRIE Insert	unable to add an entry to the filtering database
bad Sleep	an error occurred while a task was trying to go to sleep
no asic TDA	no transmit descriptor was available to transmit a system packet
bad Send	an error occurred when attempting to enqueue an item to a task
bad SW_Upgrade	an error occurred during a software upgrade
bad trap	an error occurred when attempting to generate a trap
SW Upgrade	an error occurred during a software upgrade
Trie DeAlloc	an error occurred when deallocating a partition used by the filtering database

Table A-1 Support History Log Error IDs (cont.)

Error ID	Description
bad frame	a frame addressed to the bridge was received with an unexpected type
SCC Tx q over	an error occurred when trying to enqueue an item to the serial line transmit queue
SCC Tx error	a serial line transmit error occurred
SCC Rx error	a serial line receive error occurred
Asic scoreboard	an error while attempting to free a data path buffer for the asic
Sonic scoreboard	an error while attempting to free a data path buffer for the sonic
no memory	not enough memory was available during initialization
blew prom	the software image has been written to the flash proms
sys Tx dealloc	an error occurred when trying to deallocate a system transmit buffer
start fail	an error occurred when trying to start a task (software upgrade watchdog timer task)
SW upgrade time-out	abnormal time-out occurred during software upgrade
power on diag err	an error occurred during power on diagnostics
modem init	a modem error has been detected
bad sys Tx block	an invalid buffer was detected by the routine to allocate a system transmit buffer
SNMP reset	the unit was reset by an SNMP set
bad ASIC Tx status	an error occurred when the asic attempted to transmit a packet
transit t/o	a time-out occurred in the max transit delay processing routine while waiting for the asic transmitter to go idle

Table A-1 Support History Log Error IDs (cont.)

Error ID	Description
mem checksum	a memory checksum error was detected
high temp on	the temperature alarm turned on
high temp off	the temperature alarm turned off
sonic tx error	an error occurred when the sonic attempted to transmit a packet
dump complete	happens when the upload of memory completes after an error which specifies the dump action occurs
sw upgrade needed	the bridge has reset in a mode indicating a s/w upgrade is required
restart	a restart has occurred
nvram bad	this unit cannot be upgraded from this rev of nvram
loop delay	the unit has established its loop delay
bad delta counter	an error occurred in the block sync algorithm
bad snap	an error occurred in the block sync algorithm
reset UL FSM	the block sync state machine has reset
config parameter	an invalid parameter was detected
FSM/ASIC timing	a timing problem was detected in the block sync algorithm
exception	a processor exception such as address error or bus error has occurred
hello expired	a time-out has occurred when waiting for a hello response
hello stat	an error has occurred in the hello function processing
manager q full	a queue full was detected when trying to enqueue an item to the bridge manager
TFTP	an error occurred during the TFTP portion of the software upgrade

Table A-1 Support History Log Error IDs (cont.)

Error ID	Description
Lost pacer	unit has stopped being the pacer
Lost BS	unit has lost block synchronization
Excessive Pacer attempts	unit has exceeded the maximum number of allowable pacer attempts
T/O establish BS	a time-out has occurred while trying to establish block sync
Achieved BS	the unit has achieved block sync
Achieved Pacer	the unit has become pacer
CATV freq. set failed	the SNMP set to change the frequency has failed due to an invalid password
CATV tx freq changed	the transmit frequency has been changed
CATV rx freq changed	the received frequency has been changed
IP addr(s) not set	the unit's IP address has not been configured
Freq(s) set to 0	the unit's frequencies have not been configured
asic rev	the asic revision code is invalid
invalid entry	an invalid entry in the tx op table has been detected by the asic
exception cleared	an invalid entry in the tx op table has been detected and also cleared due to auto-clear
abort due to x	an 'abort due to X in start field' has been detected by the asic
asic max retries	when attempting to transmit a packet max retries exceeded for the asic has occurred more than 255 times
lo isr	an unexpected interrupt has been detected in the asic "lo" interrupt service routine

Table A-1 Support History Log Error IDs (cont.)

Error ID	Description
tx exception	a transmit exception has been detected by the asic interrupt service routine
hi isr	an unexpected interrupt has been detected in the asic "hi" interrupt service routine
rda exhausted	no rda is available for the asic to receive a data packet
pacer drifts	the last pacer loses synch and re-attempts before the non-pacers lose synch

Table A-2 Support History Log Max Transit Delay Routine Error IDs

Error ID	Description
0x902	packets have been removed from the asic transmit queue due to the max transit delay being exceeded
0x903	packets have been removed from the asic transmit queue due to the max transit delay being exceeded
0x904	packets have been removed from the sonic transmit queue due to the max transit delay being exceeded
0x905	packets have been removed from the sonic transmit queue due to the max transit delay being exceeded

Table A-3 Support History Log Data Path Task Error IDs

Error ID	Description
0x999	unexpected event occurred when data path was recovering from all its buffers getting used up
0xff	unexpected event detected by data path when freeing a descriptor due to filtering of a packet

Table A-4 Support History Log Serial Port Service Routine Error IDs

Error ID	Description
0xa06	an error occurred when trying to enqueue an item to the serial port transmit task
0xa01, 0xa02, 0xa03, 0xa04	an error occurred when trying to enqueue an item to the serial port receive task
0xa05, 0xa07	an error occurred when the serial line isr tried to enqueue an item to the bridge manager task

Table A-5 Support History Log ASIC Interrupt Service Routine Error IDs

Error ID	Description
0x15	asic "hi" interrupt service routine has detected mac receive resource area exhausted and is unable to recover
0x79	a bad block sync buffer pointer was detected by asic "hi" interrupt service routine
0x1a	an error occurred when trying to free a block sync buffer
0x1c	the block sync buffer pointer is pointing past the end of the buffer
0xe4	a bad block sync buffer pointer was detected by asic "lo" interrupt service routine
0x1d	the status field of block sync buffer was invalid
0x1e	the status field of block sync buffer was invalid
0x1f	a bad frame control/length of the block sync buffer was detected and it was not a zero length fragment from which we can recover
0x23	a block sync packet with no timestamp was received
0x24	a block sync that we're not willing to snap to was received
0x148	an error occurred when trying to free a block sync buffer

Table A-6 Support History Log Allocator Error IDs

Error ID	Description
0x1	an error occurred when trying to retrieve an item from the allocator input queue
0x2, 0x3, 0x4	an error occurred when trying to release the high tx queue resource
0x6	an invalid item type was retrieved from the allocator input queue
0xa	max site loop delay is not modulo 32
0xb	max site loop delay is greater than 0x600

Table A-7 Support History Log Module IDs

Error ID	Description
data path task	task that receives and transmits ethernet and unilink data packets and makes forwarding and filtering decisions
spanning tree task	task that implements the 802.1d spanning tree protocol
bridge mgr task	task that handles packets addressed to the bridge including SNMP packets, MOP pacets, and other IP protocol packets
allocator task	task that handles allocation of the bandwidth on the broadband
unilink fsm task	task that implements the block sync protocol
serial Tx task	task that transmits data over the serial port
serial Rx task	task that receives data over the serial port
pacer task	task that handles pacer algorithm
statistics task	task that gathers statistics and calculates rates
timer task	task that implements the timers used by the software
housekeeping task	task that deallocates memory as needed after entries have aged out of the filtering database
upgrade wd task	a watchdog timer task used only during software upgrade
dump task	task that uploads memory to a host after certain errors occur
asic isr	asic interrupt service routine
scc rx isr	serial line receive interrupt service routine
scc tx isr	serial line transmit interrupt service routine
scc isr	serial line interrupt service routine

Table A-7 Support History Log Module IDs (cont.)

Error ID	Description
init code	initialization routines
FDB access	filtering data base routines
s/w upgrade	software upgrade routines
error handler	routines that perform actions on error including logging errors to NVRAM
sonic isr	sonic interrupt service routine
system buffer	system buffer management routines
max transit delay	routines which remove packets from sonic and asic transmit queues when they have exceeded the max transit delay time
nucleus exception	processor exceptions such as address error and bus error

Index