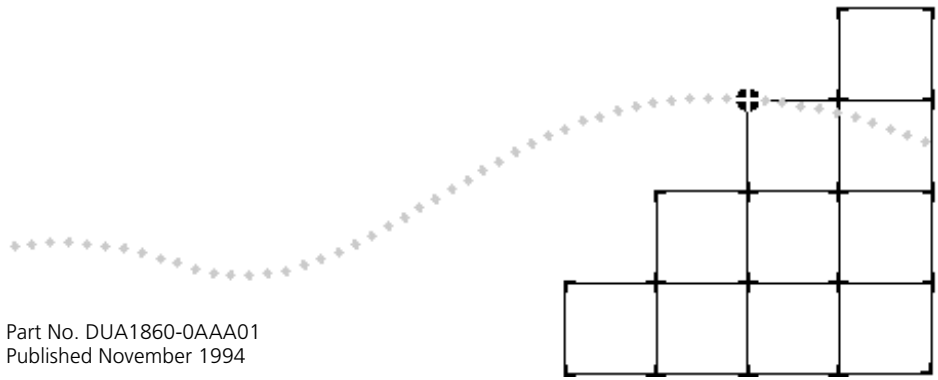
THE LINKBUILDER MSH 4 PORT ETHERNET BRIDGE MODULE USER GUIDE



Part No. DUA1860-0AAA01
Published November 1994

3Com Corporation ■ 5400 Bayfront Plaza ■ Santa Clara, California ■ 95052-8154

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:
If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following restricted rights:

For units of the Department of Defense:
Restricted Rights Legend: Use, duplication or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) for restricted Rights in Technical Data and Computer Software clause at 48 C.F.R. 52.227-7013. 3Com Corporation, 5400 Bayfront Plaza, Santa Clara, California 95052-8145.

For civilian agencies:
Restricted Rights Legend: Use, reproduction or disclosure is subject to restrictions set forth in subparagraph (a) through (d) of the Commercial Computer Software - Restricted Rights Clause at 48 C.F.R. 52.227-19 and the limitations set forth in 3Com's standard commercial agreement for the software. Unpublished rights reserved under the copyright laws of the United States.

3Com and **LinkBuilder** are registered trademarks of 3Com Corporation. Registered trademarks are registered in the United States, and may or may not be registered in other countries.

3ComFacts, Ask3Com, CardFacts, NetFacts, and **CardBoard** are service marks of 3Com Corporation.

CompuServe is a registered trademark of CompuServe, Inc.

The technology behind 3Com's LAN Security Architecture is protected by U.S. patent 5161192 (world patents pending).

Other brand and product names may be registered trademarks or trademarks of their respective holders.

Revision: 01

CONTENTS

2 GETTING STARTED

3 ADVANCED BRIDGING

ABOUT THIS GUIDE

Introduction

This guide contains all the information you need to install and use the LinkBuilder MSH 4 Port Ethernet Bridge Module. It is written for the person responsible for the management and maintenance of the network.

The guide explains:

- How to configure the 4 Port Bridge Module.
- How to identify 4 Port Bridge Module problems and possible solutions to these problems.

The guide does not explain:

- How to design your network.
- How to install and use the LinkBuilder MSH chassis, its Power Supply Units, the Management Module or any other modules. Refer to the guides listed in the Useful Publications section.

The quick reference guide that also accompanies this guide duplicates some of the information from this guide. As it is intended for reference use, we recommend that it is stored in the holder underneath the LinkBuilder MSH chassis.

Throughout this guide, we assume that you are familiar with the concepts and operation of your Local Area Network. For VT100 and Telnet management, we also assume that you are familiar with the VT100 management interface.

How To Use This Guide

The following list shows where to find specific information:

If you are looking for:	Turn to:
An introduction to the LinkBuilder MSH, the 4 Port Ethernet Bridge Module, bridging and filtering	Chapter 1
How to configure a simple bridge	Chapter 2
How to configure an advanced bridge	Chapter 3
How to perform simple bridge monitoring	Chapter 4
Information about further bridge configuration and monitoring	Chapter 5
Information about problem solving	Chapter 6
Information about link settings	Appendix A
Technical information	Appendix B
How to obtain technical support	Appendix C

We recommend that you read Chapter 2 when setting up the bridge for the first time, in a new environment. Read Chapter 3 for more advanced bridge configuration, if necessary. Read Chapter 4 when regularly checking the bridge.

Conventions

The following table lists conventions that are used throughout this guide:

"Enter" vs. "Type"	When the word "enter" is used in this guide, it means type something, then press the [Return] or [Enter] key. Do not press the [Return] or [Enter] key when an instruction simply says "type."
Text represented as `screen display`	`This typeface` is used to represent displays that appear on your terminal screen, for example: `Enter old password:`
Text represented as **`user entry`**	**`This typeface`** is used to represent commands that you enter, for example: `> set pwd`
Keys	When specific keys are referred to in the text, they are shown in brackets, for example [Return] or [Esc]. If two or more keys are to be pressed simultaneously, the keys are linked with a plus sign (+), for example: Press [Ctrl]+[Alt]+[Del].
Italics	In text, italics are used to denote *new terms* or *emphasis*.

Special Messages

A special format indicates notes, cautions, and warnings. These messages are defined as follows:

Notes call attention to important features or instructions.

CAUTION: *Cautions contain directions that you must follow to avoid immediate system damage or loss of data.*

WARNING: *Warnings contain directions that you must follow for your personal safety. Follow all instructions carefully.*

Related Publications

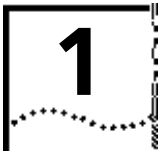
If you need more information about subjects not covered by this guide, you may find it useful to refer to the guides that accompany your other LinkBuilder products.

If you have lost or do not have a particular guide, copies can be obtained from your supplier.

The following guides are particularly useful:

How To Install And Use The LinkBuilder MSH/11
(DUA1800-0AAA0x)

The LinkBuilder MSH Management Module
Volume 1 (DUA1850-0AAA0x)
Volume 2 (DUA1850-0BAA0x)



INTRODUCTION

This chapter contains the following topics:

The LinkBuilder MSH

The LinkBuilder MSH is an extremely versatile chassis-based hub, which enables you to connect and manage large, mixed-technology, mixed-media LANs.

The basis of the LinkBuilder MSH is the chassis, into which a series of network specific modules can be installed, as shown in Figure 1-1. The modules within the chassis connect to a backplane. It is the backplane which allows communication between the various LANs and LAN segments connected to the LinkBuilder MSH. Contact your supplier for the latest list of modules available.

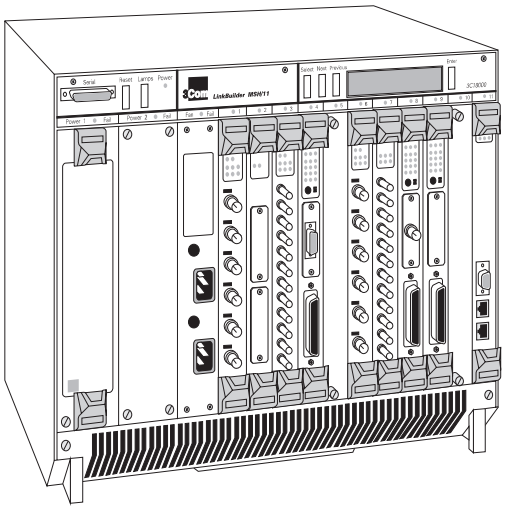


Figure 1-1 The LinkBuilder MSH

The LinkBuilder MSH's backplane contains three Ethernet busses. Ethernet modules can connect to any bus or be independent of the chassis; this is the versatility of the LinkBuilder MSH.

The LinkBuilder MSH 4 Port Ethernet Bridge Module

The bridge module provides a bridge connection between the three Ethernet busses of the MSH and an external port (the bridge module's transceiver module), as shown in Figure 1-2. The bridge's connections are referred to as ports (1, 2, 3 and E).

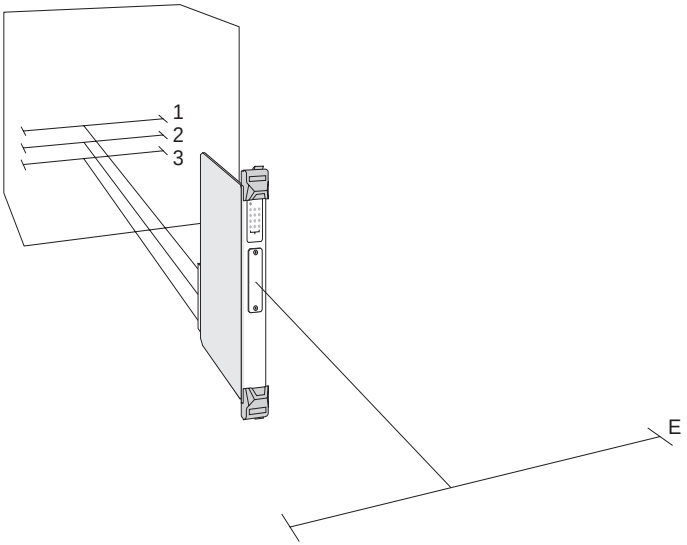


Figure 1-2 The Network Segments

The bridge module provides:

- Connection to each Ethernet bus in the MSH.
- An external connection by transceiver module.
- LEDs for indicating bridge activity and diagnosing possible problems.
- Standard IEEE 802.1 Part D transparent bridging.
- Additional custom bridge filtering:
  - Host-to-Host filtering
  - Host-to-Port filtering
  - Port-to-Port filtering
  - Multicast-to-Port filtering
  - Protocol filtering
  - Bit filtering
- Spanning Tree Algorithm and Protocol (STAP).

Below its top ejector, the bridge has a panel of LEDs that indicate bridge activity, as shown in Figure 1-3.

Each port has a row of three LEDs; transmit (TX), receive (RX) and enabled (EN). Ports with numbers signify the Ethernet bus in the LinkBuilder MSH chassis to which the port is connected. The unnumbered row is for the external port, the Transceiver Module.

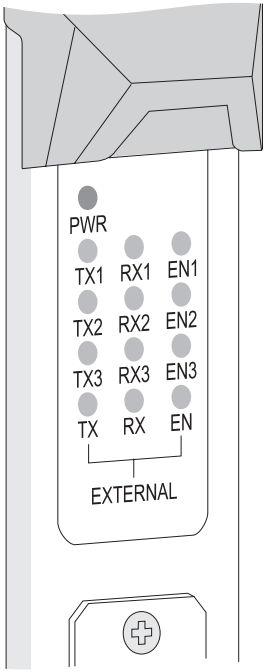


Figure 1-3 The Module's LEDs

You can also use the LEDs to help with diagnosing faults on your system, for more information refer to *Using The LEDs For Fault Diagnosis* on page 6-3.

A Transceiver Module can be fitted to the bridge, providing its fourth port, as shown in Figure 1-4. A range of Modular Transceivers are produced by 3Com, allowing you flexibility when deciding on network connections and cabling:

- 3C12060 Female AUI Transceiver Module
- 3C12065 Fiber Transceiver Module (ST)
- 3C12064 Fan Out Transceiver Module
- 3C12066 Coaxial Transceiver Module
- 3C12060 LinkBuilder Bridge MicroModule

Your supplier will know of any other Transceiver Modules not listed here.

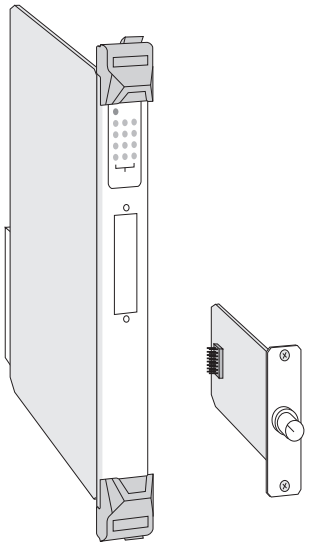


Figure 1-4 The Transceiver Module

Instructions on how to fit a Transceiver Module are given in the manual that accompanies it.

Managing The Bridge

The bridge can be managed using either the VT100 management interface or remotely via SNMP using a suitable application, as shown in Figure 1-5. SNMP provides a subset of the VT100 management facilities.

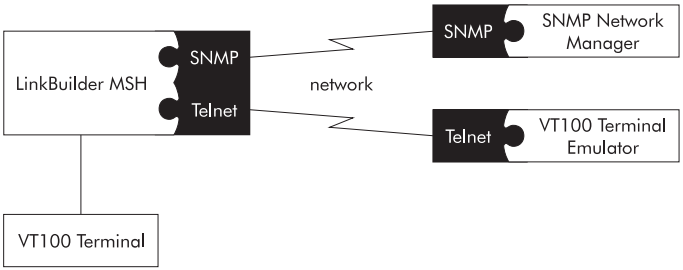


Figure 1-5 VT100 Management

To use the VT100 management interface:

- Connect a VT100 terminal or VT100 terminal emulator directly to the serial port on the display panel of the LinkBuilder MSH.
- Use a VT100 terminal emulator over a network, via Telnet.

To manage the bridge, you must have a LinkBuilder MSH Management Module (3C18500) with software version 2.1 or later installed. If you do not have a Management Module installed, contact your supplier.

Please refer to *The LinkBuilder MSH Management Module* manuals for information on connecting VT100.

Bridging

This section describes bridges and how they work.

Why Use A Bridge?

Bridges provide a way of joining two or more networks together to form a single logical and physical network.

You can overcome various network restrictions that apply to large individual networks by bridging smaller networks together. The bridge remains transparent to the users of these networks.

The original networks that form the bridged network are called *network segments*. The bridge learns, from network traffic, what devices on the network can be reached via each of its ports. It reduces the amount of traffic on each network segment by filtering traffic that does not need to be forwarded to it. Standard filtering is described in *Learning, Filtering And Forwarding* on page 1-12.

You can also apply custom filters to restrict communication through the bridge. This allows you to add some security to your network. Custom filtering is described in *Bridge Filters* on page 1-20.

Resilience can be built into a bridged network. The bridges on the network can control the flow of traffic throughout the network. Resilience is described in *Spanning Tree Algorithm And Protocol (STAP)* on page 1-16.

Local And Remote Bridges

There are two main types of bridge, *local* and *remote*. The LinkBuilder MSH 4 Port Ethernet Bridge Module is a local bridge.

Local bridges are used for bridging networks on the same site, as shown in Figure 1-6.

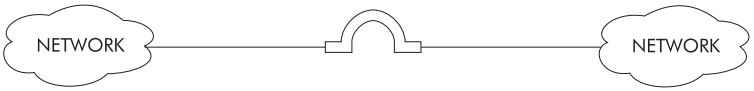


Figure 1-6 Local Bridge

Remote bridges are used for bridging networks across large areas. A remote bridge is often called a *half* bridge because each network connects to half of the remote bridge. The remote bridge halves are connected by a Wide Area Network (WAN) link, as shown in Figure 1-7.

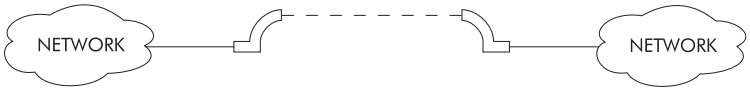


Figure 1-7 Remote Bridge

Both types of bridge have essentially the same operation and functionality.

Bridge Network Topology

The *topology* of a network is essentially its layout; how its component parts are inter-connected. The topology of your network is dependent on the amount of bridges that you use and the way in which you use them. If you use one 4 Port Ethernet Bridge Module, you may have a *star* topology.

In the example setups shown in Figure 1-8 and Figure 1-9, the bridge connects all three MSH busses and an external segment. Figure 1-8 shows how the devices, modules and MSH chassis are physically connected, and Figure 1-9 shows the resulting topology.

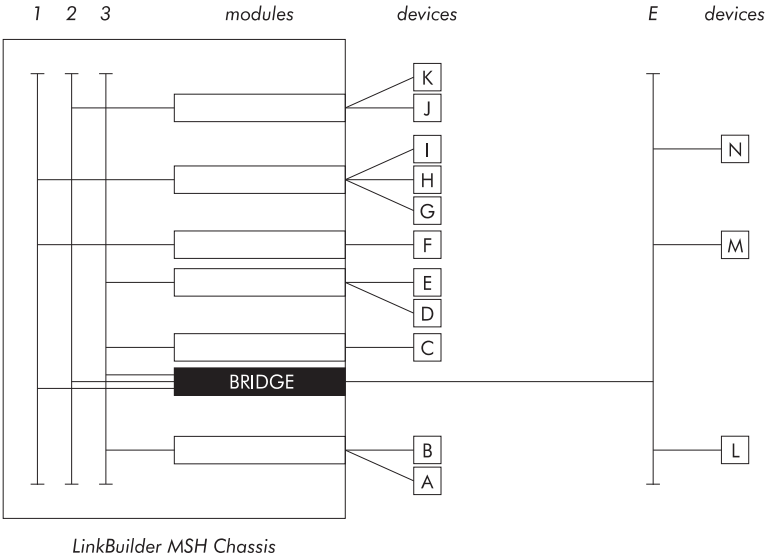


Figure 1-8 An Example Bridge Setup

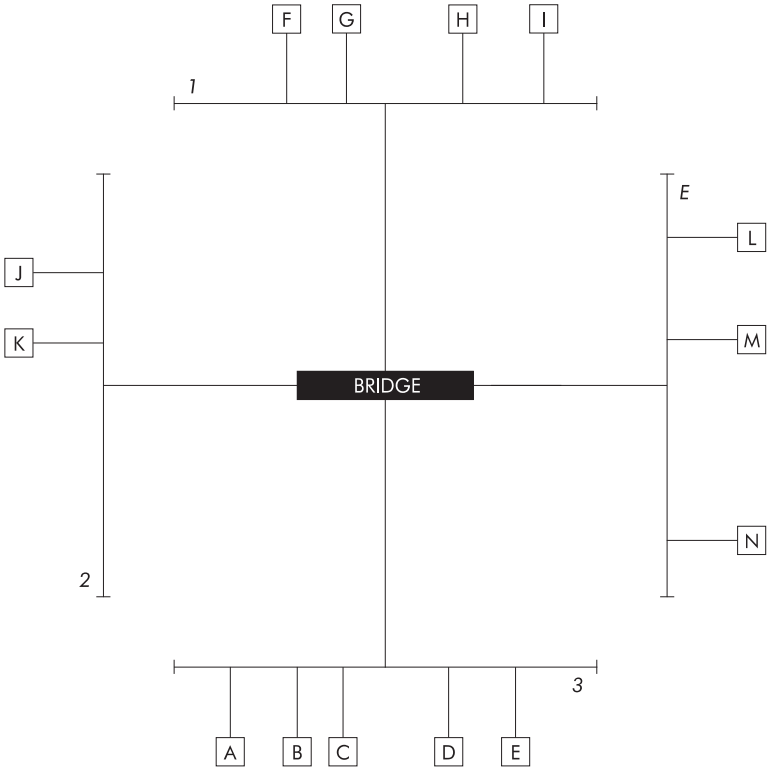


Figure 1-9 An Example Topology

Learning, Filtering And Forwarding

Transparent bridges remain transparent to the network segments, treating them as one overall network. The main operations of a transparent bridge are *learning*, *filtering* and *forwarding*. These operations are 802.1 bridge features and enable it to control the flow of traffic to each network segment.

Devices send information as frames. The two main types of frame are 802.3 and Ethernet. The destination address and source address are contained within the frame, as shown in Figure 1-10.

Destination Address	Source Address	Length	Data	Frame Checksum

802.3 frame

Destination Address	Source Address	Type	Data	Frame Checksum

Ethernet frame

Figure 1-10 Frame Contents

Every time the bridge receives a packet, it looks at the source address and destination address. If the bridge has not previously received a packet on that port from the device, it learns the source address by adding it to a list of device addresses connected to the port. The bridge then compares the destination address to the address lists for all the ports on the bridge. If the destination address appears on the address list of a port that did not receive the packet, the bridge *forwards* (duplicates) the packet to that port. If the destination address appears on the address list of the same port that received the packet, the bridge *filters* (discards) the packet. If the destination address does not appear on any of its address lists, the bridge passes it on to all but the receiving port, called *flooding*.

Figure 1-11, Figure 1-12, Figure 1-13 and Figure 1-14 illustrate how a bridge learns device addresses and uses address lists to reduce unnecessary network traffic.

Figure 1-11: The bridge does not know what devices are on the network.

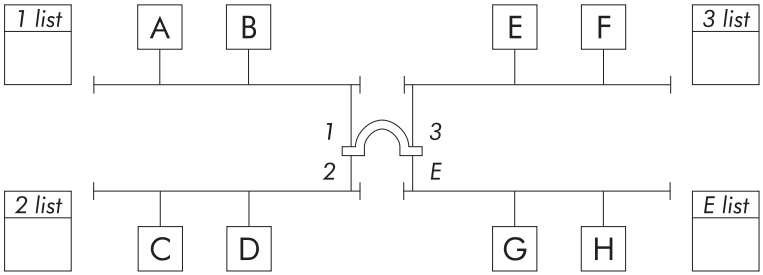


Figure 1-11 An Example Network

Figure 1-12: Device A, connected to port 1, transmits a packet for device B. The bridge learns the address of device A but does not know where device B is, so it passes the packet to ports 2, 3 and E.

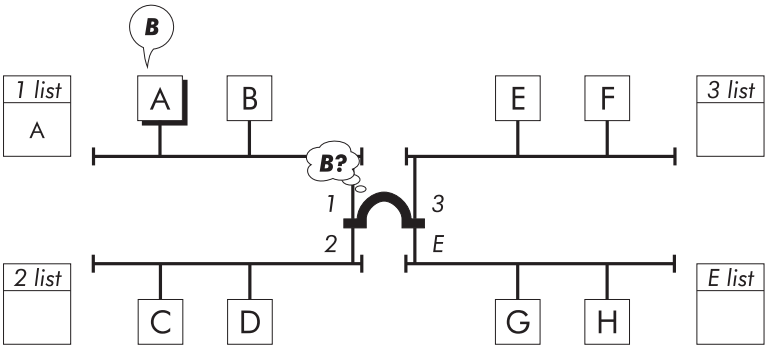


Figure 1-12 Learns A, Passes On Packet

Figure 1-13: Device C, connected to port 2, transmits a packet for device A. The bridge learns the address of device C and recognizes the address of device A, so it forwards the packet to port 1.

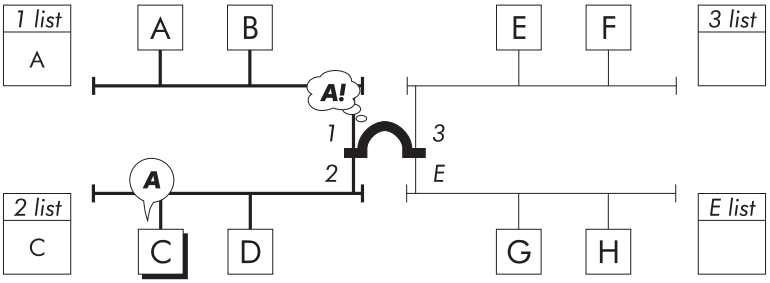


Figure 1-13 Learns C, Forwards Packet

Figure 1-14: Device D, connected to port 2, transmits a packet for device C. The bridge learns the address of device D and recognizes the address of device C is on the same address list, so it filters the packet.

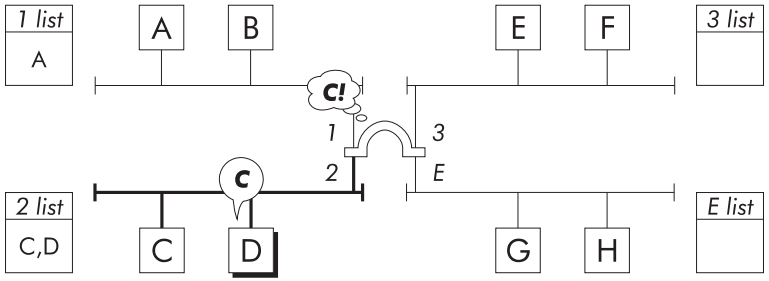


Figure 1-14 Learns D, Filters Packet

The bridge can now effectively control network traffic by forwarding packets only to relevant network segments.

The bridge performs *ageing* on address list entries. If a port has not received a packet from a device within a configured time (the *ageing time*), the device's address will be removed from the port's address list. This helps the bridge to efficiently remember devices that communicate frequently without having to cope with devices that communicate infrequently or are no longer there.

Because the bridge continually learns new addresses and ages out old addresses, it does not have to be reconfigured or initialized when a device is added to the network.

Spanning Tree Algorithm And Protocol (STAP)

You can make your network more resilient by adding bridges and network segments. If a network segment or bridge fails, traffic can still travel through the network by using the additional bridges and network segments.

The key to resilience is the number of paths through the network. Multiple paths, however, result in *active loops*. Active loops introduce redundant traffic to the network, which can quickly degrade overall network performance and, more importantly, breaks network rules.

In the example shown in Figure 1-15, three network segments are connected by three bridges, causing an active loop. Device B transmits a packet for device E. Bridges 1 and 3 receive the packet and forward it. Device E receives the packet from bridge 1 but also receives a copy from bridge 2 (via bridge 3).

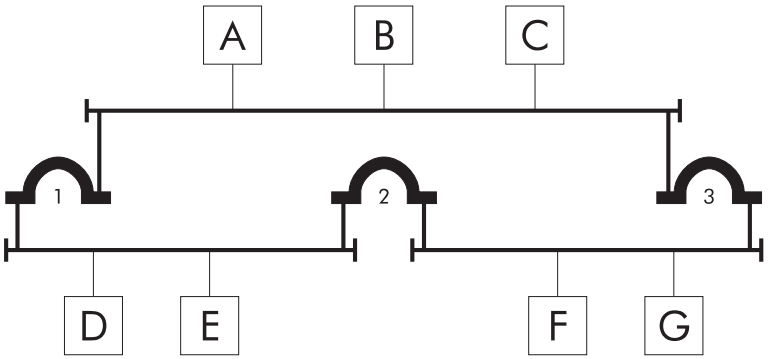


Figure 1-15 An Example Active Loop

A networking standards committee of the Institute of Electronic and Electrical Engineers (IEEE) recognized and solved the problem by introducing the *Spanning Tree Algorithm and Protocol* (STAP). The STAP has become a standard bridge feature.

In a bridged network, a *root bridge* is elected to control the other bridges. The root bridge is made aware of any active loops by consulting the other bridges. The STAP constructs a *spanning tree* which provides unique paths between all devices in the network, and applies it by putting various bridges' ports in to a blocking state, as shown in Figure 1-16.

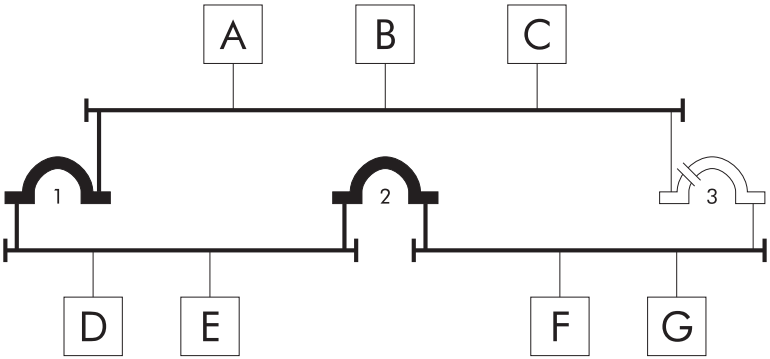


Figure 1-16 Bridge Port Blocking

The STAP is also capable of constructing a new spanning tree should the unique path fail, see Figure 1-17, leading to quick network recovery.

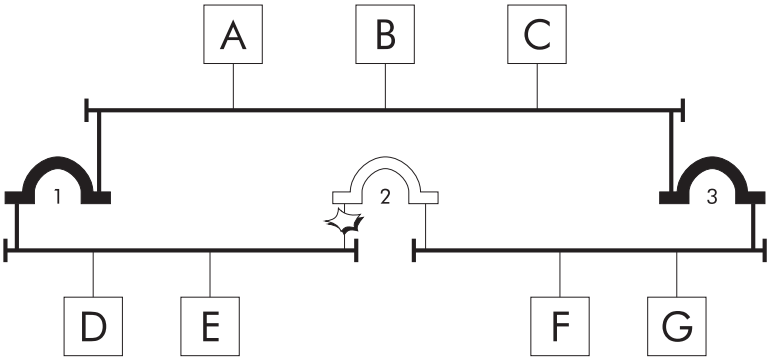


Figure 1-17 Path Fails, Bridge Port Re-enabled

Network resilience obviously leads to some path redundancy, as shown in Figure 1-18.

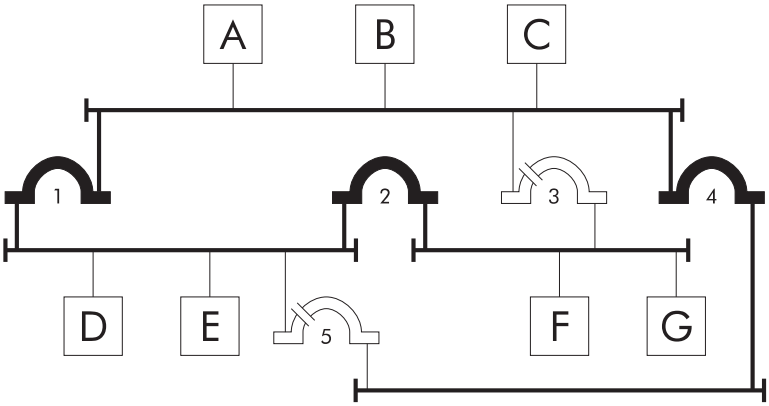


Figure 1-18 Network Resilience

For more detailed STAP information, please refer to the latest revision of the *IEEE 802.1 Part D* standard.

Bridge Filters

The LinkBuilder MSH 4 Port Ethernet Bridge Module allows the use of *customised filtering*, which can be used in addition to basic transparent filtering, as explained in *Learning, Filtering And Forwarding* on page 1-12. It supports the following custom filtering modes:

- Host-to-Host filtering
- Host-to-Port filtering
- Port-to-Port filtering
- Multicast-to-Port filtering
- Protocol filtering
- Bit filtering

This section describes these filtering modes and filtering concepts in general.

What Is Custom Filtering?

Custom filtering lets you selectively define the hosts that can communicate through the bridge. When applied, the bridge *filters* (discards) certain packets based on the contents of *filter sets*. These filter sets can be edited by the bridge operator and are used for indicating what devices' packets are to be filtered.

Figure 1-19, Figure 1-20 and Figure 1-21 illustrate how a bridge performs custom filtering. This particular example shows host-to-port filtering.

Figure 1-19: A filter set for port 2 has been set up allowing device A to communicate through the bridge and out of that port. No other device can communicate through the bridge and out of that port.

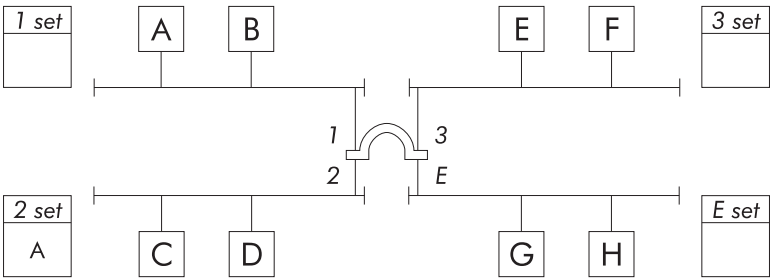


Figure 1-19 An Example Network With Filter Set

Figure 1-20: Device A transmits a packet for device C. The bridge knows that device C is connected to port 2, so it checks that port's filter set. Communication is allowed, so it forwards the packet.

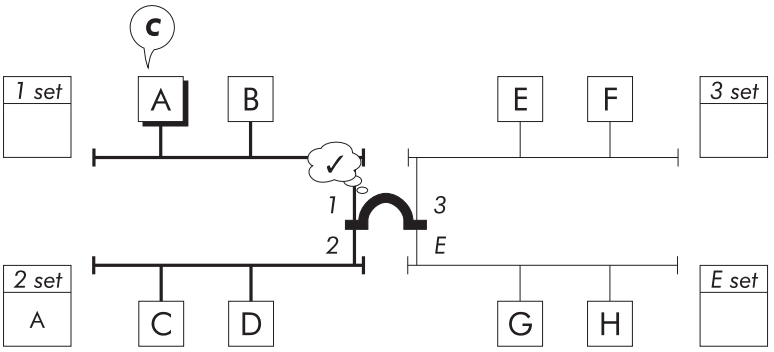


Figure 1-20 Forwards Packet

Figure 1-21: Device B transmits a packet for device C. The bridge knows that device C is connected to port 2, so it checks that port's filter set. Communication is not allowed, so it filters the packet.

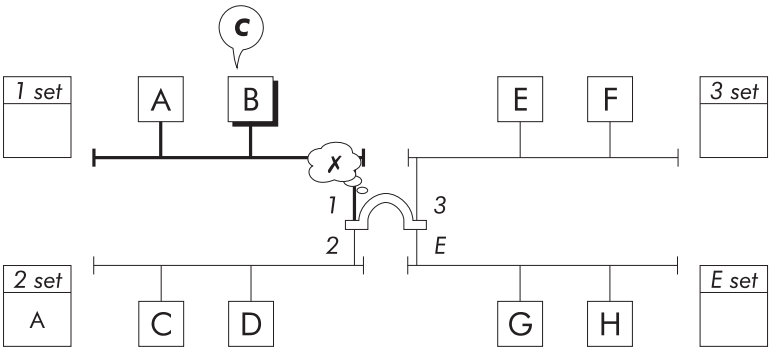


Figure 1-21 Filters Packet

Filter Sets

A *filter set* is a group of devices that are allowed to communicate with each other. The 4 Port Ethernet Bridge Module's default filter sets let all hosts and ports communicate. If you want to restrict communication, you must edit the default filter sets. Each custom filter type has specific filter sets.

Host-to-Host Filtering

A *host-to-host* filter set is a group of devices that are allowed to communicate through the bridge. There are 32 default host-to-host filter sets for you to use. Use each filter set for a specific group of devices, for example, if you have a set for each department in your business, it is easier to manage your filtering.

31 host-to-host filter sets are defined as *inclusion* (sets 2 to 32). One host-to-host filter set is defined as *absolute exclusion* (set 1).

Devices that are members of an inclusion set can only communicate with each other through the bridge.

The absolute exclusion set is a special set used for restricting device communication. A device that is a member of that set is prohibited from communicating through the bridge.

The default host group ensures that no host-to-host filtering takes place before the inclusion filter sets are set up.

If you set up an inclusion set, you must remove the default host group. If you empty an inclusion set, you must replace the default host group.

The default host group must not be added to the absolute exclusion set.

Figure 1-22 illustrates a host-to-host filter example, and shows four network segments connected by a bridge. A filter set has been set up allowing communication between devices A and D only, through the bridge. Every packet received by the bridge has its source address and destination address checked. If both addresses match the addresses in the filter sets, the packet is forwarded.

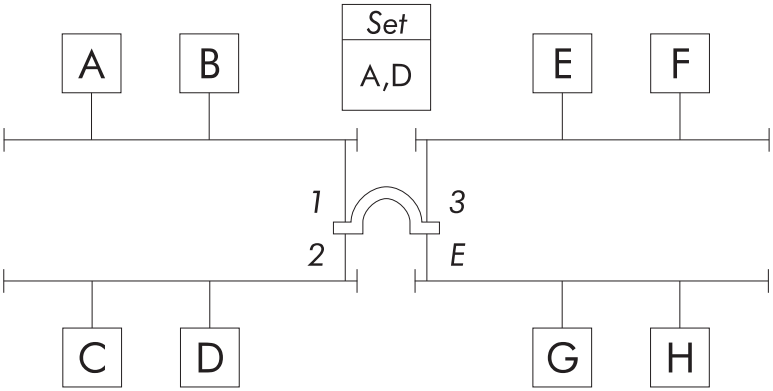


Figure 1-22 Host-to-Host Filtering Example

Host-to-Port Filtering

Host-to-port filters allow the user to define groups of devices that are allowed to communicate through the bridge with devices connected to a specific bridge port. There is a host-to-port filter set for each bridge port.

Host-to-port filter sets can be defined as *inclusion* or *exclusion*.

Inclusion means that devices in the set can communicate out of that port, and all other devices cannot. If the set is empty, no devices can communicate out of that port.

Exclusion means that devices in the set cannot communicate out of that port, and all other devices can. If the set is empty, all devices can communicate out of that port.

The default host group is contained in all host-to-port filter sets following an initialization. Sets default to inclusion. The host-to-port default host represents all hosts except those defined in the host-to-port filter sets. If you include device A in a host-to-port set and delete the default host, then device A will not be able to communicate through other ports unless you also include device A in those ports' host-to-port filter sets.

Figure 1-23 illustrates a host-to-port filter example, and shows four network segments connected by a bridge. The ports' filter sets have been set up, allowing device F to communicate with devices connected to port 1, device H to communicate with devices connected to ports 1 and 3, and device C to communicate with devices connected to port E. Every packet received by the bridge has its destination address checked. If the destination addresses appears in the source address list for that port, the packet is forwarded.

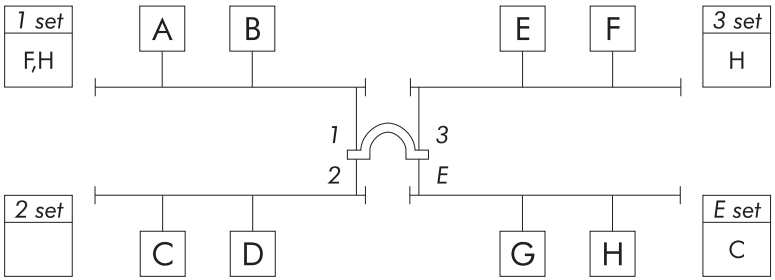


Figure 1-23 Host-to-Port Filtering Example

In the example, the bridge will forward a packet from device H to device A. However, for the bridge to forward a packet from device A to device H, device A's address must be added to port E's filter set.

Port-to-Port Filtering

A *port-to-port* filter set is a group of ports that are allowed to communicate through the bridge. There is a port-to-port filter set for each bridge port.

Figure 1-24 and Figure 1-25 illustrate a port-to-port filter example. Figure 1-24 shows four network segments connected by a bridge. The ports' filter sets have been set up, allowing communication between ports 1 and 2, ports 1 and E, and ports 2 and 3.

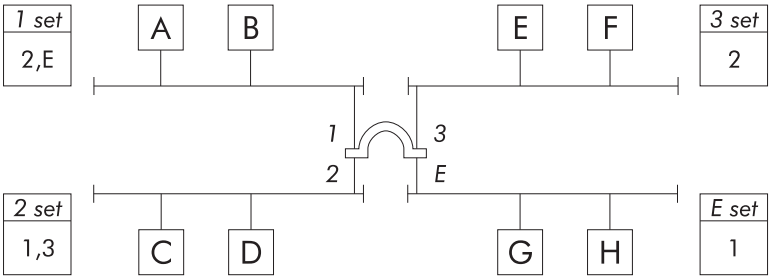


Figure 1-24 Port-to-Port Filtering Example

Figure 1-25 shows the port communications that are allowed.

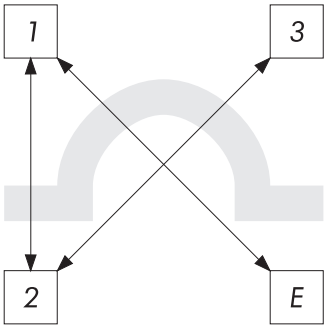


Figure 1-25 Allowable Port Communication

Changes made to port-to-port filter sets are mirrored by the other port-to-port filter sets. For example, if ports 1 and E are added to port 3's filter set, port 3 is automatically added to port 1's and port E's filter sets.

Multicast-to-Port Filtering

A *multicast-to-port* filter set is a group of ports that are allowed to send and receive broadcast and multicast packets from a specific bridge port. There is a multicast-to-port filter set for each bridge port.

The multicast-to-port filter sets operate in exactly the same manner as the port-to-port filter sets, the only difference being that multicast-to-port filter sets are used for broadcast and multicast packets only.

Protocol Filtering

A *protocol* filter set is a group of network protocol filters for which the bridge will permit or deny the forwarding of packets to a specific bridge port. There is a protocol filter set for each bridge port.

For example, if you want to prevent packets using the TCP/IP protocol from being forwarded to the network segment connected to port 2, you would edit port 2's protocol filter set to deny the TCP/IP protocol.

Bit Filtering

Bit filters selectively filter out traffic based on bit values occurring in the first 64 bytes of each frame. This provides extremely flexible filtering. You can test any combination of bits within a six-byte long field falling within the first 64 bytes of the frame and beginning on a byte boundary. You can have up to five input filters and five output filters.

When you set up a bit filter, you define a *bit pattern*. The bit pattern consists of up to 48 bit values (1 or 0), for example, 10111001. The bridge compares this pattern against the pattern found in a specified location for every packet. If the patterns match, the bridge filters or forwards the packet as specified by additional filter information.

Enabling Custom Filtering

You have to enable custom filtering before it becomes effective. You can enable and disable all custom filters or individual custom filters with ease.

As custom filtering can involve multiple checking of packets, it can have an adverse impact on bridge performance in a high traffic rate environment. Therefore, it is best to plan custom filtering carefully, enabling filters only as necessary.

The 4 Port Ethernet Bridge Module performs filtering tests in a specific order:

1 Multicast-to-Port filtering

2 Port-to-Port filtering

3 Host-to-Port filtering

4 Host-to-Host filtering

5 Protocol filtering

6 Bit filtering

In mathematical terms, the filtering operation is characteristic of a logical OR. If the filter sets of any one type indicate that a packet should be filtered out, the bridge will discard it and perform no further tests. You can improve bridge performance by using higher precedence filters when possible.

For example, you may set up port-to-port filter sets to filter out packets between ports 1 and 2. You may then create a host-to-host filter set that includes a device connected to port 1 and a device connected to port 2. These devices will not be able to communicate because their packets will be filtered out by port-to-port filtering.

Simple Network Management Protocol (SNMP)

SNMP is an application-level protocol for managing products such as bridges on TCP/IP networks. You can issue *requests* using an SNMP application. The application passes the requests to the SNMP agent software on the device to be managed. The agent carries out the requests and sends *responses* to the application. Requests and responses are referred to as *SNMP messages*.

The SNMP agent on the bridge allows it to be managed by any SNMP application. This agent complies with RFC 1157, *A Simple Network Management Protocol*.

The agent performs network management functions based on GET and SET operations. These operations retrieve and store values of variables belonging to the managed device. The variables are defined in one or more *Management Information Bases* (MIBs).

MIB variables are encoded in a subset of the data-description language *Abstract Syntax Notation One* (ASN.1), according to the rules specified by the *Structure of Management Information* (SMI). In SMI and ASN.1 terms, a MIB contains *objects*, each of which has an assigned unique name, known as an *object identifier* (OID).

The names actually used in your management application to refer to MIB variables depend entirely on that application and may be different to OIDs.

The bridge supports the following MIBs:

- Internet Standard II, as defined in RFC 1158, *Management Information Base for TCP/IP-Based Internets*
- Internet Bridge MIB, as defined in RFC 1286, *Bridge MIB*
- Internet Ethernet MIB, as defined in RFC 1284, *Definitions of Managed Objects for the Ethernet like Interface Types*

Installation And Removal

WARNING: *Please read the following safety and anti-static information before removing the module from its anti-static packaging.*

Safety Information

To avoid having dangerous equipment:

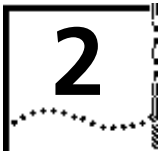
- Installation of this module should be carried out by qualified personnel only.
- This module operates under SELV conditions (Safety Extra Low Voltage) according to IEC 950, the conditions of which are maintained only if the equipment to which it is connected is also operational under SELV.
- The LinkBuilder MSH chassis must be earthed.

Anti-Static Information

To avoid damaging the module:

- Do not remove the module from its anti-static packaging until you are ready to install it into the LinkBuilder MSH chassis.
- Do not touch the pins, leads, connections or any components on the module.
- Handle the module only by its edges.
- Always wear an anti-static wristband connected to a suitable earth point.
- Always store and transport the module in anti-static packaging.

Please refer to the *How To Install And Use The LinkBuilder MSH/11* manual for information on installing and removing the bridge module.



GETTING STARTED

This chapter contains the following topics:

Introduction

This chapter describes setting up the bridge for the first time. If you have not set up the bridge before, or are setting it up again after initializing NVRAM, you should read this chapter.

The chapter contains the following information:

- A general introduction to the VT100 Management Interface, which is used to manage the bridge.
- A description of how to configure a simple bridge that connects up to four network segments. This configuration involves:
  - Logging on and off the bridge
  - Establishing operator accounts
  - Defining bridge information
  - Saving and making changes effective
  - Erasing all the changes
- A descrption of how to assign an IP address to the bridge so that the bridge can be managed remotely via Telnet. This involves:
  - Setting up IP addresses
  - Using Telnet for remote connections
  - Using the Packet Internet Groper (PING) program to test connections
- A description of how to configure the SNMP agent on the bridge so that SNMP applications can obtain information about the bridge. This involves:
  - Configuring the basic characteristics of each community and globally enabling or disabling the Authentication Failure Trap
  - Enabling traps for individual communities and specifying the IP addresses where the traps should be sent

The VT100 Management Interface

The VT100 management interface is used for bridge management. The screens are based on forms and are controlled using special interface control keys.

The bridge has different control keys to the MSH management module. When you log on to the bridge, the bridge control keys take over. The bridge control keys are described in *Bridge Control Keys on page 2-8*.

The screens are grouped hierarchically. For a complete menu map of the bridge screens, see *The VT100 Bridge Menu Map* on page 2-6. The menu map also appears on *The LinkBuilder MSH 4 Port Ethernet Bridge Module 3C18600 Quick Reference Guide*, that accompanies this manual.

This chapter assumes that you are familiar with the VT100 management interface.

Please refer to *The LinkBuilder MSH Management Module* manual for information on connecting VT100 and VT100 via Telnet. The manual also describes VT100 screen conventions and VT100 control keys.

The VT100 Bridge Screens

The VT100 bridge screens have the same general layout. The components of a bridge screen are shown in Figure 2-1.

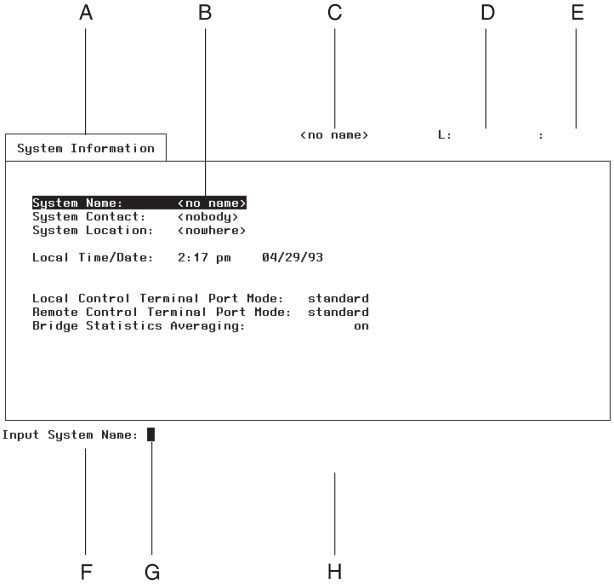


Figure 2-1 Bridge Screen Components

The components are:

A - Screen title. The boxed words starting in the top left hand corner of the screen.

B - Highlight. A dark or bright bar over the input field that receives the information you enter into the input area.

C - System name. The name you give your bridge on the System Information screen.

D - Local login identifier. The name of the user currently locally logged on to the bridge.

E - Remote login identifier. The name of the user currently remotely logged on to the bridge.

F - Input area. The line below the screen area provides the data entry location for input screens. The area starts with a short description of the highlighted field. You enter the value in the input area, where you can change or correct your typing as necessary. When you press [Enter] or [Return], your input area appears in the highlighted field. Your terminal may beep for an inappropriate entry.

G - Prompt. The small blinking box that shows where you are in the input area.

H - Message area. The line underneath the input area that displays useful information. It usually displays the bridge's software version and release date. If you make an error, it displays a reason.

The VT100 Bridge Menu Map

The VT100 bridge menu map, as shown in Figure 2-2, shows the links between the bridge management screens. The *italic number* at the bottom left of each screen box is the page in this manual, where you will find the description of that screen.

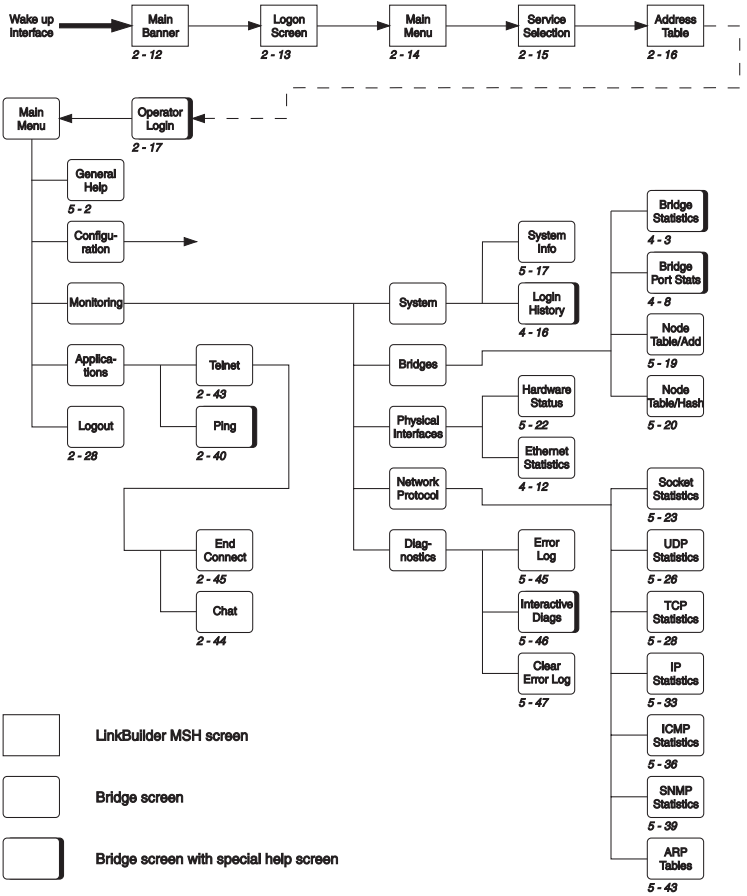
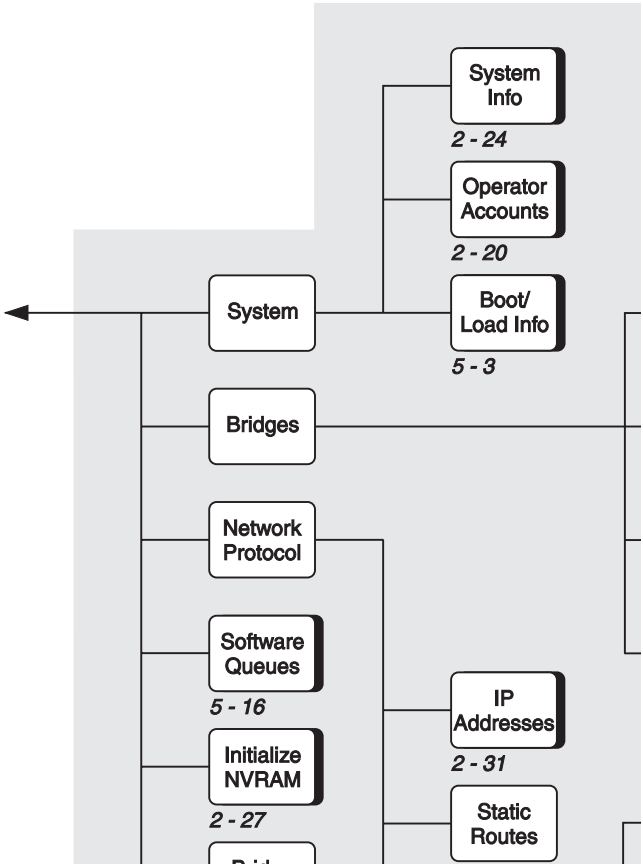


Figure 2-2 The VT100 Bridge Menu Map

Operators with Administrator privileges are unrestricted. Operators with Operator privileges cannot configure the bridge, initialize NVRAM, or reset the bridge (the Administrative Screens).



Bridge Control Keys

There are special control keys for operating the bridge. These are different to the MSH management module control keys and should be used from the time you log on to the bridge. For [Ctrl] key sequences, hold down the [Ctrl] key while pressing the specified key. For [Esc] key sequences, press [Esc] and then press the specified key.

The bridge control keys are described in Table 2-1:

Table 2-1 Bridge Control Keys

Key	Description
Help	
[?] [Esc] [H]	Displays a help screen. Many screens have their own help screens. The general help screen appears for screens without specific help screens.
Quick keys	
letters	Selects the menu item preceded by the character. You do not need to press [Return]. For example, [B] will take you from the Main Menu to the Configuration menu. [B] [A] [A] will take you from the Main Menu to the System Information screen.
Select or confirm entry	
[Return] [Enter]	Selects the current menu item or confirms the entry for a field and moves to the next entry field.
Previous screen	
[Ctrl] + [Z] [Esc] [P]	Returns you to the previous screen or menu.

Table 2-1 Bridge Control Keys

Key	Description
Return to Main Menu	
[Ctrl] + [T] [Ctrl] + [C] [Ctrl] + [Y] [Esc] [T]	Returns you to the Main Menu.
Return to MSH Management Module	
[Ctrl] + [P]	When logged on locally, this returns you to the MSH Management Module screens. We recommend you log off the bridge before entering this command.
Move up	
[Up Arrow]	Selects the previous menu item or highlights the previous entry field.
Move down	
[Down Arrow]	Selects the next menu item or highlights the next entry field.
Move left	
[Left Arrow]	Moves the cursor left one character in the entry field.
Move right	
[Right Arrow]	Moves the cursor right one character in the entry field.
Delete character	
[Backspace] [Delete] [Ctrl] + [D]	Deletes the character to the left of the cursor in the entry field. [Ctrl] + [D] has a different use when the extended bridge control keys are in use.
Delete all	
[Ctrl] + [U]	Delete all the input in the entry field.

Table 2-1 Bridge Control Keys

Key	Description
Refresh screen	
[Ctrl] + [V] [Esc] [V]	Refreshes the screen.
Next step	
[Esc] [N]	Takes you to the next menu or screen, or returns you from help. Using this from a menu, takes you to the screen associated with the highlighted item.
Interrupt Telnet	
[Break]	Interrupts a Telnet connection without waiting for it to time out.
Resume serial communication	
[Ctrl] + [Q]	Resumes serial communication if accidentally turned off (XOFF).

Simple Bridge Configuration

This section describes how to configure a simple bridge that connects up to four network segments.

Ensure all bridge connections are in place before you start.

Initially, the bridge has no IP address. Without a unique IP address, it cannot be remotely managed, so you must first log on to the LinkBuilder MSH, then log on to the bridge, then set up a unique IP address.

This simple configuration describes:

- Logging on and off the bridge
- Establishing operator accounts
- Defining bridge information
- Saving and making changes effective
- Erasing all configurations

You will need to configure the bridge for your particular installation. Write down all the changes that you make, so you have a configuration record. We recommend that before configuration, you look at the different bridge screens to understand how they are linked and what information they require.

Most screens have their own help screen. If a screen does not have one, the general help screen is displayed.

Logging On To The LinkBuilder MSH

Logging on to the LinkBuilder MSH is also described in *The LinkBuilder MSH Management Module* manual.

Connect to the LinkBuilder MSH. The Main Banner appears, as shown in Figure 2-3.

Press [Enter] to continue.

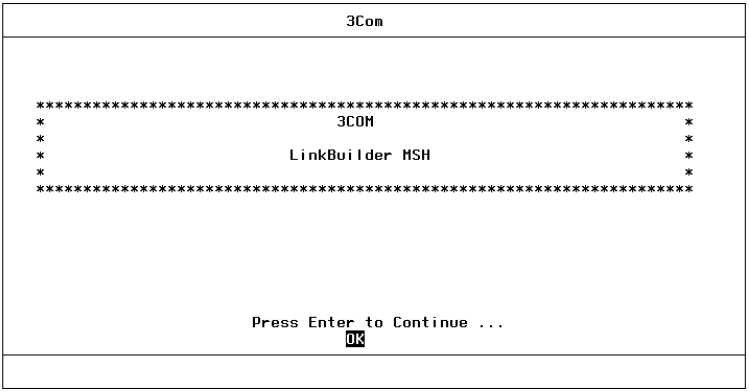


Figure 2-3 LinkBuilder MSH Main Banner

The Logon screen appears and stays displayed until a valid User Name and Password have been entered, as shown in Figure 2-4.

Enter a User Name and Password for the LinkBuilder MSH.

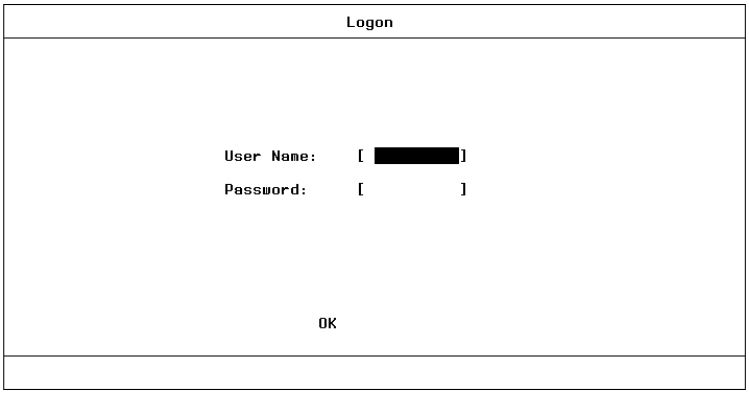


Figure 2-4 LinkBuilder MSH Logon Screen

When you are logged on to the LinkBuilder MSH, the Main Menu appears, as shown in Figure 2-5. It offers various LinkBuilder MSH management options. The LOGOFF option closes down the session, allowing the interface to 'sleep'.

Select SERVICE SELECTION.

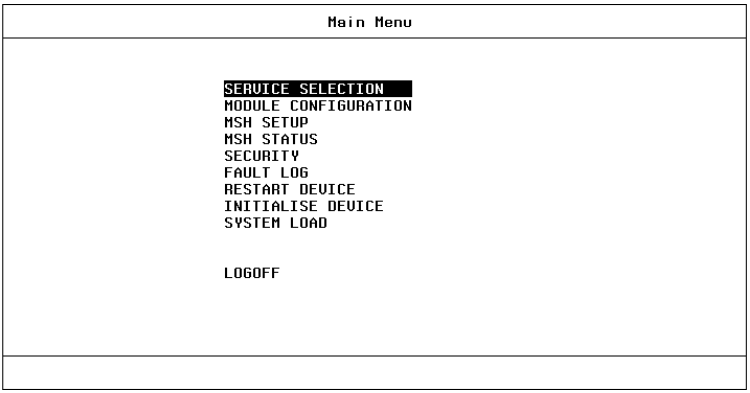


Figure 2-5 LinkBuilder MSH Main Menu

The Service Selection screen appears, listing all the services within the LinkBuilder MSH Chassis with the number of the slot or backplane to which it is attached, as shown in Figure 2-6.

Highlight 4 PORT .3 BRIDGE, press [Space] and select **OK** to select the LinkBuilder MSH 4 Port Ethernet Bridge Module.

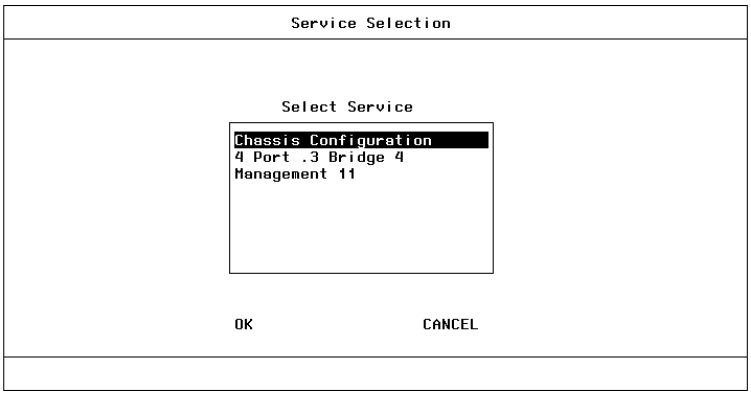


Figure 2-6 LinkBuilder MSH Service Selection

If the 4 Port Ethernet Bridge Module does not appear, either the module is self-testing, has been incorrectly installed, or the MSH management agent software is not version 2.1 or later.

The Address Table screen appears, showing default address information for the bridge, as shown in Figure 2-7. If the bridge's IP address is unconfigured, a random IP address is shown.

Select MANAGE to continue.

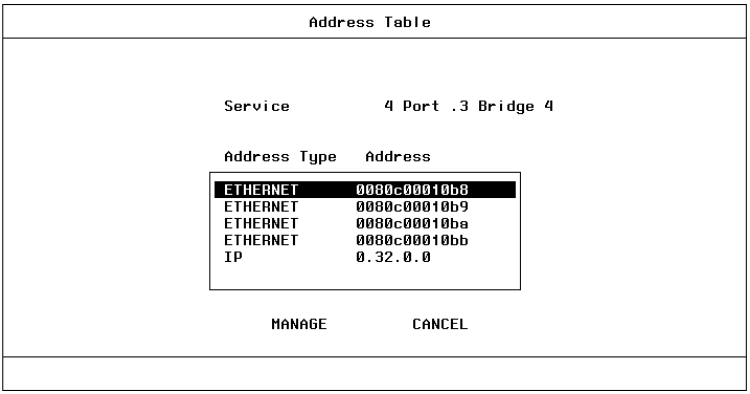


Figure 2-7 LinkBuilder MSH Address Table

Logging On To The Bridge

When you connect to the bridge, the Operator Login screen appears, as shown in Figure 2-8. Until it is configured, the bridge has no Operator IDs or Passwords, meaning that the bridge has no security. You must set up an administrator account before any security becomes active. This configuration includes this set up.

If no accounts have been set up, press [Enter] for both fields.

If you have an account with administrative privileges, enter the Operator ID and Password. If you have accounts with administrative privileges but have forgotten the Operator IDs and Passwords, you may have to reset the bridge's configuration to default values, see Appendix A.

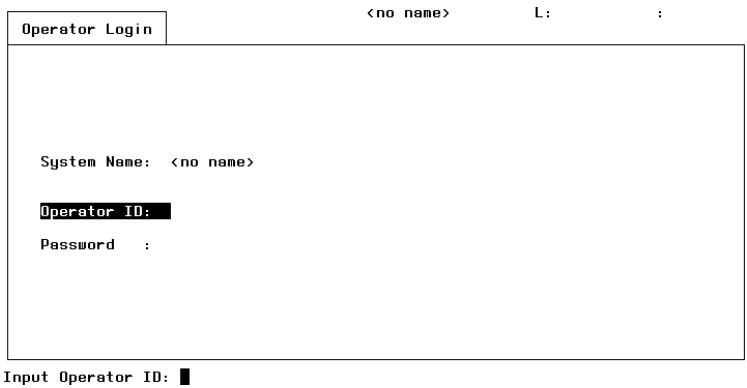


Figure 2-8 Operator Login

Operator ID: Text Field. The operator ID is a string of one to eight alpha-numeric characters and is case sensitive.

Password: Text Field. The password is a string of one to eight alpha-numeric characters and is case sensitive. One X will appear for each character typed.

Establishing Operator Accounts

When you have logged on to the bridge, the bridge's Main Menu appears, offering various management options, as shown in Figure 2-9.

The bridge's security is disabled if no administrative operator accounts have been set up, so you should set up these accounts first.

Select CONFIGURATION.

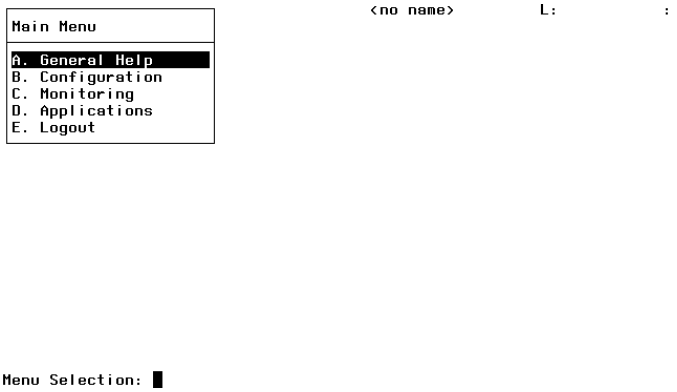


Figure 2-9 Main Menu

The Configuration menu appears, as shown in Figure 2-10. You can access all the configuration screens and sub-menus from this menu.

Select SYSTEM.

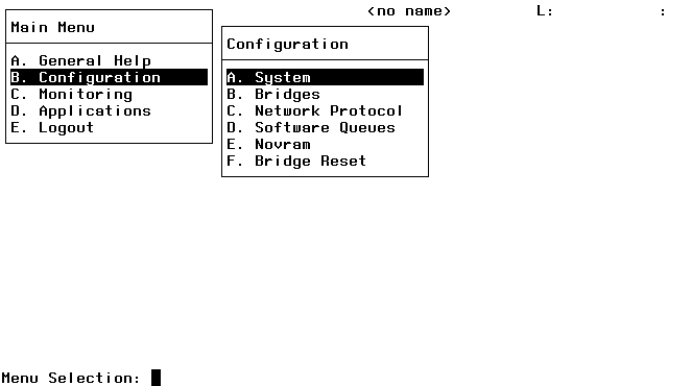


Figure 2-10 Configuration Menu

The System menu appears.

Select OPERATOR ACCOUNTS from the System menu.

The Operator Accounts screen appears, listing the operator accounts that are set up for the bridge, see Figure 2-11. You can set up 60 operator accounts for the bridge.

Enter the number of the operator account you want to set up.

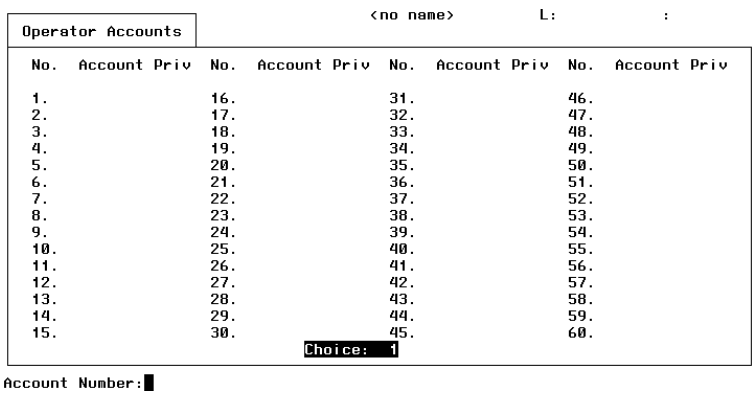


Figure 2-11 Operator Accounts

No: Display Field. The account numbers of the 60 accounts.

Account: Display Field. The operator ID for the account. This can be changed with the Edit User Accounts screen that follows on from this screen. Blank entries indicate that the account has not been assigned.

Priv: Display Field. The designated privilege for the account. A is for administrator and 0 is for operator. Accounts with operator privilege cannot configure the bridge, initialize NVRAM, or reset the bridge.

Security checking is disabled if no operators are allocated administrator privileges. This prevents a lock out from configuration areas.

Account Number: Text Field. Enter the account number of the operator you want to set up. You can set up from 1 to 60 accounts. After entering an account number, the Edit User Accounts screen appears.

The Edit User Accounts screen appears with information on the operator account you entered in the Operator Accounts screen, as shown in Figure 2-12. You use this screen for entering and modifying operator account information. Any existing information is displayed.

Set up operator accounts by entering an Operator ID, Operator Privilege and Password (repeat the Password for verification). To set up a different operator account, enter its Account Number. When you have finished, return to the System menu.

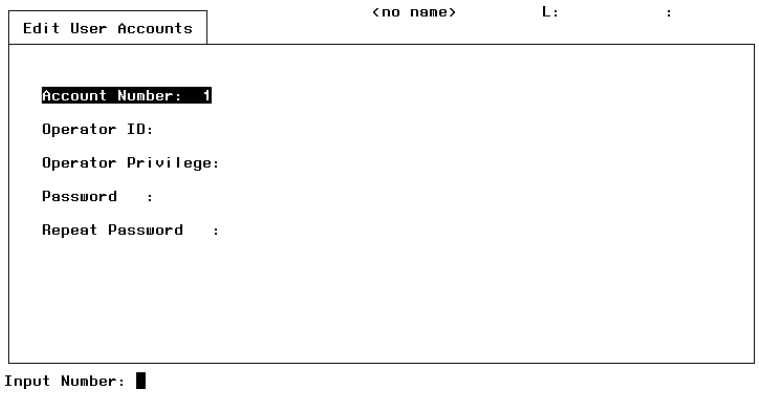


Figure 2-12 Edit User Accounts

Account Number: Text Field. The number of the operator account. To configure a different account, enter its account number and the Edit User Accounts screen changes to display this account's information. This saves having to return to the Operator Accounts screen. The account number can be from 1 to 60.

***Operator ID*:** Text Field. The operator's ID is a string of one to eight alpha-numeric characters. When entered elsewhere, the operator ID is case sensitive. Changes to this field are only saved during a bridge reset, and take effect from then on.

Operator Privilege: Choice Field (A / 0). Designate the privileges for the operator. A is for administrator and 0 is for operator. Bridge operators can be set up with either Administrator or Operator privileges. Operators with Administrator privileges are unrestricted. Operators with Operator privileges cannot configure the bridge, initialize NVRAM, or reset the bridge.

Security checking remains disabled if no operators are allocated administrator privileges. This prevents a lock out from administrative areas.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Password: Text Field. The password is a string of one to eight alpha-numeric characters. When entered elsewhere, the password is case sensitive. One X will appear for each character typed. Changes to this field are only saved during a bridge reset, and take effect from then on.

Adding Bridge Information

You should provide general device information for your bridge the first time you set it up. This information is required by all MIB II conformant devices and is generally useful because it includes the location of the bridge and the name of the person responsible for it (useful if the bridge is not operating correctly).

Select SYSTEM INFORMATION from the System menu.

The System Information screen appears, as shown in Figure 2-13. You use this screen for entering and modifying device information. Any existing information is displayed.

Enter the information and, when you are sure it is correct, return to the Configuration menu.

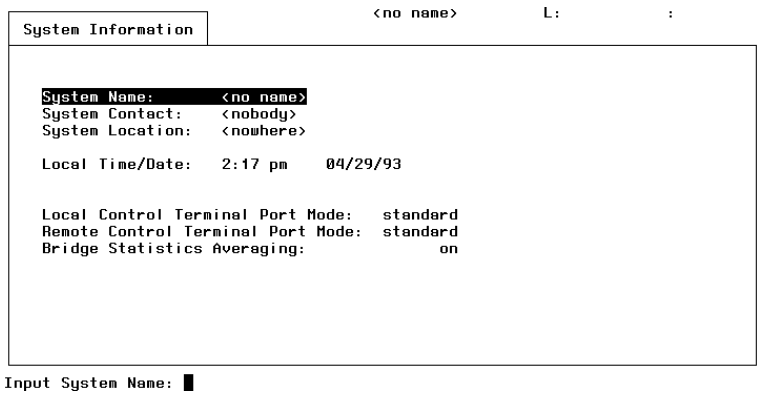


Figure 2-13 System Information

System Name: Text Field. Enter a name for the bridge. This is a string of 1 to 16 characters. Changes to this field are only saved during a bridge reset, and take effect from then on.

System Contact: Text Field. Enter the name of the person who is responsible for the bridge. This is a string of 1 to 16 characters. Changes to this field are only saved during a bridge reset, and take effect from then on.

System Location: Text Field. Enter the physical location of the bridge. This helps if ever it needs to be located. This is a string of 1 to 16 characters. Changes to this field are only saved during a bridge reset, and take effect from then on.

Local Time/Date: Text Field. Enter the local time and date. Changes to this field are only saved during a bridge reset, and take effect from then on.

Local Control Terminal Port Mode: Text Field. This field should be set to `standard`. Do not change this field.

Remote Control Terminal Port Mode: Text Field. This field should be set to `standard`. Do not change this field.

Bridge Statistics Averaging: Text Field (`on` / `off`). Set the method by which statistics are displayed on the Bridge Statistics and Bridge Port Statistics monitoring screens. If you want the accumulated statistics averaged per second, specify `on`. If you want the total accumulated statistics (since power up), specify `off`.

Saving And Making Changes Effective

Some of the changes you can make to the bridge are not saved if you simply log off. However, not all fields require a bridge reset to save them and make them effective. The field descriptions that accompany each screen, in this manual, describe the necessary procedures.

Any changes that are saved, are saved in NVRAM (Non Volatile Random Access Memory). Changes in NVRAM are remembered over a power cycle.

Select BRIDGE RESET from the Configuration menu.

The Bridge Reset screen appears, as shown in Figure 2-14. It reminds you of its effect and prompts you for a yes/no answer. Enter yes to reset the bridge or no to return to the Configuration menu.

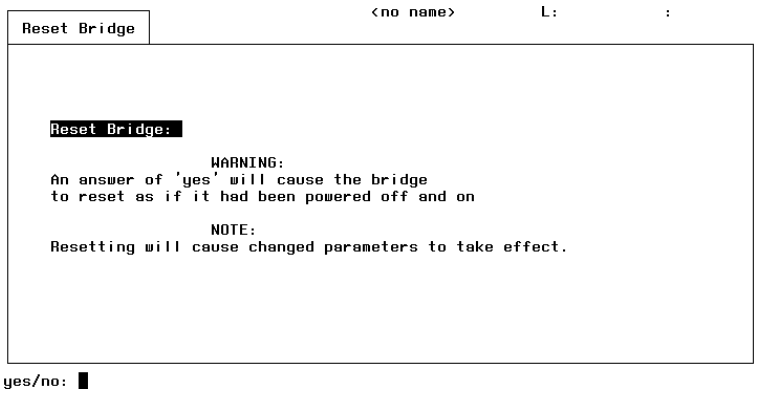


Figure 2-14 Bridge Reset

Erasing All Changes

If you want to erase all the changes made to the bridge since logging on, simply log off the bridge. However, if you want to erase all the changes ever made to the bridge, you must initialize NVRAM (Non Volatile Random Access Memory) and reset the bridge. If you initialize NVRAM but do not reset the bridge, logging off instead, the changes will not be erased.

Select INITIALIZE NOVRAM from the Configuration menu.

The Initialize NOVRAM screen appears, as shown in Figure 2-15. It warns you of its effect and prompts you for a yes/no answer. Enter `yes` to agree to initializing NVRAM or `no` to return to the Configuration menu.

If you enter `yes`, the Reset Bridge screen appears. This screen warns you of its effect and prompts you for a yes/no answer. Enter `yes` to initialize NVRAM or `no` to return to the Configuration menu.

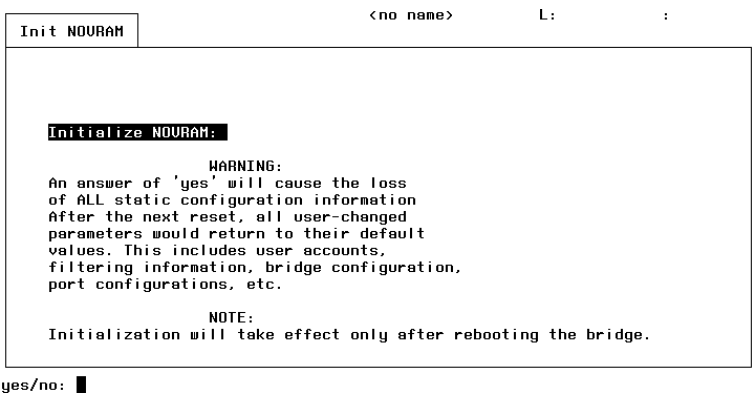


Figure 2-15 Initialize NVRAM

Logging Off The Bridge

Selecting LOGOUT from the Main Menu will log you off the bridge and return you to the display you had before logging on. Any changes that have been made since logging on will be erased. Most fields, but not all, require a bridge reset to save them and make them effective, see *Saving And Making Changes Effective* on page 2-26.

We recommend that you log off the bridge before returning to the MSH Management Module screens.

IP Address Configuration

This section describes how to assign an IP address to the bridge. When the bridge has an IP address, you can remotely manage it via Telnet, and will not need to go through the LinkBuilder MSH. Telnet is a TCP/IP application. SNMP also requires the bridge to have an IP address.

This simple configuration describes:

- Setting up IP addresses
- Using Telnet for remote connections
- Using PING to test connections

Every IP network device is identifiable by its unique IP address (Internet Protocol address). An extension to the IP addressing scheme allows you to divide networks into subnetworks. The subnet mask identifies which parts of the IP address denote the network (network number) and which denote the host (host number).

IP devices can only communicate with devices on different networks via IP routers (gateways). A subnet mask is not needed unless the network is IP routed.

If you have a private IP network, you can assign any IP address you like. However, if you are connecting to the Internet, your IP address must be unique. Network numbers can be assigned by the Network Information Center (NIC). This organization assigns a globally unique network number to each network that wishes to connect to the Internet. The host numbers are then assigned by your local system administration.

Bridge Connections

The Telnet protocol is used for remotely logging on to a device. The following requirements must be met for remote login:

- You must have an account on the host and you must know the operator ID and password for that account.
- You must know either the host name or IP address of the host. You can only use the host names configured in your local IP Host Table screen.
- If you are logging on from a remote host, the terminal must support VT100.

Logging On To The Bridge

You can log on to the bridge locally (via the LinkBuilder MSH) and remotely (via Telnet). The bridge can accept:

- Either a local or a remote log on.
- Both a local and a remote log on.

The bridge cannot accept:

- Multiple local or remote log ons.

Telnet From The Bridge

The bridge has Telnet capabilities, allowing you to Telnet from the bridge to another device. The bridge allows you to:

- Telnet from the bridge if you have locally logged on. The bridge can still accept a remote log on.

The bridge does not allow you to:

- Have multiple Telnet sessions from the bridge.
- Telnet from the bridge if you have remotely logged on.

Setting Up Remote Access

Initially, the bridge has no IP addressing information. When set up, the IP address identifies the bridge. The IP Addresses screen is used for setting up an IP address for the bridge so that other devices can communicate with its management agent.

Select CONFIGURATION from the Main Menu. Select NETWORK PROTOCOL from the Configuration menu. Select IP ADDRESSES from the Network Protocol menu.

The IP Addresses screen appears, displaying two tables, Active and Next Reset, as shown in Figure 2-16. The Active table shows the IP Address and Subnet Mask that are currently used. The Next Reset table allows you to enter a new IP Address and Subnet Mask, which will be used after the bridge is next reset. Highlight the field you wish to change and an area for entering the new information will appear at the bottom of the screen.

Enter your address information. A Subnet Mask is not needed unless the network is IP routed. After entering your information, the IP Address screen asks if you want to reset the bridge. Ignore this and reset the bridge when you've completed this section.

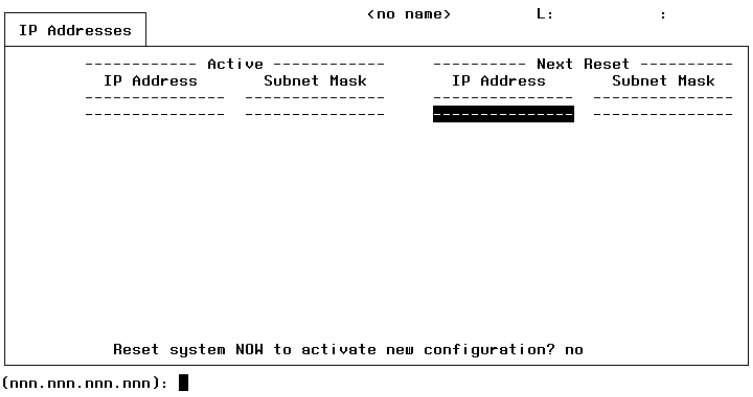


Figure 2-16 IP Addresses

Active

IP Address: Display Field. The bridge's current IP address. A line of dashes indicates that no IP address has been assigned to the bridge.

Subnet Mask: Display Field. The bridge's current subnet mask.

Next Reset

IP Address: Text Field. Enter the IP address you want to assign to the bridge. It must be unique and of the form nnn.nnn.nnn.nnn (decimal). Enter `0.0.0.0` to remove the bridge's IP address. Changes to this field are only saved during a bridge reset, and take effect from then on.

Subnet Mask: Text Field. Enter the subnet mask you want to assign to the bridge. A subnet mask is not needed unless the network is IP routed. It must be of the form nnn.nnn.nnn.nnn (decimal). Changes to this field are only saved during a bridge reset, and take effect from then on.

Static Routes

If you are using a routed network, you will need to enter a default gateway to ensure remote communication with the bridge. A more resilient network can be set up by defining a set of *static routes*. Static routes are predefined routes, with different levels of priority, through the routed network. The highest priority route will be used until a router or cable goes down, breaking the route. When this happens, the next priority route is used.

Select IP STATIC ROUTES from the Network Protocol menu.

The Static Routes screen appears, as shown in Figure 2-17. You use this table to specify gateways the IP router should use to reach specific network, host or subnet destinations.

Each static route includes a preference value. If protocols are enabled, the preference you specify in a static route to a network or subnet destination is compared to preference values for the same destination learned through protocol messages from the network. If the static route preference value is higher (less desirable) than a route learned over the network, the static route is replaced. However, since the protocols deal only with network (or subnet) destinations, enabling them does not change any static routes that you specify for hosts.

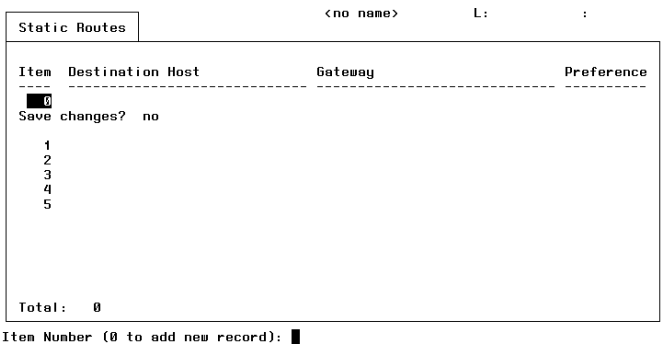


Figure 2-17 Static Routes

Item: Text Field. The number of a configured static route or `0` (to enter a new route). Static routes are sorted by IP address and assigned numbers according to their positions in the sorted list. Entering the number of a configured static route causes that route to be displayed.

Destination Host: Text Field. The IP address of a network, host, or gateway, or a [Space] character, or the keyword default. Specify the address in decimal notation, nnn.nnn.nnn.nnn. If a host name has been defined in the IP Host Table screen, you can use that name rather than the IP address.

The IP address can be an address that is configured in a static route, or an address for a new route. If the address is already configured, entering it causes its parameters to be displayed on the line you can edit. If it is not configured, the remaining fields in the line are blank.

A [Space] character deletes the route displayed. Item numbers are adjusted accordingly.

`default` is equivalent to the address `0.0.0.0`, which is the destination for the default gateway. In other words, the gateway you specify for this destination is the one that will be used for any route not defined in the routing table.

Enter `y` for the SAVE CHANGES? field to save changes to this field. Changes only take effect after a bridge reset.

Gateway: Text Field. The IP address or host name of the gateway that is the next hop for the destination host specified in the previous field. If a host name is given, it must be defined in the IP Host Table screen. Enter `y` for the SAVE CHANGES? field to save changes to this field. Changes only take effect after a bridge reset.

Preference: Text Field. A whole number from 0 to 255, designating the rank to be assigned to the route specified by the DESTINATION HOST and GATEWAY fields. `0` represents the most desirable route, `255` represents the least desirable route. The default is `50`. Enter `y` for the SAVE CHANGES? field to save changes to this field. Changes only take effect after a bridge reset.

Save changes?: Text Field. Enter `y` to save any changes made to this screen to NVRAM, or `n` to not save any changes. Changes only take effect after a bridge reset.

Assigning Host Name / IP Address Pairs

You can assign symbolic names (*host names*) for devices that can communicate with or from the bridge. If a device has an IP address, a host name can be assigned to it. This host name can then be used instead of the IP address to identify the device, when using the bridge. It is not necessary to assign host names, but they are a lot easier to remember than IP addresses. The IP Host Table screen is used for assigning IP address / host name pairs and is primarily used for Telnet.

Select HOST TABLE from the Network Protocol menu.

The IP Host Table screen appears, displaying two tables, IP Addresses and Host Name, as shown in Figure 2-18. The Host Name table lists the existing host names assigned to the corresponding IP address in the IP Addresses table.

Enter IP address / host name pairs for devices that can access the bridge. The host name must be unique for each device. For a bridge, use the name defined in its System Information screen as its host name.

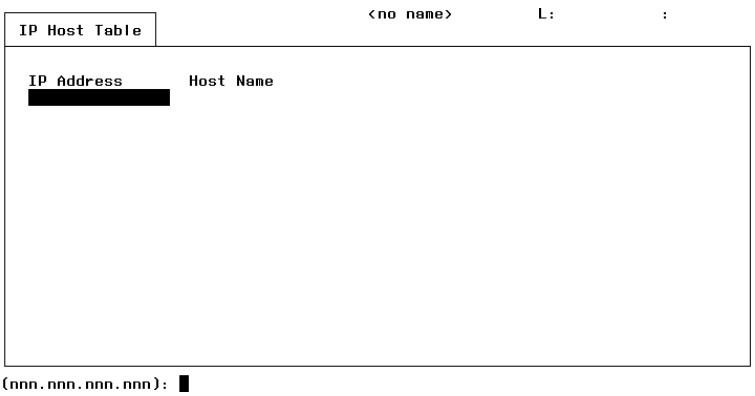


Figure 2-18 IP Host Table

IP Address: Text Field. Enter the IP address for the device. It must be in decimal and of the form nnn.nnn.nnn.nnn. Changes to this field are only saved during a bridge reset, and take effect from then on.

Host Name: Text Field. Enter the host name for the device. Changes to this field are only saved during a bridge reset, and take effect from then on.

The IP Host Table screen is updated with any new IP address / host name pairs that are entered in the custom filtering screens.

Using PING To Test Connections

The PING (Packet InterNet Groper) program checks for a valid connection to a network device. Any device with an IP address can respond to a PING session. It tests network connections by sending packets to a specified IP address and checking the response.

If you have just set up address information for the bridge, reset the bridge to save the information and for it to take effect.

We recommend that you PING the LinkBuilder MSH Management Module, in the same chassis as the bridge, to test that PING is working correctly.

You could use PING if:

- You can't connect to a remote device and are unsure if it is working.
- There is a problem on the network and you need to check all the nodes for response quickly.

If you get no response from a device, it could be because:

- You are using the wrong IP address.
- No one has assigned the IP address to the remote device or, if a host name was used, the host name is not assigned to that IP address in the bridge's host table. You may wish to contact someone at the remote site.
- The host is shut off or has crashed. You may wish to contact someone at the remote site.
- Your subnet mask is wrong.
- The default gateway is wrong.
- You have not assigned an IP address to the bridge.

Select PING from the Applications menu.

The Ping Settings screen appears, as shown in Figure 2-19. Enter the IP address or host name of the remote device and confirm the packet size and timeout parameters (modify these only if necessary).

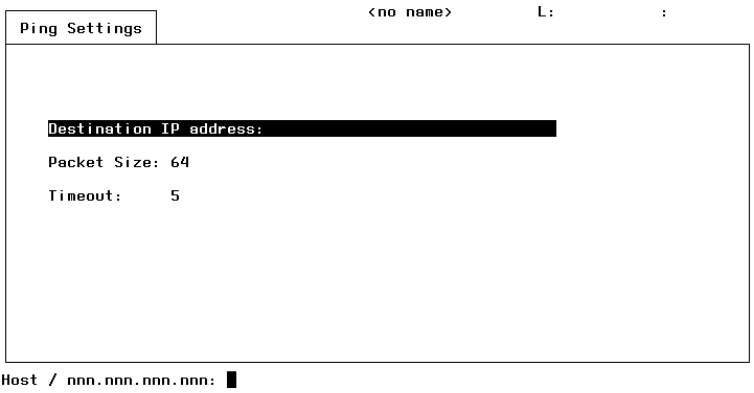


Figure 2-19 Ping Settings

Destination IP address: Text Field. Enter the IP address for the remote device. It must be in decimal and of the form nnn.nnn.nnn.nnn.

or

Enter the host name for the remote device. This host name must be in the host table of your bridge.

Packet Size: Text Field. The number of bytes in the packet, excluding the header, that contains the echo request message.

Timeout: Text Field. The number of seconds PING waits for an ICMP echo response message, before giving up and sending the next ICMP echo request message.

The Ping screen appears, as shown in Figure 2-20, after the information for the Ping Settings screen has been supplied. The Ping screen immediately starts displaying status messages when information is received.

When you've finished with the Ping screen, press [Enter] or [Return] to exit from it.

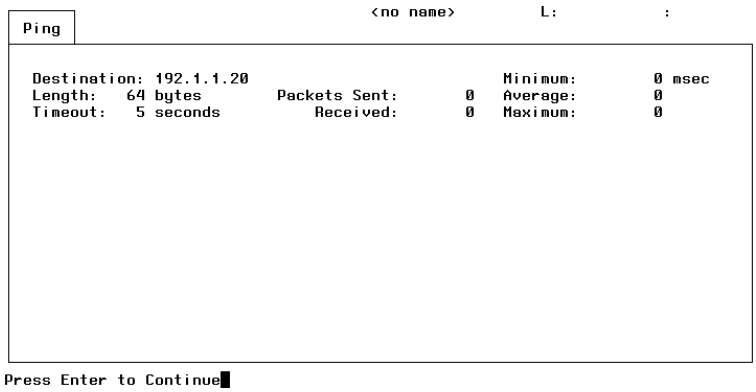


Figure 2-20 Ping

Destination: Display Field. The IP address or host name of the remote device being pinged.

Packet Size: Display Field. The number of bytes in the packet, excluding the header, that contains the echo request message.

Timeout: Display Field. The number of seconds PING waits for an ICMP echo response message, before giving up and sending the next ICMP echo request message.

Packets Sent: Display Field. The number of ICMP echo request messages that have been sent to the destination address.

Packets Received: Display Field. The number of ICMP echo response messages that have been received from the destination address.

Minimum: Display Field. The shortest amount of time (in milliseconds) that elapsed between sending an ICMP echo request and receiving an ICMP echo response.

Average: Display Field. The average amount of time (in milliseconds) that elapsed between sending an ICMP echo request and receiving an ICMP echo response.

Maximum: Display Field. The longest amount of time (in milliseconds) that elapsed between sending an ICMP echo request and receiving an ICMP echo response.

Telnet Log On To Another IP Device From The Bridge

The bridge has Telnet capabilities, allowing you to remotely log on to an IP device. This is especially useful for logging on to other LinkBuilder MSH 4 Port Bridge Modules. However, the bridge does not always allow you to Telnet out. For information on when you can Telnet, see *Bridge Connections* on page 2-30. You may wish to Telnet to the LinkBuilder MSH Management Module.

Select APPLICATIONS from the Main Menu. Select TELNET from the Applications menu, to start a Telnet session.

One of the following will happen:

- If the Connections menu appears, the bridge has already accepted a remote log on. You are not allowed to Telnet out from the bridge.

  If you are remotely logged on to the bridge, you can talk to a local user (the user who has logged on to the bridge locally), if present, by using the Chat screen (select CHAT W. LOCAL to display this screen). When you have finished, select END CONNECTION.

  If you are locally logged on to the bridge, you can talk to a remote user (the user who has logged on to the bridge remotely), if present, by using the Chat screen (select CHAT W. REMOTE to display this screen). When you have finished, select END CONNECTION.

- If the Remote Connect screen appears, as shown in Figure 2-21, you are allowed to Telnet out from the bridge. Enter the host name or IP address of the device you want to log on to. If you use a host name, it must appear in the bridge's host table. If you use an IP address, it must be in the decimal form nnn.nnn.nnn.nnn.

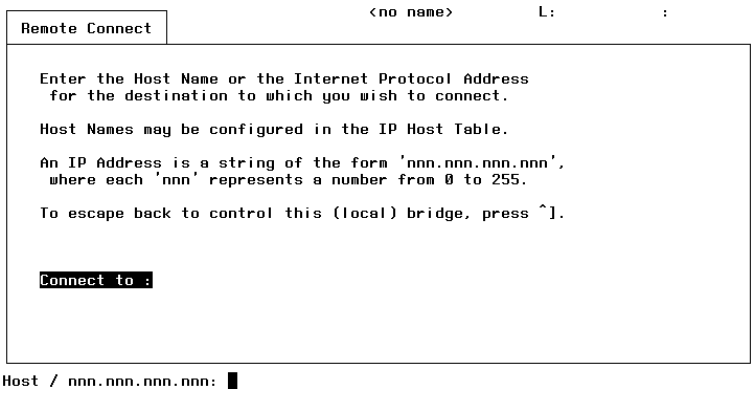


Figure 2-21 Remote Connect

Talking To Another Bridge User

The bridge can accept two users, one local and one remote. If both users are present, they can exchange messages via the Chat screen.

The Chat screen, as shown in Figure 2-22, is intended for exchanging uncomplicated information:

- Warning the other user that you are about to reset the bridge or change its configuration.
- Exchanging telephone numbers so you can discuss any network issues you may have.

The local user can get the Chat screen by selecting CHAT W. REMOTE from the Connections menu. The remote user can get the Chat screen by selecting CHAT W. LOCAL from the Connections menu.

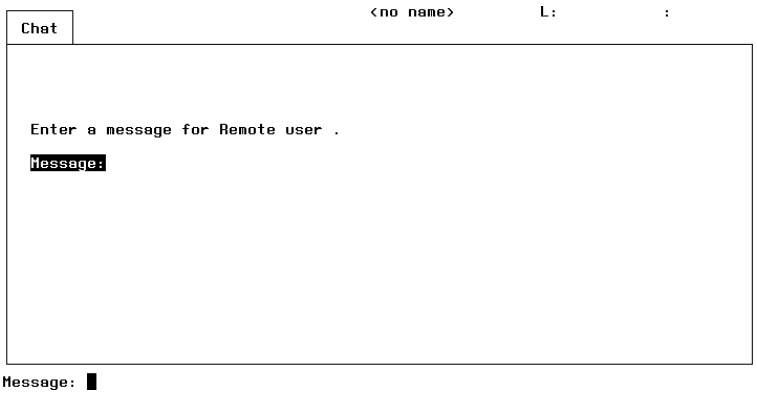


Figure 2-22 Chat

Message: Text Field. Enter your message for the other user. It can be up to 50 characters long.

Telnet Suspension

You can suspend your Telnet session from the bridge at any time. You may want to do this if you want to return to the bridge but stay connected to the remote device.

To suspend a remote session, press [Ctrl] + [ ]]. You will be returned to the Main Menu of the bridge. To resume a suspended session, press [Ctrl] + [ ]] again.

Telnet Log Off

To disconnect from the remote device, select END CONNECTION from the Connections menu. The Terminate Connection screen appears, displaying the IP address and host name of the remote host you wish to disconnect from, as shown in Figure 2-23.

If you want to disconnect from the remote device, press [Enter] or [Return]. If you do not want to disconnect from the remote device, leave the screen.

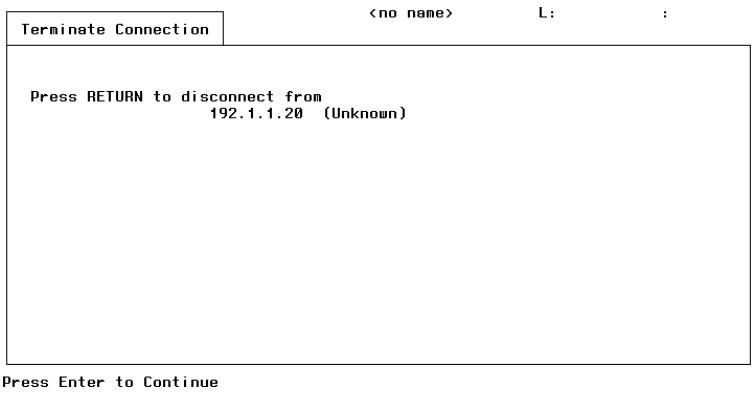


Figure 2-23 Terminate Connection

SNMP Configuration

This section describes configuration of the *SNMP agent* on the bridge. When the SNMP agent has been configured, SNMP applications can obtain information from it about the bridge.

This section describes how to:

- Configure the basic characteristics of each community and globally enable or disable the Authentication Failure trap.
- Enable traps for individual communities and specify the IP addresses to which the traps should be sent.

The basic concepts of SNMP are explained in *Spanning Tree Algorithm And Protocol (STAP)* on page 1-16.

Remember to reset the bridge after setting up the SNMP agent if you want your configuration to be saved and take effect.

Community Administration

The bridge has a *community*. A community defines an administrative relationship between a *client* (a device) and the SNMP agent it wishes to communicate with.

On the bridge, for the community you must configure:

- A *community name* used by the client and agent as a password for communicating with each other and included in all messages exchanged between them.
- A *MIB view* defining the subset of MIB variables that can be accessed by client requests containing the community name.
- An *access mode* specifying whether client requests containing the community name can perform read only (GET) operations, or read and write (GET and SET) operations on MIB variables.

Traps

An SNMP agent can send messages, *traps*, when exceptional events occur. Traps include the name of the community involved in the event. They are sent to an IP address that you define for each community during configuration of the agent.

The main advantage of traps is that you do not have to constantly monitor the bridge because it alerts you when any exceptional events occur.

The bridge's SNMP agent supports the following bridge traps:

- Authentication Failure

  An SNMP client has tried to access the agent using a community name the agent does not recognize, or requesting an action not allowed for the community.

- Cold Start

  The agent is initializing itself. The values of MIB variables may change.

- Interface Up

  A port, previously not operational, is now operational.

- Interface Down

  A port, previously operational, is now not operational.

- New Root

  The bridge on which the agent is running has become the new root of the Spanning Tree.

- Topology Change

  One of the configured bridge's configured ports has gone into or out of the Forwarding state. This could be due to STAP or manual configuration.

Configuring Basic Community Characteristics

Select CONFIGURATION from the Main Menu and then NETWORK PROTOCOL from the Configuration menu. Select SNMP from the Network Protocol menu to get the Configure SNMP menu.

Select COMMUNITIES from the Configure SNMP menu.

The SNMP Community Basic Configuration screen appears, as shown in Figure 2-24. You use this screen for enabling or disabling the authentication trap for the SNMP agent running on the bridge. You would also use this screen for configuring the community name, MIB view, and SNMP access mode for the community that will access the SNMP agent.

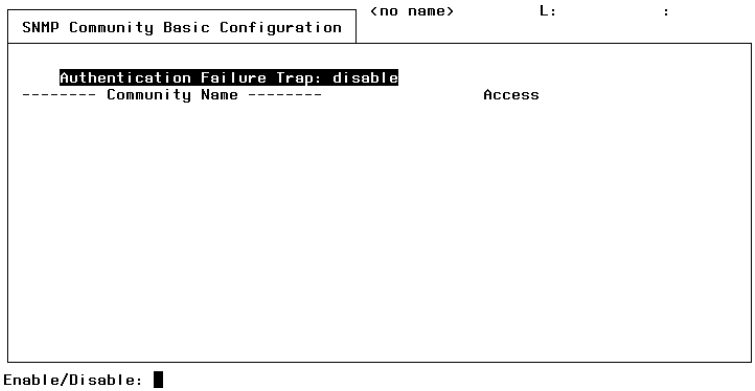


Figure 2-24 SNMP Community Basic Configuration

Authentication Failure Trap: Text Field (e / d). Enable or disable the authentication failure trap for the SNMP agent. Enter e to enable, or enter d to disable. The default is disable.

If the trap is enabled, the agent generates a trap message whenever a client tries to access it using a community name you have not defined. The message is sent to the trap destination of each community for which traps are enabled. Use the SNMP Community Trap Configuration screen to enable all traps, and define the destinations that are to receive messages reporting traps.

If the trap is disabled, no authentication failure trap messages are generated, regardless of whether or not traps have been enabled on the SNMP Community Trap Configuration Screen.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Community Name: Text Field. A community name is a name by which a client can access this agent. If the field is blank, you can use it to add a community name. The name can contain from 1 to 32 characters.

Press [Space] to delete a community name. The default is blank.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Access: Text Field (`r/o` / `r/w`). Enter the access mode for the community's MIB view. The effect this has on operations permissible for the community depends on the ACCESS: in the MIB definition of the object.

Enter `r/o` to specify that the community can perform read operations (GET and TRAP) on the value of a MIB object in the MIB view, if the object's MIB ACCESS: is `read-write` or `read-only`. The value of an object whose ACCESS: is `write-only` or `not-accessible` cannot be read. No object values can be written (SET).

Enter `r/w` to specify that the community can perform read and write operations (GET, TRAP and SET) on the value of any object in the MIB view, if the object's MIB ACCESS: is `read-write` or `write-only`.

The default is `r/o`.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Configuring Community Traps

Select COMMUNITY TRAPS from the Configure SNMP menu.

The SNMP Community Trap Configuration screen appears, as shown in Figure 2-25, displaying the existing community name (configured in the SNMP Community Basic Configuration screen). You use this screen for configuring the community name, enabling or disabling traps, defining the device to which the agent is to send trap messages, and defining the UDP port to which the agent is to send trap messages.

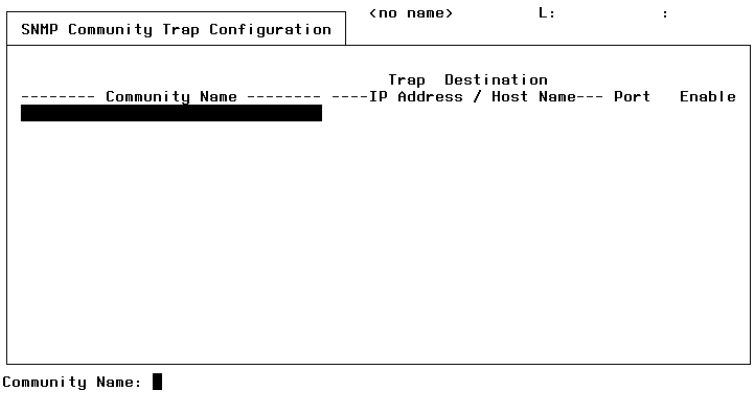


Figure 2-25 SNMP Community Trap Configuration

Community Name: Text Field. The name of the SNMP community. If this field is blank, you can enter a new community name. The name can be 1 to 32 alpha-numeric characters.

Press [Space] to delete a community name. To change a name, type over the existing one.

Changes to this field are only saved during a bridge reset, and take effect from then on.

IP Address / Host Name: Text Field. The host to which traps pertaining to the community name are to be sent. Specify either an IP address in the dotted decimal notation (nnn.nnn.nnn.nnn), or the name of the host that has been defined in the host table (via the IP Host Table screen).

If you enter a host name defined in the host table, the corresponding IP address is displayed preceding the name. This occurs as soon as you enter or change a community name on some other line on the screen.

If you enter a host name not defined in the host table, an error message is displayed, "Illegal Internet Address".

If you enter an IP address that happens to be defined in the host table (although this is not required), the corresponding host name is displayed (in parenthesis) after the address. This occurs as soon as you enter or change a community name on another line on the screen.

The default is `0.0.0.0` (unknown).

Changes to this field are only saved during a bridge reset, and take effect from then on.

Port: Text Field. The UDP port on the host that is to receive trap messages. You usually leave this as the default of `162`, the standard UDP port for SNMP communication. Changes to this field are only saved during a bridge reset, and take effect from then on.

Enable: Text Field (y / n). Enter y to enable, or n to disable the Authentication Failure, Cold Start, Interface Up, Interface Down, New Root and Topology Change traps.

An Authentication Failure trap is generated when an SNMP client has tried to access the agent using a community name the agent does not recognize. The Authentication Failure trap must also be enabled on the SNMP Community Basic Configuration screen. If it is not enabled on both screens, no authentication failure traps are generated.

A Cold Start trap is generated when the agent is initializing (or reinitializing) itself and the values of MIB variables may change.

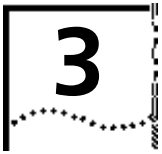
An Interface Up trap is generated when a port that was not operational is now operational.

An Interface Down trap is generated when a port that was operational is no longer operational.

A New Root trap is generated when the bridge on which the agent is running has become the new root of the spanning tree.

A Topology Change trap is generated when one of the configured ports on the bridge has gone into or out of the forwarding state.

Changes to this field are only saved during a bridge reset, and take effect from then on.



ADVANCED BRIDGING

This chapter contains the following topics:

Introduction

This chapter describes how to set up the bridge's advanced features. If you have not previously set up the bridge, read Chapter 2.

Spanning Tree Configuration

The *Spanning Tree Algorithm and Protocol* (STAP) is explained in the IEEE Computer Society's *MAC Bridges P802.1D* document.

You should not change any spanning tree parameters unless you have significant knowledge and experience with the Spanning Tree Algorithm and Protocol (STAP).

The *spanning tree* eliminates the duplication of packets and provides fault tolerance for resilient networks. During construction of the spanning tree, bridges co-operate by exchanging information. This information is transmitted in packets called *Configuration Bridge Protocol Data Units* (C-BPDUs).

In order to establish a stable spanning tree topology, the STAP bridges 'elect' a *root bridge*. The root bridge takes charge of the spanning tree topology and controls which bridges block packets and which forward packets.

Once the topology is stable, all STAP bridges listen for special 'Hello' C-BPDUs transmitted from the root bridge at regular intervals (usually every two seconds). If a STAP bridge timer expires before receiving a 'Hello' C-BPDU, it assumes that the root bridge, or a link between itself and the root bridge, has gone down. It initiates a reconfiguration of the spanning tree topology.

This section describes what spanning tree parameters can be changed. The bridge defaults to the IEEE 802.1d Revision 9 recommended settings.

Spanning Tree Bridge Configuration

Select CONFIGURATION from the Main Menu. Select BRIDGES from the Configuration menu. Select SPANNING TREE from the Bridges menu.

The Spanning Tree screen appears, as shown in Figure 3-1. You use this screen for editing the bridge's spanning tree information. The screen is split and shows the spanning tree information for this bridge (on the left) and the current root bridge (on the right). You should not change these parameters unless you understand the scope of the spanning tree as this may modify the topology of your network.

You can use the Bridge Statistics screen to check spanning tree bridge parameters. This screen is displayed, via the Monitoring menu, by selecting BRIDGE STATISTICS from the Bridges menu. Use the screen to verify port states and traffic. For more information on the Bridge Statistics screen refer to *Checking Bridge Statistics* on page 4-3.

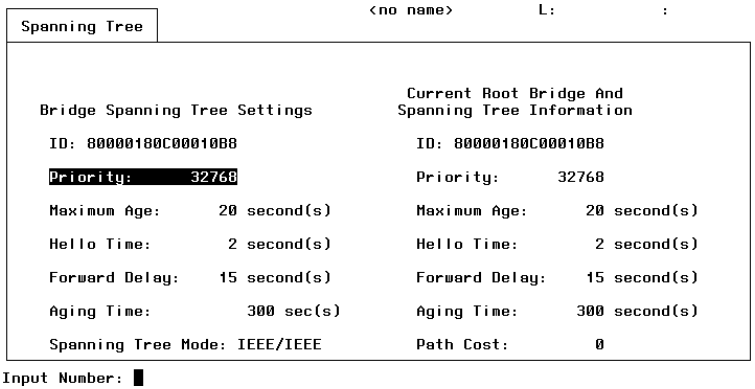


Figure 3-1 Spanning Tree

ID: Display Field. The identification number for the bridge. The ID number uniquely identifies each bridge. The number is a combination of the lowest Ethernet device address on the bridge and a hexadecimal representation of the PRIORITY field. The Ethernet device address is hard-coded in the Ethernet chip and cannot be changed.

Priority: Text Field. Enter the priority of the bridge. The priority determines which bridge to use when two or more bridges are on the same network. The highest priority bridge is the one set with the lowest number. If two bridges have the same path cost to the root bridge, the priority is used to determine which bridge to use.

The IEEE 802.1 spanning tree priority is a value between 0 and 65535. The default is 32768.

Changes to this field are saved and take effect immediately.

Maximum Age: Text Field. Enter the amount of time a bridge retains spanning tree configuration information before discarding it.

All bridges in a spanning tree network need to receive information about the configuration of the network. This information is made available in the form of Configuration Bridge Protocol Data Units (C-BPDUs) sent by the root bridge. If a bridge does not receive valid C-BPDUs from a root bridge during the time interval set by the MAXIMUM AGE field, it will assume that the root bridge has failed and will establish a new network configuration using itself as the new root bridge. This process ensures that a root bridge always exists.

The maximum age must be between 6 and 40 seconds and cannot be greater than the maximum age of the current root bridge, shown on the right hand side of the screen. The default is `20` seconds, as recommended by the IEEE 802.1d specification. The maximum age must be larger than the hello time of every bridge in the network.

Changes to this field are saved and take effect immediately.

Hello Time: Text Field. Enter the hello time for the bridge. The hello time is the amount of time the bridge pauses between sending spanning tree configuration C-BPDUs.

The hello time must be between 1 and 10 seconds and must be lower than the maximum age. The default is 2 seconds.

Changes to this field are saved and take effect immediately.

Forward Delay: Text Field. Enter the forward delay for the bridge. The forward delay is a two-step timer that prevents a bridge from forwarding packets until changes, if any, to the topology are reported.

In a typical cycle the bridge is in the listening state for the amount of time set by the forward delay, waiting to hear spanning tree configuration C-BPDUs. If no changes are reported, the bridge moves into the learning state. While in the learning state, the bridge waits another forward delay interval to see if any configuration C-BPDUs are transmitted that would change the topology. If no C-BPDUs are received, the bridge then moves to the forwarding state. The forward delay timer must be set between 4 and 30 seconds. The default is 15 seconds.

Changes to this field are saved and take effect immediately.

Ageing: Text Field. Enter the ageing time. The ageing time is the amount of time a bridge allows each entry transmitted from a source address to remain in the forwarding database. If the bridge does not receive packets from a source address during the ageing time interval, it discards packets from that source address and relearns the network. The ageing time must be between 10 and 10000 seconds. The default is 300 seconds.

Changes to this field are saved and take effect immediately.

Spanning Tree Mode: Text Field. This field shows the current entry (before the `/`) and the entry that will take effect after resetting the bridge (after the /). Enter `IEEE` for the IEEE 802.1d version of the spanning tree, or enter `off` to disable the spanning tree.

Spanning Tree Port Configuration

Select SPANNING PORT from the Bridges menu.

The Port Settings screen appears, as shown in Figure 3-2. You use this screen for editing various port spanning tree information. The screen is split and shows the spanning tree information for this bridge (on the left) and the current root bridge (on the right). You should not change these parameters unless you understand the scope of the spanning tree as this may modify the topology of your network.

The settings for the port entered in the field at the top left of the screen will be shown. Change this field to display the port you wish to change parameters for. The screen will automatically display the next port after the previous one.

You can use the Bridge Port Statistics screen to check spanning tree port parameters. This screen is displayed, via the Monitoring menu, by selecting BRIDGE PORT STATS from the Bridges menu. Use the screen to verify port states and traffic. For more information on the Bridge Port Statistics screen refer to *Checking Port Activity* on page 4-8.

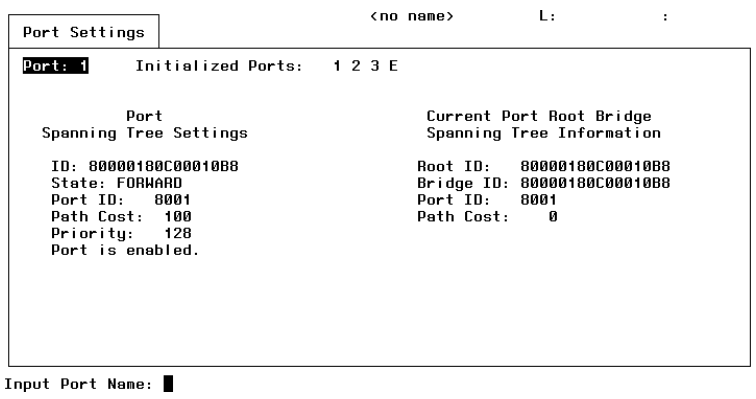


Figure 3-2 Port Settings

Port: Text Field. Enter the name of the port who's spanning tree parameters you want to change. Use `1`, `2`, `3` or `E`.

ID: Display Field. The identification number for the port. The port's ID is the same as the bridge's ID, which is a combination of two numbers, the bridge priority and the Ethernet address of the bridge.

State: Display Field. The current status of the port. This value changes depending on when you view it, or when you enable or disable a port.

`Blocked` indicates the port is listening for spanning tree information only. The port ignores all other information.

`Listening` indicates the port is waiting to be placed in the forwarding state.

`Learning` indicates the port is learning information collected during the listening state. The forwarding database is built from learned information.

`Forwarding` indicates the port is sending data.

`MOS` (Manually Out of Service) indicates the port is disabled and receives no network traffic. Ports are enabled or disabled by the PORT IS ENABLED/DISABLED field.

Port ID: Display Field. The hexadecimal number that uniquely identifies the port. This number is a combination of the port priority and the physical number of the port in the bridge. This number changes if you change the PRIORITY field.

Path Cost: Text Field. Enter the path cost. The path cost represents the performance cost of sending information through a port and measures the impact of sending packets through the network. The path cost setting establishes a hierarchy among the ports of the spanning tree topology. A high cost indicates a low position in the topology. A low cost indicates a high position in the topology. By setting a high path cost to a port, you discourage high-volume traffic and eliminate slow data links.

The port path cost is based on the root path cost, when the port is the root port of the bridge. The path cost must be a number between 0 and 65535.

Changes to this field are saved and take effect immediately.

Priority: Text Field. Enter the priority of the port. When you change this field you change the first two digits of the priority number. The priority determines the port to use when two ports have the same calculated path cost. The port with the lowest ID number is the one that is used.

Changes to this field are saved and take effect immediately.

Port is enabled, Port is disabled. No Field. Press [E] to enable the port, or [D] to disable the port. Changes to this field are saved and take effect immediately.

Custom Filter Configuration

You can control the traffic that flows through the bridge by using the bridge's custom filters. For example, you can prevent communication between specific devices, and allow only TCP/IP communication between specific bridge ports. The basic concepts of custom filtering are explained in *Bridge Filters* on page 1-20.

If you are unfamiliar with filtering, it is easy to produce unexpected results. You should plan your filter sets carefully before configuring custom filters.

This section describes how to set up the custom filters. The Filter Options screen is used for saving and making custom filtering effective. This is also explained in this section.

Setting Up A Host-to-Host Filter Set

Select CONFIGURATION from the Main Menu. Select BRIDGES from the Configuration menu. Select BRIDGE FILTERS from the Bridges menu.

The Bridge Filters menu lists each filter option. Selecting the relevant filter will take you through to that filter's setup screen.

Select HOST-TO-HOST from the Bridge Filters menu.

The Host-to-Host screen appears, as shown in Figure 3-3. You use this screen for setting up host-to-host filter sets. The screen displays the devices included in the filter set denoted in the SET NUMBER field. Simply alter this field to work on a different filter set. There are 32 host-to-host filter sets. Remember that filter set number 1 is reserved for absolute exclusion.

For host-to-host filtering information, refer to *Filter Sets* on page 1-23.

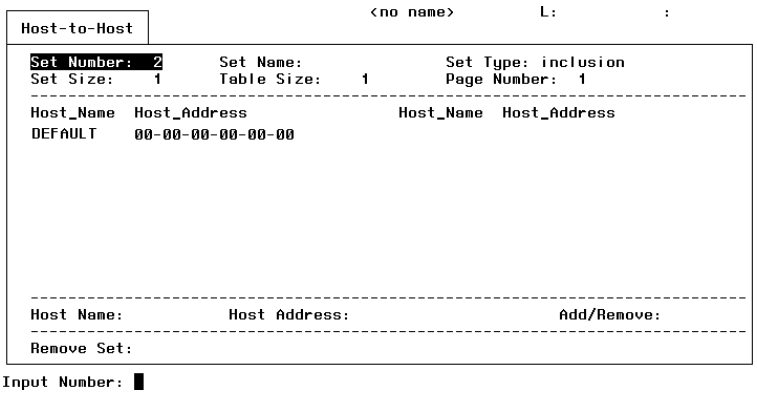


Figure 3-3 Host-to-Host

Set Number: Text Field. Enter the number of the filter set you want to set up. You can use any number from 1 to 32 but remember that set number 1 is the absolute exclusion set. Press [Return] to accept the set number.

Set Name: Text Field. This is optional. Enter a name for the filter set. The set name helps you identify the set.

Set Type: Text Field. Ensure this is `inclusion' (for sets 2 to 32). Set number 1 is the absolute exclusion set.

Host Name: Text Field. Enter the host name for the device you want in your filter set. Each host name / host address pair must be unique across all set tables. You cannot have more than one name for the same host address, nor can you have the same name for multiple addresses. The host name / host address pair will be added to the bridge's host table if it does not already appear.

Host Address: Text Field. Enter the host address for the device you want in your filter set. The format is nn-nn-nn-nn-nn-nn (hexadecimal). This will appear automatically if you entered a known host name.

Add/Remove: Text Field (A / R). To add the device that you've entered, to the filter set, enter A. To remove a device from the filter set, enter R. The device who's host name is in the HOST NAME field, and host address is in the HOST ADDRESS field will be added or removed from the filter set.

To add or remove the default host group, use DEFAULT for the host name. You do not need to enter a host address for the default host.

Remove Set: Text Field. Enter y to remove all the members from the set.

Saving Host-to-Host Filters

When you have set up your filter sets, you must use the Filter Options screen to save them. Exit from the Host-to-Host screen and select FILTER SWITCHES from the Bridge Filters menu. You also use the Filter Options screen for enabling and disabling filters.

Enter y for the SAVE HTOH SETS INFO? field and the SAVE HOST TABLE INFO? field.

Reset the bridge.

Setting Up A Host-to-Port Filter Set

Select HOST-TO-PORT from the Bridge Filters menu.

The Host-to-Port screen appears, as shown in Figure 3-4. You use this screen for setting up a port's host-to-port filter set. The screen displays the hosts included in the filter set of the port denoted in the PORT NAME field. Simply alter this field to work on a different filter set. There are four host-to-port filter sets, one for each port.

Enter all hosts that belong to the set.

For host-to-port filtering information, refer to *Filter Sets* on page 1-23.

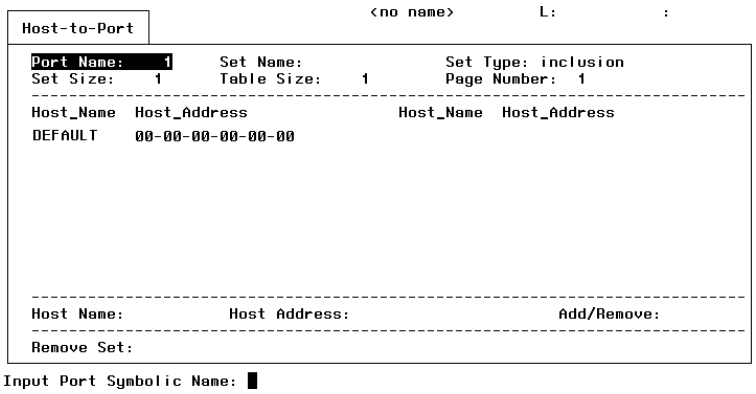


Figure 3-4 Host-to-Port

Port Name: Text Field. Enter the name of the port who's filter set you want to set up. Use `1`, `2`, `3` or `E`. Press [Return] to accept the port name.

Set Name: Text Field. This is optional. Enter a name for the filter set. The set name helps you identify the set. For example, you may want to name a set `finance`.

Set Type: Text Field (`inclusion` / `exclusion`). Enter the filter set's type. You can define a filter set by inclusion or exclusion. Enter `inclusion` to define the filter set as inclusion, or `exclusion` to define the filter set as exclusion. The default is `inclusion`.

For example, if you want to allow communication between a few devices and a port, list the devices and define the set by inclusion. If, however, you want to disallow communication between just a few devices and a port, list the devices and define the set by exclusion.

Host Name: Text Field. Enter the host name for the device you want in your filter set. Each host name / host address pair must be unique across all set tables. You cannot have more than one name for the same host address, nor can you have the same name for multiple addresses. The host name / host address pair will be added to the bridge's host table if it does not already appear.

Host Address: Text Field. Enter the host address for the device you want in your filter set. The format is nn-nn-nn-nn-nn-nn (hexadecimal).

Do not enter broadcast or multicast addresses in this field. Use Multicast-to-Port filtering to do this.

Add/Remove: Text Field (A / R). To add the device that you've entered, to the filter set, enter A. To remove a device from the filter set, enter R. The device who's host name is in the HOST NAME field, and host address is in the HOST ADDRESS field will be added or removed from the filter set.

Remove Set: Text Field. Enter y to remove all the members from the set.

Saving Host-to-Port Filters

When you have set up your filter sets, you must use the Filter Options screen to save them. Exit from the Host-to-Port screen and select FILTER SWITCHES from the Bridge Filters menu. You also use the Filter Options screen for enabling and disabling filters.

Enter y for the SAVE HTOP SETS INFO? field and the SAVE HOST TABLE INFO? field.

Reset the bridge.

Setting Up A Port-to-Port Filter Set

Select PORT-TO-PORT from the Bridge Filters menu.

The Port-to-Port screen appears, as shown in Figure 3-5. You use this screen for setting up a port's port-to-port filter set. The screen displays the ports included in the filter set of the port denoted in the SET PORT SYMBOLIC NAME field. Simply alter this field to work on a different port's filter set. There are four port-to-port filter sets, one for each port.

Remember that port-to-port filter sets are reciprocal. This means that any changes made to a port's filter set will be mirrored by the other ports' filter sets. For example, if you include port's 2 and E in port 1's filter set, port 2's filter set will change to include port 1, and port E's filter set will also change to include port 1.

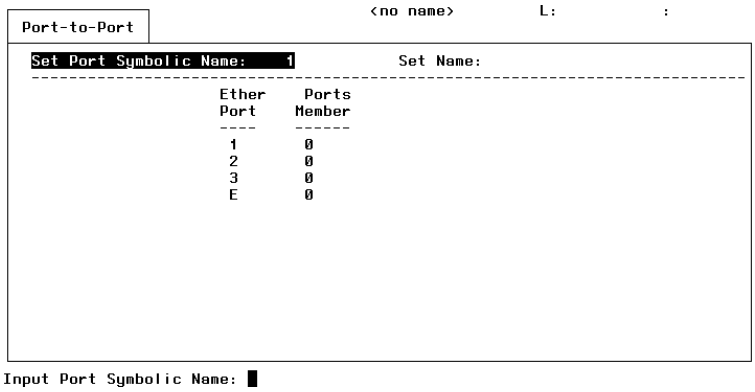


Figure 3-5 Port-to-Port

Set Port Symbolic Name: Text Field. Enter the name of the port who's filter set you want to set up. Use 1, 2, 3 or E. Press [Return] to accept the port name.

Set Name: Text Field. This is optional. Enter a name for the filter set. The set name helps you identify the set. If you enter a name that is already used for a port-to-port filter set, that filter set will be displayed.

Ports Member: Text Field (`1` / `0`). Move to the field, under PORTS MEMBER, next to the relevant port. Enter `1` to include the port as a member of the filter set, or `0` to exclude the port as a member of the filter set. The default is `1`.

Saving Port-to-Port Filters

When you have set up your filter sets, you must use the Filter Options screen to save them. Exit from the Port-to-Port screen and select FILTER SWITCHES from the Bridge Filters menu. You also use the Filter Options screen for enabling and disabling filters.

Enter `y` for the SAVE PTOP SETS INFO? field.

Reset the bridge.

Setting Up A Multicast-to-Port Filter Set

Select MULTICAST from the Bridge Filters menu.

The Multicast screen appears, as shown in Figure 3-6. You use this screen for setting up a port's multicast-to-port filter set. The screen displays the ports included in the filter set of the port denoted in the SET PORT SYMBOLIC NAME field. Simply alter this field to work on a different port's filter set. There are four multicast-to-port filter sets, one for each port.

Remember that multicast-to-port filter sets are reciprocal. This means that any changes made to a port's filter set will be mirrored by the other ports' filter sets. For example, if you include port's 2 and E in port 1's filter set, port 2's filter set will change to include port 1, and port E's filter set will also change to include port 1.

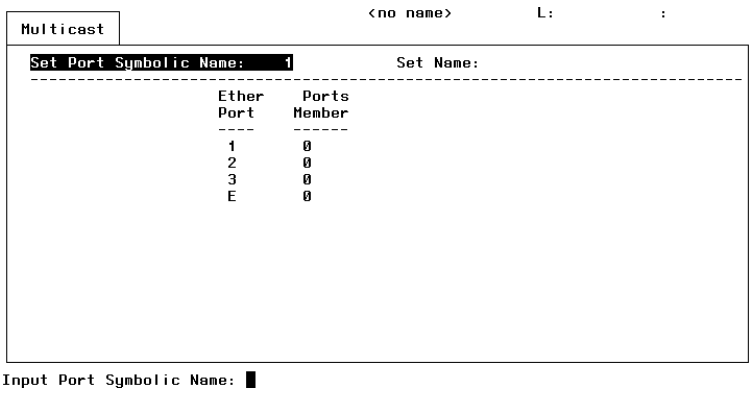


Figure 3-6 Multicast

Set Port Symbolic Name: Text Field. Enter the number of the port who's filter set you want to set up. Use 1, 2, 3 or E. Press [Return] to accept the port name.

Set Name: Text Field. This is optional. Enter a name for the filter set. The set name helps you identify the set. If you enter a name that is already used for a multicast-to-port filter set, that filter set will be displayed.

Ports Member: Text Field (`1` / `0`). Move to the field, under PORTS MEMBER, next to the relevant port. Enter `1` to include the port as a member of the filter set, or `0` to exclude the port as a member of the filter set. The default is `1`.

Saving Multicast-to-Port Filters

When you have set up your filter sets, you must use the Filter Options screen to save them. Exit from the Multicast-to-Port screen and select FILTER SWITCHES from the Bridge Filters menu. You also use the Filter Options screen for enabling and disabling filters.

Enter `y` for the SAVE MULT SETS INFO? field.

Reset the bridge.

Setting Up A Protocol Filter Set

Select PROTOCOL from the Bridge Filters menu.

The Protocol screen appears, as shown in Figure 3-7. You use this screen for setting up a protocol filter set. The screen displays protocol families (on the left) and individual protocols (on the right), included in the filter set of the port denoted in the SET PORT SYMBOLIC NAME field. Simply alter this field to work on a different port's filter set. There are four protocol filter sets, one for each port.

Ensure you enter the SET PORT SYMBOLIC NAME before you proceed with setting up protocol filter sets.

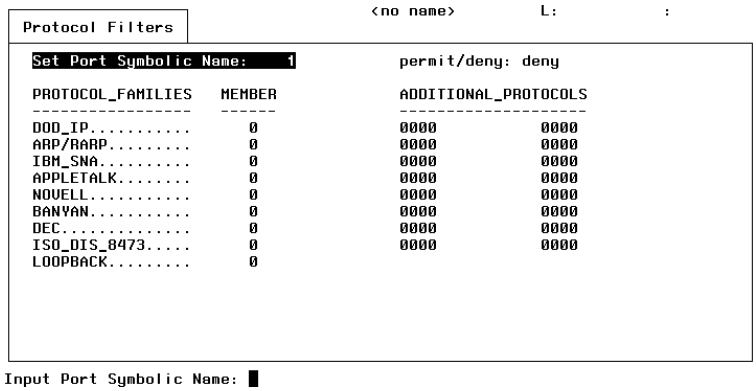


Figure 3-7 Protocol Filters

Set Port Symbolic Name: Text Field. Enter the number of the port who's filter set you want to set up. Use 1, 2, 3 or E. Press [Return] to accept the port name.

permit/deny: Text Field (`permit` / `deny`). Denote whether you want the protocols listed as members of the filter set to be forwarded (permitted) or filtered (denied). Enter `permit` to forward all packets with protocols listed as members, or `deny` to filter all packets with protocols listed as members. The default is `deny` with no protocols listed as members.

MEMBER: Text Field (`1` / `0`). Move to the field, under MEMBER, next to the relevant protocol family. Enter `1` to include to protocol family as a member of the filter set, or `0` to exclude the protocol family as a member of the filter set. The default is `0`.

Help lists the protocol IDs of the members of each family.

ADDITIONAL PROTOCOLS: Text Field. Enter an individual protocol's type to make it a member of the filter set. You can have up to 16. The format is nnnn (hexadecimal). The individual protocol filters are blank by default, `0000`.

For 802.3 networks, the protocol type is a Link-level Service Access Point (LSAP), a hexadecimal number between 1 and 255. For 802.3 networks you can also enter SNAP types, which are the same as Ethernet types. For Ethernet, the protocol type is the value of the type field in the Ethernet frame, a two-byte hexadecimal number.

Saving Protocol Filters

When you have set up your filter sets, you must use the Filter Options screen to save them. Exit from the Protocol screen and select FILTER SWITCHES from the Bridge Filters menu. You also use the Filter Options screen for enabling and disabling filters.

Enter y for the SAVE PROTOCOL INFO? field.

Reset the bridge.

Setting Up A Bit Filter

Select BIT FILTERS from the Bridge Filters menu.

The Configure Bit Filters screen appears, as shown in Figure 3-8. You use this screen for setting up bit filters, of which you can have up to five input and five output bit filters. The screen displays the bit filters' names (on the left) and a bit filter edit area (on the right).

Bit filters selectively filter out traffic based on bit values occurring in the first 64 bytes of each frame and can be of two types, input and output. Input filters will test packets as they are received and output filters will test packets as they are transmitted. When you use the Configure Bit Filters screen to set up and edit bit filters, you must choose the filter type first.

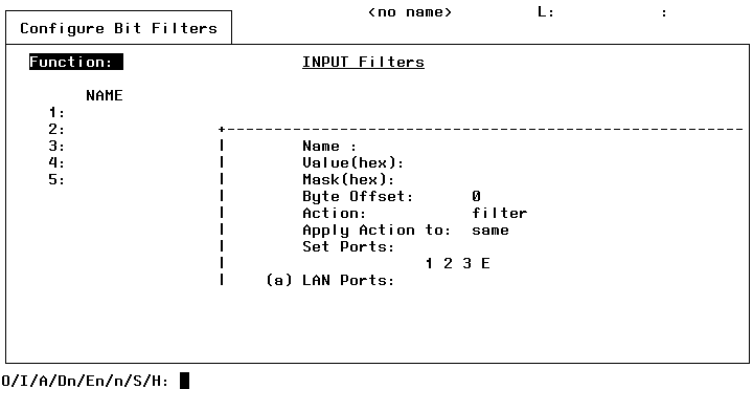


Figure 3-8 Configure Bit Filters

Function: Text Field (`O` / `I` / `A` / `Dn` / `En` / `n` / `S` / `H`). Enter `O` to choose the output filter type, or `I` to choose the input filter type. Press [Return]. The NAME list will change to show existing filters of the chosen type.

Enter `A` to add a bit filter of the chosen filter type.

Enter `Dn` to delete filter entry n from the list. For example, `D2` will delete the second entry.

Enter `En` to edit filter entry n in the list.

Enter `n` to adjust the list to begin with entry n.

Enter `S` to save the bit filters shown in the NAME list. This has the same effect as using the Filter Options to save bit filtering information.

Enter `H` to display help.

Name: Text Field. Enter the name of the filter. If you are editing or deleting an existing filter, use its name. The other fields in the bit filter edit area will reflect the bit filter's setup. You can enter up to eight characters with no spaces.

Value (hex): Text Field. Enter the bit values of the filter's bit pattern. The format is nn-nn-nn-nn-nn-nn (hexadecimal).

Mask (hex): Text Field. Enter the mask for the filter's bit pattern. The format is nn-nn-nn-nn-nn-nn (hexadecimal). The mask defines which of the bits in the VALUE pattern are to be included in the bit pattern. A value of `1` for any bit means that the bit in this location (in VALUE) is to be part of the bit pattern. A value of `0` means that the value of the bit in this location doesn't matter. For example, if VALUE is `81-37-00-00-00-00` and mask is `FF-FF-00-00-00-00`, the bit pattern is `81-37`.

Byte Offset: Text Field. Defines the location of the beginning of VALUE as the number of bytes from the beginning of the frame. It can be a number from 0 to 58.

For example, a byte offset of 12 lines up VALUE with the Ethernet type field, as shown in Figure 3-9.

Destination	Source	Type	Data (including other headers)
0	6	12	14

Figure 3-9 Ethernet Header Showing Byte Offsets

Action: Text Field (`filter` / `pass`). The action the filter set will take with relevant packets. Enter `filter` to filter the packets, or `pass` to forward the packets.

Apply Action to: Text Field (`same` / `different`). The set of packets the bridge will take action upon. Enter `same` to refer to packets matching the bit pattern, or `different` to refer to the packets not matching the bit pattern.

Set Ports: Text Field (`+n` / `+n-n` / `-n` / `-n-n`). The ports to which the filter applies. The ports are numbered from `1` to `4` (`4` refers to the external port). An `X` under the port number means that the filter applies to that port.

To include a port, enter `+n`, where n is the port number (for example, `+4` includes port 4).

To include a range of ports, enter `+n-n`, where n-n is the range (for example, `+2-4` includes ports 2 to 4).

To exclude a port, enter `-n`, where n is the port number (for example, `-4` excludes port 4).

To exclude a range of ports, enter `-n-n`, where n-n is the range (for example, `-2-4` excludes ports 2 to 4).

Saving Bit Filters

When you have set up your bit filters, you can use the Configure Bit Filters screen or the Filter Options screen to save them.

To save bit filters with the Configure Bit Filters screen, enter s for the FUNCTION: field.

To save bit filters with the Filter Options screen, enter y for the SAVE BIT FILTER INFO? field.

Reset the bridge.

The Host Filtering Table

It can be confusing to know which host-to-host and host-to-port filter sets devices are in. All devices entered into these filter sets are added to the bridge's *host filtering table*. The Host Filter Info screen is a very useful screen which uses this host filtering table to show which sets devices are in. You can also use it to change the contents of the filter sets.

Select HOST FILTER INFO from the Bridge Filters menu.

The Host Filter Info screen appears, as shown in Figure 3-10. The screen lists all the host-to-host and host-to-port filter sets. Next to each set is a number, `0` or `1`. If the device entered in the HOST NAME field is a member of any of the filter sets, a `1` will be shown next to it. A `0` will be shown next to the sets the device is not a member of.

```
                                    <no name>          L:            :
 Host Filter Info
 Host Name: DEFAULT       Host Address: 00-00-00-00-00-00      Table Size:     1
 ------------------------------------------------------------------------------
 Set Name M   Set Name M   Set Name M   Set Name M   Set Name M   Set Name M
 -- ----- -   -- ----- -   -- ----- -   -- ----- -   -- ----- -   -- ----- -
  1       0    8       1  15       1  22       1  29       1
  2       1    9       1  16       1  23       1  30       1
  3       1   10       1  17       1  24       1  31       1
  4       1   11       1  18       1  25       1  32       1
  5       1   12       1  19       1  26       1
  6       1   13       1  20       1  27       1
  7       1   14       1  21       1  28       1
 -- ----- -   -- ----- -   -- ----- -   -- ----- -   -- ----- -   -- ----- -
  1       1
  2       1
  3       1
  E       1
 ------------------------------------------------------------------------------
 Add htoh: 0 Remove htoh: 0 Add htop: 0 Remove htop: 0 Add/Remove Host:

Input Name:
```

Figure 3-10 Host Filter Info

Host Name: Text Field. Enter the device's host name. The screen changes to show the device's set membership.

Host Address: Text Field. Enter the address of the device. If the host name was recognized, the address will appear automatically.

Table Size: Display Field. The number of devices in the host filtering table (including the default host).

Add htoh: Text Field. Enter the number of the host-to-host set you want to add the device to. Enter `0` if you do not want to add the device to any host-to-host set.

Remove htoh: Text Field. Enter the number of the host-to-host set you want to remove the device from. Enter `0` if you do not want to remove the device from any host-to-host set.

Add htop: Text Field. Enter the number of the host-to-port set you want to add the device to. Enter `0` if you do not want to add the device to any host-to-port set.

Remove htop: Text Field. Enter the number of the host-to-port set you want to remove the device from. Enter `0` if you do not want to remove the device from any host-to-port set.

Add/Remove Host: Text Field (A / R). Enter A if you want to make the add and remove changes to the host filtering table (and to the filter sets). Enter R if you want to remove the device from the host filtering table (and from the filter sets).

Saving Host Filtering Table And Filter Set Changes

Use the Filter Options screen to save any changes made. Exit from the Host Filter Info screen and select FILTER SWITCHES from the Bridge Filters menu. You also use the Filter Options screen for enabling and disabling filters.

To save changes to the host-to-host filter sets, enter y for the SAVE HTOH SETS INFO? field and the SAVE HOST TABLE INFO? field.

To save changes to the host-to-port filter sets, enter y for the SAVE HTOP SETS INFO? field and the SAVE HOST TABLE INFO? field.

Reset the bridge.

Saving And Turning Filters On And Off

You will need to turn bridge filters on for them to take effect. You can turn them all on individually or all at once.

Select FILTER SWITCHES from the Bridge Filters menu.

The Filter Options screen appears, as shown in Figure 3-11. You use this screen for saving filters and enabling / disabling them.

This screen is used for saving custom filtering information. Each custom filtering description, within this chapter, describes what you need to do.

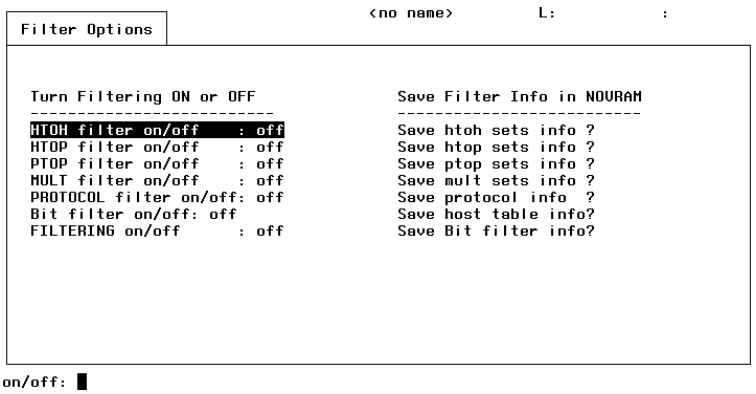


Figure 3-11 Filter Options

To enable filters:

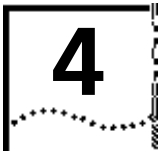
1. Next to the filters you want to turn on, enter `on`. Next to the filters you don't want to turn on, enter `off`.
2. Enter `on` for the FILTERING ON/OFF field.
3. Reset the bridge.

To disable all filters:

1 Enter `off` for the FILTERING ON/OFF field.

2 Reset the bridge.

In all cases, resetting the bridge causes the desired filtering to take effect. Any changes to filter sets that are in operation, take effect immediately.



MONITORING

This chapter contains the following topics:

Introduction

This chapter describes simple checks you can make at regular intervals to ensure the bridge and network are working as you intend. If you want information on other monitoring screens, refer to Chapter 5.

Monitoring the bridge and network is a good way of ensuring that the bridge and network are working as you intend. It is a good idea to have a regular checklist of monitoring screens. As you become familiar with your configuration, you can develop your own schedule of what you check and when.

Checking Bridge Statistics

Select MONITORING from the Main Menu. Select BRIDGES from the Monitoring menu. Select BRIDGE STATISTICS from the Bridges menu.

The Bridge Statistics screen appears, as shown in Figure 4-1. You use this screen for monitoring the various port and spanning tree parameters. These statistics display the state of the ports and the traffic on the bridge. This screen is useful as a problem solving aid.

The help screen for this screen displays port states that you will not see in this version of the product.

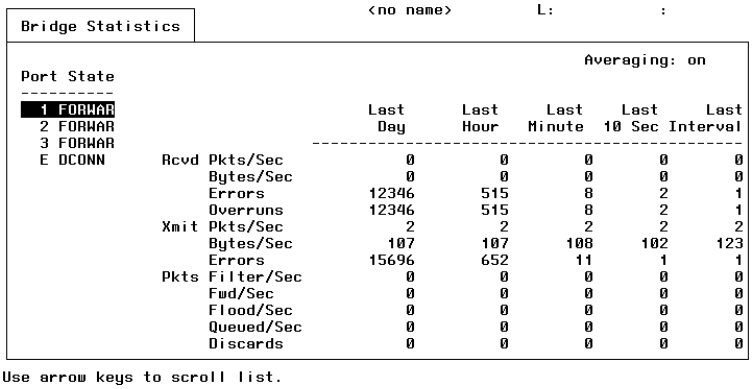


Figure 4-1 Bridge Statistics

Averaging: Display Field. This field displays whether the averaging feature has been turned `on` or `off`. If it is `on`, the number of packets or bytes displayed on this screen reflect averages per second. If it is `off`, the screen displays the numbers of packets or bytes accumulated since power-up. This feature is set on the System Information screen. The default is `on`.

Port State: Display Field. Displays the ports and their present state. The possible states are `MOS`, `Forwarding`, `Blocking`, `Listening` and `Learning`.

The external port may go into a disconnected state (`DCONN`) when a segment has not been attached, or a transceiver module is not fitted.

`MOS` (Manually Out of Service) means that the port has been manually disabled by a bridge administrator. No network traffic passes through it.

`Forwarding` means that the port is bridging packets and spanning tree calculations. All root ports and designated ports are in forwarding state, and these are the only ports that are ever in the forwarding state. If one bridge receives information from another bridge indicating that one of its ports should not be a root bridge or a designated port, that port is placed in the blocked state.

`Blocking` means that the port does not forward packets but is included in the spanning tree calculations. Ports enter the blocking state by a network administrator who enables a disabled port, or when spanning tree determines that the port creates an active loop in the network.

`Listening` means that the port is preparing to enter the active topology. At this point the port is not used for bridging packets, but C-BPDUs are received and transmitted on it, and it is included in the spanning tree calculations. If, after a predetermined amount of time, no information has been received indicating that the port should be blocked, the port passes into the learning state.

`Learning` means that the port is one step closer to bridging packets. Since the active topology may still be changing, a port in this state receives packets but does not bridge them. However, because the active topology is more stable than when the port is in the listening state, the port participates in the learning process of its bridge. In the learning process, the bridge associates the source address of each packet it receives with the identifier of the port on which it received the packet.

Rcvd

Pkts: Display Field. The number of packets received by the bridge.

Bytes: Display Field. The number of bytes received by the bridge.

Errors: Display Field. The number of packets with errors, received by the bridge.

Overruns: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost.

Xmit

Pkts: Display Field. The number of packets transmitted by the bridge.

Bytes: Display Field. The number of bytes transmitted by the bridge.

Errors: Display Field. The number of packets with errors, transmitted by the bridge.

Pkts

Filter: Display Field. The number of packets filtered by the bridge.

Fwd: Display Field. The number of packets forwarded by the bridge. Also counts flooded packets.

Flood: Display Field. The number of packets flooded by the bridge, regardless of whether they are filtered by ports.

Queued: Display Field. This indicates that buffers allocated to bridge ports have been full. Receptions from or transmissions out of them have therefore been queued.

Discards: Display Field. The number of packets discarded by the bridge.

There are three major observations you can make from the Bridge Statistics screen:

- Note the status of each port.

  You can check the status of each port to see if it is abnormal.

- Note the overall traffic.

  Occasional errors and overruns are normal in busy networks but you should investigate unusually high numbers in these fields. Familiarize yourself with normal received and transmitted traffic volumes for your configuration. This activity is called *baselining* and will help you spot unusual activity more quickly.

- Compare the forwarded traffic against other received and transmitted traffic.

  Bridges are used for restricting traffic between network segments. If your bridge is forwarding an unusually large amount of traffic, you may need to rearrange some of the nodes. Nodes that communicate frequently should, if possible, be on the same network segment.

Checking Port Activity

You can monitor individual bridge port activity for more specific traffic information if you suspect a problem with a port.

Select BRIDGE PORT STATS from the Bridges menu.

The Bridge Port Statistics screen appears, as shown in Figure 4-2. You use this screen for viewing statistics on packets received, transmitted and filtered by a port.

The help screen for this screen displays port states that you will not see in this version of the product.

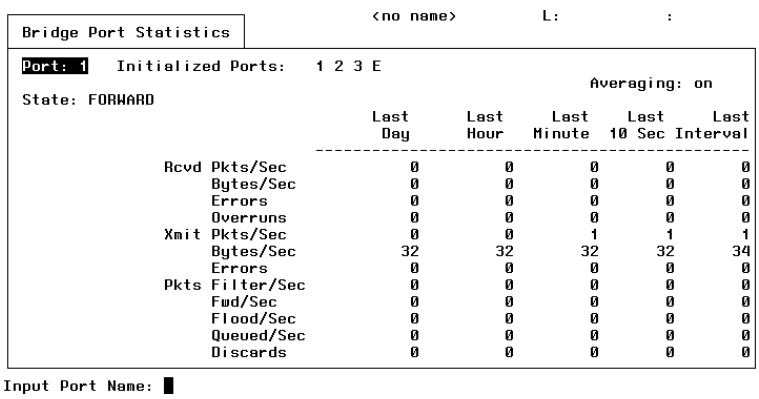


Figure 4-2 Bridge Port Statistics

Port: Text Field. Enter the name of the port who's statistics you want to view. Use 1, 2, 3 or E.

Averaging: Display Field. This field displays whether the averaging feature has been turned `on` or `off`. If it is `on`, the number of packets or bytes displayed on this screen reflect averages per second. If it is `off`, the screen displays the numbers of packets or bytes accumulated since power-up.

This feature is set on the System Information screen. The default is `on`.

Port State: Display Field. Displays the ports and their present state. The possible states are `MOS`, `Forwarding`, `Blocking`, `Listening` and `Learning`.

The external port may go into a disconnected state (`DCONN`) when a segment has not been attached, or a transceiver module is not fitted.

`MOS` (Manually Out of Service) means that the port has been manually disabled by a bridge administrator. No network traffic passes through it.

`Forwarding` means that the port is bridging packets and spanning tree calculations. All root ports and designated ports are in forwarding state, and these are the only ports that are ever in the forwarding state. If one bridge receives information from another bridge indicating that one of its ports should not be a root bridge or a designated port, that port is placed in the blocked state.

`Blocking` means that the port does not forward packets but is included in the spanning tree calculations. Ports enter the blocking state by a network administrator who enables a disabled port, or when spanning tree determines that the port creates an active loop in the network.

`Listening` means that the port is preparing to enter the active topology. At this point the port is not used for bridging packets, but C-BPDUs are received and transmitted on it, and it is included in the spanning tree calculations. If, after a predetermined amount of time, no information has been received indicating that the port should be blocked, the port passes into the learning state.

`Learning` means that the port is one step closer to bridging packets. Since the active topology may still be changing, a port in this state receives packets but does not bridge them. However, because the active topology is more stable than when the port is in the listening state, the port participates in the learning process of its bridge. In the learning process, the bridge associates the source address of each packet it receives with the identifier of the port on which it received the packet.

Rcvd

Pkts: Display Field. The number of packets received by the port.

Bytes: Display Field. The number of bytes received by the port.

Errors: Display Field. The number of packets with errors, received by the port.

Overruns: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost.

Xmit

Pkts: Display Field. The number of packets transmitted by the port.

Bytes: Display Field. The number of bytes transmitted by the port.

Errors: Display Field. The number of packets with errors, transmitted by the port.

Pkts

Filter: Display Field. The number of packets filtered by the port.

Fwd: Display Field. The number of packets forwarded by the port. Also counts flooded packets.

Flood: Display Field. The number of packets flooded by the port, regardless of whether they are filtered by ports.

Queued: Display Field. This indicates that the buffer allocated to the bridge port has been full. Receptions from or transmissions out of it have therefore been queued.

Discards: Display Field. The number of packets discarded by the port.

Viewing Ethernet Statistics

You can use the Ethernet Statistics screen to check for suspected hardware problems on a port.

Select MONITORING from the Main Menu. Select PHYSICAL INTERFACES from the Monitoring menu. Select ETHER STATISTICS from the Physical Interfaces menu.

The Ethernet Statistics screen appears, as shown in Figure 4-3. You use this screen for viewing statistics of individual bridge ports. These statistics are useful for measuring performance and as a problem solving aid.

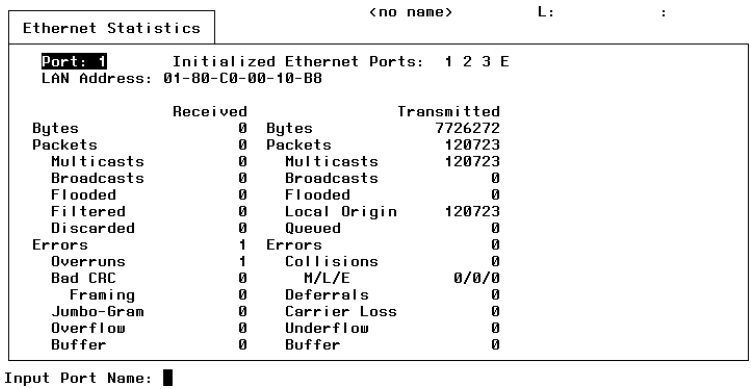


Figure 4-3 Ethernet Statistics

Port: Text Field. Enter the name of the port who's statistics you want to view. Use 1, 2, 3 or E.

Interface: Display Field. The Ethernet address of the port.

Received

Bytes: Display Field. The number of bytes received by the port.

Packets: Display Field. The number of packets received by the port.

Multicasts: Display Field. The number of multicast packets received by the port.

Broadcasts: Display Field. The number of broadcast packets received by the port.

Flooded: Display Field. The number of packets 'flooded' by the port. When the destination address is unknown, packets are forwarded to all but the receiving port.

Filtered: Display Field. The number of packets filtered by the port.

Discarded: Display Field. The number of packets due to be transmitted by the port that are discarded due to exceptional loading.

Errors: Display Field. The total number of errors on the receive port. There is always a minimum of error.

Overruns: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost. There is always a minimum of error.

Bad CRC: Display Field. The number of packets received with a bad checksum by the port.

Framing: Display Field. The number of packets received with framing errors by the port.

Jumbo-Gram: Display Field. The number of oversized packets (packets that have more than 1518 characters) received by the port.

Overflow: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost.

Buffer: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost.

Transmitted

Bytes: Display Field. The number of bytes transmitted by the port.

Packets: Display Field. The number of packets transmitted by the port.

Multicasts: Display Field. The number of multicast packets transmitted by the port.

Broadcasts: Display Field. The number of broadcast packets transmitted by the port.

Flooded: Display Field. The number of packets flooded by the port.

Local Origin: Display Field. Frames that originated within the bridge.

Queued: Display Field. This indicates that the transmit buffers associated with this port have become full and frames to be transmitted have been queued elsewhere.

Errors: Display Field. The total number of transmit errors on this port.

Collisions: Display Field. The total number of collision types on this port.

M/L/E: Display Field. The classification of the collision types. `M` is multiple, `L` is late and `E` is excess.

Deferrals: Display Field. The total number of deferrals on this port.

Carrier Loss: Display Field. During a transmission, carrier loss was detected.

Underflow: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost.

Buffer: Display Field. Due to exceptional loading conditions, the bridge has become overloaded and packets have been lost.

Checking User Access

Select MONITORING from the Main Menu. Select SYSTEM from the Monitoring menu. Select LOGIN HISTORY from the System menu.

The Login History screen appears, as shown in Figure 4-4. You use this screen to view details of logins since the bridge was last reset. This is useful for detecting attempted security breaches.

The screen displays entries for the ten most recent logins. Each entry contains the operator ID of the person logging in, and tells whether the login was local or remote. If the login was from a remote node, the entry also contains the node's IP address.

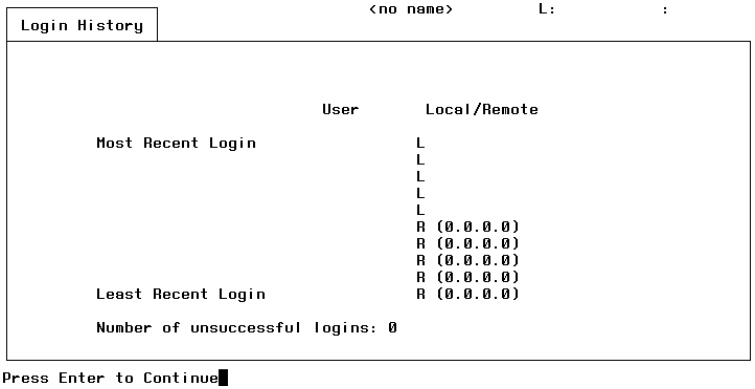


Figure 4-4 Login History

User: Display Field. The operator ID of the person who logged in.

Local/Remote: Display Field. Indicates whether the user logged in locally (shown by L) or remotely (shown by R). For remote logins, the screen also displays the IP address of the remote node (in brackets).

Number of unsuccessful logins: Display Field. The number of logins since the last bridge reset. An unsuccessful login can result from an incorrect entry of an operator ID or password.

5 Further Configuration And Monitoring

This chapter contains the following topics:

General Help

Select GENERAL HELP from the Main Menu.

The General Help screen appears, providing information on how to control the VT100 bridge management screens.

When you are looking at a screen or menu, you can obtain help by typing ? at the prompt. Some screens have their own, more specific, help screens which will appear instead of the General Help screen.

Configuration

Downloading Software Upgrades

Select CONFIGURATION from the Main Menu. Select SYSTEM from the Configuration menu. Select BOOT/LOADER INFO from the System menu.

The Boot/Loader Info screen appears, as shown in Figure 5-1. You use this screen for downloading any upgrades to the bridge's software.

Ensure the bridge has an IP address before attempting this procedure.

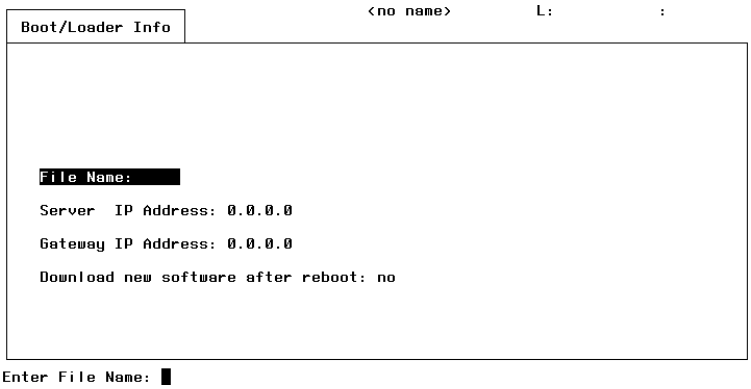


Figure 5-1 Boot/Loader Info

File Name: Text Field. Enter the name of the file to be downloaded onto the bridge.

Server IP Address: Text Field. Enter the IP address of the server where the file is located.

Gateway IP Address: Text Field. If you're on a routed network, you will need to enter the IP address of a suitable gateway through which the server can be accessed.

Download new software after reboot: Text Field. Enter yes to download the new software. Reset the bridge to start the procedure. Enter no to return to the FILE NAME field. To leave this screen, back out as normal. The default is no.

After agreeing to download new software, one of the following will happen when the bridge is reset:

- Software downloads

  The Boot Block User Interface appears, as shown in Figure 5-2, and the software downloads automatically. When complete, the Operator Login screen appears.

```
                BOOT BLOCK USER INTERFACE


          (1) Update download parameters
          (2) Restart download
          (3) Stop download
          (4) Reboot


          Enter selection:


Boot Block 1.0A4 released on Mon Mar 14 15:31:23 EST 1994
```

Figure 5-2 Boot Block User Interface

- Software does not download

  The Boot Block User Interface appears, as shown in Figure 5-2, prompting you to change download information. You can do one of two things:

  - Change the download information

    Enter 1 to update download parameters. The screen for changing download information appears, as shown in Figure 5-3. Enter the correct information and save the changes (enter 5). Return to the Boot Block User Interface and enter 2. The software downloads automatically and the Operator Login screen appears, when complete.

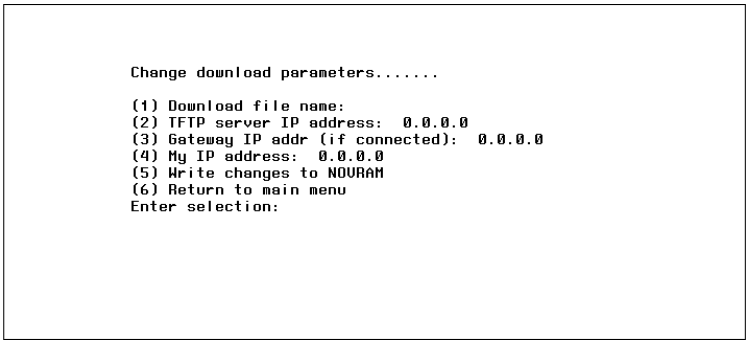


Figure 5-3 Changing Download Parameters

  - Stay with the current software

    Enter 3 to stop the download and return to normal bridge operation. The bridge resets itself and the Operator Login screen appears

The Permanent Database

Upto 1000 entries in the filtering database can be made permanent. Permanent entries are non-volatile and will not age. Entries can be added, deleted or transferred.

Add Permanent Entry

Select CONFIGURATION from the Main Menu. Select BRIDGES from the Configuration menu. Select PERMANENT DATABASE from the Bridges menu. Select ADD ENTRY from the Permanent Database menu.

The Add Permanent Entry screen appears, as shown in Figure 5-4. You use this screen for adding permanent entries to the filtering database.

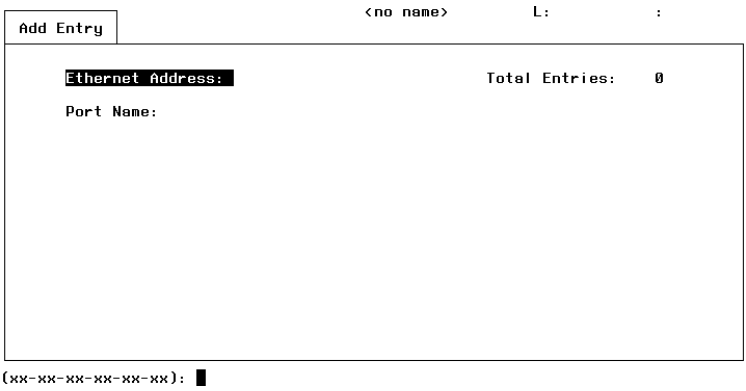


Figure 5-4 Add Permanent Entry

Ethernet Address: Text Field. The device address you want to make permanent.

Changes to this field are saved immediately. Reset the bridge for the change to take effect.

Port Name: Text Field. The port you want to make the device permanent for.

Changes to this field are saved immediately. Reset the bridge for the change to take effect.

Total Entries: Display Field. The total number of permanent entries in the filtering database.

Delete Permanent Entry

Select CONFIGURATION from the Main Menu. Select BRIDGES from the Configuration menu. Select PERMANENT DATABASE from the Bridges menu. Select DELETE ENTRY from the Permanent Database menu.

The Delete Permanent Entry screen appears, as shown in Figure 5-5. You use this screen for deleting permanent entries from the filtering database.

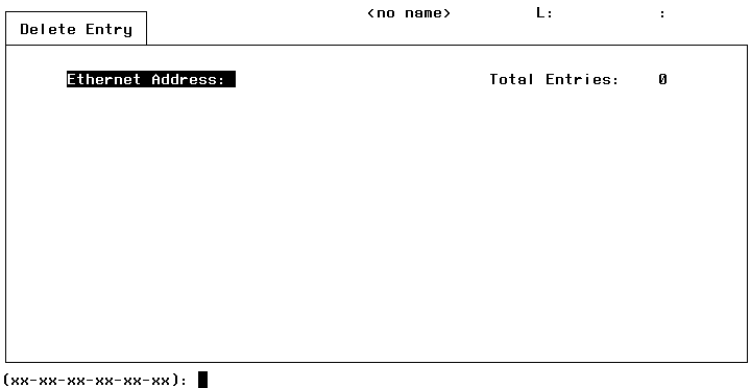


Figure 5-5 Delete Permanent Entry

Ethernet Address: Text Field. The permanent entry you want to make non-permanent.

Changes to this field are saved immediately. Reset the bridge for the change to take effect.

Total Entries: Display Field. The total number of permanent entries in the filtering database.

Transfer Permanent Entries

Select CONFIGURATION from the Main Menu. Select BRIDGES from the Configuration menu. Select PERMANENT DATABASE from the Bridges menu. Select TRANSFER ENTRIES from the Permanent Database menu.

The Transfer Permanent Entries screen appears, as shown in Figure 5-6. You use this screen for transferring learnt addresses from the filtering database to the permanent database. The permanent database can hold up to 1000 entries. The number of entries transferred depends on the number of vacant entries in the permanent database.

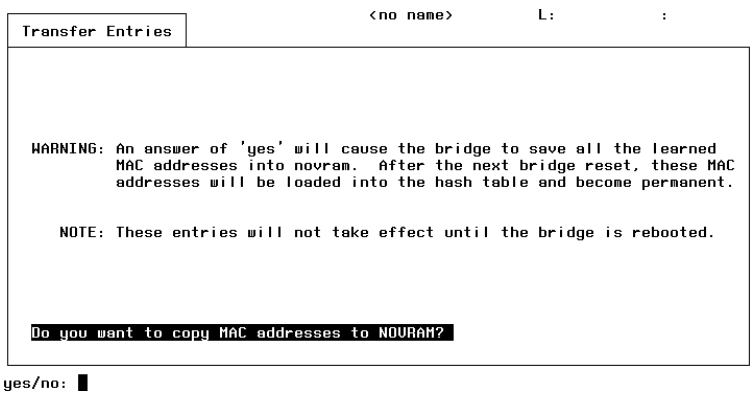


Figure 5-6 Transfer Permanent Entries

Enter y to confirm the transfer. Leave the screen if you do not want to transfer the entries.

Editing ARP Information

ARP Parameters

Select CONFIGURATION from the Main Menu. Select NETWORK PROTOCOL from the Configuration menu. Select ARP from the Network Protocol menu. Select PARAMETERS from the ARP menu.

The ARP Parameters screen appears, as shown in Figure 5-7. You use this screen for configuring the way in which the bridge manages the local ARP (Address Resolution Protocol) tables.

The bridge uses ARP to obtain from the network the physical address that corresponds to a specific IP address. It stores the learned IP/physical address pairs in ARP tables. This screen is intended for use by Product Support Engineering personnel only.

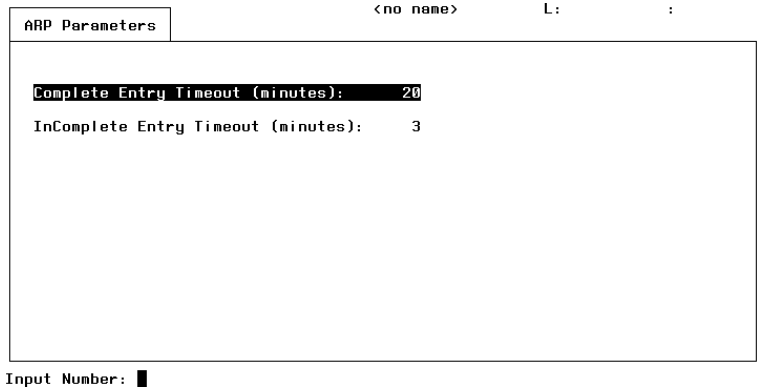


Figure 5-7 ARP Parameters

Add ARP Entry

Select CONFIGURATION from the Main Menu. Select NETWORK PROTOCOL from the Configuration menu. Select ARP from the Network Protocol menu. Select ADD ENTRY from the ARP menu.

The Add ARP Entry screen appears, as shown in Figure 5-8. This screen is used for manually adding entries to the ARP tables and is intended for use by Product Support Engineering personnel only.

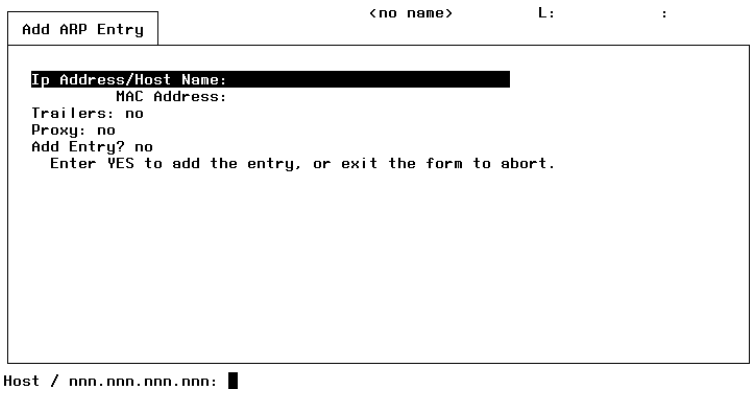


Figure 5-8 Add ARP Entry

Delete ARP Entry

Select CONFIGURATION from the Main Menu. Select NETWORK PROTOCOL from the Configuration menu. Select ARP from the Network Protocol menu. Select DELETE ENTRY from the ARP menu.

The Delete ARP Entry screen appears, as shown in Figure 5-9. This screen is used for manually deleting entries from the ARP tables and is intended for use by Product Support Engineering personnel only.

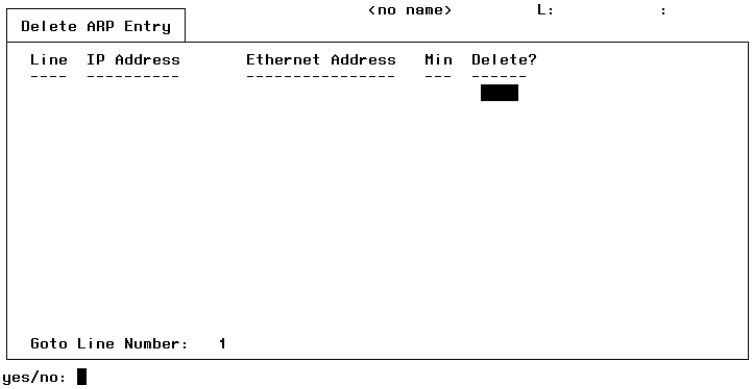


Figure 5-9 Delete ARP Entry

Changing TCP Characteristics

Select CONFIGURATION from the Main Menu. Select NETWORK PROTOCOL from the Configuration menu. Select TCP from the Network Protocol menu.

The TCP Protocol Settings screen appears, as shown in Figure 5-10. You use this screen for changing operational characteristics of the bridge's TCP (Transmission Control Protocol) software. TCP supports the operation of Telnet, which allows users to log into remote devices from the bridge.

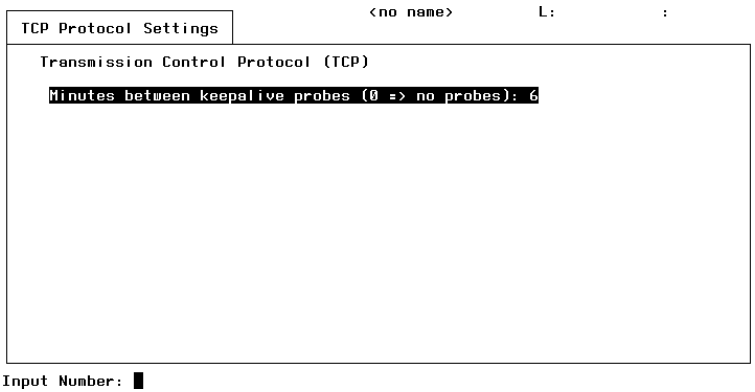


Figure 5-10 TCP Protocol Settings

Minutes between keepalive probes: Text Field. A keepalive probe is a packet that the TCP software sends to the remote system to request the status of a connection. If the remote system fails to respond, the local system ends the connection. The range should be between `0` and `65536`. The default is `6` minutes.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Changing Telnet Characteristics

Select CONFIGURATION from the Main Menu. Select NETWORK PROTOCOL from the Configuration menu. Select TELNET from the Network Protocol menu.

The Telnet Protocol Settings screen appears, as shown in Figure 5-11. You use this screen for changing operational characteristics of the bridge's Telnet software. Telnet allows users to log into remote devices from the bridge.

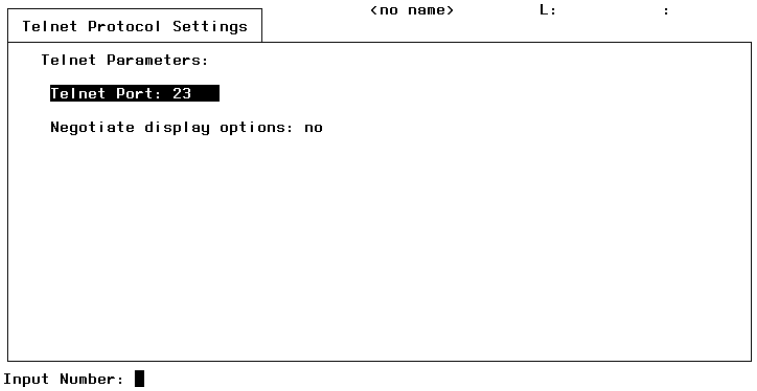


Figure 5-11 Telnet Protocol Settings

Telnet Port: Text Field. Lets you reassign the Telnet port number to a value other than the default value of 23. This shouldn't normally need to be changed.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Negotiate display options: Text Field. Causes the local system to display a transcription of the negotiation of virtual terminal options. This negotiation takes place regardless of the value of this parameter, which controls the display of the transcription only. This intended for use by Product Support Engineering personnel only.

Enter yes to display negotiations, or no to not display negotiations. The default is no.

Changes to this field are only saved during a bridge reset, and take effect from then on.

Port Queuing

Select CONFIGURATION from the Main Menu. Select SOFTWARE QUEUES from the Configuration menu.

The Software Queues screen appears, as shown in Figure 5-12. Do not change the default values of `14` (for MAX SIZE) and `10` (for MAX LIFE).

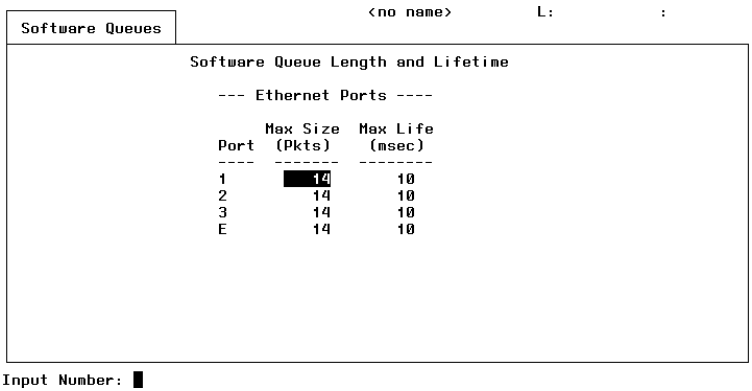


Figure 5-12 Software Queues

Monitoring

Viewing General Bridge Information

Select MONITORING from the Main Menu. Select SYSTEM from the Monitoring menu. Select SYSTEM INFO from the System menu.

The General System Information screen appears, as shown in Figure 5-13. You use this screen for viewing general bridge information and statistics.

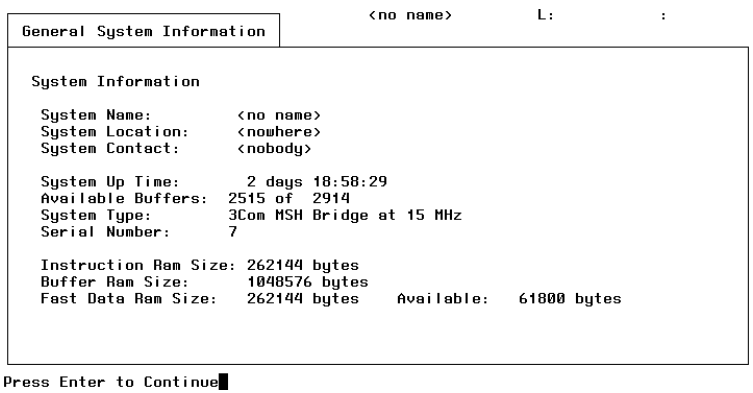


Figure 5-13 General System Information

System Name: Display Field. The name by which the bridge is known. This is not it's host name.

System Location: Display Field. The physical location of the bridge.

System Contact: Display Field. The name of the system administrator or person responsible for the bridge.

System Up Time: Display Field. The days, hours, minutes and seconds since the bridge was initialized.

Available Buffers: Display Field. The number of buffers currently free in the bridge. This number changes over time.

System Type: Display Field. The type of bridge. This entry is automatically set.

Serial Number: Display Field. The serial number of the bridge, as recorded in the hardware.

Instruction Ram Size: Display Field. The number of bytes of instruction RAM in the bridge. This number only changes if the motherboard changes.

Buffer Ram Size: Display Field. The number of bytes of buffer RAM in the bridge. This number only changes if the motherboard changes.

Fast Data Ram Size: Display Field. The number of bytes of data RAM in the bridge. This number only changes if the motherboard changes.

Viewing Node Table Information

Node Table By Address

Select MONITORING from the Main Menu. Select BRIDGES from the Monitoring menu. Select NODE TABLE/ADDRESS from the Bridges menu.

The Node Table By Address screen appears, as shown in Figure 5-14. You use this screen for monitoring traffic by displaying information from the bridge's forwarding database. This screen displays running data on a selected Ethernet address and the port which most recently received a packet from that address.

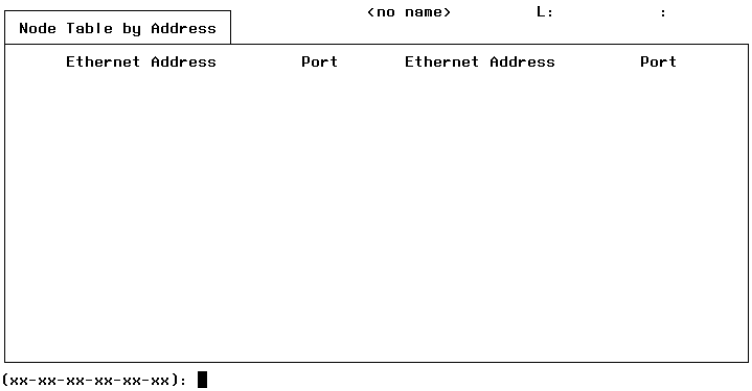


Figure 5-14 Note Table By Address

Ethernet Address: Text Field. Enter the address you want to monitor, in hexadecimal (nnn-nnn-nnn-nnn).

Port: Display Field. The port that most recently received a packet from that specified address.

Node Table By Hash Bucket

Select MONITORING from the Main Menu. Select BRIDGES from the Monitoring menu. Select NODE TABLE/HASH from the Bridges menu.

The Node Table By Hash Bucket screen appears, as shown in Figure 5-15. This screen shows the bridge's filtering database, with the permanent and learnt devices. This screen displays a subset of the hash values used by the database.

There are approximately 20 permanent entries (16 fixed addresses and the 4 ports' MAC addresses, required for bridge operations).

The bridge applies a hashing algorithm to each Ethernet address in the forwarding database to produce a hash value between 0 and 511. The algorithm groups multiple Ethernet addresses under a single hash number, called a *hash bucket*, reducing the time it takes to look up an address in the database.

To empty the filtering database of non-permanent entries, reset the bridge. Use the permanent database screens for adding and removing permanent entries.

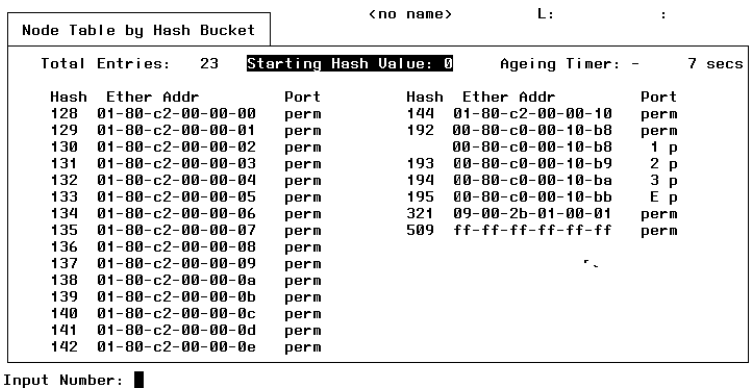


Figure 5-15 Node Table By Hash Bucket

Total Entries: Display Field. The total number of entries in the filtering database. You can have `4953` entries (additional to the permanent entries).

Starting Hash Value: Text Field. The first value of the subset you want to display. Enter a number from `0` to `511`. The default is `0`.

Ageing Timer: Display Field. The number of seconds left in the current ageing time interval. The ageing timer keeps the bridge's forwarding database current. When the ageing timer reaches zero, the bridge discards all table entries that were not verified during the last ageing time interval. For an entry to be verified for an address, the bridge must receive a frame from that address on the port specified in the entry.

Hash: Display Field. A subset of the individual hash values from the forwarding database. The hash column starts with the starting value specified in the STARTING HASH VALUE field.

Ether Addr: Display Field. The Ethernet address that corresponds to the value in the HASH field.

Port: Display Field. The port that last received a packet from the corresponding Ethernet address. `p` is appended to entries containing the address of a port. perm identifies an address that will never be discarded from the database, such as the address of a bridge port. `v` identifies entries that have been made permanent by a user, using the permanent database screens. After a port number, a + or - is shown, indicating the ageing time status of the port.

+ indicates that the packet with the corresponding source address has arrived at the port during the current ageing time interval. When the ageing time interval expires, this entry is set to - and the address remains in the forwarding database.

- indicates that the address has not yet appeared at the port as a source address during the current ageing time interval. When the ageing time interval expires, entries set as - are discarded.

Viewing The Hardware Configuration

Select MONITORING from the Main Menu. Select PHYS INTERFACES from the Monitoring menu. Select HARDWARE STATUS from the Phys Interfaces menu.

The Hardware Configuration screen appears, as shown in Figure 5-16. You use this screen for viewing the hardware configuration of the bridge. This screen displays the status of each LAN address in the bridge.

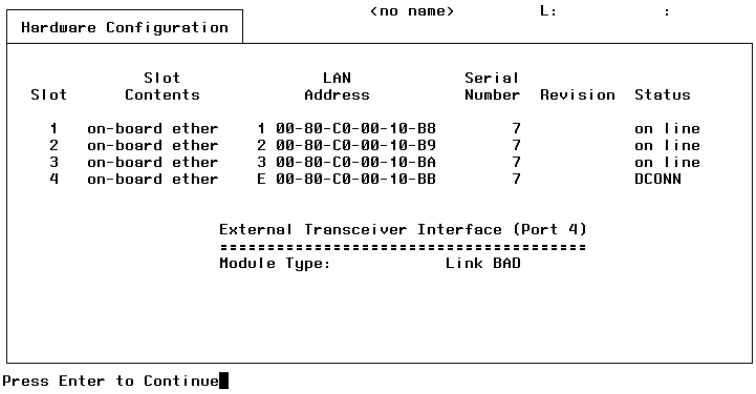


Figure 5-16 Hardware Configuration

LAN Address: Display Field. The LAN address of the port.

Status: Display Field. The current state of the LAN address.

Module Type: Display Field. Indicates the transceiver module type or, if one is not present, displays `Link BAD`.

Viewing Socket Statistics

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select SOCKET STATISTICS from the Network Protocol menu.

The Socket Statistics screen appears, as shown in Figure 5-17. You use this screen for checking the status of active socket addresses being used by the bridge.

A socket is an address of an application that is using the services of a transport protocol, either UDP or TCP. Some socket addresses are permanently assigned to TCP socket 23. These are called well-known sockets. Other sockets are assigned dynamically.

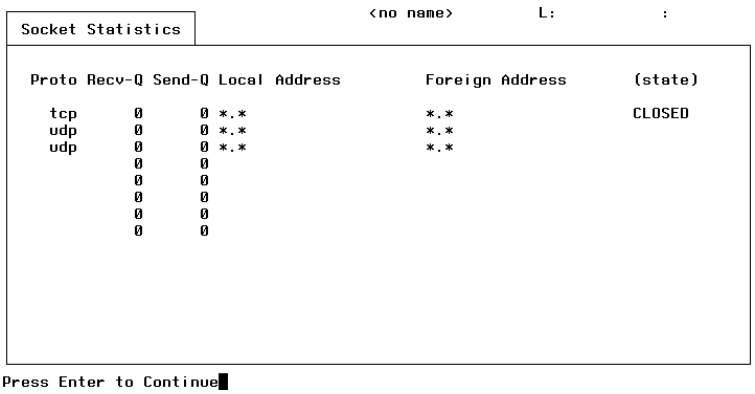


Figure 5-17 Socket Statistics

Proto: Display Field. The type of protocol in use at the local address displayed in the local address column.

Recv-Q: Display Field. The number of bytes of data that have been received and are in the socket buffer waiting to be delivered.

Send-Q: Display Field. The number of bytes of data that are in the socket buffer ready to be sent.

Local Address: Display Field. The IP address and socket number of the local interface (separated by a period). Asterisks represent addresses that are not yet determined. For example, the TCP address `*.23` represents the Telnet socket for any local IP address. The UDP address `*.161` represents the SNMP socket for any local IP address.

Foreign Address: Display Field. The IP address and socket number of the remote entity (separated by a period). Asterisks represent addresses and socket numbers that are not yet determined.

State: Display Field. The current state of TCP sockets. The states are:

`CLOSED` which means that the socket is not being used.

`LISTEN` which means that the socket is listening for incoming connections.

`SYN_SENT` which means that the socket is trying to establish a connection.

`SYN_RECEIVED` which means that the synchronization of the connection is in progress.

`ESTABLISHED` which means that the connection is established.

`CLOSE_WAIT` which means that the remote connection has shut down and the socket is waiting to close.

`FIN_WAIT_1` which means that the socket is closed and the connection is being closed.

`CLOSING` which means that the local socket has closed and is awaiting remote shutdown acknowledgement.

`LAST_ACK` which means that the remote socket has shut down and is awaiting acknowledgement.

`FIN_WAIT_2` which means that the local socket is closed and is waiting for remote shutdown.

`TIME_WAIT` which means that the local socket is closed and is waiting for remote shutdown re-transmission.

Viewing UDP Statistics

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select UDP STATISTICS from the Network Protocol menu.

The UDP Statistics screen appears, as shown in Figure 5-18. You use this screen for viewing statistics for the bridge's UDP (User Datagram Protocol) activity.

UDP is a transport-layer protocol of the Internet Protocol suite. SNMP uses UDP as its transport protocol. Consequently, the data displayed on this screen, such as the number of UDP packets discarded because of headed errors, can be of interest if you are using the SNMP agent.

All statistic values displayed in this screen reset to zero when the bridge is reset.

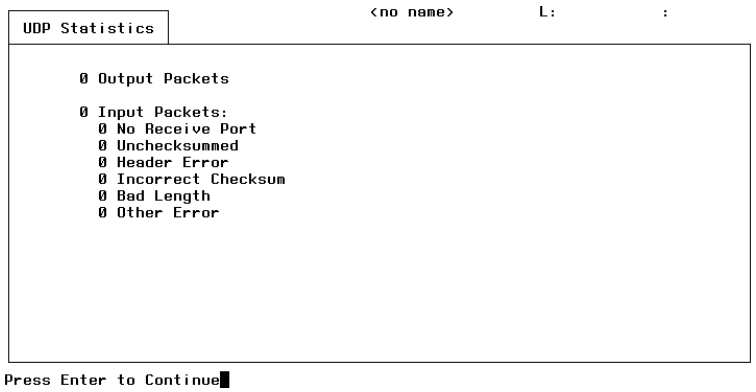


Figure 5-18 UDP Statistics

Output Packets: Display Field. The total number of UDP packets transmitted by the system. (`udpOutDatagrams` in the MIB.)

Input Packets: Display Field. The total number of UDP packets received by the system. (`udpInDatagrams` in the MIB.)

No Receive Port: Display Field. The number of UDP packets discarded by the system because there was no application at the destination protocol port. (`udpNoPorts` in the MIB.)

Unchecksummed: Display Field. The number of UDP packets received by the system without a checksum in the header (i.e. with a checksum of 0). This is permissible with UDP, but not advisable. (`cUdpNoChecksum` in the MIB.)

Header Error: Display Field. The number of UDP packets discarded by the system because of a header error other than incorrect checksum. (`cUdpHdrDrops`, a component of `udpInErrors` in the MIB.)

Incorrect Checksum: Display Field. The number of UDP packets discarded by the system because of an incorrect checksum. (`cUdpBadCheckSum`, a component of `udpInErrors` in the MIB.)

Bad Length: Display Field. The number of UDP packets discarded by the system because of a problem with the packet length. For example, the length in the header was longer than the number of bytes of data. (`cUdpBadLength`, a component of `udpInErrors` in the MIB.)

Other Error: Display Field. The number of UDP packets discarded by the system because of an error other than one of the preceding. Typically, 'other' errors are caused by problems internal to the software on the bridge. (`cUdpOtherErrors`, a component of `udpInErrors` in the MIB.)

Viewing TCP Information

TCP Data Statistics

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select TCP STATISTICS from the Network Protocol menu.

The TCP Data Statistics screen appears, as shown in Figure 5-19. You use this screen for viewing statistics on a bridge's TCP (Transmission Control Protocol) activity. TCP is a transport-layer protocol of the Internet Protocol suite. Telnet uses TCP as its transport protocol. This screen is only of use in rare cases involving Telnet.

This screen is followed by the TCP Connection Statistics screen.

```
                                <no name>        L:          :
 TCP Data Statistics
      0 Packets Received                        0 Packets Sent
        0 acks (for 0 bytes)                      0 data pkts (0 bytes)
        0 duplicate acks                          0 data pkts retransmit
        0 acks for unsent data                          (0 bytes)
        0 pkts (0 bytes)                          0 ack-only pkts (0 delayed)
          rcvd in-sequence                        0 URG only pkts
        0 dupl pkts (0 bytes)                     0 window probe pkts
        0 pkts w. some dup. data                  0 window update pkts
          (0 bytes duped)                         0 control pkts
        0 pkts (0 bytes)
          rcvd out-of-order
        0 pkts (0 bytes) of data after window
        0 window probes
        0 window update pkts
        0 pkts rcvd after close
        0 discarded for bad checksum
        0 discarded for bad header offset fields
        0 discarded because pkt too short

Press Enter to Continue
```

Figure 5-19 TCP Data Statistics

Packets Received

Packets Received: Display Field. The number of packets received.

acks: Display Field. The number of frames received where the TCP ACK bit was set.

duplicate acks: Display Field. The number of frames received where the TCP ACK bit was set and the Acknowledgement number was the same as the previously received ACK.

acks for unsent data: Display Field. The number of frames received where the TCP ACK bit was set and the Acknowledgement number is greater than the last byte number in the datastream sent so far.

pkts rcvd in-sequence: Display Field. The number of packets received where the sequence numbers follow one another.

dupl pkts: Display Field. The number of packets received where the sequence number is the same.

pkts w. some dup. data: Display Field. The number of packets received where some of the data is a repetition of data already sent, but the remaining data in the packet is new.

pkts rcvd out-of-order: Display Field. The number of packets received where the sequence number has not followed on from previous packets.

pkts of data after window: Display Field. The number of packets received containing data after the window size has reached zero.

window probes: Display Field. The number of packets sent by the data sender containing the last byte of data in order to ascertain if it can send any more data.

window update pkts: Display Field. The number of packets received containing no data but updating the window size.

pkts rcvd after close: Display Field. The number of packets received after a FIN has been received for the session.

discarded for bad checksum: Display Field. The number of packets received where the TCP checksum was invalid.

discarded for bad header offset fields: Display Field. The number of packets received that were discarded because the header offset is invalid.

discarded because pkt too short: Display Field. The number of frames received and discarded because the data section ends before the length specified by the TCP LENGTH field.

Packets Sent

Packets Sent: Display Field. The number of TCP packets sent.

data pkts: Display Field. The number of TCP packets sent containing data.

data pkts retransmit: Display Field.The number of TCP packets containing data that were retransmitted.

ack-only pkts: Display Field. The number of TCP packets sent where the ACK flag was set and no data.

URG only pkts: Display Field. The number of TCP packets sent containing no data but with the URGENT flag set.

window probe pkts: Display Field. The number of TCP window probe packets sent.

window update pkts: Display Field. The number of TCP packets sent containing no data but a new window size.

control pkts: Display Field. The number of TCP control packets sent (packets containing no data such as SYN, FIN RST).

TCP Connection Statistics

The TCP Connection Statistics screen appears, as shown in Figure 5-20, after the TCP Data Statistics screen. You use this screen for viewing statistics on a bridge's TCP (Transmission Control Protocol) activity. TCP is a transport-layer protocol of the Internet Protocol suite. Telnet uses TCP as its transport protocol. This screen is only of use in rare cases involving Telnet.

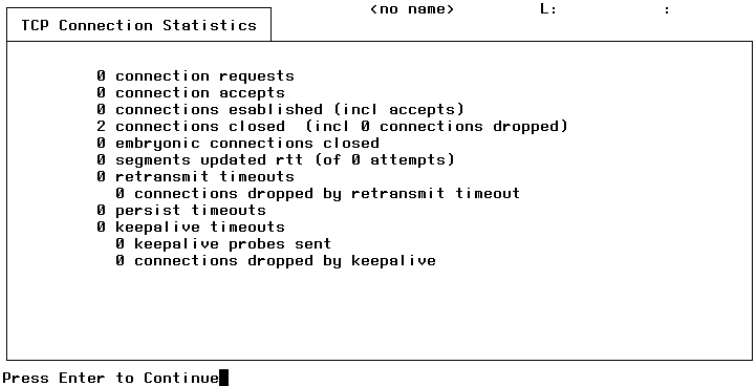


Figure 5-20 TCP Connection Statistics

connection requests: Display Field. The number of connection requests (the number of SYN packets received).

connection accepts: Display Field. The number of connections accepted (the number of SYN-ACKs transmitted).

connections established: Display Field. The number of connections where an ACK was received to a transmitted SYN-ACK.

connections closed: Display Field. The number of connections closed by receiving/transmitting a FIN.

embryonic connections closed: Display Field. The number of connections where a FIN followed a SYN SYN-ACK sequence without an ACK to the SYN-ACK.

segments updated rtt: Display Field. The `segment updated rtt' counter.

retransmit timeouts: Display Field. The number of times the retransmit timer has fired resulting in retransmission of the previous packet.

connections dropped by retransmit timeout: Display Field. The number of times a connection has been closed because the maximum number of retransmit timeouts has been exceeded for the connection.

persist timeouts: Display Field. The 'persist timeouts' counter.

keepalive timeouts: Display Field. The number of times the keepalive timer has expired resulting in the transmission of a keepalive frame.

keepalive probes sent: Display Field. The number of keepalive packets transmitted.

connections dropped by keepalive: Display Field. The number of connections terminated because the maximum number of keepalive frames have been exceeded on a connection.

Viewing IP Statistics

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select IP STATISTICS from the Network Protocol menu.

The IP Statistics screen appears, as shown in Figure 5-21. You use this screen for viewing a statistical summary for all IP activity on the bridge.

All statistic values displayed in this screen reset to zero when the bridge is reset.

```
                                    <no name>          L:            :
 IP Statistics
          0 total packets received:              0 with bad header checksums
                                                 0 with size smaller than minimum
                                                 0 with data size < data length
                                                 0 header length < data size
                                                 0 with data length < header length

          0 fragments received:                  0 frags dropped (dup or no space)
                                                 0 frags dropped after timeout

          0 packets were fragmented on transmit (        0 fragments created)

          0 packets forwarded
          0 packets not forwardable
          0 packets redirects sent

       0 network broadcasts received for local networks
       0 network broadcasts forwarded by media broadcast
       0 network broadcasts partially processed

 Press Enter to Continue
```

Figure 5-21 IP Statistics

total packets received

total packets received: Display Field. The number of IP packets received by the bridge. This includes only packets addressed to the bridge, destined for an upper-layer destination on the bridge (such as Telnet).

bad header checksums: Display Field. The number of TCP packets containing an invalid TCP checksum in the TCP header.

with size smaller than minimum: Display Field. The number of TCP packets received where the size of the packet is too small.

with data size < data length: Display Field. The number of TCP packets received where the actual data is smaller than that specified in the TCP header.

header length < data size: Display Field. The number of TCP packets received where the length specified in the header is smaller than the data received.

with data length < header length: Display Field. The number of TCP packets received where the length of the data is smaller than that specified in the TCP header.

fragments received

fragments received: Display Field. The number of IP fragments received. Before an IP packet is forwarded, it must sometimes be divided into smaller pieces (called *fragments*), which are transmitted as individual packets. The destination host stores the fragments until it has received them all, then it reassembles the original message.

fragments dropped (dup or no space): Display Field. The number of fragments the bridge discarded because they were duplicates, or because there was no memory available in which to store them.

This refers only to fragments for which the bridge is the final destination.

fragments dropped after timeout: Display Field. The number of fragments the bridge discarded because the amount of time allowed to collect all of a message's fragments has expired.

This refers only to fragments for which the bridge is the final destination.

packets were fragmented on transmit: Display Field. The number of fragments the bridge transmitted. The FRAGMENTS CREATED subcount (in brackets) shows the number of fragments this bridge created, as opposed to those that it simply forwarded.

packets forwarded: Display Field. The number of packets the bridge has forwarded.

packets not forwardable: Display Field. The number of packets the bridge was unable to forward.

packets redirects sent: Display Field. The number of packets for which the bridge sent redirects. When a bridge receives a packet that it knows could have gone by a better route, it sends a redirect packet to the originating host informing it of the better route.

network broadcasts received for local networks: Display Field. The number of network broadcasts received that were destined for networks to which the bridge is directly attached.

network broadcasts forwarded by media broadcast: Display Field. The number of network broadcasts received that the bridge sent to the physical broadcast address on the specified network.

network broadcasts partially processed: Display Field. The number of network broadcasts received for which the bridge was unable to complete the physical broadcasting.

Viewing ICMP Packet Statistics

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select ICMP STATISTICS from the Network Protocol menu.

The ICMP Packet Statistics screen appears, as shown in Figure 5-22. You use this screen for viewing statistics on the bridge's ICMP (Internet Control Message Protocol) activity.

ICMP supports several IP activities, including flow control.

All statistic values displayed in this screen reset to zero when the bridge is reset.

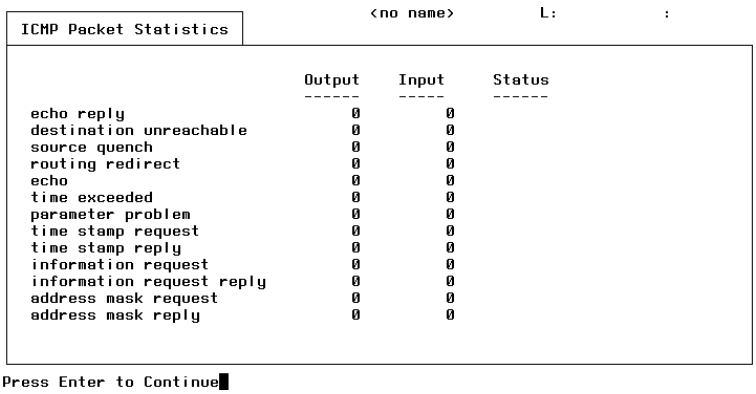


Figure 5-22 ICMP Packet Statistics

echo reply: Display Field. The number of 'echo reply' messages sent (output) and received (input). The 'echo reply' message acknowledges an 'echo request'.

destination unreachable: Display Field. The number of 'destination unreachable' messages sent (output) and received (input). When a node receives an IP packet that it cannot forward to its destination, it sends a 'destination unreachable' message to the sending node.

source quench: Display Field. The number of 'source quench' messages sent (output) and received (input). A 'source quench' is a flow control message that requests a reduction in the rate of datagram transmission.

routing redirect: Display Field. The number of 'redirect' messages sent (output) and received (input). When a node receives a packet to be forwarded which should have been sent by a different route, it sends an ICMP 'redirect' message to the sending node.

echo: Display Field. The number of 'echo request' messages sent (output) and received (input). 'Echo request' works in conjunction with the 'echo reply'.

time exceeded: Display Field. The number of 'time exceeded' messages sent (output) and received (input). The 'time exceeded' message tells a node that a packet it sent was discarded before reaching its destination, because its 'time-to-live' timer expired.

parameter problem: Display Field. The number of 'parameter problem' messages sent (output) and received (input). A 'parameter problem' message tells a node that a packet it sent was discarded, because it contained an error in an IP header parameter.

time stamp request: Display Field. The number of 'time stamp' messages sent (output) and received (input). A 'time stamp' message is a request for the value of the receiving node's system clock.

time stamp reply: Display Field. The number of 'time stamp reply' messages sent (output) and received (input). 'Time stamp reply' is an answer to a 'time stamp' request. Time information in the 'time stamp reply' allows the requesting host to estimate the differences between local and remote clocks. This headings displays the reply form of the original 'time stamp'.

information request: Display Field. The number of 'information request' messages sent (output) and received (input). 'Information request' messages are considered obsolete but were intended to allow hosts to discover their internet addresses at startup.

information request reply: Display Field. The number of 'information reply' messages sent (output) and received (input). 'Information reply' messages are considered obsolete.

address mask request: Display Field. The number of 'address mask request' messages sent (output) and received (input). 'Address mask request' messages ask for the subnet mask for the network.

address mask reply: Display Field. The number of 'address mask reply' messages sent (output) and received (input). 'Address mask reply' messages respond to 'address mask requests'.

Viewing SNMP Information

SNMP Statistics

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select SNMP STATISTICS from the Network Protocol menu.

The SNMP Statistics screen appears, as shown in Figure 5-23. You use this screen for viewing statistics on the SNMP (Simple Network Management Protocol) activity of the bridge.

This screen is followed by the SNMP Authentication Statistics screen.

All statistic values displayed in this screen reset to zero when the bridge is reset.

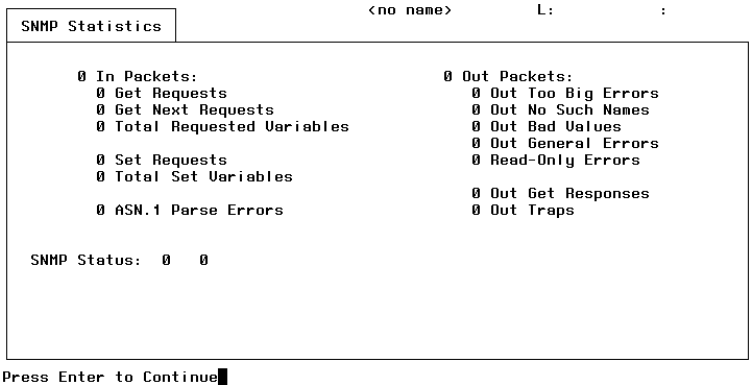


Figure 5-23 SNMP Statistics

In Packets

In Packets: Display Field. The total number of SNMP requests received by the SNMP agent on the bridge.

Get Requests: Display Field. The number of GET requests received by the SNMP agent.

Get Next Requests: Display Field. The number of GET-NEXT requests received by the SNMP agent.

Total Requested Variables: Display Field. The number of MIB variables retrieved by the SNMP agent as the result of GET and GET-NEXT requests.

Set Requests: Display Field. The number of SET requests received by the SNMP agent.

Total Set Variables: Display Field. The number of variables received by the SNMP agent as the result of the SET requests.

ASN.1 Parse Errors: Display Field. The number of SNMP requests discarded because they contained an ASN.1 encoding error.

Out Packets

Out Packets: Display Field. The total number of SNMP messages sent by the SNMP agent.

Out Too Big Errors: Display Field. The number of messages sent by the agent that contained the value 'tooBig' in the error-status field. These messages respond to client requests that are either too long to be held in the system's buffers, or require a response from the agent that would be too long.

Out No Such Names: Display Field. The number of messages sent by the agent that contained the value 'noSuchName' in the error-status field. These messages respond to client requests that contain variable names (OBJECT-IDENTIFIERS) the agent does not recognize.

Out Bad Values: Display Field. The number of messages sent by the agent that contained the value 'badValue' in the error-status field. These messages respond to requests that contain invalid values.

Out General Errors: Display Field. The number of messages sent by the agent that contained the value 'genErr' in the error-status field. These messages respond to requests that contain errors not covered by any other error-status value.

Read-Only Errors: Display Field. The number of requests that generated a read-only error.

Out Get Responses: Display Field. The number of GET requests to which the agent has responded.

Out Traps: Display Field. The number of traps sent by the agent.

SNMP Status: Display Field. An internal status indicator.

SNMP Authentication Statistics

The SNMP Authentication Statistics screen appears, as shown in Figure 5-24, after the SNMP Statistics screen. You use this screen for viewing access errors detected by the bridge's SNMP agent.

All statistic values displayed in this screen reset to zero when the bridge is reset.

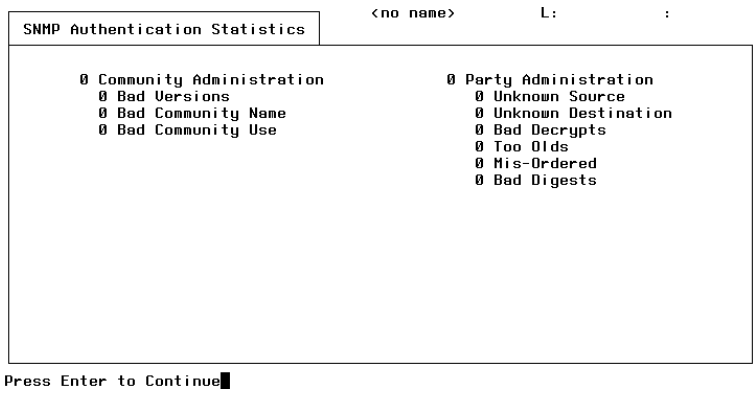


Figure 5-24 SNMP Authentification Statistics

Community Administration: Display Field. The number and type of community authentication checks performed by SNMP.

Bad Version: Display Field. The number of requests discarded by the agent because they specified an unsupported version of SNMP.

Bad Community Name: Display Field. The number of requests discarded because they contained a community name unknown to the bridge SNMP agent.

Bad Community Use: Display Field. The number of SNMP messages discarded because they requested an operation not allowed for the community.

Viewing ARP Tables

Select MONITORING from the Main Menu. Select NETWORK PROTOCOL from the Monitoring menu. Select ARP TABLES from the Network Protocol menu.

The ARP Tables screen appears, as shown in Figure 5-25. You use this screen for viewing the ARP table.

The ARP (Address Resolution Protocol) defines a standard for mapping 32-bit IP addresses to 48-bit physical (MAC) Ethernet addresses and communicating this mapping to the network node that requested the information.

Each node that implements ARP maintains a table of recently resolved IP addresses and their corresponding Ethernet addresses. When one node prepares to send an IP packet to another, it checks the ARP table for the physical address of the node's IP address. If it is not present, the sending node uses ARP to resolve the address and enters it in the ARP table.

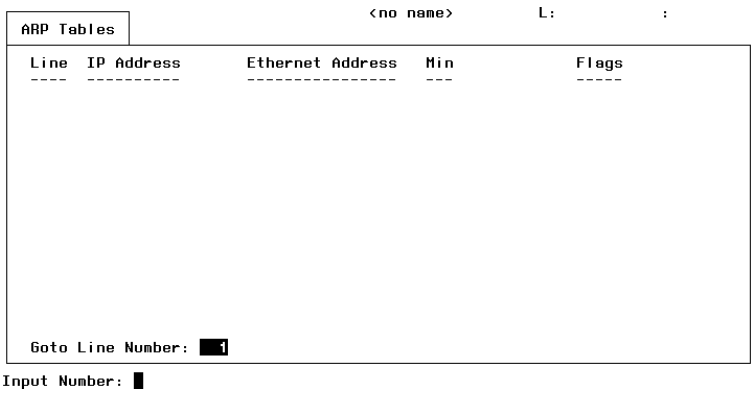


Figure 5-25 ARP Tables

Goto Line Number: Text Field. Enter the line number to go to a specific line.

Line: Display Field. The line number of the entry.

IP Address: Display Field. The 32-bit internet address of a remote node.

Ethernet Address: Display Field. The 48-bit physical (MAC) address of the remote node whose IP address is displayed in the IP ADDRESS field.

Min: Display Field. The number of minutes since this entry in the table was updated. When this value reaches `20`, the entry is removed from the table.

Interface: Display Field. The name of the interface through which the node is attached to the bridge.

Flags: Display Field. The entry `trailers` in this field indicates that the header and data fields in the address were reversed.

Viewing Diagnostic Information

Error Log

Select MONITORING from the Main Menu. Select DIAGNOSTICS from the Monitoring menu. Select ERROR LOG from the Diagnostics menu.

The Error Log screen is shown in Figure 5-26. You use this screen for viewing start-up errors and logged errors. When a bridge is booted up, it runs through a series of diagnostics that, if faulty, are recorded in this screen.

Any errors recorded here that impede the boot-up process indicate a problem that should be reported.

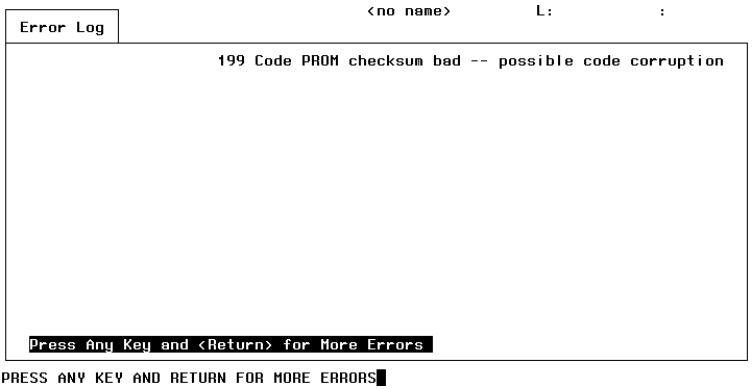


Figure 5-26 Error Log

Press Any Key and <Return> for More Errors: Text Field. Press a key and press [Return] to view more logged hardware errors. Use this when the first Error Log screen is full. Approximately two full screens of logged errors will display. When both screens are full of logged errors, newly logged errors begin to appear at the top of the first screen. The error log operates on a first-in first-out (FIFO) basis.

Interactive Diags

Select MONITORING from the Main Menu. Select DIAGNOSTICS from the Monitoring menu. Select INTERACTIVE DIAGS from the Diagnostics menu.

The Interactive Diags screen appears, as shown in Figure 5-27. You use this screen for selecting the type of hardware diagnostics you wish to view. You can set up four fields, each with three options; `yes`, `no`, or `periodically`.

`Yes` (y) always records data with errors. `No` (n) never records data with errors. `Periodically` (p) records data with errors every 5 seconds. Periodical error logging may degrade bridge performance.

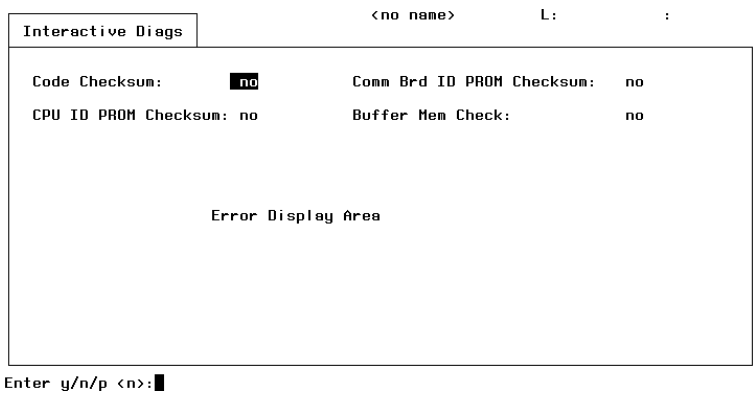


Figure 5-27 Interactive Diags

Code Checksum: Text Field. This records the code checksum. The code checksum test performs a 32-bit cyclical redundancy check (CRC) which verifies that the code is not corrupted.

CPU ID PROM Checksum: Text Field. This verifies the ID PROM of the CPU.

Buffer Mem Check: Text Field. This verifies the memory buffers. Each time the test is performed, it will randomly allocate a buffer of memory to verify.

Clear Error Log

Select MONITORING from the Main Menu. Select DIAGNOSTICS from the Monitoring menu. Select CLEAR ERROR LOG from the Diagnostics menu.

The Clear Error Log screen appears, as shown in Figure 5-28. You use this screen for clearing the accumulated data recorded in the error log. The error log displays start-up errors and is saved independently of other data on the bridge. Clearing the error log will have no impact on the operation of the bridge.

Use the Error Log screen to view the error log.

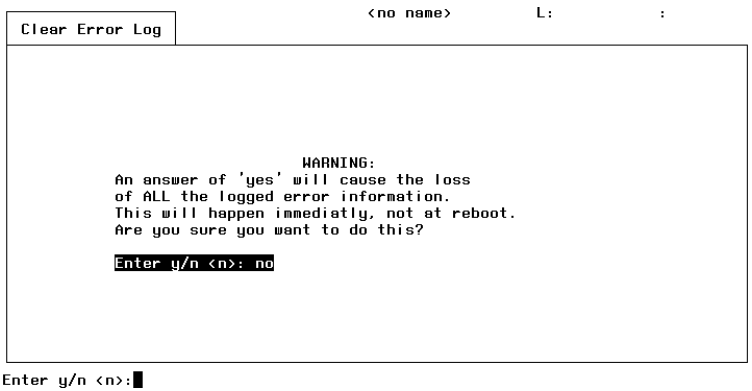


Figure 5-28 Clear Error Log

Enter y/n <n>: Text Field. Enter y to clear the error log, or n to not clear the error log.

Problem Solving

This chapter contains the following topics:

Spot Checks

This chapter explains how to check for problems and solve them. It is good practice to carry out regular checks of your LinkBuilder MSH equipment.

Check the following:

- LEDs

  Press the LAMP TEST button, on the LinkBuilder MSH's Display Panel. All yellow LEDs should light continuously and all bi-color LEDs should flash red/green alternately.

- Cabling

  Check that all external cabling connections are secure and that no cables are pulled taut. All AUI cables should be secured by the fitted slide locks.

- Modules

  Check that all modules are secured in position and that their ejectors are locked. All modules should be flush with each other.

  If individual LEDs do not respond to the lamp test, then the LEDs are at fault. However, if all a module's LEDs do not respond, and all other checks are satisfied, then there is a fault with either the module or the LinkBuilder MSH chassis. In both cases, see *What To Do Next* on page 6-10 for further action.

Using The LEDs For Fault Diagnosis

The LEDs on the front of the module indicate bridge activity and faults:

- PWR (Power)

  Green on - Normal: power present, self-test completed successfully and bridge operating normally.

  Green flashing - Self-test is in progress (this lasts about one second).

  Red on - Fault: a fault has occurred during power-up self-test or in operation. You should contact your supplier immediately for advice.

- TX*n* or TX (Transmit)

  Yellow flashing - Flashes every time a frame is transmitted from port *n* or external port.

- RX*n* or RX (Receive)

  Yellow flashing - Flashes every time a frame is received by port *n* or external port.

- EN*n* or EN (Enabled)

  Yellow on - Port *n* or external port is enabled, listening or learning.

  Yellow flashing - Port *n* or external port is enabled and blocking.

  Off - Port *n* or external port is disabled.

Correcting Problems

By working through this section, you should be able to isolate faults or find some possible causes and recommended actions.

Network Problems

Symptom: Network communication problems.

Action:

- Check the cabling in your network and that it meets the IEEE standard for cabling.
- Find out whether any other devices on your network are also having communication problems.

PING Or Telnet Problems

Symptom: Cannot PING or Telnet another bridge after entering an IP address.

Action:

- The unit must be reset for an IP address change to take effect.
- Check that the IP address is correct for that bridge.
- Check that the IP address is unique.
- Check that the subnet mask is correct.
- Check that the default gateway address is correct.
- Check that your address, port, or IP protocol is not being filtered by the other bridge. If you are unsure, turn off its filters.
- Check the port is forwarding traffic.
- Check the received packets field (RCVD PKTS/SEC) on the Bridge Port Statistics screen, for the other bridge.

- If no other action works, there may be a problem with the other bridge's configuration. Erase the other bridge's parameters. Remember, this will erase all configurations ever made to it. Re-enter it's IP address and reset it.

Port Problems

Symptom: One of the bridge ports is unexpectedly blocking.

Action:

- Check that you do not have a redundant link, causing the port to block.
- Try turning off Spanning Tree. If there is a redundant link in the network, this will cause an active loop resulting in further network problems.
- Remove the bridge module from the LinkBuilder MSH chassis, and reinstall it. It is unlikely that any problems will result from this operation. For more information on possible problems, see *Removing And Replacing Equipment* on page 6-8.

Performance Problems

Symptom: Bridge performance is slow.

Action:

- Check the Bridge Statistics and Ethernet Statistics screens for excessive CRC errors.
- Check external port's connection.
- Excessive use of custom filtering - disable unnecessary custom filtering.
- Time taken updating monitoring screens - return to the Main Menu whenever possible.

Collision Problems

Symptom: Excessive collisions on an Ethernet port.

Action:

- Check that your network is not too long or too large.
- Check that there are not too many repeaters on your network.
- Check that there are not too many users on a single Ethernet.

STAP Problems

Symptom: Spanning Tree problems.

Action:

- Return all Spanning Tree settings to their default settings.

Filter Problems

Symptom: Filters not working properly.

Action:

- Check that the main filtering switch has been turned on (see the FILTERING ON/OFF/FAST field on the Filter Options screen).
- If you want individual filters to take effect, check that they have been turned on.
- Check that there are no filter clashes or overrides.

SNMP Problems

Symptom: Cannot establish communication via SNMP.

Action:

- Check that you have an IP address entered. If you cannot PING or Telnet the bridge, check the IP address and default gateway address.
- Check that SNMP is properly configured.
- If you have not reset the bridge since enabling SNMP, do so.

Operation Problems

Symptom: The bridge does not respond to the keyboard, or freezes in operation.

Action:

- Press [Ctrl] + [P] to return to the management module, and reset the MSH chassis slot that the bridge is in (slot reset).
- Remove and install the bridge into the LinkBuilder MSH chassis.

Removing And Replacing Equipment

Inserting additional modules or a second Power Supply Unit into an active LinkBuilder MSH, known as hot insertion, should not cause any damage to your equipment. However, the following points should be noted:

- Packets of data passing through the unit at the time of insertion can be corrupted.
- Inserting a second Power Supply Unit can cause a dip in the logic supply which would reset all modules.

The removal of modules or Power Supply Units that have failed should not generally interrupt the operation of the LinkBuilder MSH.

If you hot insert a module or Power Supply Unit into the LinkBuilder MSH chassis, it may cause problems with the Management Module or 4 Port Bridge Module. In the unlikely event of the software becoming corrupted after hot insertion, we recommend that you press RESET and ENTER on the LinkBuilder MSH's display panel.

Spares

We recommend that you have one spare module or Power Supply Unit for every ten in use. In the unlikely event that you should have problems with the LinkBuilder MSH, you should swap the faulty item with a spare. This allows you to continue operation and may also help in singling out a fault, if the replacement solves the problem.

It is advisable to hold spare replaceable components, such as fuses and Transceiver Modules, even though they are unlikely to fail. The bridge module has one replaceable fuse, see Figure 6-1.

Fuse..... 12V 2A anti-surge (20mm cartridge)

Only fuses of the same manufacturer, type and rating should be used with the module.

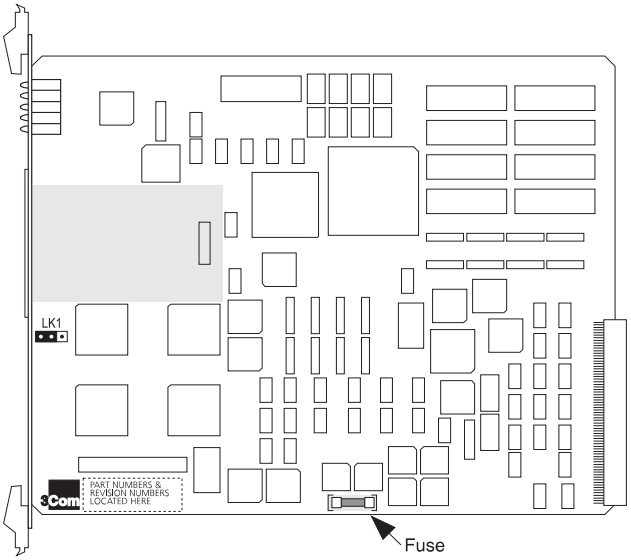


Figure 6-1 The Location of the Fuse

What To Do Next

If any of your LinkBuilder MSH equipment fails to operate correctly, contact your supplier with the following information before returning the equipment:

- Serial Number
- Revision Number
- A brief description of the fault

For modules, the Serial Number and Revision Number are printed on the circuit board. The reference guides that accompany these modules show the location of these numbers. For the LinkBuilder MSH chassis, both numbers are on a label attached to one of its sides.

When returning equipment to your supplier make sure it is suitably packed for transit. When returning the LinkBuilder MSH chassis, remove all modules.

Please make sure that you have carried out the recommended checks and observations in the rest of this chapter.

A LINK SETTINGS

The LinkBuilder MSH 4 Port Ethernet Bridge Module has a link, LK1, for resetting its configuration to default values, see Figure A-1.

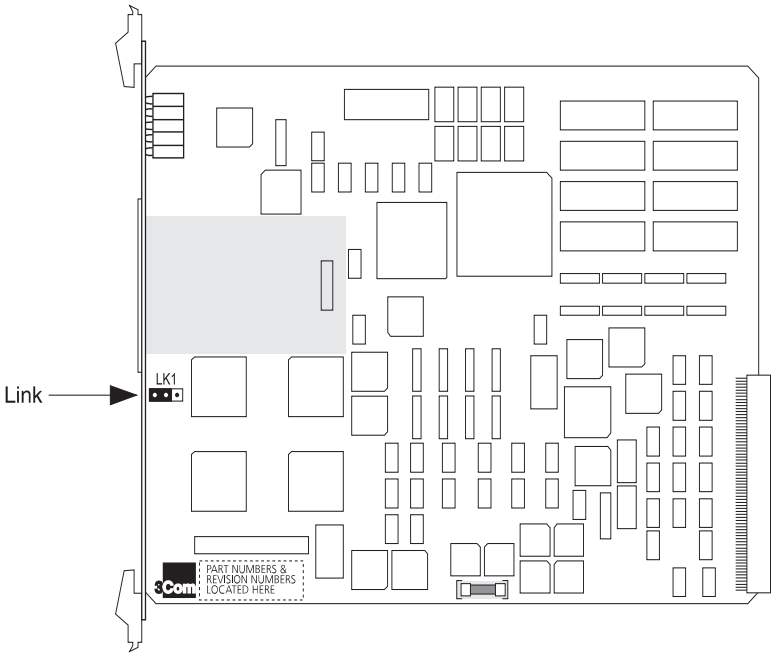


Figure A-1 The Location Of The Link

WARNING: *This method of resetting the module has the same effect as initializing NVRAM via the VT100 management interface. All changes ever made to the bridge will be reset to default settings.*

We recommend that the link method is only used when VT100 management is not possible, for example, when you've forgotten your password, as this method involves physically removing and installing the module twice. For information on resetting the module via VT100, see *Erasing All Changes* on page 2-27.

To reset the bridge module:

1 Remove the module from the LinkBuilder MSH chassis.

2 Change the link to the reset position, see Figure A-2.

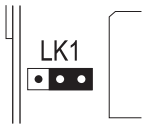


Figure A-2 The Link In The Reset Position

3 Install the module into the LinkBuilder MSH chassis.

4 When the module has finished its self-test (self-test is indicated by the PWR LED flashing), remove it from the LinkBuilder MSH chassis.

5 Change the link to the normal position, see Figure A-3.

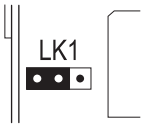
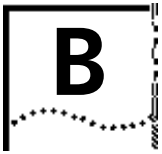


Figure A-3 The Link In The Normal Position

6 Install the module into the LinkBuilder MSH chassis. The module is now reset to its default settings.



TECHNICAL INFORMATION

The LinkBuilder MSH 4 Port Ethernet Bridge Module conforms to the following standards:

Electrical

- IEEE 802.3, ISO DIS 8802/3

Safety

- EN 60950 (BS 7002)
- UL 1950
- CSA 222 #950
- ECMA 97

EMC

- Vfg 243 'B'
- EN 55022 A
- FCC 20780 15J Level A
- IEC 801 part 2, 3, 4 and 5
- EN 55101 part 5

Environmental

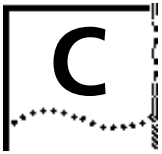
- IEC 68

Reliability

- MIL HDBK 217

MIB

- IETF Bridge MIB (RFC 1286)
- RFC 1213 (MIB II) and RFC 1229/1239 extensions



TECHNICAL SUPPORT

3Com provides easy access to technical support information through a variety of services. This appendix describes these services.

On-line Technical Services

3Com offers worldwide product support seven days a week, 24 hours a day, through the following on-line systems:

- 3Com Bulletin Board Service
- Ask3Com℠ on CompuServe®
- 3ComFacts℠ Automated Fax Service

3Com Bulletin Board Service (3ComBBS)

3ComBBS contains patches, software, and drivers for all 3Com products, as well as technical articles. This service is available via modem seven days a week, 24 hours a day. To reach the service, set your modem to 8 data bits, no parity, and 1 stop bit. Call the telephone number nearest you:

Country	Baud Rate	Telephone Number
Australia	up to 14400 baud	(61) (2) 955 2073
France	up to 14400baud	(33) (1) 69 86 69 54
Germany	up to 9600 baud up to 9600 baud	(49) (89) 627 32 188 (49) (89) 627 32 189
Hong Kong	up to 9600 baud	(852) 537 5601
Italy (fee required)	up to 9600 baud	(39) (2) 273 00680

Country	Baud Rate	Telephone Number
Japan	up to 14400 baud	(81) (3) 3243 9245
Singapore	up to 9600 baud	(65) 534 5693
Taiwan	up to 14400 baud	(886) (2) 577 6160
U.K.	up to 14400 baud	(44) (442) 278278
U.S.	up to 14400 baud	(1) (408) 980 8204

Ask3Com on CompuServe

Ask3Com is a CompuServe-based service containing patches, software, drivers, and technical articles about all 3Com products, as well as an interactive forum for technical questions. To use Ask3Com, you need a CompuServe account.

To use Ask3Com:

1. Log on to CompuServe.
2. Enter **`go threecom`**
3. Press [Enter] to see the Ask3Com main menu.

3ComFacts Automated Fax Service

3Com Corporation's interactive fax service, 3ComFacts℠, provides data sheets, technical articles, diagrams, and troubleshooting instructions on 3Com products 24 hours a day, seven days a week. Within this service, you may choose to access CardFacts℠ for adapter information, or NetFacts℠ for network system product information.

- *CardFacts* provides adapter installation diagrams, configuration drawings, troubleshooting instruction, and technical articles.

  Document 9999 provides you with an index of adapter documents.

- *NetFacts* provides data sheets and technical articles on 3Com Corporation's hub, bridge, router, terminal server, and software products.

  Document 8888 provides you with an index of system product documents.

  Call 3ComFacts using your touchtone telephone. International access numbers are:

Country	Fax Number
Hong Kong	(852) 537 5610
U.K.	(44) (442) 278279
U.S.	(1) (408) 727 7021

Local access numbers are available within the following countries:

Country	Fax Number
Australia	800 123853
Denmark	800 17319
Finland	98 001 4444
France	05 90 81 58
Germany	0130 8180 63

Country	Fax Number
Italy	1678 99085
Netherlands	06 0228049
Norway	05 01 1062
Sweden	020 792954
U.K.	0800 626403

3Com Documentation on CD-ROM

An extensive library of 3Com product documentation is available in CD-ROM format through Support On-Site® for Networks subscription service. This multivendor CD-ROM service, offered by Computer Library™, a division of Ziff Communication, contains technical information and documentation from major data networking hardware and software manufacturers. Stand-alone and concurrent user subscriptions are available. For more information, call Computer Library at the following numbers:

Country	Telephone Number	Fax Number
U.S. and Canada	(800) 827 7889, ext. 515	(212) 503 4487
Outside the U.S. and Canada	(212) 503 4400, ext. 515	(212) 503 4487

Support from Your Network Supplier

If additional assistance is required, contact your network supplier. Many suppliers are authorized 3Com service partners who are qualified to provide a variety of services, including network planning, installation, hardware maintenance, application training, and support services.

When you contact your network supplier for assistance, have the following information ready:

- Diagnostic error messages
- A list of system hardware and software, including revision levels
- Details about recent configuration changes, if applicable

If you are unable to contact your network supplier, see the following section on how to contact 3Com.

Support from 3Com

If you are unable to receive support from your network supplier, technical support contracts are available from 3Com.

In the U.S. and Canada, call **(800) 876-3266** for customer service.

If you are outside the U.S. and Canada, contact your local 3Com sales office to find your authorized service provider.

Country	Telephone Number
Australia (Sydney)	(61) (2) 959 3020
(Melbourne)	(61) (3) 653 9515
Belgium	(32) (2) 7164880
Brazil	(55) (11) 241 1571
Canada	(905) 882 9964
France	(33) (1) 69 86 68 00
Germany	(49) (89) 6 27 32 0
Hong Kong	(852) 868 9111
Italy	(39) (2) 273 02041
Japan	(81) (3) 3243 9234

Country	Telephone Number
Mexico	(525) 531 0591
Netherlands	(31) (3) 402 55033
Singapore	(65) 538 9368
South Africa	(27) (11) 803 7404
Spain	(34) (1) 3831700
Sweden	(46) (8) 632 91 00
Taiwan	(886) (2) 577 4352
United Arab Emirates	(971) (4) 311303
U.K.	(44) (628) 897000
U.S.	(1) (408) 492 1790

Returning Products for Repair

A product sent directly to 3Com for repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to 3Com without an RMA number will be returned to the sender unopened, at the sender's expense.

To obtain an RMA number, call or fax:

Country	Telephone Number	Fax Number
U.S and Canada	(800) 876 3266, option 2	(408) 764 7120
Europe	(44) (44) 2 278000	(44) (442) 236824
Outside Europe, U.S. and Canada	(1) (408) 492 1790	(1) (408) 764 7290

INDEX

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

RADIO FREQUENCY INTERFERENCE STATEMENTS

FCC Statement

This equipment has been tested with a class A computing device and has been found to comply with part 15 of FCC Rules. Operation in a residential area may cause unacceptable interference to radio and TV receptions requiring the operator to take whatever steps are necessary to correct the interference.

CSA Statement

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus as set out in the interference-causing equipment standard entitled "Digital Apparatus", ICES-003 of the Department of Communications.

Cet appareil numérique respecte les limites de bruits radioélectriques applicables aux appareils numériques de Classe A prescrites dans la norme sur le matériel brouilleur: "Appareils Numériques", NMB-003 édictée par le ministre des Communications.

Information To The User

If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient the receiving antenna.
- Relocate the equipment with respect to the receiver.
- Move the equipment away from the receiver.
- Plug the equipment into a different outlet so that equipment and receiver are on different branch circuits.

If necessary, the user should consult the dealer or an experienced radio/television technician for additional suggestions. The user may find the following booklet prepared by the Federal Communications Commission helpful:

How to Identify and Resolve Radio-TV Interference Problems

This booklet is available from the U.S. Government Printing Office, Washington, DC 20402, Stock No. 004-000-00345-4.

In order to meet FCC emissions limits, this equipment must be used only with cables which comply with IEEE 802.3.

LIMITED WARRANTY

HARDWARE: 3Com warrants its hardware products to be free from defects in workmanship and materials, under normal use and service, for the following lengths of time from the date of purchase from 3Com or its Authorized Reseller:

Internetworking products	**One year**
Network adapters	**Lifetime**
Ethernet stackable hubs and Unmanaged Ethernet fixed port repeaters	**Lifetime* (One year if not registered)**
***Power supply and fans in these stackable hubs and unmanaged repeaters**	**One Year**
Other hardware products	**One Year**
Spare parts and spares kits	**90 days**

If a product does not operate as warranted during the applicable the warranty period, 3Com shall, at its expense, correct any such defect by repairing the defective product or part or, at its option, by delivering to Customer an equivalent product or part to replace the defective item. All products that are replaced will become the property of 3Com. Replacement products may be new or reconditioned. Any replaced or repaired product or part has a ninety (90) day warranty or the remainder of the initial warranty period, whichever is longer.

3Com shall not be responsible for any software, firmware, information, or memory data of Customer contained in, stored on, or integrated with any products returned to 3Com pursuant to any warranty.

SOFTWARE: 3Com warrants that the software programs licensed from it will perform in substantial conformance to the program specifications therefor for a period of ninety (90) days from the date of purchase from 3Com or its Authorized Reseller. 3Com warrants the magnetic media containing software against failure during the warranty period. No updates are provided. 3Com's sole obligation hereunder shall be (at 3Com's discretion) to refund the purchase price paid by Customer for any defective software products, or to replace any defective media with software which substantially conforms to 3Com's applicable published specifications. Customer assumes responsibility for the selection of the appropriate applications program and associated reference materials. 3Com makes no warranty that its software products will work in combination with any hardware or applications software products provided by third parties, that the operation of the software products will be uninterrupted or error free, or that all defects in the software products will be corrected. For any third party products listed in the 3Com software product documentation or specifications as being compatible, 3Com will make reasonable efforts to provide compatibility, except where the non-compatibility is caused by a "bug" or defect in the third party's product.

STANDARD WARRANTY SERVICE: Standard warranty service for hardware products may be obtained by delivering the defective product, accompanied by a copy of the dated proof of purchase, to 3Com's Corporate Service Center or to an Authorized 3Com Service Center during the applicable warranty period. Standard warranty service for software products may be obtained by telephoning 3Com's Corporate Service Center or an Authorized 3Com Service Center, within the warranty period. Products returned to 3Com's Corporate Service Center must be pre-authorized by 3Com with a Return Material Authorization (RMA) number marked on the outside of the package, and sent prepaid, insured, and packaged appropriately for safe shipment. The repaired or replaced item will be shipped to Customer, at 3Com's expense, not later than thirty (30) days after receipt by 3Com.

WARRANTIES EXCLUSIVE: If a 3Com product does not operate as warranted above, Customer's sole remedy shall be repair, replacement, or refund of the purchase price paid, at 3Com's option. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, STATUTORY OR OTHERWISE, INCLUDING WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. 3COM NEITHER ASSUMES NOR AUTHORIZES ANY OTHER PERSON TO ASSUME FOR IT ANY OTHER LIABILITY IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE OR USE OF ITS PRODUCTS.

3COM SHALL NOT BE LIABLE UNDER THIS WARRANTY IF ITS TESTING AND EXAMINATION DISCLOSE THAT THE ALLEGED DEFECT IN THE PRODUCT DOES NOT EXIST OR WAS CAUSED BY CUSTOMER'S OR ANY THIRD PERSON'S MISUSE, NEGLECT, IMPROPER INSTALLATION OR TESTING, UNAUTHORIZED ATTEMPTS TO REPAIR, OR ANY OTHER CAUSE BEYOND THE RANGE OF THE INTENDED USE, OR BY ACCIDENT, FIRE, LIGHTNING, OR OTHER HAZARD.

Limitation of Liability. IN NO EVENT, WHETHER BASED IN CONTRACT OR TORT (INCLUDING NEGLIGENCE) SHALL 3COM BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, INDIRECT, SPECIAL, OR PUNITIVE DAMAGES OF ANY KIND, OR FOR LOSS OF REVENUE, LOSS OF BUSINESS, OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE SALE, INSTALLATION, MAINTENANCE, USE, PERFORMANCE, FAILURE, OR INTERRUPTION OF ITS PRODUCTS, even if 3com or its authorized reseller has been advised of the possibility of such damages.

Some states do not allow the exclusion of implied warranties or the limitation of incidental or consequential damages for consumer products, so the above limitations and exclusions may not apply to you. This warranty gives you specific legal rights which may vary from state to state.

GOVERNING LAW: This Limited Warranty shall be governed by the laws of the state of California.

3Com Corporation
5400 Bayfront Plaza
Santa Clara, CA 95052-8145
(408) 764-5000