8371 Networking Multilayer Ethernet Switch

Software User's Guide and Configuration Reference

GC30-9688-00

8371 Networking Multilayer Ethernet Switch

Software User's Guide and Configuration Reference

GC30-9688-00

Note
Before using this document, read the general information under “Notices” on page xvii.

First Edition (March 1999)

This edition applies to Version 4.0 of the IBM 8371 and to all subsequent releases and modifications until otherwise indicated in new editions or technical newsletters.

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address below.

IBM welcomes your comments. A form for readers' comments is provided at the back of this publication. If the form has been removed, you may address your comments to:

International Business Machines Corporation

Design and Information Development

Department CGF

P.O. Box 12195

Research Triangle Park, NC 27709-9990

U.S.A.

Contents

Figures

Tables

Notices

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program, or service. Evaluation and verification of operation in conjunction with other products, except those expressly designated by IBM, are the user's responsibility.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785, U.S.A.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement.

This document is not intended for production use and is furnished as is without any warranty of any kind, and all warranties are hereby disclaimed including the warranties of merchantability and fitness for a particular purpose.

Notice to Users of Online Versions of This Book

For online versions of this book, you are authorized to:

- Copy, modify, and print the documentation contained on the media, for use within your enterprise, provided you reproduce the copyright notice, all warning statements, and other required statements on each copy or partial copy.
- Transfer the original unaltered copy of the documentation when you transfer the related IBM product (which may be either machines you own, or programs, if the program's license terms permit a transfer). You must, at the same time, destroy all other copies of the documentation.

You are responsible for payment of any taxes, including personal property taxes, resulting from this authorization.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

Your failure to comply with the terms above terminates this authorization. Upon termination, you must destroy your machine-readable documentation.

Trademarks

The following terms are trademarks of the IBM Corporation in the United States or other countries or both:

Advanced Peer-to-Peer Networking	CUA	Operating System/2
AIX	IBM	RS/6000
AIXwindows	Micro Channel	System/370
APPN	NetView	VTAM
BookManager	Nways	Web Explorer
Common User Access	OS/2	PS/2

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks or registered trademarks of Microsoft Corporation.

Other company, product, and service names may be trademarks or service marks of others.

Preface

This manual contains the information you will need to use the command line interface for configuration and operation of the IBM 8371, hereafter referred to as the switch. With the help of this manual, you should be able to perform the following processes and operations:

- Configure, monitor, and use the base code on your 8371
- Configure, monitor, and use the interfaces and Link Layer software supported by the switch.

Who Should Read This Manual: This manual is intended for persons who install and manage computer networks. Although experience with computer networking hardware and software is helpful, you do not need programming experience to use the protocol software.

Conventions Used in This Manual

The following conventions are used in this manual to show command syntax and program responses:

1. The abbreviated form of a command is underlined as shown in the following example:

   reload

   In this example, you can enter either the whole command (reload) or its abbreviation (rel).
2. Keyword choices for a parameter are enclosed in brackets and separated by the word or. For example:

   ```
   command [keyword1 or keyword2]
   ```

   Choose one of the keywords as a value for the parameter.
3. Three periods following an option mean that you enter additional data (for example, a variable) after the option. For example:

   time host ...

   In this example, you enter the IP address of the host in place of the periods, as explained in the description of the command.
4. In information displayed in response to a command, defaults for an option are enclosed in brackets immediately following the option. For example:

   ```
   Media (UTP/STP) [UTP]
   ```

   In this example, the media defaults to UTP unless you specify STP.
5. Keyboard key combinations are indicated in text in the following way::

   Ctrl-P

   The key combination **Ctrl P** indicates that you should press the Ctrl key and the P key simultaneously. In certain circumstances, this key combination changes the command line prompt.
6. Names of keyboard keys are indicated like this: **Enter**

8371 Library

The following publication is shipped in displayable softcopy form on the 8371 CD-ROM (SK2T-0446-00). This CD-ROM is shipped with initial orders for the IBM 8371.

- *Networking Multilayer Ethernet Switch Installation and Planning Guide*, GA27-4226-00

Part 1. User's Guide

Chapter 1. Getting Started

This chapter shows you how to get started with using the following components related to the IBM Multilayer Ethernet Switch (IBM 8371):

- Device console terminals
- Device software (IBM 8371)
- Device software user interface

The information in this chapter is divided into the following sections:

Before You Begin

Before you begin, refer to the following checklist to verify that your device is installed correctly.

Have you...

- Installed all necessary hardware?
- Connected the console terminal (video terminal) to the device?

  Attention: If you are using a service port-attached terminal to configure or monitor your IBM 8371 and your service terminal is unreadable, you need to change some parameters in your configuration. (See "Service Terminal Display Unreadable" in 8371 Networking Multilayer Ethernet Switch Installation and Planning Guide.)

  Refer to your hardware documentation.
- Connected your device to the network using the correct network interfaces and cables?
- Run all necessary hardware diagnostics?

For more information on any of these procedures, refer to the *Networking Multilayer Ethernet Switch Installation and Planning Guide*.

Accessing the Software Using Local and Remote Consoles

The device console lets you use the device user interface to monitor and change the function of the device's networking software. The device supports local and remote consoles.

Local Consoles

Local consoles are either directly connected by an EIA 232 (RS-232) cable, or connected via modems to the device. You may need to use a local console during the initial software installation. After the initial setup connection, you can connect using Telnet, as long as IP forwarding has been enabled. (Refer to *Protocols and Features* for more information on enabling IP forwarding.)

When the configured device is started for the first time, a boot message appears on the screen, followed by the OPerator's CONsole or OPCON prompt (*). The * prompt indicates that the device is ready to accept OPCON commands.

Your IBM 8371 software may have been pre-configured at the factory. If it was, you do not need to use a local console to perform initial configuration. If, however, your IBM 8371 was not pre-configured at the factory, you will need to use an ASCII terminal attached to the 8371 service port to initially configure it.

Important: Garbage, random characters, reverse question marks, or the inability to connect your terminal to the 8371 service port can have many causes. The following list contains some of those causes:

- The most common cause of garbage or random characters on the service console is that the baud rate is not synchronized with the IBM 8371.

  If the IBM 8371 is set to a specific baud rate, the terminal or terminal emulator must be set to the same baud rate.

  If the IBM 8371 is set to autobaud (this is the default), press the terminal break key sequence and press **Enter**.

  A typical break key sequence for PC terminal emulators is Alt-B (refer to the terminal emulator documentation). Most ASCII terminals have a **Break** key (often used in conjunction with the **Ctrl** key).

  Refer to your hardware documentation for more information.
- Defective terminal or device (ac) grounds.
- Defective, incorrectly shielded, or incorrectly grounded EIA 232 (RS-232) cable between the terminal and the IBM 8371.
- Defective terminal or terminal emulator.
- Defective IBM 8371 system board.
- High ambient electromagnetic interference (EMI) levels.
- Power line disturbances.

(See “Service Terminal Display Unreadable” in the *8371 Networking Multilayer Ethernet Switch Installation and Planning Guide* .)

Once the IBM 8371 is initially configured, you will not need a local console for device operation, as long as IP is enabled.

The device software automatically handles console activity. When upgrading the software, you might have to use the local console. For information on attaching and configuring local consoles, refer to the *Networking Multilayer Ethernet Switch Installation and Planning Guide*.

Remote Consoles

Remote consoles attach to the device using a standard remote terminal protocol. Remote consoles provide the same function as local consoles, except that a local console must be used for initial configuration if your IBM 8371 was not pre-configured at the factory.

Telnet Connections

The device supports both Telnet Client and Server. The remote console on the device acts as a Telnet server. The device acts as a Telnet client when connecting from the device to either another device or a host using the **telnet** command in the OPCON (*) process.

Remote Login Names and Passwords

During a remote login, the device prompts you for a login name and password. You can display the login name when logged in to the device from a remote console by using a device **status** command.

Logging In Remotely or Locally

Logging in to a local console is the same as logging in to a remote console except that you must connect to the device by starting Telnet on your host system. To log in remotely, begin at step 1. To log in locally, begin at step 3.

To log in from a remote console:

1. Connect to the device by starting Telnet on your host system. Your host system is the system to which remote terminals are connected.
2. Supply the device's name or Internet Protocol (IP) address.

   To use device names, your network must have a name server. Issue either the device name or the IP address as shown in the following example:

   ```
   % telnet brandenburg
   ```

   or

   ```
   % telnet 128.185.132.43
   ```

   At this point, it makes no difference whether you have logged in remotely or locally.
3. If you are prompted, enter your login name and password.

   ```
   login:
   Password:
   ```

   It is possible that there is a login and no password. The password controls access to the device. If a password has not been set, press the **Enter** key at the `Password:` prompt. Logins are not set automatically. For security, you can set up user names and passwords using the **add user** command in the CONFIG process. For additional information, see the **add user** configuration command, on page 59. Remember to reload to activate any changes.

   Note: If you do not enter a login name and valid password within 1 minute of the initial prompt, or if you enter an incorrect password three times in succession, the device drops the Telnet connection.
4. Press the **Enter** key to display the asterisk (*) prompt.

   You may have to press the **Enter** key more than once or press **Ctrl-P** to obtain the * prompt.

   Once at this level, you can begin to enter commands from the keyboard. Press the **Backspace** key to delete the last character typed in on the command line. Press the **Delete** key or **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See "Command Completion" on page 19 and "Command History" on page 22 for more information.

You can also use local Telnet commands on your Telnet client to close the Telnet connection.

Note: If you use a VT100 terminal, do not press the **Backspace** key, because it inserts invisible characters. Use the **Delete** key.

5. Exit the device as described in “Exiting the Device”.

Reloading the Device

Use the **reload** command to reboot the device by loading a new copy of the configuration from memory. Whenever you change a user-configurable parameter that is not dynamically configurable, you must reload the device for the change to take effect. For example:

```
* reload

The configuration has been changed, save it? (Yes or [No] or Abort)

Are you sure you want to reload the gateway? (Yes or [No]): yes
```

Exiting the Device

Return to the * prompt and use the **logout** command to close the Telnet connection. For example:

```
IP Config> exit
Config> Ctrl-P
* logout

%
```

You can also use local Telnet commands on your Telnet client to close the Telnet connection.

Discussing the User Interface System

The software is a multitasking system that schedules use of the CPU among various processes and hardware devices. The device software:

- Provides timing and memory management, and supports both local and remote operator consoles from which you can view and modify the device’s operational parameters.
- Consists of functional modules that include various user interface processes, all network interface drivers, and all protocol forwarders purchased with the device.

Understanding the First-Level User Interface

The user interface to the software consists of the main menu (process) and several subsidiary menus (processes). These menus are related to the multiple levels of processes in the software.

The first level of processes consists of the OPCON and CONFIG-ONLY processes. In most cases, you will use the OPCON process to access the second level to configure or operate the base services, features, interfaces, and protocols you will run on your IBM 8371.

The second level contains processes such as Configuration (CONFIG), Console (GWCON) and Event Logging System (MONITR). You may use the OPCON

commands **configuration**, **console** or **event** to access these second level processes. Alternatively, you may use the **status** command to list the second level processes and then use the **talk** *pid* command to access the second-level processes. There are processes that you cannot use in the software. See Table 1 on page 10 for an overview of the processes.

Figure 1 shows the processes and how they fit within the structure of the device software.

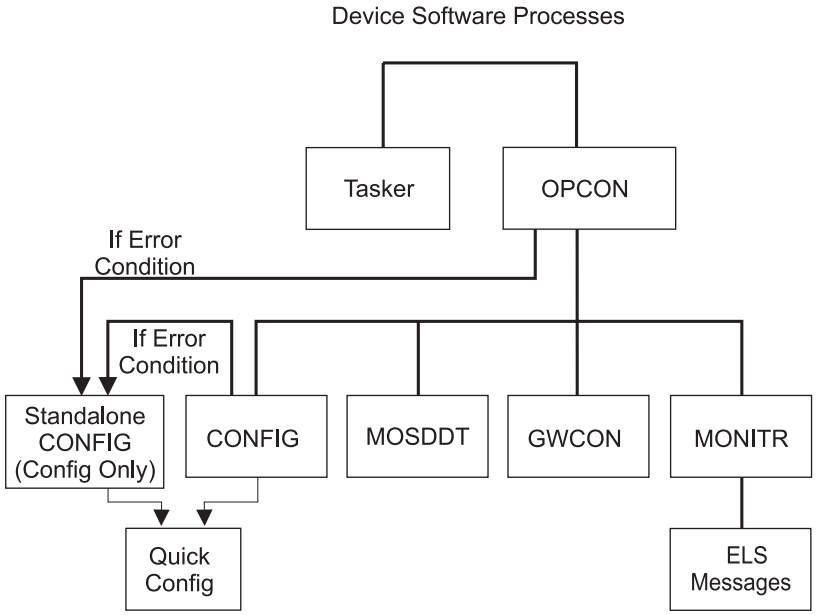

Figure 1. IBM 8371

Figure 2 on page 8 is an example of the relationship between the various process levels.

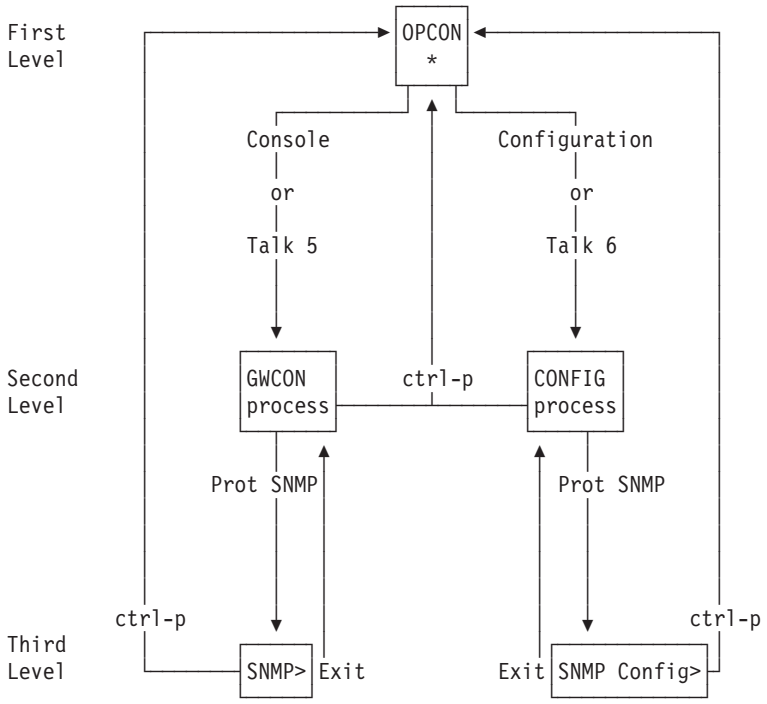

Figure 2. Relationship of Processes and Commands

Note: Also shown in Figure 2 are the various commands to access each process level and return from each process level.

See “What is the OPCON Process?” on page 43 for more information about OPCON.

The ROPCON process handles processing from remote consoles and is essentially the same as the OPCON process.

System Security

Multiple users with login permissions can be added using the **add user** command. See “Configuring User Access” on page 56 for details on security issues and for information on the **set password** and **add user** commands.

Chapter 2. Using the Software

This chapter describes how to use the software. It consists of:

Entering Commands

When typing a command, remember the following:

- You may type only enough sequential letters of the command to make it unique among the available commands. For example, to execute the **reload** command you must enter **rel** as a minimum. The minimum number of required characters are underlined in the command syntax chapters.
- Commands are not case-sensitive.
- Sometimes, only the first letter of the command (and subsequent options) is required to execute the command. For example, typing **s** at the * prompt followed by pressing the **Enter** key causes the **status** command to be executed.
- You may type **Escape ?** to obtain help on entering commands. See "Command Completion" on page 19 and "Command History" on page 22 for more information.

Connecting to a Process

When you start the device, the console displays a boot message. The OPCON prompt (*) then appears on the screen indicating that you are in the OPCON process and you can begin entering OPCON commands. This is the command prompt from which you communicate with different processes.

Commands that are needed more often appear before the "- - - - -" separator. Enter the appropriate command at the OPCON prompt (*). See Table 9 on page 44 for a list of commands.

Alternatively, you can:

1. Find out the process ID (PID) number of a process by entering the **status** command at the * prompt.

   The **status** command displays information about the device processes, such as the process IDs (PIDs), process names and status of the process. Issuing the **status** command is shown in the following example:
2. Use the **talk** *pid* command, where *pid* is the number of the process to which you want to connect. (For more information about these and other OPCON commands, refer to "What is the OPCON Process?" on page 43.)

Note: Not every process listed has a user interface (for example, the **talk 3** process). The **talk 4** command is for use by IBM service representatives.

Identifying Prompts

Each process uses a different prompt. You can tell which process your console is connected to by looking at the prompt. (If the prompt does not appear when you enter the **talk** *pid* command, press **Enter** again.)

The following list shows the prompts for the five main processes:

Table 1. Processes, Their Purpose, and Commands to Access

Process	Level and Purpose	Command to Access	Input Prompt
OPCON	Level 1 - access to all secondary levels	**Ctrl-P**	asterisk (*)
CONFIG	Level 2 - base services configuration and access to configuration third level	**Configuration or talk 6**	Config >
GWCON	Level 2 - base services operation and monitoring and access to operations and monitoring on third level	**Console or talk 5**	plus sign (+)
MONITR	Level 2 - message display	**Event or talk 2**	(none)
ELSCon	Level 2 - direct monitoring and access to ELS console	**els or talk 7**	ELS Secondary Console>
MOSDBG	Level 2 - diagnostic environment	**talk 4**	db>
Note: Only enter the **talk 4** command under the direction of a service representative.			

At the OPCON prompt level, you can begin to enter commands from the keyboard. Use the **Backspace** key to delete the last character typed in on the command line. Use **Ctrl-U** to delete the whole command line entry so that you can reenter a command. See “Command Completion” on page 19 and “Command History” on page 22 for additional details or press **Escape ?**.

Getting Help

At the command prompts, you can obtain help in the form of a listing of the commands available at that level. To do this, type **?** (the **help** command), and then press **Enter**. Use **?** to list the commands that are available from the current level. You can usually enter a **?** after a specific command name to list its options. For example, the following information appears if you enter **?** at the * prompt:

```
*?
        CONFIGURATION         (Talk 6)
        CONSOLE                 (Talk 5)
        EVENT Logging System  (Talk 2)
        ELS Console              (Talk 7)
        LOGOUT
        PING (IP-Address)
        RELOAD
        RESTART
        TELNET to IP-Address (this terminal type)
-----------------------------------------------
        DIVERT output from process
        FLUSH output from process
        HALT output from process
        INTERCEPT character is
        MEMORY statistics
```

```
        STATUS of Processes(es)
        TALK to process
(you may cycle through these commands by pressing the TAB key)
```

Exiting a Lower Level Environment

The multiple-level nature of the software places you in secondary, tertiary, and even lower level environments as you configure or operate the 8371. To return to the next higher level, enter the **exit** command. To get to the secondary level, continue entering **exit** until you receive the secondary level prompt (either `Config>` or `+`).

For example, to exit the ASRT protocol configuration process:

```
ASRT config> exit
Config>
```

If you need to get to the primary level (OPCON), enter the intercept character (**Ctrl-P** by default).

Getting Back to OPCON

To get back to the OPCON prompt (*), press **Ctrl-P**. You must always return to OPCON before you can communicate with another process. For example, if you are connected to the console (GWCON) process and you want to connect to the CONFIG process, you must press **Ctrl-P** to return to OPCON first. The **Ctrl-P** key combination is the default *intercept character*.

If you use the intercept character from a third-level or lower level menu to return to the * prompt, the next time you use the **talk** command to talk to the same process, you will reenter that same level menu. This link goes away when the device is re-initialized.

Accessing the Second-Level Processes

All interfaces, features, and protocols have commands that you use to access the following processes:

- The configuration process to initially configure and enable the interface, feature, or protocol, as well as perform later configuration changes.
- The operating/monitoring process to display information about each interface, feature, or protocol, to make temporary configuration changes, or to activate configuration changes.

You can also configure or operate some base system services through the second-level processes. The commands to perform these functions are described starting in “What is CONFIG?” on page 55.

The next sections describe the procedures for accessing the second-level processes.

Accessing the Configuration Process, CONFIG (Talk 6)

Each protocol configuration process is accessed through the device’s CONFIG process. CONFIG is the second-level process of the device user interface that lets you communicate with third-level processes. Protocol processes are examples of third-level processes.

The CONFIG command interface is made up of levels of menus. Protocol configuration command interfaces are menus within the CONFIG interface. Each protocol configuration interface has its own prompt. For example, the prompt for the SNMP protocol command interface is `SNMP config>`.

The next sections describe these procedures in more detail.

Entering the CONFIG Process

To enter the CONFIG process from OPCON and obtain the CONFIG prompt, enter the **configuration** command. Alternatively, you can enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* configuration
```

or

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Enter** key again.

Reloading the Device

Changes that you make to the protocol parameters through CONFIG do not take effect until you either activate the net that contains any dynamic changes or the device software.

Accessing the Console Operating/Monitoring Process, GWCON (Talk 5)

To view information about the interfaces, features, or protocols or to change parameters while running, you must access and use the operating (monitoring) process. Operating command interfaces are modes of the GWCON interface. Within the GWCON mode, each interface, feature, or protocol interface has its own prompt. For example, the prompt for the SNMP protocol is `SNMP>`.

Note: Any parameters you change in this process will not remain active across any event that causes the 8371 to reload the operational code, such as a power outage or entering the **reload** command.

The next sections describe these procedures in more detail.

Entering the GWCON Command Process

To enter the GWCON process from OPCON and obtain the GWCON prompt, enter the **console** command. Alternatively, you may enter the **talk** command and the PID for GWCON. The PID for GWCON is 5. For example:

```
* console
```

or

```
* talk 5
```

The GWCON prompt (+) then displays on the console. If the prompt does not appear, press **Enter** again.

Accessing the Secondary ELS Console Process, ELSCon (Talk 7)

The Secondary ELS Console provides convenient access to GWCON `talk 5` ELS without disrupting the current state of GWCON. You may be in the middle of a **ping** in `talk 5`, or deep inside a `talk 5` menu structure, and want to control ELS without disrupting the current state of GWCON. The secondary ELS console (Talk 7) serves this purpose.

To enter the Secondary ELS Console (ELScon) process from OPCON and obtain the Secondary ELS Console prompt, enter the **els** command. Alternatively, you may enter the **talk 7** command.

In the following example, another ELS event is displayed while performing a **ping** command.

Note: The intercept character (Ctrl-P by default) is used to obtain the OPCON prompt (*).

```
*talk 5
+protocol hst
HST>ping 10.0.0.9
PING 10.0.0.2 -> 10.0.0.9: 56 data bytes, ttl=64, every 1 sec.

*talk 7

ELS Secondary Console>display event ip.7
Complete
ELS Secondary Console>
*talk 2
00:20:48   IP.007: 10.0.0.2 -> 10.0.0.9
00:20:49   IP.007: 10.0.0.2 -> 10.0.0.9
```

Accessing the Third-Level Processes

After accessing the second level, you must enter commands on the third level to configure or operate the interfaces, features, and protocols in your IBM 8371. The following sections describe how to access the third level processes.

Accessing Network Interface Configuration and Operating Processes

This section describes how to get started with accessing the network interface configuration and operating processes. Accessing these processes lets you change and monitor software-configurable parameters for network interfaces used in your device.

Accessing the Network Interface Configuration Process

Use the following procedure to access the device's configuration process. This process gives you access to a specific interface's *configuration* process.

1. At the OPCON prompt, enter the **configuration** command.

   ```
   * configuration
   ```

   After you enter the **configuration** command, the CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter **configuration**, press **Enter** again.
2. At the `Config>` prompt, enter the **list devices** command to display the network interface numbers for which the device is currently configured, as follows:

```
Config> list devices

Ifc 0     1-port 10/100 Ethernet             Slot: 0   Port: 1
Ifc 1     1-port 10/100 Ethernet             Slot: 0   Port: 2
Ifc 2     1-port 10/100 Ethernet             Slot: 0   Port: 3
Ifc 3     1-port 10/100 Ethernet             Slot: 0   Port: 4
Ifc 4     1-port 10/100 Ethernet             Slot: 0   Port: 5
Ifc 5     1-port 10/100 Ethernet             Slot: 0   Port: 6
Ifc 6     1-port 10/100 Ethernet             Slot: 0   Port: 7
Ifc 7     1-port 10/100 Ethernet             Slot: 0   Port: 8
Ifc 8     1-port 10/100 Ethernet             Slot: 0   Port: 9
Ifc 9     1-port 10/100 Ethernet             Slot: 0   Port: 10
Ifc 10    1-port 10/100 Ethernet             Slot: 0   Port: 11
Ifc 11    1-port 10/100 Ethernet             Slot: 0   Port: 12
Ifc 12    1-port 10/100 Ethernet             Slot: 0   Port: 13
Ifc 13    1-port 10/100 Ethernet             Slot: 0   Port: 14
Ifc 14    1-port 10/100 Ethernet             Slot: 0   Port: 15
Ifc 15    1-port 10/100 Ethernet             Slot: 0   Port: 16
Ifc 16    1-port 10/100 Ethernet             Slot: 1   Port: 1
Ifc 17    1-port 10/100 Ethernet             Slot: 1   Port: 2
Ifc 18    1-port 10/100 Ethernet             Slot: 1   Port: 3
Ifc 19    1-port 10/100 Ethernet             Slot: 1   Port: 4
Ifc 20    1-port 10/100 Ethernet             Slot: 1   Port: 5
Ifc 21    1-port 10/100 Ethernet             Slot: 1   Port: 6
Ifc 22    1-port 10/100 Ethernet             Slot: 1   Port: 7
Ifc 23    1-port 10/100 Ethernet             Slot: 1   Port: 8
Ifc 24    1-port 10/100 Ethernet             Slot: 2   Port: 1
Ifc 25    1-port 10/100 Ethernet             Slot: 2   Port: 2
Ifc 26    1-port 10/100 Ethernet             Slot: 2   Port: 3
Ifc 27    1-port 10/100 Ethernet             Slot: 2   Port: 4
Ifc 28    1-port 10/100 Ethernet             Slot: 2   Port: 5
Ifc 29    1-port 10/100 Ethernet             Slot: 2   Port: 6
Ifc 30    1-port 10/100 Ethernet             Slot: 2   Port: 7
Ifc 31    1-port 10/100 Ethernet             Slot: 2   Port: 8
Ifc 32    NULL Device                        Slot: 3   Port: 1
Ifc 33    NULL Device                        Slot: 3   Port: 2
Ifc 34    NULL Device                        Slot: 3   Port: 3
Ifc 35    NULL Device                        Slot: 3   Port: 4
Ifc 36    ATM                                Slot: 1   Port: 1
Ifc 37    ATM                                Slot: 1   Port: 2
Ifc 38    ATM                                Slot: 2   Port: 1
Ifc 39    ATM                                Slot: 2   Port: 2
Ifc 40    ATM Ethernet LAN Emulation
Ifc 41    ATM Ethernet LAN Emulation
Ifc 42    ATM Ethernet LAN Emulation
Ifc 43    ATM Ethernet LAN Emulation
Ifc 44    ATM Ethernet LAN Emulation
Ifc 45    ATM Ethernet LAN Emulation
Ifc 46    ATM Ethernet LAN Emulation
Ifc 47    ATM Ethernet LAN Emulation
Ifc 48    ATM Ethernet LAN Emulation
Ifc 49    ATM Ethernet LAN Emulation
Ifc 50    ATM Ethernet LAN Emulation
Ifc 51    ATM Ethernet LAN Emulation
Ifc 52    ATM Ethernet LAN Emulation
Ifc 53    ATM Ethernet LAN Emulation
Ifc 54    ATM Ethernet LAN Emulation
Ifc 55    ATM Ethernet LAN Emulation
Ifc 56    ATM Ethernet LAN Emulation
Ifc 57    ATM Ethernet LAN Emulation
Ifc 58    ATM Ethernet LAN Emulation
Ifc 59    ATM Ethernet LAN Emulation
Ifc 60    ATM Ethernet LAN Emulation
Ifc 61    ATM Ethernet LAN Emulation
Ifc 62    ATM Ethernet LAN Emulation
Ifc 63    ATM Ethernet LAN Emulation
Config>
```

3. Record the interface numbers.
4. Enter the CONFIG **network** command and the number of the interface you want to configure. For example:

   ```
   Config> network 1
   ```

   The appropriate configuration prompt (such as `Eth Config>` for Ethernet), now displays on the console.

Note: Not all network interfaces are user-configurable. For interfaces that cannot be configured, you receive the message:

```
That network is not configurable
```

Configuring the Network Interface: Refer to the specific chapters in this guide for complete information on configuring your IBM 8371's network interfaces.

Accessing the Network Interface Console Process

To monitor information related to a specific interface, access the interface console process by using the following procedure:

1. At the OPCON prompt, enter the **console** command . For example:

   ```
   * console
   ```

2. The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **Enter** again.
3. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the device is configured. For example:

   ```
   + configuration

   Num Name  Protocol
   11  SNMP  Simple Network Management Protocol
   23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
   29  MPOA  Multi-Protocol Over ATM
   Num Name  Feature
   6   QOS   Quality of Service
   17  Self  Self Learning IP
   18  RMON  Remote Network Monitor

   64 Total Networks:
   Net Interface  MAC/Data-Link         Hardware         State
   0   Eth/0      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   1   Eth/1      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   2   Eth/2      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   3   Eth/3      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   4   Eth/4      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   5   Eth/5      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   6   Eth/6      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   7   Eth/7      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   8   Eth/8      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   9   Eth/9      Ethernet/IEEE 802.3   10/100 Ethernet  Up
   10  Eth/10     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   11  Eth/11     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   12  Eth/12     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   13  Eth/13     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   14  Eth/14     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   15  Eth/15     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   16  Eth/16     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   17  Eth/17     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   17  Eth/18     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   19  Eth/19     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   20  Eth/20     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   21  Eth/21     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   22  Eth/22     Ethernet/IEEE 802.3   10/100 Ethernet  Up

   23  Eth/23     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   24  Eth/24     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   25  Eth/25     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   26  Eth/26     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   27  Eth/27     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   28  Eth/28     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   29  Eth/29     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   30  Eth/30     Ethernet/IEEE 802.3   10/100 Ethernet  Up
   ```

```
31  Eth/31     Ethernet/IEEE 802.3   10/100 Ethernet  Up
32  NULL/0     Null device           None             Not present
33  NULL/1     Null device           None             Not present
34  NULL/2     Null device           None             Not present
35  NULL/3     Null device           None             Not present
36  ATM/0      ATM                   ATM              Up
37  ATM/1      ATM                   ATM              Up
38  ATM/2      ATM                   ATM              Down
39  ATM/3      ATM                   ATM              Down
40  Eth/32     Ethernet/IEEE 802.3   ATM              Up
41  Eth/33     Ethernet/IEEE 802.3   ATM              Up
42  Eth/34     Ethernet/IEEE 802.3   ATM              Up
43  Eth/35     Ethernet/IEEE 802.3   ATM              Up
44  Eth/36     Ethernet/IEEE 802.3   ATM              Up
45  Eth/37     Ethernet/IEEE 802.3   ATM              Up
46  Eth/38     Ethernet/IEEE 802.3   ATM              Up
47  Eth/39     Ethernet/IEEE 802.3   ATM              Up
48  Eth/40     Ethernet/IEEE 802.3   ATM              Up
49  Eth/41     Ethernet/IEEE 802.3   ATM              Up
50  Eth/42     Ethernet/IEEE 802.3   ATM              Up
51  Eth/43     Ethernet/IEEE 802.3   ATM              Up
52  Eth/44     Ethernet/IEEE 802.3   ATM              Up
53  Eth/45     Ethernet/IEEE 802.3   ATM              Up
54  Eth/46     Ethernet/IEEE 802.3   ATM              Up
55  Eth/47     Ethernet/IEEE 802.3   ATM              Up
56  Eth/48     Ethernet/IEEE 802.3   ATM              Up
57  Eth/49     Ethernet/IEEE 802.3   ATM              Up
58  Eth/50     Ethernet/IEEE 802.3   ATM              Up
59  Eth/51     Ethernet/IEEE 802.3   ATM              Up
60  Eth/52     Ethernet/IEEE 802.3   ATM              Up
61  Eth/53     Ethernet/IEEE 802.3   ATM              Up
62  Eth/54     Ethernet/IEEE 802.3   ATM              Up
63  Eth/55     Ethernet/IEEE 802.3   ATM              Up
```

4. Enter the GWCON **network** command and the number of the interface you want to monitor. For example:

```
+ network 36
```

Monitoring the Network Interface: Refer to the specific chapters in this manual for complete information on monitoring your IBM 8371's network interfaces.

Accessing Feature Configuration and Operating Processes

To help you access the IBM 8371 feature configuration and operating processes, this section outlines both of these procedures.

Accessing the Feature Processes

Use the **feature** command from the CONFIG process to access configuration commands for specific IBM 8371 features outside of the protocol and network interface configuration processes.

Use the **feature** command from the GWCON process to access console commands for specific features that are outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to display a listing of the features available for your software release. For example:

```
Config> feature ?

QOS
```

```
Self Learning IP
RMON
Feature name or number [Self Learning IP] ?
```

To access a particular feature's configuration or operating prompt, enter the **feature** command at the Config> or + (GWCON) prompt, respectively, followed by the feature number or short name. For example:

```
Config> feature self learning ip

Self Learning IP configuration

Self Learning IP Config>
```

Table 13 on page 64 lists the available feature numbers and names.

Once you access the configuration or operating prompt for a feature, you can begin entering specific commands for the feature. To return to the previous prompt level, enter the **exit** command at the feature's prompt.

Accessing Protocol Configuration and Operating Processes

This section describes how to access the protocol configuration and operating processes.

Entering a Protocol Configuration Process

To enter the desired protocol configuration process from the CONFIG> prompt:

1. At the CONFIG> prompt, enter the **list configuration** command to see the numbers and names of the protocols purchased in your copy of the software. See page 65 for sample output of the **list configuration** command.
2. From the Config> prompt, enter the **protocol** command with the number or short name (for example, SNMP) of the protocol you want to configure. The protocol number and short name is obtained from the **list configuration** command display. In the following example, the command has been entered for accessing the SNMP protocol configuration process:

   ```
   Config> protocol SNMP
   ```

   or

   ```
   Config> protocol 11
   SNMP user configuration
   ```

   The protocol configuration prompt then displays on the console. The following example shows the SNMP protocol configuration prompt:

   ```
   SNMP config>
   ```

You can now begin entering the protocol's configuration commands. See the corresponding protocol section of the *Protocols and Features* for more information on specific protocol configuration commands.

In summary, the **protocol** command lets you enter the configuration process for the protocol software installed in your device. The **protocol** command enters a protocol's command process. After entering the protocol command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol.

Entering a Protocol Operating Process

To enter a protocol console process from the GWCON prompt:

1. At the GWCON prompt, enter the **configuration** command to see the protocols and networks configured for the device. For example:

```
+ configuration

Num Name  Protocol
11  SNMP  Simple Network Management Protocol
23  ASRT  Adaptive Source Routing Transparent Enhanced Bridge
29  MPOA  Multi-Protocol Over ATM
Num Name  Feature
6   QOS   Quality of Service
17  Self  Self Learning IP
18  RMON  Remote Network Monitor

64 Total Networks:
Net Interface  MAC/Data-Link         Hardware         State
0   Eth/0      Ethernet/IEEE 802.3   10/100 Ethernet  Up
1   Eth/1      Ethernet/IEEE 802.3   10/100 Ethernet  Up
2   Eth/2      Ethernet/IEEE 802.3   10/100 Ethernet  Up
3   Eth/3      Ethernet/IEEE 802.3   10/100 Ethernet  Up
4   Eth/4      Ethernet/IEEE 802.3   10/100 Ethernet  Up
5   Eth/5      Ethernet/IEEE 802.3   10/100 Ethernet  Up
6   Eth/6      Ethernet/IEEE 802.3   10/100 Ethernet  Up
7   Eth/7      Ethernet/IEEE 802.3   10/100 Ethernet  Up
8   Eth/8      Ethernet/IEEE 802.3   10/100 Ethernet  Up
9   Eth/9      Ethernet/IEEE 802.3   10/100 Ethernet  Up
10  Eth/10     Ethernet/IEEE 802.3   10/100 Ethernet  Up
11  Eth/11     Ethernet/IEEE 802.3   10/100 Ethernet  Up
12  Eth/12     Ethernet/IEEE 802.3   10/100 Ethernet  Up
13  Eth/13     Ethernet/IEEE 802.3   10/100 Ethernet  Up
14  Eth/14     Ethernet/IEEE 802.3   10/100 Ethernet  Up
15  Eth/15     Ethernet/IEEE 802.3   10/100 Ethernet  Up
16  Eth/16     Ethernet/IEEE 802.3   10/100 Ethernet  Up
17  Eth/17     Ethernet/IEEE 802.3   10/100 Ethernet  Up
17  Eth/18     Ethernet/IEEE 802.3   10/100 Ethernet  Up
19  Eth/19     Ethernet/IEEE 802.3   10/100 Ethernet  Up
20  Eth/20     Ethernet/IEEE 802.3   10/100 Ethernet  Up
21  Eth/21     Ethernet/IEEE 802.3   10/100 Ethernet  Up
22  Eth/22     Ethernet/IEEE 802.3   10/100 Ethernet  Up
23  Eth/23     Ethernet/IEEE 802.3   10/100 Ethernet  Up
24  Eth/24     Ethernet/IEEE 802.3   10/100 Ethernet  Up
25  Eth/25     Ethernet/IEEE 802.3   10/100 Ethernet  Up
26  Eth/26     Ethernet/IEEE 802.3   10/100 Ethernet  Up
27  Eth/27     Ethernet/IEEE 802.3   10/100 Ethernet  Up
28  Eth/28     Ethernet/IEEE 802.3   10/100 Ethernet  Up
29  Eth/29     Ethernet/IEEE 802.3   10/100 Ethernet  Up
30  Eth/30     Ethernet/IEEE 802.3   10/100 Ethernet  Up
31  Eth/31     Ethernet/IEEE 802.3   10/100 Ethernet  Up
32  NULL/0     Null device           None             Not present
33  NULL/1     Null device           None             Not present
34  NULL/2     Null device           None             Not present
35  NULL/3     Null device           None             Not present
36  ATM/0      ATM                   ATM              Up
37  ATM/1      ATM                   ATM              Up
38  ATM/2      ATM                   ATM              Down
39  ATM/3      ATM                   ATM              Down
40  Eth/32     Ethernet/IEEE 802.3   ATM              Up
41  Eth/33     Ethernet/IEEE 802.3   ATM              Up
42  Eth/34     Ethernet/IEEE 802.3   ATM              Up
43  Eth/35     Ethernet/IEEE 802.3   ATM              Up
44  Eth/36     Ethernet/IEEE 802.3   ATM              Up
45  Eth/37     Ethernet/IEEE 802.3   ATM              Up
46  Eth/38     Ethernet/IEEE 802.3   ATM              Up
```

```
47  Eth/39     Ethernet/IEEE 802.3   ATM             Up
48  Eth/40     Ethernet/IEEE 802.3   ATM             Up
49  Eth/41     Ethernet/IEEE 802.3   ATM             Up

50  Eth/42     Ethernet/IEEE 802.3   ATM             Up
51  Eth/43     Ethernet/IEEE 802.3   ATM             Up
52  Eth/44     Ethernet/IEEE 802.3   ATM             Up
53  Eth/45     Ethernet/IEEE 802.3   ATM             Up
54  Eth/46     Ethernet/IEEE 802.3   ATM             Up
55  Eth/47     Ethernet/IEEE 802.3   ATM             Up
56  Eth/48     Ethernet/IEEE 802.3   ATM             Up
57  Eth/49     Ethernet/IEEE 802.3   ATM             Up
58  Eth/50     Ethernet/IEEE 802.3   ATM             Up
59  Eth/51     Ethernet/IEEE 802.3   ATM             Up
60  Eth/52     Ethernet/IEEE 802.3   ATM             Up
61  Eth/53     Ethernet/IEEE 802.3   ATM             Up
62  Eth/54     Ethernet/IEEE 802.3   ATM             Up
63  Eth/55     Ethernet/IEEE 802.3   ATM             Up
```

2. Enter the GWCON **protocol** command with the protocol number or short name of the desired protocol displayed in the configuration information.

   In the following example, the command has been entered for accessing the SNMP protocol console process.

   ```
   + protocol 11
   ```

   or

   ```
   + protocol SNMP
   ```

   The protocol console prompt then displays on the console. This example shows the SNMP protocol console prompt:

   ```
   SNMP>
   ```

You can now begin entering the protocol's commands. See the corresponding protocol section of the *Protocols and Features* for more information on specific protocol console commands.

Command Completion

The automatic command completion function assists you with the syntax for commands entered at the command line.

To illustrate the behavior of Command Completion, assume that the following commands are allowed in a given menu context. (This is an example menu only.)

enable
- auto-refresh
- caching

set
- cache-size
- cache-timeout
- priority

- If you type **ena** and press the Space Bar, the full command is shown as **ENABLE**. If you now type **?**, a list of possible items to enable are shown (**auto-refresh** and **caching**) and the command **ENABLE** remains on the command line.

- If you type **ena** and press **Enter**, a message is printed that the command is not fully specified, and a list of possible items to enable are shown (**auto-refresh** and **caching**) and the command **ENABLE** remains on the command line.
- Because the **ENABLE** command requires an item to enable, it appears in a list of possible command completions with "..." in the left margin to indicate that more input is required for the command.
- If your input matches multiple commands, a list of possible completions is displayed. Your input on the new command line is expanded to the longest common prefix. For example, if you enter **set ca**, and then press the space bar, **CACHE-SIZE** and **CACHE-TIMEOUT** will be listed, and the new command line will be expanded to **SET cache-**, since "cache-" is common to both possible completions. Now you must type the letter "s" or the letter "t" to distinguish between the possible completions ″size″ or ″timeout″.
- Common commands sometimes appear in an alternate form (**SHOW**, **DISPLAY**, **LIST**). If the Command Completion does not yield a match on a common command, such as **SHOW**, the alternatives **DISPLAY** or **LIST** will be displayed, if found.
- If the search for a command (and alternatives) does not yield an exact match, you are presented with a list of possible completions, using some portion of your input. For example, **enanle** followed by the Space Bar would be replaced with **ena** and **ENABLE** would be listed as the possible completion.
- When a list of possible commands is shown, you can use the Tab key to cycle through one command at a time on the current command line. You can use the Space Bar or Enter key to select the command shown.

Online Help When Command Completion is Enabled

The following online help is available when command-completion is enabled.

See 62 for the **enable command-completion** syntax.

? Question mark displays a list of possible completions. A message appears if the command is already complete.

Space Bar
Attempts to complete the current word on the command line. If a unique match is not found, possible completions are listed.

Tab Attempts to complete the current word on the command line. If a unique match is not found, possible completions are listed and you may cycle through these possible completions using the Tab key. Use the Space Bar or the Enter key to select the currently displayed command.

Enter Attempts to complete the current word on the command line. If the command is complete, Enter executes the command and stores it in the Command History. If the command is incomplete, a list of possible completions is displayed.

Ctrl-P Returns to the MOS Operator Console prompt (*). (Ctrl-P is the default Intercept Character.)

Backspace
Deletes the last character on the command line.

Ctrl-W Deletes the last word on the command line.

Ctrl-U Aborts the current command.

Ctrl-L Refreshes the current command line to display its contents.

Ctrl-B Retrieve Backward. Replaces the current command line with the previous command in the circular Command History.

Ctrl-F Retrieve Forward. Replaces the current command line with the next command in the Command History.

Ctrl-R Marks the start of a Repeat Sequence in the Command History. Use with the **Ctrl-N** function.

Ctrl-N Replaces the current command line with the next command in the Repeat Sequence whose starting command was marked with **Ctrl-R**.

Ctrl-C Cancels Easy-Start, if active.

Escape ?
Escape, followed by "?" prints this Command Line Help:

The following rules apply to automatic command completion:

- Completed commands are shown in UPPERCASE on the command line.
- Common commands sometimes appear in an alternate form (**ADD** versus **CREATE**). If the command completion does not yield a match on a common command, any alternative commands will be displayed.
- If the search for a command (and alternative commands) does not yield a unique match, a list of possible completions is shown, and the longest common prefix is presented.
- When possible completions are listed, commands requiring further command input are shown with "..." in the left margin.
- When a Command History retrieve key (Ctrl-B,F,N) is pressed, the Command History is scanned for a command that successfully parses in the current command context. A tone will be sounded if no such command exists.
- Some command menus are built dynamically. Command Completion cannot always follow these dynamic links. '?' can be entered in these cases.
- To disable Command Completion for just one command (to enter a comment), type any Comment Character as the first character on the command line. The Comment Characters are !@#$%*:;/'"
- Command Completion will be disabled in the event of an internal error. Report the Debug information on the screen to Customer Support.
- Command Completion is currently Enabled. To Disable this option, use the **disable command-completion** command from Configuration `talk 6`.

Online Help When Command Completion is Disabled

The following online help is available when command-completion is disabled:

? When a ? (Question Mark) is entered at the end of the command line, a list of possible completions is shown.

Enter Executes the command and stores it in the Command History. A message is printed if the command is not fully specified

Ctrl-P Returns to the MOS Operator Console prompt (*). (Ctrl-P is the default Intercept Character.)

Backspace
Deletes the last character on the command line.

Ctrl-U Aborts the current command.

Ctrl-B Retrieve Backward. Replaces the current command line with the previous command in the circular Command History.

Ctrl-F Retrieve Forward. Replaces the current command line with the next command in the Command History.

Ctrl-R Marks the start of a Repeat Sequence in the Command History. Use with the **Ctrl-N** function.

Ctrl-N Replaces the current command line with the next command in the Repeat Sequence whose starting command was marked with **Ctrl-R**.

Ctrl-C Cancels Easy-Start, if active.

Escape ?
Escape, followed by "?" prints this Command Line Help:

•

```
Command Completion is currently Disabled.  To Enable this option,
use the enable command-completion command from Configuration talk 6.
```

Command History

The Command History contains up to the last 50 commands entered by the user in OPCON, GWCON (Talk 5) or CONFIG (Talk 6) command line menus.

Backward and Forward retrieve keys can be used to recall previously entered commands. In addition, a facility is provided to enable the advanced user to repeat a particular series of commands.

Repeating a Command in the Command History

By pressing **Ctrl-B** (backward) or **Ctrl-F** (forward) at any command line prompt in an OPCON, GWCON or CONFIG menu, the current command line is replaced by the previous or next command in the Command History. The Command History is common across the command line interface. That is, a command entered while in a GWCON menu can be retrieved from within CONFIG and a command entered while in a CONFIG menu can be retrieved from within GWCON.

When automatic Commmand Completion is enabled (See"Command Completion" on page 19) and a Command History retrieve key (CTL-B,F,N) is pressed, the Command History is scanned for a command that successfully parses in the current command context. A tone will be sounded if no such command exists.

The Command History contains the most recently entered commands, up to a maximum of the last 50 commands. If only three commands have been entered since a restart, pressing **Ctrl-F** or **Ctrl-B** circles through only those three commands. If no commands have been entered thus far, **Ctrl-F** or **Ctrl-B** results in tone sound.

Note: A command aborted by pressing **Ctrl-U** will not be entered into the Command History. When Command Completion is enabled, only complete commands are entered into the Command History.

To enter two similar commands:

```
display sub les
```

display sub lec

Enter:

display sub les, then press **Enter**

Ctrl-B for Backward, and the current line is replaced with-

display sub les

Press **Backspace** and replace “s” with “c” to get

display sub lec and then press **Enter**

Repeating a Series of Commands in the Command History

There is an additional feature for advanced users to facilitate repeating a particular series of GWCON or CONFIG commands. C1, C2,...,Cn in the Command History is referred to as a *repeat sequence*. This feature may be more convenient than simply using **Ctrl-B** and **Ctrl-F** when you must repeat a given task that requires multiple commands. Enter **Ctrl-R** (repeat) to set the start of the *repeat sequence* at command C1. Enter **Ctrl-N** (next) successively to retrieve the next command in the repeat sequence. Commands are not automatically entered, but are placed on the current command line allowing you to modify or enter the command.

To produce the desired behavior of a repeat sequence, the first command retrieved using the first **Ctrl-N** (next) depends on the manner in which the start of the repeat sequence was set using **Ctrl-R** (repeat).

Setting the start of the repeat sequence with **Ctrl-R** can be done in two ways:

1. When C1 is initially entered
2. When C1 is retrieved from the Command History with **Ctrl-B** or **Ctrl-F**.

Starting a Repeat Sequence As Commands Are Entered

If you enter **Ctrl-R** as command C1 is being keyed in, and then enter commands C2, C3... Cn. **Ctrl-N** will successively bring commands C1, C2, ... Cn, C1, C2, ... Cn, C1, ... to the command line.

In Example 1, the start of the repeat sequence is set as the first command is keyed in. The user knows ahead of time that the same commands to be entered in GWCON need to be repeated in CONFIG.

Example 1

1. As the first command in the sequence is keyed in, use **Ctrl-R** (repeat) to set the start of the repeat sequence.

   ```
   *console
   +event Ctrl-R
   ```

   then press **Enter** to set the start of the repeat sequence.
2. Continue typing the subsequent commands in the sequence:

   ```
   Event Logging System user console
     ELS>display sub les
     ELS>display sub lec
     ELS>exit
     +
   ```
3. To enter these same commands in CONFIG, press

   Ctrl-P (the default OPCON intercept character) and go to CONFIG.

```
+-press Ctrl-P-
*configuration
Config>Ctrl-N for NEXT to retrieve the start of this sequence-
Config>event Enter
Event Logging System user configuration
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>display sub les Enter
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>display sub lec Enter
ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
ELS config>exit Enter
Config>
```

Starting a Repeat Sequence After All Commands Are Entered

On the other hand, if you first enter C1, C2, ... Cn, and retrieve C1 via **Ctrl-B** or **Ctrl-F**. Entering **Ctrl-R**, entering **Ctrl-N** successively brings commands C2,..., Cn, C1, C2,..., Cn, C1,...,Cn to the command line (see Example 2). The first occurrence of C1 is bypassed since C1 is already available on the command line at the time it was retrieved, and does not need to be recalled again by the first **Ctrl-N**.

In Example 2, all the commands are entered and then the first command in the sequence to be repeated is retrieved. A sequence of commands has been entered in GWCON, and the same sequence needs to be repeated in CONFIG.

Example 2

1. Enter the following commands in GWCON:

```
*console
+event
Event Logging System user console
ELS>display sub les
ELS>display sub lec
ELS>exit
+
```

2. To enter these same commands in CONFIG, press **Ctrl-P** (the default OPCON intercept character) and go to CONFIG.

```
+Ctrl-P-
*configuration
Config>Ctrl-B four times to retrieve the start of
        the four command sequence in this example-
Config>event
Config>event Ctrl-R for REPEAT to set the start of the repeat sequence-
 Config>event Enter
 Event Logging System user configuration
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>display sub les Enter
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>display sub lec Enter
 ELS config>Ctrl-N for NEXT to retrieve the next command in sequence-
 ELS config>exit Enter
 Config>
```

Chapter 3. Using Service Functions in the IBM 8371 Firmware

This section covers boot options that can be set from the Firmware bootstrap menus. For information about file transfer and file management, refer to *Networking Multilayer Ethernet Switch Installation and Planning Guide*.

The purpose of the bootstrap firmware is to provide a Power On Self Test (POST) for the IBM 8371 processor card and to boot from the active operating system image stored in the FLASH memory.

Two operating system images are stored in system FLASH. The active boot image is selected by using the `Configuration` **boot** command. See “Boot” on page 59 and “Understanding Change Management” on page 75.

The active image selected using the **boot** command is used to boot the device. You can select the backup boot image using commands available from the firmware bootstrap menus. See “Select Boot Mode” on page 26.

Accessing the Firmware Bootstrap Menus

Before booting the device, note that:

- You will need a terminal or terminal emulator connected to the 8371 RS232 service port with a line speed of 19200 baud. This can be a VT100 TTY device connected directly through the service port.

To display the bootstrap main menu, power on the 8371, and press **Ctrl-C** on the terminal keyboard after one second.

Important: To access the Firmware prompt, you must stop the 8371 boot. To stop it, you must have a TTY console directly attached to the serial port. When the 8371 starts its boot sequence, press **Ctrl-C** from the console to interrupt the boot sequence.

From the Main Menu panel shown in Figure 3 on page 26, you can select one of four services. The following sections explain these services and provide instructions for going through the associated panels:

- “Bootstrap Utilities” on page 26
- “Select Boot Mode” on page 26
- “Select POST Mode” on page 27
- “Issue a Hardware Reset” on page 28

```
7381 System Bootloader
VERSION: 1.00
(C) Copyright IBM Corporation, 1998 All Rights Reserved.


                      Bootstrap Main Menu

       1) Bootstrap Utilities
       2) Select Boot Mode
       3) Select POST Mode

       9) Issue Reset

    Enter option:
```

Figure 3. Main Menu Panel

Bootstrap Utilities

The following options are available from the Utilities menu:

```
                    Bootstrap Utility Menu

       1) Display Error Log
       2) Clear Error Log
       3) Zmodem (restore boot images)

       8) Return to Bootstrap Main Menu
       9) Issue Reset


              Enter option:
```

Figure 4. Utilities Menu Panel

The utilities provide the following functions:

Table 2. Utilities

Function	Description
Display Error Log	Displays the self-test error log.
Clear Error Log	Clears the self-test error log.
ZMODEM (boot image recovery)	Activates the ZMODEM function to restore operating system images in FLASH. Indicates that the next boot of the IBM 8371 is to be from the ZMODEM port. The ZMODEM boot is intended for recovery when both the active and the backup images have become corrupted and neither can be booted.
Return to Bootstrap Main Menu	Displays main menu as shown in Figure 3.
Issue Reset	Resets the hardware.

Select Boot Mode

The following options are available from the Select Boot Mode menu:

```
              Boot Sequence Selection Menu


      1) Normal Boot
      2) Backup Boot

      8) Return to Bootstrap Main Menu
      9) Issue Reset

      Current Setting : Normal Boot


             Enter option:
```

Figure 5. Select Boot Mode Menu Panel

Table 3 contains a description of the Boot Mode menu functions.

Table 3. Select Boot Mode Functions

Function	Description
Normal Boot	Two copies of the operational code exist in FLASH. The active image is the image from which a normal boot occurs.
Backup Boot	Indicates that the next boot only of the IBM 8371 is to be from the alternate (backup) image. The alternate image is intended for recovery when the active image has become corrupted and cannot be booted. Once the device has been booted, the boot mode will be automatically set back to the normal boot mode.
Return to Main Menu	Displays main menu as shown in Figure 3 on page 26.
Issue Reset	Resets the hardware.

Select POST Mode

The following options are available from the Select Post Mode menu:

```
              Select Post Mode Menu

      1) Set POST ON (Next Hard Reset only)
      2) Set POST OFF

      8) Return to Bootstrap Main Menu
      9) Issue Reset

      Current Setting :  OFF


             Enter option:
```

Figure 6. Select Post Mode Menu Panel

Table 4 contains a description of the Boot Mode menu functions.

Table 4. Select POST Mode Functions

Function	Description
Set POST on (next reset only)	This option causes a more extensive POST to be executed the next time the device is reset or powered on. Once the extended POST executes successfully, the normal, short POST will be executed on successive executions of POST.
Set POST off	Indicates that the normal, short POST will be executed.
Return to Bootstrap Main Menu	Displays main menu as shown in Figure 3 on page 26.
Issue Reset	Resets the hardware.

Issue a Hardware Reset

This function resets the IBM 8371 and boots the operating system. This reset causes a POST to execute.

Hardware Error Codes

The following error codes are displayed on the service terminal and logged in the POST log when POST detects a hardware failure:

Table 5. Hardware Error Codes

Error Code	Physical Location	Explanation
00010106	CPU Card	Processor Dual Port RAM Failure (fatal)
00010206	CPU Card	Processor Register Read/Write Data Miscompare
00040101	CPU Card	SCC2 UART No Transmit
00040102	CPU Card	SCC2 UART No Receive
00040106	CPU Card	SCC2 UART Wrap Data Miscompare
00060201	CPU Card	CPU I2C EEPROM write failure
00060202	CPU Card	CPU I2C EEPROM Read address command failure
00060203	CPU Card	CPU I2C EEPROM Read command failed
00060204	CPU Card	CPU I2C EEPROM Read receive failed
00070101	CPU Card	On Card Flash Status Error
00070102	CPU Card	On Card Flash Write Operaton Failure
00070103	CPU Card	On Card Erase Operation Failure
00070104	CPU Card	On Card Flash ID Error
00070105	CPU Card	On Card Flash Erase Verify Failure
00070106	CPU Card	On Card Flash Read/Compare Failure
00080106	CPU Card	SIL Bridge Chip Read/Write Data Miscompare
01000202	SDRAM SE	SDRAM EEPROM read address command failure
01000203	SDRAM SE	SDRAM EEPROM read command failure

Table 5. Hardware Error Codes (continued)

Error Code	Physical Location	Explanation
01000204	SDRAM SE	SDRAM EEPROM read receive failure
01000206	SDRAM SE	Invalid row+column read from SDRAM EEPROM
01000207	SDRAM SE	Invalid # banks read from SDRAM EEPROM
01030106	SDRAM CS3	Data Storage Read/Write Data Miscompare (pattern test)
01030206	SDRAM CS3	Data Line Read/Write Data Miscompare (walking ones test)
01030306	SDRAM CS3	Address Line Read/Write Data Miscompare (address test)
01030406	SDRAM CS3	Clear memory failed
01040106	SDRAM CS3	Data Storage Read/Write Data Miscompare (pattern test)

Chapter 4. Getting Started with Configuring the 8371

The 8371 is a plug-and-play device that boots with a default configuration. All possible interfaces are automatically configured at boot time. The following table shows the network interfaces available on the 8371.

Network Interfaces on the 8371

Table 6. Network Interfaces Automatically Configured on the 8371

Device Type	Slot	Ports	Interface Net Numbers
10/100 Ethernet (fixed ports on base switch)	0	1 - 16	0 - 15
10/100 Ethernet Feature Card	1	1 - 8	16 - 23
10/100 Ethernet Feature Card	2	1 - 8	24 - 31
Reserved	3	1 - 4	32 - 35
ATM	1	1 - 2	36 - 37
ATM	2	1 - 2	38 - 39
Ethernet LAN Emulation Client	3	5 - 29	40 - 63

Note: All of the above interfaces cannot be active at the same time. For example, if Ethernet Feature cards are installed in both slots 1 and 2, there is no place to install ATM interfaces.

In addition to the network interfaces, the transparent bridge is also automatically configured. All the Ethernet interfaces and all of the LECs are configured as ports on the transparent bridge. Interfaces that are configured but are disabled or not actually present, are inactive bridge ports.

Network Interfaces on the 8371 Blade

Table 7. Network Interfaces Automatically Configured on the 8371 Blade

Device Type	Slot	Ports	Interface Net Numbers
10/100 Ethernet (fixed ports on base switch)	0	1 - 16	0 - 15
10/100 Ethernet Feature Card	2	1 - 8	24 - 31
Reserved	1	1 - 8	16 - 23
Reserved	3	1 - 8	32 - 35
Reserved	2	1 - 2	38 - 39
ATM (connection to 8265 backplane)	1	1	36
Reserved	1	2	37
Ethernet LAN Emulation Client	3	5 - 29	40 - 63

LEC Configuration Details

Only one of the 24 automatically Ethernet LEC interfaces is enabled by default. The LEC with an interface number of 40 is enabled, while LECs with interface numbers of 41 - 63 are disabled. The configured LEC has:

ATM interface	36
ELAN name	ELAN*j*, where *j* is the interface number of the LEC and *j*= (interface number of the LEC – 39)
LECS Auto-config	yes
MAC Address/ESI	Burned-in MAC address for net *i*
Selector	0

This chapter explains how to access the 8371 using a workstation and how to manage operational software images and configuration files. It also provides a brief overview of the configuration methods available for the 8371.

Configuration and Monitoring Tools

These are the various configuration and monitoring tools that are supported by the physical connections:

Web browser Hypertext Markup Language (HTML) interface

The Web browser interface is a configurator that is a home page and is accessed by a Web browser from a workstation that is connected to the 8371. You need a Web browser that can display clickable images and tables. The Web browser interface can be accessed using SLIP or IP. You must use the serial line connection and SLIP before the 8371 is operational in the network.

If you supply the Web browser the SLIP address, one of the configured IP addresses of the 8371, or its name (when using an IP name server), the Web browser interface will come up.

Note: The configured IP addresses of the 8371 include the IP addresses of all the LAN emulation clients and Classical IP clients.

Command line interface

The command line interface is a teletypewriter (TTY) text interface that requires you to enter commands to use it. The workstation that accesses it must be either an ASCII terminal, a personal computer (PC), or other intelligent programmable workstation emulating an ASCII terminal.

This interface must be reached over a serial link before the 8371 is operational in the network; you can use TTY or SLIP to access it. If you use SLIP, you can Telnet into the 8371.

After the 8371 is operational in the network, you can Telnet into the 8371 over IP to bring up this interface. If one connection to the 8371 is a Telnet session, the 8371 can support two connections at one time.

The command line interface is marked by an asterisk (*) prompt.

Important: If you use a serial connection, (either local or remote), you ***must press a key*** to bring up the asterisk that is the prompt for the command line interface. When you make the connection, the message `Please press a key to obtain console` appears and reminds you to do this.

Local and Remote Console Access

When accessing the 8371 locally on a null modem cable attached to the EIA service port, use VT100 terminal emulation. Because VT100 does not define function keys above F4, edit the keyboard mapping manually as follows: For F6, enter the mapping (ESC)OU. For F9, enter the mapping (ESC)(Left square bracket)009q.

Note: (ESC) represents the carat symbol followed by the left square bracket.

File Transfer

Table 8 defines the ways in which configuration files and operational software files can be transferred to and from the 8371.

Table 8. File Transfer

File Transfer Method	Type of Connection
TFTP Get command from the 8371 to the workstation that has the binary configuration file, to download operational software images and configuration files to the 8371. Files sent using TFTP must be binary, or the 8371 cannot use them. You should use the Create command of the Configuration Program to save configuration files in binary format before downloading them to the 8371. After the 8371 is operational in the network, you can use the TFTP Put command over IP to upload a file from the 8371 to a workstation. The file will be uploaded in binary format. Both operational software and configuration files can be uploaded. You should use the Read device configuration option of the Configuration Program to make an uploaded configuration file usable by the Configuration Program so that you can change some parameter values in it. **Note:** Using TFTP Put is a way to retrieve files from the 8371 if the Retrieve option of the Configuration Program is not available.	• SLIP connection (using the TFTP Get command to download files to the 8371). • IP connection of operational 8371 over functioning network (using the TFTP Get and Put commands to download and upload files).
The Communications Option of the Configuration Program (actually, the protocol for this is SNMP). This method cannot be used until the 8371 is operational in the network. The files are not binary, but are in a format that is internal to the Configuration Program. This function can send configuration files to the 8371 and retrieve them from the server.	IP connection of operational 8371 over functioning network.

Tips for Managing Configuration Problems

Important: After the IBM 8371 is configured and operational, ***always*** back up the active configuration file. Keeping this file enables you to re-establish the IBM 8371 on the network should the active configuration become corrupted.

Back up the active configuration file by retrieving it and storing it in the workstation. See “File Transfer” for more information.

Reconfiguring

You may find it hard to detect problems caused by configuration errors. A configuration error can initially appear to be a hardware problem because the IBM 8371 will not start or data will not flow through a port. In addition, problems with configuration may not result in an error initially; an error may occur only when specific conditions are encountered or when heavy network traffic occurs.

If you cannot resolve a problem after making a few changes to the configuration or after restoring the active configuration file, it is recommended that you generate a new configuration. Too many changes to a configuration often compound the problem, whereas you can usually generate and test a new configuration within a few hours.

How Software Files Are Managed

To help manage operational software upgrades and configurations, the IBM 8371 has a software change management feature. This utility enables you to determine which operational software file and which configuration file is active while the IBM 8371 is running. In addition to storing the active operational software and the active configuration file, the IBM 8371 stores two backup images of the operational software and up to 11 configuration files in non-volatile memory.

How to View the Files

To use the change management tool in the command line interface to view the operational software image and the configuration files, follow these steps:

1. From the prompt for OPCON, which is an asterisk (*), type **talk 6**. The prompt `Config>` appears.
2. Enter **boot**. You will see the prompt `Boot config>`.
3. Enter **list** to display information about which load images and configuration files are available and active.

   See “List” on page 81 for sample list output and a description of file statuses.

How to Reset the IBM 8371

Note: A reset interrupts the function of the IBM 8371 for up to 90 seconds. Be sure that the network is prepared for the interruption.

As previously stated, PENDING and LOCAL files are not loaded into active memory until you reset the IBM 8371.

You can reset the IBM 8371 using any one of these methods:

- Press the hardware reset button.
- At the OPCON prompt (*), type **reload**.

File Transfer Using TFTP

See “TFTP” on page 83 for a sequence of commands to transfer a file from a workstation or server to the IBM 8371 using TFTP. You will need to substitute your own values for the IP address and path, which are given as examples.

Storing Configuration Files Using the Command Line Interface or the Web Browser Interface

To store a configuration file created using the command line interface, type **write** at the `Config>` prompt. When using the Web browser interface, select **Write**. The Write command creates a binary configuration file that contains the most current value of each of the configuration parameters.

This file is stored in the ACTIVE bank and is given PENDING status. If the status of the file is not changed by a Set command, it becomes the ACTIVE configuration when the IBM 8371 is reset.

Changing the Statuses of Files

These are the ways to change the statuses of image and configuration files:

- You can cause the IBM 8371 to perform a reset by using the Send command from the Communications Option of the Configuration Program. When you do this, the file sent can arrive as a PENDING file or as an AVAIL file. If it is a PENDING file, it becomes the ACTIVE configuration and the previously ACTIVE file becomes AVAIL when the IBM 8371 is reset.

  If it is an AVAIL file, resetting the IBM 8371 does not change its status.
- Use the Set config (set config) commands from the `Boot config>` prompt manually to change the status of any files except the ACTIVE files. If you set a file to PENDING, it becomes ACTIVE and the ACTIVE file becomes AVAIL when a reset is performed.
- Use the Write command to store a configuration file that you have created using the command line interface or the Web browser interface, it is stored with a PENDING status.
- If you copy a file from one location to another, the file receives the status of the file that was there before it and that it overwrites. For example, copying a file with the status of AVAIL over a file that has the status of PENDING, the new file will keep the status of the original file, which is PENDING.

Using the Set Commands

See “Set” on page 82 for information about the **set** command.

Other Change Management Functions

These are the other change management commands:

- Describe load images
- Describe config images
- Disable dumping
- Enable dumping
- Erase files

Describe

See “Describe” on page 79 for information about the **Describe** function.

Disable Dumping

The IBM 8371 can be set up to dump the contents of memory to permanent storage in the unlikely event of a complete system failure. If dumping is enabled, using this selection will cause the IBM 8371 *NOT* to dump to disk.

To disable dumping, type **t 6** at the *, press **Enter** and then type **disable dump** or **dis du** at the `Config>` prompt. You will see the message:

```
Config> Automatic memory dump disabled
```

Enable Dumping

This command enables the dumping of memory without intervention from anyone in the event that the IBM 8371 has a catastrophic error. The IBM 8371 will dump memory onto the hard disk. Once a successful dump has been taken, the IBM 8371 attempts to restart. Depending upon the failure of the IBM 8371, it cannot always restart. In this case, you should restart it manually and call a service person, who will dial into the IBM 8371 to determine the nature and the causes of the failure.

To enable dumping, type **t 6** at the *, press **Enter** and then type **enable dump** or **ena du** at the `Config>` prompt. You will see the message:

```
Config> Automatic memory dump enabled
```

The default state is to have dumping enabled.

Erase Files

See “Erase” on page 79 for information about the **erase** command.

Using the Copy Command

The Copy command moves a file from one location in the storage area to another. This command allows you to change the status as well. The file moved always receives the status of the storage area that it is moved to. For example, suppose that you have this scenario:

- The configuration file in BANK A CONFIG 1 is AVAIL. The configuration file in BANK B CONFIG 1 is PENDING.
- You copy the configuration in BANK A CONFIG 1 to BANK B CONFIG 1.

In this case, the original configuration file in BANK A CONFIG 1 remains unchanged and AVAIL. The configuration that was in BANK B CONFIG 1 is overwritten by a copy of the configuration file that is in BANK A CONFIG 1. This copy retains the status of the file that it overwrote, in this case, PENDING.

See “Copy” on page 78 for additional information about the **copy** command.

Using the Lock Command

The **lock** command prevents the device from overwriting the selected configuration with any other configuration.

See “Lock” on page 81 for additional information about the **lock** command.

Using the Unlock Command

The **unlock** command removes the lock from a configuration allowing the configuration to be updated.

See “Unlock” on page 83 for additional information about the **unlock** command.

Chapter 5. Using the World Wide Web Interface

The IBM 8371 provides a World Wide Web interface to monitor and configure the product. The Web browser interface performs all of the functionality of the command line interface, but in a graphical, more user-friendly manner.

Connecting to the World Wide Web Interface

Use any Web browser that supports HyperText Markup Language (HTML) tables and clickable images. Examples of browsers that support this feature are WebExplorer Version 1.03 or higher, Netscape Navigator Version 1.1N or higher, and Mosaic Version 2.1.1 or higher.

Access the Web interface through TCP/IP Host Services on the bridged network to which the IBM 8371 is connected.

You will be shown the Home Page that is described in the next section.

Rules for Using the Web Interface

When configuring using the Web browser interface, observe the following guidelines:

- Many configuration options require you to enter data on two or more Web pages (or forms). If you fill in and submit the first form in a series, be sure to complete the remaining forms. If you do not fill in and submit all the forms, the configuration parameter could be left in an unknown state.
- More than one person should not perform configuration at the same time. They can interfere with one another. For example, one person could delete an interface while the other person is in the middle of configuring a protocol on that interface.
- Disable the caching feature of the browser. If you do not do this, the browser may pull a page out of memory instead of going to the IBM 8371 to get the latest information. The browser will display old data. This problem is more likely to occur when you use the *Back* button on the browser.
- Do not use your Web browser's reload, back, or forward navigation buttons when using the Web browser interface. Using these buttons could cause problems during configuration. Instead, use the command history list or any of the navigation buttons on the Web pages themselves.

Home Page Structure

The Home Page provides a graphic that shows the status of the IBM 8371. It indicates the current network interfaces installed and shows the status of each port (for example, installed, enabled, or disabled). The current state of each LED is also shown, as well as the indication of the devices that are installed.. If the Web browser supports dynamic refresh, then this page will automatically refresh itself approximately every 80 seconds. If you click any of these ports or interfaces, a more detailed description of its status will be shown on a separate Web page.

Click **How to use this Web Site** for instructions about using this site.

Using the World Wide Web Interface

Click **Configuration and Console** to bring up the menu shown in Figure Figure 7.

Click **Diagnostics** to bring up the menu shown in Figure Figure 8.

Click **Vital Product Data** for information about the hardware and operational software. This panel, which is usually used for diagnostics, is not displayed here.

Note to Developers
Need new screen captures for 8371.

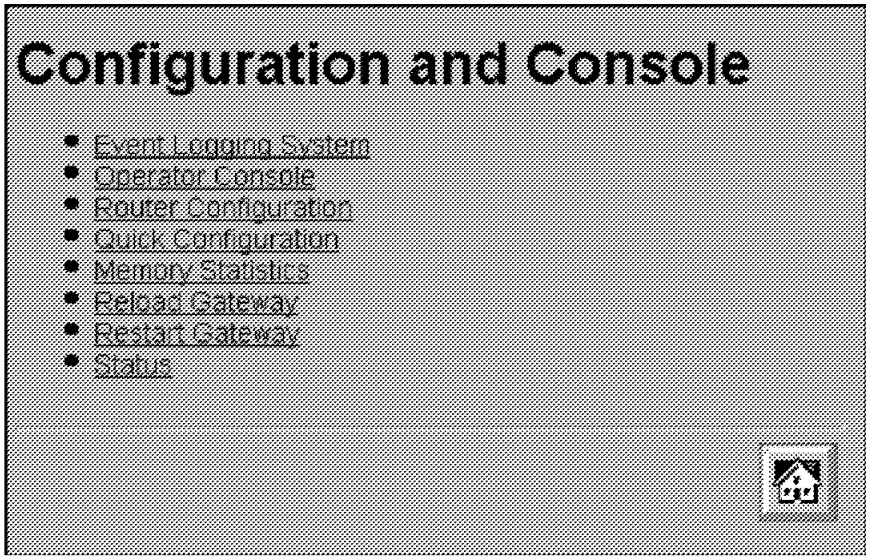

Figure 7. Configuration and Console Page 1

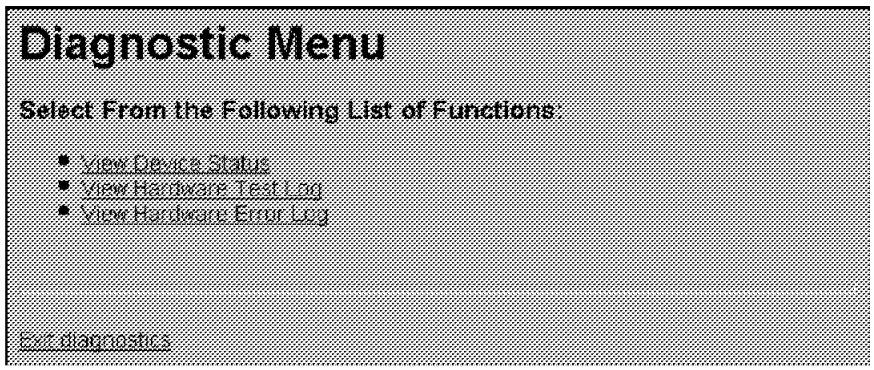

Figure 8. Diagnostic Menu

Event Logging System

One of the links on the Configuration and Console page 1 is to the Event Logging System (ELS). The ELS display is similar to the one provided on the command line interface. On the Web interface, going into the ELS will display the most recent events stored in the system memory. In order to get future updates, press the Reload button on your browser. For more details about the ELS message facility, refer to the *Event Logging System Messages Guide*.

Operator Console

The console monitoring interface provides real-time status information very similar to that offered in the command line interface. The menus from the command line interface are presented as a hierarchy of Web links that can easily be traversed with the click of a mouse button. It is possible to jump back several levels in the hierarchy with a single push of a button.

Device Configuration

Important: Exercise caution when using the Web browser to change configuration parameters. Changes to the configuration that are made using the Web browser are written directly to static random access memory (SRAM). You can make unintentional configuration changes that do not take effect until you reset the IBM 8371. To check that you have the correct parameters, look over the settings for any parameters that you have configured before submitting them.

The Web interface greatly simplifies the configuration of network and protocol parameters. In many cases where it is necessary to remember the individual network numbers on the command line interface, those options are now all presented as menu options on the Web. Also, the Web interface uses the graphical features available to it, such as pick lists, selection lists, radio buttons, and check boxes.

If a particular configuration option needs to prompt you for answers to several questions, those questions will be presented on a single Web page. After all of the questions are filled in, you should press the *Submit* button to send the data back to the IBM 8371 for validation.

The hierarchy of the Web browser interface is very similar to that of the command line interface.

History Function

The Web Configurator uses a selection list and a *Return to* button to provide an advanced history function. Depending upon your choice of HTML browser, a pick list, choice box or pull-down list box will be displayed. This list of selections contains the names of the pages visited under the current branch of the software structure. To return to a previously visited page within the current command pathway, select that entry from the list and click the *Return To* button.

Help System for the Web Browser Interface

Optional, free-of-charge, help files for the Web browser interface can be downloaded from the Web. Use of the help button located at the bottom of Web browser configuration panels requires the installation of these help files.

For download instructions and additional information about the help files, point your browser to `http://www.networking.ibm.com/support`.

Chapter 6. The OPCON Process and Commands

This chapter describes the OPCON interface configuration and operational commands. It includes the following sections:

- "What is the OPCON Process?"
- "Accessing the OPCON Process"
- "OPCON Commands"

What is the OPCON Process?

The Operator Console process (OPCON) is the root-level process of the device software user interface. The main function of OPCON is to communicate with processes at the secondary level, such as Configuration, Console, and Event Logging. Using OPCON commands, you may also:

- Display information about device memory usage
- Reload the device software (reboot)
- Telnet or ping to other devices or hosts
- Display status information about all device processes
- Manipulate the output from a process
- Change the OPCON intercept character

Accessing the OPCON Process

When the device starts for the first time, a boot message appears on the console. Then the OPCON prompt (*) appears on the console, indicating that the OPCON process is active and ready to accept commands.

The OPCON process allows you to configure, change, and monitor all of the device's operating parameters. While in the OPCON process, the device is forwarding data traffic. When the device is booted and enters OPCON, a copyright logo and an asterisk (*) prompt appears on the locally attached console terminal. This is the OPCON (OPerator's CONsole) prompt, the main user interface that allows access to second-level processes.

Some changes to the device's operating parameters made while in OPCON take effect immediately without requiring reinitializing of the device. If the changes do not take effect, use the **reload** command at the * prompt.

At the * prompt, an extensive set of commands enables you to check the status of various internal software processes, monitor the performance of the device's interfaces and packet forwarders, and configure various operational parameters.

OPCON Commands

This section describes the OPCON commands. Commands that are needed more often appear before the "- - - - -" separator. Each command includes a description, syntax requirements, and an example. The OPCON commands are summarized in Table 9 on page 44. To use them, access the OPCON process and enter the appropriate command at the OPCON prompt (*).

Table 9. OPCON Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Configuration*	Accesses the device’s configuration process. (`talk 6`)
Console*	Accesses the device’s console process. (`talk 5`)
Event Logging System*	Accesses the device’s event logging process. (`talk 2`)
ELS Console*	Accesses the device’s secondary ELS Console process. (`talk 7`)
Logout	Logs off a remote console.
Ping	Pings a specified IP address.
Reload	Reloads the device.
Telnet	Connects to another device.
- - - - - -	- -
Diags	Displays device status and the contents of the hardware test log and the hardware error log.
Divert	Sends the output from a process to a console or other terminal.
Flush	Discards the output from a process.
Halt	Suspends the output from a process.
Intercept	Sets the OPCON default intercept character.
Memory	Reports the device’s memory usage.
Status	Shows information about all device processes.
Talk	Connects to another device process and enables the use of its commands.

* When you use this command for the first time, you will be reminded that you can use **Ctrl-P** to return to the MOS Operator Console prompt (*).

***:**

Configuration

Use the **configuration** command to access the device’s configuration process (`talk 6`). See “Chapter 7. The CONFIG Process (CONFIG - Talk 6) and Commands” on page 55 for more information.

Syntax:

configuration

Example:

```
* configuration

(To return to the MOS Operator Console prompt (*), press Control-P)

Gateway user configuration
Config>
```

Console

Use the **console** command to access the device’s console and monitoring process (`talk 5`). See “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 85 for more information.

Syntax:

console

Example:

```
* console

CGW Operator Console

+
```

Diags

Use the **diags** command to display the Diagnostic Main Menu. The diagnostic menus allow you to enable, disable and test hardware adapters or ports. Diagnostic menus have on-screen help for the various options and status information that is available.

You can use the “b” (back) key to return to any previous menu. Use the “e” (exit) key to exit the diagnostics and return to the OPCON command prompt.

Syntax:

diags

Divert

Use the **divert** command to send the output from a specified process to a specified terminal. This command allows you to divert the output of several processes to the same terminal to simultaneously view the output. The **divert** command is commonly used to redirect MONITR output messages to a specific terminal. The device allows only certain processes to be redirected.

The **divert** command requires the PID and tty# (number of the output terminal). To obtain these values, use the OPCON **status** command. The terminal number can be the number of either the local console (tty0) or one of the remote consoles (tty1, tty2). The following example shows Event Logging System messages generated by the MONITR process (2) being sent to a remote console *tty1* (1).

Event messages are displayed immediately even though you may be in the middle of typing a command. The display and keyboard have separate buffers to prevent command confusion. The following example shows the MONITR process connected to TTY0 after executing the **divert 2 0** command. If you want to stop the output, enter **halt 2**. The **halt** command is described in “Halt” on page 47.

Syntax:

divert *pid tty#*

Example:

```
* divert 2 0
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL    TTY0
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
```

```
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2 jlg@128.185.40.40
10   WEBCon    IDL    --
```

Els

Use the **els** command to access the device's secondary ELS console process, (`talk 7`). See "Accessing the Secondary ELS Console Process, ELSCon (Talk 7)" on page 13 for more information.

Syntax:

els

Event

Use the **event** command to access the device's event logging process, (`talk 2`). See "Chapter 12. Using the Event Logging System (ELS)" on page 99 for more information.

Syntax:

event

Flush

Use the **flush** command to clear the output buffers of a process. This command is generally used before displaying the contents of the MONITR's FIFO buffer to prevent messages from scrolling off the screen. Accumulated messages are discarded.

The device allows only certain processes to be flushed. To obtain the PID and tty#, use the OPCON **status** command. In the following example, after executing the **flush 2** command, the output of the MONITR process is sent to the Sink (it has been flushed).

Syntax:

flush *pid*

Example:

```
* flush 2
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL    Sink
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2
10   WEBCon    IDL    --
*
```

Halt

Use the **halt** command to suspend all subsequent output from a specified process until the **divert**, **flush**, or **talk** OPCON command is issued to the process. The device cannot redirect all processes. **Halt** is the default state for output from a process. To obtain the PID for this command, use the OPCON **status** command. In the following example, after executing the **halt 2** command, the MONITR process is no longer connected to TTY0. Event messages no longer appear.

Syntax:

halt *pid*

Example:

```
* halt 2
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    DET     --
6    Config    DET     --
7    ELSCon    DET     --
8    ROpCon    IDL    TTY1
9    ROpCon    RDY    TTY2
10   WEBCon    IDL    --
```

Intercept

Use the **intercept** command to change the OPCON intercept character. The intercept character is what you enter from other processes to get back to the OPCON process. The default intercept key combination is **Ctrl-P**.

The intercept character ***must*** be a control character. Enter the ^ (shift 6) character followed by the letter character you want for the intercept character.

Syntax:

intercept ^ *character*

Example:

```
* intercept ^a
```

From this example, the intercept character is now **Ctrl-A**.

Logout

Use the **logout** command to terminate the current session for the user who enters the logout command. If the console login is enabled, this command will require the next user to log in using an authorized userid/password combination. If the console login is not enabled, the OPCON prompt appears again.

Syntax:

logout

Memory

Use the **memory** command to obtain and display information about the device's global heap memory usage. The display helps you to determine if the device is being utilized efficiently. For an example of memory utilization, see Figure 9.

See "Memory" on page 91 for memory usage via talk 5.

Syntax:

memory

Example:

```
* memory
Number of bytes:  Busy = 319544, Idle = 1936, Free = 1592
```

Busy Specifies the number of bytes currently allocated.

Idle Specifies the number of bytes previously allocated but freed and available for reuse.

Free Specifies the number of bytes that were never allocated from the initial free storage area.

Note: The sum of the Idle and Free memory equals the total available heap memory.

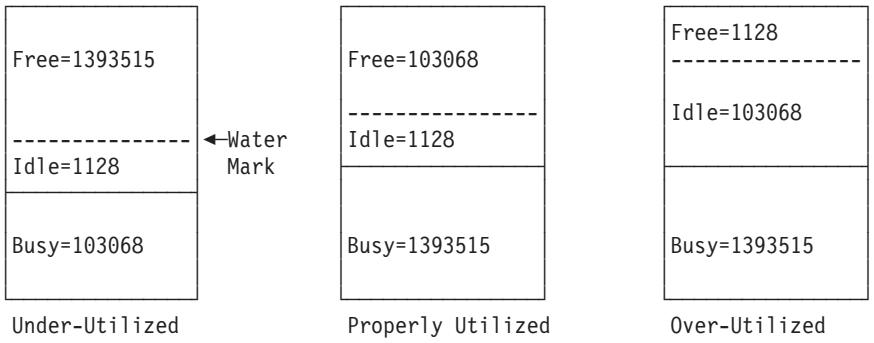

Figure 9. Memory Utilization

Ping

Use the **ping** command to have the device send ICMP Echo messages to a given destination (that is, "pinging") and watch for a response. This command can be used to isolate trouble in the internetwork.

Syntax:

ping *dest-addr [src-addr data-size ttl rate tos data-value]*

The ping process is done continuously, incrementing the ICMP sequence number with each additional packet. Each matching received ICMP Echo response is reported with its sequence number and the round-trip time. The granularity (time resolution) of the round-trip time calculation is usually around 20 milliseconds, depending on the platform.

To stop the ping process, type any character at the console. At that time, a summary of packet loss, round-trip time, and number of unreachable ICMP destinations will be displayed.

When a broadcast or multicast address is given as destination, there may be multiple responses printed for each packet sent, one for each group member. Each returned response is displayed with the source address of the responder.

You can specify the size of the ping (number of data bytes in the ICMP message, excluding the ICMP header), value of the data, time-to-live (TTL) value, rate of pinging, and TOS bits to set. You can also specify the source IP address. If you do not specify the source IP address, the device uses its local address on the outgoing interface to the specified destination. If you are validating connectivity from any of the device's other interfaces to the destination, enter the IP address for that interface as the source address.

Only the destination parameter is required; all other parameters are optional. By default the size is 56 bytes, the TTL is 64, the rate is 1 ping per second, and the TOS setting is 0. The first 4 bytes of the ICMP data are used for a timestamp. By default the remaining data is a series of bytes with values that are incremented by 1, starting at X'04', and rolling over from X'FF' to X'00' (for example, X'04 05 06 07 . . . FC FD FE FF 00 01 02 03 . . .'). These values are incremented only when the default is used; if the data byte value is specified, all of the ICMP data (except for the first 4 bytes) is set to that value and that value is not incremented. For example, if you set the data byte value to X'FF', the ICMP data is a series of bytes with the value X'FF FF FF . . .'.

Example:

```
* ping
Destination IP address [0.0.0.0]? 192.9.200.1
Source IP address [192.9.200.77]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
Ping TOS (00-FF) [0]? e0
Ping data byte value (00-FF) [ ]?
PING 192.9.200.77-> 192.9.200.1:56 data bytes,ttl=64,every 1 sec.
56 data bytes from 192.9.200.1:icmp_seq=0.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=1.ttl=255.time=0.ms
56 data bytes from 192.9.200.1:icmp_seq=2.ttl=255.time=0.ms


----192.9.200.1 PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max=0/0/0 ms
```

Reload

Use the **reload** command to reboot the device by loading in a new copy of the device software. When you use this command from a remote console, you install a new software load without going to the device. This command executes the same functions as pressing the reset button except that the device will not dump (if so configured). Before the reload takes effect, you are prompted to confirm the reload. You are also prompted if you have not saved the configuration changes.

Syntax:

reload

Example:

```
* reload
Are you sure you want to reload the gateway (Yes or No)?
```

Status

Use the **status** command to display information about all device processes. By entering the PID after the **status** command, you can look at the status of only the desired process. The following example shows the total status display.

Syntax:

status *pid*

Example:

```
* status
Pid  Name      Status TTY  Comments
1    COpCon    IDL    TTY0
2    Monitr    IDL     --
3    Tasker    RDY     --
4    MOSDBG    DET     --
5    CGWCon    IOW     --
6    Config    IOW     --
7    ELSCon    DET     --
8    ROpCon    IOW    TTY1
9    ROpCon    RDY    TTY2
10   WEBCon    IDL    --
```

Pid Specifies the PID. This is the process to talk to from OPCON, or it can be an argument to the STATUS command to request status information about a specific process.

Name Specifies the process name. It usually corresponds to the name of the program that is running in the process.

Status

Specifies one of the following:

IDL Specifies that the process is idle and waiting for completion of some external event, such as asynchronous I/O.

RDY Specifies that the process is ready to run and is waiting to use the CPU.

IOW Specifies that the process is waiting for synchronous I/O, usually its expected standard input, to complete.

DET Specifies that the process has output ready to be displayed and it is either waiting to be attached to a display console or waiting to have its output diverted to a specified console.

FZN Specifies that the process is frozen due to an error. This usually means the process is trying to use a device which is faulty or incorrectly configured.

TTY*n* Specifies the output terminal, if any, to which the process is currently connected.

TTY0 Local console

TTY1 or TTY2
Telnet consoles.

Sink Process has been flushed.

Two dashes (--)
Process has been halted.

Comments

Specifies the user's login IP address provided during login when a user is logged in using Telnet (ROpCon).

Talk

You can use the **configuration**, **console**, or **event** comands to connect to other processes, such as CONFIG, GWCON, or MONITR, or use the **talk** command. After connecting to a new process, you can send specific commands to and receive output from that process. You cannot talk to the TASKER or OPCON processes.

To obtain the PID, use the OPCON **status** command. Once you are connected to the second-level process, such as CONFIG, use the intercept character, **Ctrl-P**, to return to the * prompt.

Syntax:

talk *pid*

Example:

```
* talk 5

CGW Operator Console

+
```

When using third-level processes, such as `SNMP Config>` or `SNMP>`, use the **exit** command to return to the second level.

Telnet

Use the **telnet** command to remotely attach to another device or to a remote host. The only optional parameter is the terminal type that you want to emulate.

You can use the **telnet** command with IPv4 or with IPv6 addresses.

A device has a maximum of five Telnet sessions: two servers (inbound to the device), and three clients (outbound from the device).

Note: To use Telnet in a pure bridging environment, enable Host Services.

Syntax:

telnet *ip-address terminal-type*

Example 1: `telnet 128.185.10.30` or **`telnet 128.185.10.30 23`** or **`telnet 128.185.10.30 vt100`**

```
Trying 128.185.10.30  ...
Connected to 128.185.10.30
Escape character is '^]'
```

Example 2: `telnet 1:9::10`

```
Trying 1:9::10  ...
Connected to 1:9::10
Escape character is '^]'
```

When telneting to a non-existent IP address, the device displays:

```
Trying 128.185.10.30  ...
```

To enter the Telnet command mode, type the escape character-sequence, which is **Ctrl-]**, at any prompt.

```
telnet>
```

If you Telnet into a device,

- Press ← **Backspace** to delete the last character typed on the command line.

  Note: When using a VT100 terminal, do not press ← **Backspace** because it inserts invisible characters. Press **Delete** to delete the last character.
- Press **Ctrl-U** at the `telnet>` prompt to delete the whole command line entry so that you can reenter a command.

The Telnet command mode consists of the following subcommands:

close Close current connection

display
Display operating parameters

mode Try to enter line-by-line or character-at-a-time mode

open Connect to a site

quit Exit Telnet

send Transmit special characters (send ? for more)

set Set operating parameters (set ? for more)

status Print status information

toggle Toggle operating parameters (toggle ? for more)

z Suspend Telnet

? Print help information

The **status** and **send** subcommands have one of two responses depending on whether or not the user is connected to another host. For example:

Connected to a host:

```
   telnet>    status
Connected to 128.185.10.30    Operating in character-at-a-time mode.    Escape character is ^].

   telnet>    send ayt
```

Note: The send command currently supports only ayt.

Not connected to a host:

```
   telnet>    status
   Need to be connected first.

   telnet>    send ayt

   Need to be connected first.
```

Use the **close** subcommand to close a connection to a remote host and terminate the Telnet session. Use the **quit** subcommand to exit the **telnet** command mode, close a connection, and terminate a Telnet session.

```
telnet>    close
```

or

```
telnet>    quit

logout
*
```

Chapter 7. The CONFIG Process (CONFIG - Talk 6) and Commands

This chapter describes the CONFIG process configuration and operational commands. It includes the following sections:

What is CONFIG?

The Configuration process (CONFIG) is a second-level process of the device user interface. Using CONFIG commands, you can:

- Set or change various configuration parameters
- Enter the Boot CONFIG command mode
- List or update configuration information
- Enable or disable console login
- Communicate with third-level processes, including protocol environments

Note: Refer to the chapter "Migrating to a New Code Level" in *8371 Networking Multilayer Ethernet Switch Installation and Planning Guide* for information about migrating to a new code level.

CONFIG lets you display or change the configuration information stored in the device's nonvolatile configuration memory. Changes to system and protocol parameters do not take effect until you reload the device software. (For more information, refer to the OPCON **reload** command in "What is the OPCON Process?" on page 43).

Note: You must enter the **write** command to save the changes in the device's flash memory.

The CONFIG command interface is made up of levels that are called modes. Each mode has its own prompt. For example, the prompt for the SNMP protocol is `SNMP config>`.

If you want to know the process and mode you are communicating with, press **Enter** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access and exit the various levels in CONFIG. See Table 11 on page 58 for a list of the commands you can issue from the CONFIG process.

Automatic Configuration

When the switch is booted, the following interfaces are allocated:

Table 10. Interfaces Added at Boot Time

Slot	Port	Device Type	Interface Number
0	1-16	10/100MB Ethernet	0-15

Table 10. Interfaces Added at Boot Time (continued)

Slot	Port	Device Type	Interface Number
1	1-8	10/100MB Ethernet	16-23
2	1-8	10/100MB Ethernet	24-31
1	1-2	ATM*	36-37
2	1-2	ATM*	38-39
3	5-29	LEC	40-63

Note: * Only 2 ATM ports are supported at one time. You can have 4 independent configurations of ATM ports, but only 2 are active at any one time.

When a feature card is hot-plugged into the switch, interface numbers are assigned from the above table. Feature cards can be added and removed to and from the feature card slots. However, the card being swapped must have been present at boot time, and only the same type of card may be swapped with the one being removed.

Dynamic Activation of a LEC

When a LEC is activated, the LEC must be associated with an ATM interface. The following default configuration values are associated with the LEC**:

ELAN Name ELAN1

ESI Set to MAC address stored in flash memory for this interface value

LES ATM Address set to use autoconfig via the LECS

ATM Interface 36

ELAN Type Ethernet

Bridging Enabled

Selector 2

Note: **These values guarantee that the box comes up with a known configuration. However, attempting to configure a LEC using all default values will probably fail. You need to provide network-specific information when configuring the LEC. See “Chapter 20. Configuring and Monitoring LAN Emulation Clients” on page 207 for LEC configuration detail.

Configuring User Access

The device configuration process allows for a maximum of 50 user names, passwords, and levels of permission. Each user needs to be assigned a password and level of permission. There are three levels of permission: *Administration, Operation,* and *Monitoring*.

Technical Support Access

If you are the system administrator, when you add a new user for the first time, you are asked if you want to add Technical Support access. If you answer yes, Technical Support is granted the same access privileges that you have as system administrator.

The password for this account is automatically selected by the software and is known by your service representative. This password can be changed using the **change user** command; however, if you do change the password, customer service cannot provide remote support. For additional information on the use of the **change user** command, see “Change” on page 60.

Resetting Interfaces

Occasionally, you might need to change the configuration of a network interface along with its bridging and routing protocols without restarting the device. The **reset** command allows you to disable a network interface and then enable it using new interface, bridging and routing configuration parameters.

The interface, protocols and features configuration parameters are changed using the CONFIG process (talk 6) commands. The talk 6 commands affect the contents of the configuration memory. The configuration changes are activated by issuing the GWCON process (talk 5) **reset** command.

To reset an interface:

1. Access the CONFIG process (talk 6).
2. Use the **net** command and other commands to change configuration parameters.
3. Use the **protocol** and **feature** commands to change the interface-based configuration parameters.
4. Exit the CONFIG process by pressing **Ctrl-P**.
5. Access the GWCON process (talk 5).
6. Use the **reset** command to reset the interface and the protocols and features on the interface.

Example:

```
* configuration
Config> net 0
ATM User Configuration
ATM Config> le-client
ATM LAN Emulation Clients Configuration
LE Client config> config 6

. . . change ATM LAN Emulation Client parameters . . .

Ethernet Forum Compliant LEC Config> exit
LE Client config> exit
ATM Config> exit
```

Note: When using the configuration program, do the following to make configuration changes to existing interfaces:

1. Make the configuration changes for the interface on the device
2. Enter the **reset** command to reset interface, protocol and feature parameters
3. Retrieve the configuration using the configuration program
4. Save the retrieved configuration into the configuration program database

Entering and Exiting CONFIG

To enter the CONFIG process from OPCON and obtain the CONFIG prompt, enter the **configuration** command. Alternatively, you can enter the OPCON **talk** command and the PID for CONFIG. The PID for CONFIG is 6.

```
* configuration
```

or

```
* talk 6
```

The console displays the CONFIG prompt (`Config>`). If the prompt does not appear, press the **Enter** key again.

To exit CONFIG and return to the OPCON prompt (*), enter the intercept character. (The default is **Ctrl-P** .)

CONFIG Commands

This section describes each of the CONFIG commands. Each command includes a description, syntax requirements, and an example. The CONFIG commands are summarized in Table 11.

After accessing the CONFIG environment, enter the configuration commands at the `Config>` prompt.

Table 11. CONFIG Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a user to the device.
Boot	Enters Boot CONFIG command mode.
Change	Changes a user’s password or a user’s parameter values associated with this interface. Also changes a slot/port of an interface.
Clear	Clears configuration information. Forces a re-boot for re-autoconfig. See Table 6 on page 31.
Disable	Disables command completion, login from a remote console, system memory dumping and rebooting, or a specified interface.
Enable	Enables command completion, login from a remote console, system memory dumping and rebooting, or enables a specified interface.
Event	Enters the Event Logging System configuration environment.
Feature	Provides access to configuration commands for independent device features outside the usual protocol and network interface configuration processes.
List	Displays system parameters, hardware configuration, a complete user list.
Network	Enters the configuration environment of the specified network.
Patch	Modifies the device’s global configuration.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Set	Sets system-wide parameters for buffers, host name, inactivity timer, packet size, prompt level, number of spare interfaces, dump parameters, location, and contact person.
Time	Keeps track of system time and displays it on the console.
Unpatch	Restores patch variables to default values.

Add

Use the **add** command to add user-access.

Syntax:

add user . . .

user *user_name*

Gives a user access to the device. You can authorize up to 50 users to access the device. Each *user_name* is eight characters and is case-sensitive.

When the first user is added, console login is automatically enabled. Each user added must be assigned one of the permission levels defined in the table below.

When users are added, set login authentication to local. Otherwise a remote server must be used.

Table 12. Access Permission

Permission Level	Description
Administrator (A)	Displays configuration and user information, adds/modifies/deletes configuration and user information. The Administrator can access any device function.
Operator (O)	Views device configuration, views statistics, runs potentially disruptive tests, dynamically changes device operation, and restarts the device. Operators cannot modify the permanent device configuration. All actions can be undone with a system restart.
Monitor (M)	Views device configuration and statistics but cannot modify or disrupt the operation of the device.
Tech Support	Allows your service representative to gain access to the device if a password is forgotten. Cannot be assigned to users.

Note: To add a user, you must have administrative permission. You do not have to reinitialize the switch after adding a user.

Example:

```
add user John
Enter password:
Enter password again:
Enter permission (A)dmin, (O)perations, (M)onitor [A]?
Do you want to add Technical Support access? (Yes or [No]):
```

Enter password

Specifies the access password for the user. Limited to 80 alphanumeric characters and is case-sensitive.

Enter password again

Confirms the access password for the user.

Enter permission

Specifies the permission level for the user: A, O, or M.

Boot

Use the **boot** command to enter the Boot CONFIG command environment. For Boot CONFIG information, see “Chapter 8. Using BOOT Config to Perform Change Management” on page 75.

Syntax:

boot

Change

Use the **change** command to change your own password, or change user information.

Syntax:

change user

user Modifies the user information that was previously configured with the **add user** command.

Note: To change a user, you must have administrative permission.

Example:

```
change user
User name: []
Change password? (Yes or No)
Change permission? (Yes or [No])
```

Clear

Use the **clear** command to delete the device's configuration information from nonvolatile configuration memory.

Attention: Use this command only after calling your service representative.

Syntax:

clear

- all
- atm (Asynchronous Transfer Mode)
- boot
- device
- els (Event Logging System Information)
- hostname
- prompt
- snmp
- tcp/ip-host
- time (Time of day information)
- user

To clear a process from nonvolatile configuration memory, enter the **clear** command and the process name. To clear all information from configuration memory, except for device information, use the **clear all** command. To clear all information, including the device information, use the **clear all** command and then the **clear device** command.

The **clear user** command clears all user information except the device console login information. This is left as enabled (if it was configured as enabled) even though the default value is “disabled”.

Notes:

1. To clear user information, you must have administrative permission.
2. There may be other items in the list, depending upon what is included in the software load.

Example: `clear els`

```
You are about to clear all Event Logging configuration information
Are you sure you want to do this (Yes or No):
```

Note: The previous message appears for any parameter configuration you are clearing.

Delete

Use the **delete** command to remove a user. To use the **delete** command, you must have administrative permission.

Syntax:

delete user . . .

user *user_name*
Removes user access to the device for the specified user.

Disable

Use the **disable** command to disable command completion, login from a remote console, system memory dumping, rebooting, or a specified interface.

Syntax:

disable command-completion
console-login
dump-memory . . .
interface . . .
reboot-system . . .

command-completion

Use the **disable command-completion** command to disable the automatic command completion function. See “Command Completion” on page 19 for a discussion of the automatic command completion function.

console-login
Disables the user from being prompted for a user ID and password on the physical console. The default is disabled.

interface *interface#*
Causes the specified interface to be disabled after issuing the **reload** command. The default is enabled.

dump-memory
Disables the dumping of system memory to the installed hard disk when a serious error occurs.

reboot-system
Disables the rebooting of the system when a serious error occurs. This may be desirable if the network service personnel wish to troubleshoot the error on-line. System rebooting cannot be disabled unless memory dumping is also disabled. If you attempt to disable system rebooting while memory dumping is enabled, system rebooting is aborted and the following message is displayed:

```
System reboot not disabled:  memory dumping must be disabled first
```

Enable

Use the **enable** command to enable command completion, login from a remote console, system memory dumping, rebooting, or a specified interface.

Syntax:

enable
- command-completion
- console-login
- dump-memory . . .
- interface . . .
- reboot-system . . .

command-completion

Use the **enable command-completion** command to enable the automatic command completion function, which assists with the command syntax. See “Command Completion” on page 19 for a discussion of the automatic command completion function.

console-login
Enables the user to be prompted for a user ID and password on the physical console. This is useful for security situations. If you do not configure any administrative users and you enable this feature, the following message appears:

```
Warning: Console login is disabled until an
administrative user is added.
```

Attention: Before enabling console login, save the configuration with console login disabled. If login authentication is set to a remote server using Radius or Tacacs+ and the device is unable to reach the authentication server, then access to the device is denied. By disabling the console login, a lock-out situation is prevented.

dump-memory
Enables the dumping of system memory to the target device specified by the **set dump target** command (described on page on page 70) if a serious error occurs. This may be desirable so that the state of the unit at the time of the error can be preserved for troubleshooting later. The dump memory function cannot be enabled unless system rebooting is enabled. If you attempt to enable the dump memory function while system rebooting is disabled, the dump memory function is not enabled and the following message is displayed:

```
System memory dump function not enabled:  rebooting must be enabled first
```

If you configured system dumping to save the first 3 dump files and 3 dump files already exist, the system displays the following message when you enable dump memory:

```
*** System dump cannot be enabled until the    ***
*** existing dump files are deleted.           ***
```

Note: If the dump target is set to *Network*, only small dump summary files will exist on the local disk. The full dump files are sent to a remote host.

See the **set dump enable-mode** and **set dump save-mode** commands.

Example:

```
Config> enable dump

Current System Dump Status:
   System dump is currently disabled.
   Number of existing dump files:  0

Enable system memory dumping? [No]: Yes

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  0
```

Note: If you enter this command and a hard drive is not available, you will receive a message indicating that the drive is unavailable.

interface *interface#*

Causes the interface to be enabled after issuing the **reload** command.

modem-control [carrier-wait or ring-wait] [service1 or service2]

Sets up the device for login on the physical console, if the physical console is connected to the device through a modem. Before using this command, be sure to:

Set your modem for auto-answer.

Verify that the console baud rate is equal to the modem baud rate.

Verify that the cable connecting the modem to the device is configured correctly.

Turn echo off by using the ATE0 command.

Run in quiet mode by using the ATQ1 command.

Verify that any necessary jumpers are set. Refer to your device's *User's Guide* more information. The device automatically hangs up the modem when you log out. Also, if your modem becomes disconnected from the device while you are using it, the device logs you out.

Specify the service port for both the **enable modem-control carrier-wait** and the **enable modem-control ring-wait** commands. For devices with two service ports, also specify to which service port you connected the modem, either **service1** or **service2**. To enable *both* service ports, enable them separately.

Note: No console connection can be made with the device after enabling modem control unless you clear all configuration and restart the device.

You can tell the device to wait for the carrier-detect signal from the modem before sending Request to Send. This is the standard method of modem control.

You can tell the device to wait for the ring-indication signal before raising Request to Send or Data Terminal Ready. This is provided for countries requiring an earlier handshake.

Example:

```
Config> enable modem-control carrier-wait service1
```

reboot-system
Enables the rebooting of the system when a serious error occurs.

Event

Use the **event** command to enter the Event Logging System (ELS) environment so that you can define the messages that will appear on the console. Refer to "Chapter 12. Using the Event Logging System (ELS)" on page 99 for information about ELS.

Syntax:

event

Feature

Use the **feature** command to access configuration commands for specific device features outside of the protocol and network interface configuration processes.

Syntax:

feature [*feature#* or *feature-short-name*]

All IBM 8371 features have commands that are executed by:

- Accessing the configuration process to initially configure and enable the feature, as well as perform later configuration changes.
- Accessing the console process to monitor information about each feature, or make temporary configuration changes.

The procedure for accessing these processes is the same for all features. The following information describes the procedure.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access a feature's configuration prompt, enter the **feature** command followed by the feature number or short name. Table 13 lists available feature numbers and names.

Table 13. IBM 8371 Feature Numbers and Names

Feature Number	Feature Short Name	Accesses the following feature configuration process
6	QoS	Quality of Service
17	Self Learning IP	

Table 13. IBM 8371 Feature Numbers and Names (continued)

Feature Number	Feature Short Name	Accesses the following feature configuration process
18	RMON	

Once you access the configuration prompt for a feature, you can begin entering specific configuration commands for the feature. To return to the CONFIG prompt, enter the **exit** command at the feature's configuration prompt.

List

Use the **list** command to display configuration information for all network interfaces, or configuration information for the device.

Syntax:

list configuration
devices
named-profile
patches . . .
users . . .

configuration

Displays configuration information about the device.

Example: `list configuration`

```
Hostname: [none]
Maximum packet size: [autoconfigured]
Maximum number of global buffers: [autoconfigured]
Number of spare interfaces: 0
Console inactivity timer (minutes): 0
Physical console login: disabled
Command Completion: enabled
Contact person for this node: [none]
Location of this node: [none]

Configurable Protocols:
Num Name  Protocol
11  SNMP   Simple Network Management Protocol
23  ASRT   Adaptive Source Routing Transparent Enhanced Bridge
24  HST    TCP/IP Host Services
29  MPOA   Multi-Protocol Over ATM

Configurable Features:
Num Name  Feature
6   QOS    Quality of Service
17  Self   Self Learning IP
18  RMON   Remote Network Monitor

119168 bytes of configuration memory free
```

devices [*device* **or** *devicerange***]**

Displays the relationship between an interface number and the hardware interface. You can also use this command to check that a device was added correctly issuing the **add** command.

Example: `list devices`

```
Ifc 0     1-port 10/100 Ethernet            Slot: 0   Port: 1
Ifc 1     1-port 10/100 Ethernet            Slot: 0   Port: 2
Ifc 2     1-port 10/100 Ethernet            Slot: 0   Port: 3
Ifc 3     1-port 10/100 Ethernet            Slot: 0   Port: 4
Ifc 4     1-port 10/100 Ethernet            Slot: 0   Port: 5
Ifc 5     1-port 10/100 Ethernet            Slot: 0   Port: 6
Ifc 6     1-port 10/100 Ethernet            Slot: 0   Port: 7
Ifc 7     1-port 10/100 Ethernet            Slot: 0   Port: 8
Ifc 8     1-port 10/100 Ethernet            Slot: 0   Port: 9
```

```
Ifc 9     1-port 10/100 Ethernet            Slot: 0   Port: 10
Ifc 10    1-port 10/100 Ethernet            Slot: 0   Port: 11
Ifc 11    1-port 10/100 Ethernet            Slot: 0   Port: 12
Ifc 12    1-port 10/100 Ethernet            Slot: 0   Port: 13
Ifc 13    1-port 10/100 Ethernet            Slot: 0   Port: 14
Ifc 14    1-port 10/100 Ethernet            Slot: 0   Port: 15
Ifc 15    1-port 10/100 Ethernet            Slot: 0   Port: 16
Ifc 16    1-port 10/100 Ethernet            Slot: 1   Port: 1
Ifc 17    1-port 10/100 Ethernet            Slot: 1   Port: 2
Ifc 18    1-port 10/100 Ethernet            Slot: 1   Port: 3
Ifc 19    1-port 10/100 Ethernet            Slot: 1   Port: 4
Ifc 20    1-port 10/100 Ethernet            Slot: 1   Port: 5
Ifc 21    1-port 10/100 Ethernet            Slot: 1   Port: 6
Ifc 22    1-port 10/100 Ethernet            Slot: 1   Port: 7
Ifc 23    1-port 10/100 Ethernet            Slot: 1   Port: 8
Ifc 24    1-port 10/100 Ethernet            Slot: 2   Port: 1
Ifc 25    1-port 10/100 Ethernet            Slot: 2   Port: 2
Ifc 26    1-port 10/100 Ethernet            Slot: 2   Port: 3
Ifc 27    1-port 10/100 Ethernet            Slot: 2   Port: 4
Ifc 28    1-port 10/100 Ethernet            Slot: 2   Port: 5
Ifc 29    1-port 10/100 Ethernet            Slot: 2   Port: 6
Ifc 30    1-port 10/100 Ethernet            Slot: 2   Port: 7
Ifc 31    1-port 10/100 Ethernet            Slot: 2   Port: 8
Ifc 32    NULL Device                       Slot: 3   Port: 1
Ifc 33    NULL Device                       Slot: 3   Port: 2
Ifc 34    NULL Device                       Slot: 3   Port: 3
Ifc 35    NULL Device                       Slot: 3   Port: 4
Ifc 36    ATM                               Slot: 1   Port: 1
Ifc 37    ATM                               Slot: 1   Port: 2
Ifc 38    ATM                               Slot: 2   Port: 1
Ifc 39    ATM                               Slot: 2   Port: 2

Ifc 40    ATM Ethernet LAN Emulation
Ifc 41    ATM Ethernet LAN Emulation
Ifc 42    ATM Ethernet LAN Emulation
Ifc 43    ATM Ethernet LAN Emulation
Ifc 44    ATM Ethernet LAN Emulation
Ifc 45    ATM Ethernet LAN Emulation
Ifc 46    ATM Ethernet LAN Emulation
Ifc 47    ATM Ethernet LAN Emulation
Ifc 48    ATM Ethernet LAN Emulation
Ifc 49    ATM Ethernet LAN Emulation
Ifc 50    ATM Ethernet LAN Emulation
Ifc 51    ATM Ethernet LAN Emulation
Ifc 52    ATM Ethernet LAN Emulation
Ifc 53    ATM Ethernet LAN Emulation
Ifc 54    ATM Ethernet LAN Emulation
Ifc 55    ATM Ethernet LAN Emulation
Ifc 56    ATM Ethernet LAN Emulation
Ifc 57    ATM Ethernet LAN Emulation
Ifc 58    ATM Ethernet LAN Emulation
Ifc 59    ATM Ethernet LAN Emulation
Ifc 60    ATM Ethernet LAN Emulation
Ifc 61    ATM Ethernet LAN Emulation
Ifc 62    ATM Ethernet LAN Emulation
Ifc 63    ATM Ethernet LAN Emulation
Config>
```

patches

Displays the values of patch variables that have been entered using the **patch** command.

Example:

```
list patches
Patched variable            Value

mosheap-lowmark             20
```

users Displays the users configured to access the system.

Example:

```
list users
USER           PERMISSION
joe            operations
mary           administrative
peter          monitor
```

vpd Displays the hardware and software vital product data.

Network

Use the **network** command to enter the network interface configuration environment for supported networks. Enter the interface or network number as part of the command. (To obtain the interface number, use the CONFIG **list device** command.) The appropriate configuration prompt (for example, `TKR Config>`) will be displayed. See the network interface configuration chapters in this book for complete information on configuring your types of network interfaces.

Syntax:

network *interface#*

Notes:

1. If you change a user-configurable parameter, you may use the GWCON **reset interface** command, or you may **reload** the device for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).
2. Not all network interfaces are user-configurable. For interfaces that you cannot configure, you receive the message: `That network is not configurable.`

Patch

Use the **patch** command for modifying the device's global configuration. Patch variables are recorded in nonvolatile configuration memory and take effect immediately; you do not have to wait for the next restart of the device. This command should be used only for handling uncommon configurations. Anything that you commonly configure should still be handled by using the specific configuration commands. The following is a list of the current patch variables documented and supported for this release.

Syntax:

patch mosheap-lowmark

mosheap-lowmark *new value*

This parameter specifies the percentage of free MOS heap memory, at which the device notifies the operator that an out-of-memory error is imminent. This notification allows the operator to take action to free up MOS heap memory before the device receives an error and stops.

When the operator receives notification, the operator can reconfigure the device and then reboot, minimizing the outage to the network. Specifying 0 for this parameter suppresses this warning.

Valid Values: 0 to 100

Default Value: 10

Note: You must specify the complete name of the patch variable that you want to change. You cannot use an abbreviated syntax for the patch name.

Performance

Use the **performance** command at the `Config>` prompt to enter the configuration environment for performance. See "Chapter 14. Configuring and Monitoring Performance" on page 169 for more information.

performance

Protocol

Use the **protocol** command at the Config> prompt to enter the configuration environment for the protocol software installed in the device.

Syntax:

protocol [*prot#* or *prot_name*]

The **protocol** command followed by the desired protocol number *or* short name lets you enter a protocol's command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands specific to that protocol. To return to Config>, enter the **exit** command.

Notes:

1. To see the names and numbers of the protocols in your software load, at the Config> prompt, enter **list configuration**.
2. When you change a user-configurable parameter, you may be able to use the protocol's GWCON **reset** command, or you may have to restart the device for the change to take effect. To do so, enter the **reload** command at the OPCON prompt (*).

   The changes you make through CONFIG are kept in a configuration database in nonvolatile memory and are recalled when you restart the device.

Set

Use the **set** command to configure various system-wide parameters.

Syntax:

set
- contact-person . . .
- down-notify . . .
- dump enable-mode
- dump save-mode
- dump target
- global-buffers
- hostname
- inactivity-timer
- input-low-water
- location . . .
- packet-size
- prompt
- receive-buffers
- spare-interfaces

contact-person *sysContact*

Sets the name or identification of the contact person for this managed SNMP node. There is a limit of 80 characters for the *sysContact* name length.

This variable is for information purposes only and has no effect on device operation. It is useful for SNMP management identification of the system.

down-notify *interface# # of seconds*

Allows the user to specify the number of seconds before declaring an interface as being down. The normal maintenance packet interval is 3 seconds, and it takes four maintenance failures to declare the interface as down.

The **set down-notify** command is used primarily when tunneling LLC traffic over an IP network using OSPF. If an interface goes down, OSPF cannot detect it fast enough because of the length of time that it takes for an interface to be declared down. Therefore, LLC sessions would begin to timeout. You can set the down-notify timer to a lower value, allowing OSPF to sense that an interface is down quicker. This enables an alternate route to be chosen more quickly, which will prevent the LLC sessions from timing out.

Note: If the **set down-notify** command is executed on one end of a serial link, the same command must be performed at the other end of the link or the link may not come up and stay up.

Interface#

The number of the interface you are configuring.

# of seconds

The down notification time value that specifies the maximum time that will elapse before a down interface is marked as such. Large values will cause the device to ignore transient connection problems, and smaller values will cause the device to react more quickly. The range of values is 1 to 300 seconds and the default is 0, which sets the 3-second period. Setting the down notification time to 0 will restore the default time for that interface.

The **list devices** command will show the down notification time setting for any interface that has the default value overridden.

dump enable-mode

Specifies whether dumping is enabled following the next system dump. If you configure the save mode (see the **set dump save-mode** command) to save the first three dumps and the system has already created the third dump file, dumping is disabled regardless of your specification. At the time the system creates the third dump file, you will receive the following message:

```
Active Dump Detected.
Dump Compression in Progress, please be patient ...

*** System dumping is being DISABLED because dumping is ***
*** configured to save the 3 initial dumps, but 3       ***
*** dump files already exist.                           ***
```

Example:

```
Config> set dump enable-mode

Current System Dump Settings:
   Disable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Do you want to change system dump enable-mode to
re-enable System Dump following the next system dump ? (Yes, No): [No] Yes
```

```
Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  2
```

Default value: disable

Note: Dumping is enabled with the **enable dump-memory** command.

dump save-mode

Specifies whether to save the first three (initial) system dump files or the last three (most recent). See the **dump enable-mode** for a consideration for using recent mode as opposed to initial mode.

Example:

```
Config> set dump save-mode

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the last 3 (most recent) dump files.

Do you want to change system dump save-mode to
save the first (initial) dump files ? (Yes, No): [No] Yes

Current System Dump Settings:
   Re-enable System Dump following the next system dump.
   Save the first 3 (initial) dump files, then disable system dump.

Current System Dump Status:
   System dump is currently enabled.
   Number of existing dump files:  2
```

Default value: recent

dump target

Specifies the location where the system memory image information will be written. Valid targets are the local hard disk, if one is present, or a remote host on a LAN.

If the target is a network, then IP and TFTP parameters of both the local LAN interface and the remote host are required. An additional parameter determines whether the file will be sent by TFTP as compressed or uncompressed data.

Example:

```
Config>set dump target

Current System Dump Target Settings:

   Dump Target:  Local Hard Disk

Do you want to change the System Dump Target ? (Yes, No): [No] Yes
Enter Dump Target (D-Disk or N-Network): [D]? N
Setting Dump Target to "Network".
Set or Change settings for dumping to the Network ? (Yes, No): [No] Yes
Enter Local LAN Interface Type (E-Eth or T-Tkr): [E]? E
Enter Slot Number (1-2): [1]? 1
Enter Port Number (1-2): [1]? 1
Enter Local IP Address: [9.9.9.6]? 9.9.9.5
Enter Local Netmask: [255.255.255.0]?
Enter Remote IP Address: [9.9.9.1]? 9.9.9.11
Remote Path and File name:  /tmp/netdump
Enter Path and File name (32 chars max):  /tmp/dump_to_host
Enter File Compression Mode (C-Comp or U-Uncomp): [U]? C
Do you want to save your changes ? (Yes, No): [No] Yes

New System Dump Target Settings:

   Dump Target:  Remote Host on Network
   Local Interface Settings:
     Device Type:  Ethernet
```

```
    Slot Number:  1
    Port Number:  1
    IP address:  9.9.9.5
    Net Mask:  255.255.255.0
  Remote Host Settings:
    IP address:  9.9.9.11
    Remote Filename:  /tmp/dump_to_host
    Remote file will be compressed and "0.cmp", "1.cmp", or "2.cmp" will be
    appended to the end of the filename.
```

When the system dump file is sent by TFTP to the remote host, it will be written as multiple files, which must first be concatenated. For example, if the remote file was specified as /tmp/dump_to_host, and remote files are sent as compressed. The files written on the remote workstation are:

- dump_to_host0.cmp
- dump_to_host0.cm1

Depending on the total size of the dump, there may be additional files, named as:

- dump_to_host0.cm2
- dump_to_host0.cm3, and so forth.

In order to decompress and view the dump information, the files must be combined as follows into a single file (note that order is critical):

/tmp> **cat dump_to_host0.cmp dump_to_host0.cm1 dump_to_host0.cm2 dump_to_host0.cm3 > dump_to_host0_cat.cmp**

As a result, the combined file dump_to_host0_cat.cmp will contain a complete system memory dump image.

If the file was sent by TFTP as uncompressed, the file extensions are .unc, .un1, .un2, and .un3 instead of .cmp, .cm1, .cm2, and .cm3. The uncompressed files must also be concatenated to create a complete system memory dump image. For Example:

/tmp>**cat dump_to_host0.unc dump_to_host0.un1 dump_to_host0.un2 dump_to_host0.un3 > dump_to_host0_cat**

Note: The output file, dump_to_host0_cat. does not require a file extension because the file is not compressed.

global-buffers *max#*

Sets the maximum number of global packet buffers, which are the packet buffers used for locally originated packets. The default is to autoconfigure for the maximum number of buffers (up to 1000). To restore the default, set the value to 0. To display the setting for global-buffers, use the **list configuration** command.

hostname *name*

Adds or changes the device name. The device name is for identification only; it does not affect any device addresses. The *name* must be less than 78 characters and is case sensitive.

inactivity-timer *#_of_min*

Changes the setting of the Inactivity Timer. The Inactivity Timer logs out a user if the remote or physical console is inactive for the period of time specified in this command. This command affects only consoles that require login. The default setting of 0 turns the inactivity timer off, indicating that no logoff is performed, no matter how long a console remains inactive.

input-low-water *interface# low_ #_of_receive_buffers*

Allows you to configure the value of the low number of receive buffers, or packets, on a per-interface basis, thus overriding the default values.

The memory allocation strategy changes to conserve buffers when the number of free buffers is equal to or less than the low or low-water mark value. When a packet is received, and the current value of the interface is less than the low water value, then that packet is eligible for flow control (dropping).

The range of values is 1 to 255. The default is both platform and device specific. Setting the value to 0 restores the autoconfigured default.

Interface# is the number of the interface you are configuring.
Low_#_of_receive_buffers is the low water value.

Lowering the value will make it less likely that packets from this interface will be dropped when sent on congested networks. However, lowering the value may negatively affect performance if it drops packets to the extent that the receive queue is frequently empty. Raising the value has the opposite effect.

Type the **QUEUE** or **BUFFER** command at the GWCON prompt (**+**) to show the low setting.

location *sysLocation*

Sets the physical location of an SNMP node. There is a limit of 80 characters for the *sysLocation* name length. This variable is for information purposes only and has no effect on device operation. It is useful for SNMP management identification of the system.

packet-size *max_packet_size_in_bytes*

Establishes or changes the maximum size for global buffers and receive buffers. If you specify a value of 0 as the maximum packet size, the size of receive buffers for an interface is based on that interface's configured packet size and the packet size of global buffers are autoconfigured. If you specify a non-zero value, the configured value is used as the global buffer packet size and any interfaces that have a configured packet size that is larger than the maximum packet size will use the maximum packet size for their receive buffers. A value of 0 (for autoconfigure) is the default.

Attention: Use this command only under direct instructions from your service representative. ***Never*** use it to reduce packet size – ***only*** to increase it.

prompt *user-defined-name*

Adds a user-defined name as a prefix to all operator prompts, replacing the hostname.

The user-defined-name can be any combination of characters, numbers, and spaces up to 80 characters. Special characters may be used to request additional functions as described in Table 14 on page 73.

Example:

```
set prompt
What is the new MOS prompt [y]? AnyHost 99
AnyHost 99 Config>
```

Table 14. Additional Functions Provided by the Set Prompt Level Command

Special Characters	Function Provided by the Set Prompt Level Command

$n	Displays the hostname. This is useful when you want the hostname included in the prompt. For example:
	`Config> set prompt`
	`What is the new MOS prompt [y]? $n`
	`hostname:: Config>`

$t	Displays the time. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $t`
	`02:51:08[GMT-300] Config>`

$d	Displays the current date-month-year. For example:
	`Config> set prompt.`
	`What is the new MOS prompt [y]? $d`
	`26-Feb-1997 Config>`

$v	Displays the software VPD information in the following format: `program-product-name Feature xxxx Vx.x PTFx RPQx`
$e	Erases one character *after* this combination within the user-defined prompt.
$h	Erases one character *before* this combination within the user-defined prompt.
$_	Adds a carriage return to the user-defined prompt.
$$	Displays the $.

Note: You can combine these commands. For example:
`Config> set prompt`
`What is the new MOS prompt [y]? $n::$d`
`hostname::26-Feb-1997 Config>`	

receive-buffers *interface# max#*

Adjusts the number of private receive buffers for most interfaces.

The range is 5 to 1000.

Time

Use the **time** command to set the IBM 8371 system clock and date, and to display the values on the user console. These values can then be used to time-stamp ELS messages.

Syntax:

time host . . .
list
offset
set . . .
sync . . .

host *IP_address*

Sets the IP address of the RFC 868-compliant host that will be used as the

time source. This is the address of a host which will respond to an empty datagram on UDP port 37 with a datagram containing the current time.

list Displays all configured time-related parameters. This includes the current time (if set) and the source of the time (operator or IP address from which time was last received).

```
Example: time list
05:20:27  Wednesday December 7, 1994
Set by: operator
Time Host:  131.210.4.1
Sync Interval: 10 seconds GMT
Offset:  -300 minutes
```

offset *minutes*

Defines the time zone, in minutes, offset from GMT (Greenwich Mean Time). Note that values west of GMT are negative. For example, EST is 5 hours earlier than GMT, so the command would be **time offset -300**.

Valid values: -720 to 720

Default value: 0

set <*year month date hour minute second***>**

Prompts you to set the current time. If you do not specify the entire time in the command, you are prompted for the remaining values. You can change the date as shown in the following example.

```
Example: time set
year [1996] 1997
month [12]?
date [6]? 7
hour [11]? 12
minute [3]?
second [2]?
```

sync *seconds*

Sets the period, in seconds, at which the device will poll the time host for the current time.

Unpatch

Use the **unpatch** command to restore the values of the patch variables entered with the **patch** command to their default values. See the **patch** command in “Patch” on page 67 for details.

Syntax:

unpatch *variable_name*

Note: You ***must*** specify the complete name of the patch variable to be restored.

Update

Use the **update** command to update the configuration memory when you receive a new software load.

Syntax:

update version-of-SRAM

Follow the instructions on the release notice sent with the software. The **update** command is the last command that you enter when loading new software. After you enter this command, the console displays a message indicating configuration memory is being updated.

Chapter 8. Using BOOT Config to Perform Change Management

This chapter describes how to use the Boot/Dump Configuration process. This chapter includes the following sections:

- "Understanding Change Management"
- "Using the Trivial File Transfer Protocol (TFTP)"

Understanding Change Management

Change management is the handling of software and configuration data for an IBM 8371. This involves:

1. Moving code and configuration data to and from the IBM 8371
2. Moving code and configuration data on the IBM 8371 system FLASH.
3. Selecting and activating specific combinations of software and configuration.

The change management functions are available by entering the **boot** command at the `Boot config>` prompt (talk 6), or the firmware should the box be in a condition where the hard drive or compact flash does not contain viable software (that is, you cannot access talk 6).

The IBM 8371 code and configuration data storage resource is divided into areas called "system banks" (banks for short), each containing a single version of the operational code and any other files pertinent to that release of the code. Up to four configuration files are associated with each bank's software.

The general change management model of the IBM 8371 is to introduce new code and/or configuration data to the system while the system runs at its present level and then activate the changed code or configuration data set later. If for some reason the new code or configuration does not function as expected, you have the ability to revert to the previous version of the configuration.

Using the Trivial File Transfer Protocol (TFTP)

TFTP is a file transfer protocol that runs over the Internet UDP protocol. This implementation provides multiple, simultaneous TFTP file transfers between an IBM 8371's non-volatile configuration memory, image bank, and remote hosts.

TFTP allows you to:

- Get a configuration file from a server to an IBM 8371
- Put a configuration file from an IBM 8371 to a server

TFTP transfers involve a *client* node and a *server* node. The client node generates a TFTP Get or Put request onto the network. The IBM 8371 acts as a client node by generating TFTP requests from the IBM 8371 console using the `Boot config>` process **tftp** command.

The client can transfer a copy of a configuration file or image file stored in the image bank of a server.

Using BOOT Config

The server is any device (for example, a personal computer or workstation) that receives and services the TFTP requests. Use the ELS subsystem TFTP message log to view the transfer in progress.

Chapter 9. Configuring Change Management

This chapter describe the Change management configuration commands. It includes the following sections:

- "Accessing the Change Management Configuration Environment"
- "Change Management Configuration Commands"

Accessing the Change Management Configuration Environment

To enter the change management configuration command environment, use the CONFIG **boot** command. When the device's software is initially loaded, it is running in the OPCON process, signified by the * prompt. From the * prompt:

1. Enter **talk 6**.
2. At the `Config>` prompt, type **boot**.

To return to the CONFIG process, type **exit**.

Change Management Configuration Commands

This section describes the Change Management Configuration commands. Each command includes a description, syntax requirements, and an example. Table 15 summarizes the Change Management Configuration commands.

After accessing the Change Management Configuration environment, enter the configuration commands at the `Boot config>` prompt.

Table 15. Change Management Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds an optional description to a configuration file.
Copy	Copies boot files and configuration files to or from banks.
Describe	Displays information about the stored loadfile images.
Erase	Erases a stored image or a configuration file.
List	Displays information about configuration files and scheduled load information.
Lock	Prevents the device from overwriting the selected configuration with any other configuration.
Set	Selects code bank and configuration to be used.
Tftp	Initiates TFTP file transfers between the IBM 8371 and remote servers.
Unlock	Removes the lock from a configuration allowing the configuration to be updated by the device.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Add

Use the **add** command to add an optional description to a configuration file.

Syntax:

add configuration *file description*

load *image description*

Example: Boot config> **add**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:30 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Select the source bank:  (A, B): [A]
Select the source configuration:  (1, 2): [1] 1
Enter the description of the file: () New config for today

Attempting to set description for bank A configuration 1.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:58 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Copy

Use the **copy** command to copy configuration files and load images to and from banks.

Syntax:

copy configuration *file*

load *image*

Example: Boot config>**copy load**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Select the source bank:  (A, B): [A] b
Select the destination bank:  (A, B): [B] a
Copy SW load image from: bank B
```

```
                    to: bank A.

Operation completed successfully.
```

Example: Boot config>**copy configuration**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - CORRUPT        |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       |                                 | 01 Jan 1970 00:14 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A]
Select the source configuration:  (1, 2): [1]
Select the destination bank:  (A, B): [B]

Select the destination configuration:  (1, 2): [1]
Copy SW configuration from: bank A, configuration 1
                         to: bank B, configuration 1.

Operation completed successfully.
```

If the copy fails you may receive one of the following messages:

Error: Active bank cannot be overwritten or erased.
You attempted to copy a configuration into the bank currently in use by the IBM 8371.

Error: File copy failed.
This condition occurs when the copy operation fails for reasons other than copying to the active configuration. The most common cause is specifying the same source and destination configurations. When you list (see “List” on page 81) the configurations, CORRUPT appears next to the bank that is damaged.

Describe

Use the **describe** command to display information about a stored image.

Syntax: describe

Example: Boot config>**describe**

```
+-------------------------+-------------------------+
|         BANK A          |         BANK B          |
| Product ID -   8371     | Product ID -   8371     |
| Version   4 Release   0 | Version   4 Release   0 |
| Mod       0 PTF       0 | Mod       0 PTF       0 |
| Feat.  2822 RPQ       0 | Feat.  2822 RPQ       0 |
| Date        31 Dec 1996 | Date        31 Dec 1996 |
+-------------------------+-------------------------+
```

Erase

Use the **erase** command to erase a stored image or a configuration file.

Syntax:

erase configuration [file]

load [image]

config or load

Erases a configuration file or a load image. Enter the config number to be erased after the **erase** command.

Example: Boot config>**erase load**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - CORRUPT        |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

 Select the bank to erase:  (A, B): [A] a

Erase SW load image from bank A.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Example: Boot config>**erase configuration**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A] A
Select the configuration to erase:  (1, 2,): [1]2
Erase SW configuration file from bank A, configuration 2.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:14 |
| CONFIG 2 - NONE        | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Notice that the list command displays **NONE** by bank A, config 2.

If the erasure fails, a message indicating the failure appears on the console with the banks that failed.

List

Use the **list** command to display information about which load images and configuration files are available and active. This command may also be used to display boot options and scheduled load information.

Syntax:

list

Example: Boot config>**list**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - AVAIL          |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 01:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-----------------+
  * - Last Used Config      L - Config File is Locked

 Time Activated Load Schedule Information...

The device is scheduled to reload as follows.

Date:  June 26, 1997
Time:  16:30
The load modules are in bank A.
The configuration is CONFIG 1 in bank A.
Boot config>
```

The possible file status descriptors are:

ACTIVE
: The file is currently loaded and is running on the 8371

AVAIL This is a valid file that can be made ACTIVE.

CORRUPT
: The file was damaged or not loaded into the 8371 completely. The file must be replaced.

LOCAL
: The file will be used only on the next reload or reset. After the file is used, it will be placed in AVAIL state.

PENDING
: This file will be loaded on the next reload, reset, or power-up of the 8371.

Lock

Use the **lock** command to prevent the device from overwriting the selected configuration with any other configuration.

Syntax:

lock

Example: Boot config>**lock**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:26 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked

Select the source bank:  (A, B): [A]

Select the source configuration:  (1, 2): [1] 2
Attempting to lock bank A and configuration 2.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   L   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Note: Note that bank A config 4 is marked with an “L.”

Set

Use the **set** command to select the code bank, the configuration to use, and the duration of use. The valid durations are:

once The configuration is active for the next boot only.

always
The configuration is active for all subsequent boots until changed again.

Syntax:

set

Example: Boot config>**set**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A] b
Select the source configuration:  (1, 2, 3, 4): [1] 2
Select the duration to use for booting:  (once, always): [always]
Set SW to boot using bank B and configuration 2, always.

Operation completed successfully.


Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970       |
```

```
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - ACTIVE      |                                | 01 Jan 1970 00:01 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

TFTP

Use the **tftp** command to initiate TFTP file transfers between the 8371 and remote servers.

Syntax:

tftp get config

load

tftp put config

load

Example: Boot config>**tftp get load**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs           | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs           | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                | 01 Jan 1970 00:01 |
+------------------------+--------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Specify the server IP address (dotted decimal): : [1.2.3.4] 192.9.200.1
Specify the remote file name: : (/u/bin) /usr/8371load/8371.img
Select the destination bank:  (A, B, F): [A] a
  TFTP SW load image
  get:   /usr/8371load/8371.img
  from:  192.9.200.1
  to:    bank A.

Operation completed successfully.
```

Notes:
When putting files to a server:

1. Make sure that the files on the target server have the appropriate permissions that would allow anyone to write to those files. If not, the put operation will fail.
2. You must be aware of the files you are putting to the target server.

Unlock

Use the **unlock** command to allow the device to overwrite the selected configuration that was previously locked.

Syntax:

unlock

Example: Boot config>**unlock**

```
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 | 01 Jan 1970 01:03 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:13 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970 00:01 |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL   L   |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked


Select the source bank:  (A, B): [A] B
Select the source configuration:  (1, 2): [1] 2
Attempting to unlock bank B and configuration 2.

Operation completed successfully.
Boot config>list
+------ BankA -----------+--------- Description ----------+------ Date -------+
| IMAGE - NONE           |                                 |                   |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:01 |
| CONFIG 2 - AVAIL   *   | test config for pubs            | 01 Jan 1970 01:13 |
+------ BankB -----------+--------- Description ----------+------ Date -------+
| IMAGE - ACTIVE         |                                 | 01 Jan 1970       |
| CONFIG 1 - AVAIL       | test config for pubs            | 01 Jan 1970 00:54 |
| CONFIG 2 - AVAIL       |                                 | 01 Jan 1970 00:01 |
+------------------------+---------------------------------+-------------------+
  * - Last Used Config      L - Config File is Locked
```

Note: Note that bank A config 4 is no longer marked with an “L.”

Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands

This chapter describes the GWCON process and includes the following sections:

What is GWCON?

The Gateway Console (monitoring) process, GWCON (also referred to as CGWCON), is a second-level process of the device user interface.

Using GWCON commands, you can:

- List the protocols and interfaces currently configured in the device.
- Display memory and network statistics.
- Set current Event Logging System (ELS) parameters.
- Test a specified network interface.
- Communicate with third-level processes, including protocol environments.
- Enable and disable interfaces.

The GWCON command interface is made up of levels called modes. Each mode has its own prompt. For example, the prompt for the SNMP protocol is `SNMP>`.

If you want to know the process and mode you are communicating with, press **enter** to display the prompt. Some commands in this chapter, such as the **network** and **protocol** commands, allow you to access the various modes in GWCON.

Entering and Exiting GWCON

To enter GWCON from OPCON (*), choose one of the following methods:

1. Enter the OPCON **console** command:

   ```
   * console
   ```

2. At the OPCON prompt, enter the **status** command to find the PID of GWCON. (See page 9 for a sample output of the **status** command.)

   ```
   * status
   ```

   Then, enter the **talk** command followed by the PID number for GWCON:

   ```
   * talk 5
   ```

The console displays the GWCON prompt (+). If the prompt does not appear, press **enter**. Now you can enter GWCON commands.

To return to OPCON, enter the OPCON intercept character. (The default is **Ctrl-P**.)

GWCON Commands

This section contains the GWCON commands. Each command includes a description, syntax requirements, and an example. The GWCON commands are summarized in Table 16.

To use the GWCON commands, access the GWCON process by entering **talk 5** and enter the GWCON commands at the (+) prompt.

Table 16. GWCON Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Buffer	Displays information about packet buffers assigned to each interface.
Clear	Clears network statistics.
Configuration	Lists status of the current protocols and interfaces.
Disable	Takes the specified interface off line.
Error	Displays error counts.
Event	Enters the Event Logging System environment.
Feature	Provides access to console commands for independent device features outside the usual protocol and network interface console processes.
Interface	Displays network hardware statistics or statistics for the specified interface.
Memory	Displays memory, buffer, and packet data.
Network	Enters the console environment of the specified network.
Performance	Provides a snapshot of the main processor utilization statistics.
Protocol	Enters the command environment of the specified protocol.
Queue	Displays buffer statistics for a specified interface.
Reset	Disables the specified interface and then re-enables it using new interface, protocol and feature configuration parameters.
Statistics	Displays statistics for a specified interface.
Test	Enables a disabled interface or tests the specified interface.
Uptime	Displays time statistics for the device.

Buffer

Use the **buffer** command to display information about packet buffers assigned to each interface.

Note: Each buffer on a device is the same size and is dynamically built. Buffers vary in size from one device to another.

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

buffer [*network#* or]

Example:

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Buffers:

Req Number of buffers requested.

Alloc Number of buffers allocated.

Low Low water mark (flow control).

Curr Current number of buffers on this device. The value will be 0 if the device is disabled. When a packet is received, if the value of *Curr* is below *Low*, then the packet is eligible for flow control. (See the **queue** command for conditions.)

Buffer Sizes:

Hdr Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Data Maximum data link layer packet size.

Trail Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer.

Bytes Alloc
Amount of buffer memory for this device. This value is determined by multiplying the values of *Alloc x Total*.

Clear

Use the **clear** command to delete statistical information about one or all of the device's network interfaces. This command is useful when tracking changes in large counters. Using this command does not save space or speed up the device.

Enter the interface (or net) number as part of the command. To get the interface number, use the GWCON **configuration** command.

Syntax:

clear *interface#*

Configuration

Use the **configuration** command to display information about the protocols and network interfaces. The output is displayed in three sections, the first section lists the device identification, software version, boot ROM version, and the state of the auto-boot switch. The second and third sections list the protocol and interface information.

Syntax:

configuration

Example:

- The first line gives the product name.
- The second line lists the program/product number, Feature Number, Version, Release, PTF and RPQ information.

- The remaining lines list the configured protocols, followed by the configured features.

The following information is displayed for protocols:

Num Number that is associated with the protocol.

Name Abbreviated name of the protocol.

Protocol
Full name of the protocol.

The following information is displayed for features:

Num Number associated with the feature.

Name Abbreviated name of the feature.

Feature
Full name of the feature.

The following information is displayed for networks:

Net Network number that the software assigns to the interface. Networks are numbered starting at 0. These numbers correspond to the interface numbers discussed under the CONFIG process.

Interface
Name of the interface and instance of this type of interface.

MAC/Data Link
Type of MAC/Data link configured for the interface.

Hardware
Specific kind of interface by hardware type.

State Current state of the network interface.

Testing
Indicates that the interface is undergoing a self-test. Occurs when the device is first started, when a problem is detected on the interface, or when the **test command** is used.

When an interface is operational, the interface periodically sends out maintenance packets and/or checks the physical state of the port or line to ensure that the interface is still functioning correctly. If the maintenance fails, the interface is declared down and a self-test is scheduled to run in 5 seconds. If a self-test fails, the interface transitions to the down state and the interval until the next self-test is increased up to a maximum of 2 minutes. If the self-test is successful, the network is declared up.

Up Indicates the interface is operational.

Down Indicates that the interface is not operational and has failed a self-test. The network will periodically transition to the testing state to determine if the interface can become operational again.

Disabled
Indicates that the interface is disabled. An interface can be disabled by the following methods:

- An interface can be configured as disabled using the CONFIG **disable** command. Each time the device is reinitialized, the

interface's initial state will be disabled. It will remain in the disabled state until an action is taken to enable it.

- An interface can be disabled using the GWCON **disable** command. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the device is reinitialized.
- The network manager can disable the interface through SNMP. This method is temporary because the interface will revert to its configured state (enabled or disabled) when the device is reinitialized.

When an interface is disabled, it remains disabled until one of the following methods is used to enable it:

- The GWCON **test** command is used to start a self-test of the interface.
- The network manager initiates a self-test of the interface through SNMP.

Not Present
Indicates that the interface's adapter is not plugged in.

Not Present is also used as the state for a null device. Spare interfaces are displayed as null devices until they are activated.

HW Mismatch
Indicates that the configured adapter type does not match the adapter type that is actually present in the slot.

Disable

Use the **disable** command to take a network interface off-line, making the interface unavailable. This command immediately disables the interface. You are not prompted to confirm, and no verification message displays. If you disable an interface with this command, it remains disabled until you use the GWCON **test** command or an OPCON **reload** command to enable it.

Enter the interface, or net number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

disable *interface#*

Error

Use the **error** command to display error statistics for the network. This command provides a group of error counters.

Syntax:

error

Example:

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Discards
Number of inbound packets which were discarded even though no errors were detected to prevent their being deliverable to a higher-layer protocol. The packets may have been discarded to free buffer space.

Input Errors
Number of packets that were found to be defective at the data link.

Input Unk Proto
Number of packets received for an unknown protocol.

Input Flow Drop
Number of packets received that are flow controlled on output.

Output Discards
Number of packets that the device chose to discard rather than transmit due to flow control.

Output Errors
Number of output errors, such as attempts to send over a network that is down or over a network that went down during transmission.

Note: The sum of the discarded output packets is not the same as input flow drops over all networks. Discarded output may indicate locally originated packets.

Event

Use the **event** command to access the Event Logging System (ELS) console environment. This environment is used to set up temporary message filters for troubleshooting purposes. All changes made in the ELS console environment will take effect immediately, but will go away when the device is reinitialized. See “Chapter 12. Using the Event Logging System (ELS)” on page 99 for information about the Event Logging System and its commands. Use the **exit** command to return to the GWCON process.

Syntax:

event

Feature

Use the **feature** command to access console commands for specific IBM 8371 features outside of the protocol and network interface console processes.

Enter a question mark after the **feature** command to obtain a listing of the features available for your software release.

To access that feature’s console prompt, enter the **feature** command at the GWCON prompt followed by the feature number or short name. Table 13 on page 64 lists available feature numbers and names.

Once you access the prompt for that feature, you can begin entering specific commands to monitor that feature. To return to the GWCON prompt, enter the **exit** command at the feature’s console prompt.

Syntax:

feature *feature#* or *feature-short-name*

Interface

Use the **interface** command to display statistical information about the network interfaces (for example, Ethernet). This command can be used without a qualifier to provide a summary of all the interfaces (shown in the following output) or with a qualifier to reveal detailed information about one specific interface.

Descriptions of detailed output for each type of interface are provided in the specific interface *Monitoring* chapters found in this guide. To obtain the interface number, use the GWCON **configuration** command.

Syntax:

interface [*interface#*]

Example: `interface`

Note: The display varies depending on the device.

Nt Global interface number.

Interface
Interface name.

Slot-Port
Slot number and port number of the interface.

Port Name
Port number, if applicable on the slot.

Self-Test Passed
Number of times self-test succeeded (state of interface changes from down to up).

Self-Test Failed
Number of times self-test failed (state of interface changes from up to down).

Maintenance Failed
Number of maintenance failures.

Memory

Use the **memory** command to display the current CPU memory usage in bytes, the number of buffers, and the packet sizes.

To use this command, free memory must be available. The number of free packet buffers may drop to zero, resulting in the loss of some incoming packets; however, this does not adversely affect device operations. The number of free buffers should remain constant when the device is idle. If it does not, contact your service representative.

Syntax:

memory

Example:

```
memory
Physical installed memory:        16 MB
Total routing (heap) memory:      12 MB
Routing memory in use:            13 %
```

```
                  Total  Reserve    Never     Perm     Temp     Prev
                                    Alloc    Alloc    Alloc    Alloc
Heap memory    12231155    26488 10687312  1438487   104924      432

Number of global buffers: Total = 300, Free = 300, Fair = 77, Low = 60
Global buff size: Data = 2048, Hdr = 17, Wrap = 72, Trail = 65, Total = 2208
```

Physical installed memory
The total amount of physical RAM installed in the device.

Total routing memory
The amount of memory available to the routing function, not including that allocated to the base operating system, system extensions, or options such as APPN. This is also called ″heap″ memory, and matches the ″Total″ heap memory size given in bytes shortly thereafter.

Routing memory in use
The percentage of total routing memory that is currently being used by the routing function. Heap memory currently in use is counted under the following headings **Perm Alloc** and **Temp Alloc**.

Heap memory:
Amount of memory used to dynamically allocate data structures.

Total Total amount of space available for allocation for memory.

Reserve
Minimum amount of memory needed by the currently configured protocols and features.

Never Alloc
Memory that has never been allocated.

Perm Alloc
Memory requested permanently by device tasks.

Temp Alloc
Memory allocated temporarily to device tasks.

Prev Alloc
Memory allocated temporarily and returned.

Number of global buffers:

Total Total number of global buffers in the system.

Free Number of global buffers available.

Fair Fair number of buffers for each interface. (See “Low”.)

Low The number of free buffers at which the allocation strategy changes to conserve buffers. If the value of *Free* is less than *Low*, then buffers will not be placed on any queue that has more than the *Fair* number of buffers in it.

Global buff size:
Global buffer size.

Data Maximum data link packet size of any interface.

Header
Sum of the maximum hardware, MAC, and data link headers.

Wrap Allowance given for MAC, LLC, or Network layer headers due to protocol wrapping.

Trailer Sum of the largest MAC and hardware trailers.

Total Overall size of each packet buffer

Network

Use the **network** command to enter the console environment for supported networks. This command obtains the console prompt for the specified interface.

Syntax:

network *interface#*

At the GWCON prompt (+), enter the **configuration** command to see the protocols and networks for which the device is configured. See “Configuration” on page 87 for more information on the configuration command.

Enter **interface** at the + prompt for a display of the networks for which the device is configured.

Enter the GWCON **network** command and the number of the interface you want to monitor or change. For example:

```
+network 0
ATM+
```

In the example, the `ATM+` prompt is displayed. You can then view information about the ATM interface by entering the ATM operating commands.

After identifying the interface number of the interface you want to monitor, for interface-specific information, see the corresponding monitoring chapter in this manual for the specified network or link-layer interface. Console support is offered for the following network and link-layer interfaces:

- ATM
- Ethernet
- Ethernet LECs

Performance

Use the **performance** command at the `GWCON` prompt to enter the monitoring environment for performance. See “Chapter 14. Configuring and Monitoring Performance” on page 169 for more information.

Protocol

Use the **protocol** command to communicate with the device software that implements the network protocols installed in your device. The **protocol** command accesses a protocol’s command environment. After you enter this command, the prompt of the specified protocol appears. From the prompt, you can enter commands that are specific to that protocol.

Syntax:

protocol *prot#*

Enter the protocol number or short name as part of the command. To obtain the protocol number or short name, enter the CONFIG command environment (`Config>`), and then enter the **list configuration** command. See “Accessing the Configuration Process, CONFIG (Talk 6)” on page 11 for instructions on accessing `Config>`. To return to GWCON, enter **exit**.

See the corresponding monitoring chapter in this manual or in the *Protocols and Features* for information on a specific protocol's console commands.

Queue

Use the **queue** command to display statistics about the length of input and output queues on the specified interfaces. Information about input and output queues provided by the queue command includes:

- The total number of buffers allocated
- The low-level buffer value
- The number of buffers currently active on the interface.

Syntax:

queue *interface#*

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Nt Network interface number associated with the software.

Interface
Type of interface.

Input Queue:

Alloc Number of buffers allocated to this device.

Low Low water mark for flow control on this device.

Curr Current number of buffers on this device. The value will be 0 if the device is disabled.

Output Queue:

Fair Fair level for the length of the output queue on this device.

Curr Number of packets currently waiting to be transmitted on this device. For locally originated packets, the eligibility discard depends on the global low water mark described in the **memory** command.

The device attempts to keep at least the Low value packets available for receiving over an interface. If a packet is received and the value of Curr is less than Low, then the packet will be subject to flow control. If a buffer subject to flow control is to be queued on this device and the Curr level is greater than Fair, then the buffer is dropped instead of queued. The dropped buffer is displayed in the Output Discards column of the **error** command. It will also generate ELS event GW.036 or GW.057.

Due to the scheduling algorithms of the device, the dynamic numbers of Curr (particularly the Input Queue Curr) may not be fully representative of typical values during packet forwarding. The console code runs only when the input queues have been drained. Thus, Input Queue Curr will generally be nonzero only when those packets are waiting on slow transmit queues.

Reset

Use the **reset** command to disable the specified interface and then re-enable it using new interface, protocol and feature configuration parameters. See "Resetting Interfaces" on page 57 for more information.

Syntax:

reset *interface#*

Statistics

Use the **statistics** command to display statistical information about the network software, such as the configuration of the networks in the device.

Syntax:

statistics *interface#*

To display information about one interface only, enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command.

Example:

Nt Network interface number associated with the software.

Interface
Type of interface.

Unicast Pkts Rcv
Number of non-multicast, non-broadcast specifically-addressed packets at the MAC layer.

Multicast Pkts Rcv
Number of multicast or broadcast packets received.

Bytes Received
Number of bytes received at this interface at the MAC layer.

Packets Trans
Number of packets of unicast, multicast, or broadcast type transmitted.

Bytes Trans
Number of bytes transmitted at the MAC layer.

Test

Use the **test** command to verify the state of an interface or to enable an interface that was previously disabled with the **disable** command. If the interface is enabled and passing traffic, the **test** command will remove the interface from the network and run self-diagnostic tests on the interface.

Syntax:

test *interface#*

Note: For this command to work, you must enter the ***complete*** name of the command followed by the interface number.

Enter the interface or network number as part of the command. To obtain the interface number, use the GWCON **configuration** command. For example, when testing starts, the console displays the following message:

```
Testing net 0 ATM/0...
```

When testing completes or fails, or when GWCON times out (after 30 seconds), the following possible messages are displayed:

```
Testing net 0 Eth/0 ...successful
Testing net 0 Eth/0 ...failed
Testing net 0 Eth/0 ...still testing
Testing net 0 ATM/0 ...successful
Testing net 0 ATM/0 ...failed
Testing net 0 ATM/0 ...still testing
Network is already undergoing test, attempting restart
```

Some interfaces may take more than 30 seconds before testing is done.

Uptime

Use the **uptime** command to display time statistics about the device, including the following:

- Number of restarts.
- Number of known crashes.
- Whether the device was last reloaded or restarted.
- Time elapsed since the last reload.
- Time elapsed since the last restart.

Syntax:

uptime

Chapter 11. The Messaging (MONITR - Talk 2) Process

This chapter explains how to collect and display messages. (Refer to “Chapter 12. Using the Event Logging System (ELS)” on page 99 for information about ELS and message formats. Refer also to the *Event Logging System Messages Guide* for a description of each message. This chapter includes the following sections:

- “What is Messaging (MONITR)?”
- “Commands Affecting Messaging”
- “Entering and Exiting the Messaging (MONITR) Process”
- “Receiving Messages”

What is Messaging (MONITR)?

The MONITR process provides a view of activity inside the device and the networks. MONITR also displays logging messages from the software.

Commands Affecting Messaging

The following commands affect the messaging process:

- OPCON commands:
  - **divert** temporarily diverts output to a different device.
  - **flush** causes the software to discard the messages it collects.
  - **halt** reverses the action of the divert command.
  - **talk** displays message output.
- CONFIG **set logging disposition** command sets the initial device to which the software sends its output.

Entering and Exiting the Messaging (MONITR) Process

To enter the messaging process from OPCON enter the **event** command or the **talk 2** command.

The console displays the messages the software has accumulated.

To exit messaging and return to OPCON, enter the OPCON intercept character (the default is **Ctrl-P**).

Receiving Messages

To receive messages at your console, enter the messaging process as described in the previous section. The software then displays all the messages it has recorded since it was last invoked. While you are connected to the messaging process, it displays all messages as they arrive.

Use the OPCON **divert** and **halt** commands to view software messages while you are doing something else with the device. Permitted devices divert output to TTY0 (the local console), TTY1, or TTY2 (the remote consoles).

Chapter 12. Using the Event Logging System (ELS)

This chapter describes the Event Logging System (ELS). The ELS continually logs all events, filtering them according to parameters that you select. A combination of operational counters and the ELS provides information for monitoring the health and activity of the system. The information is divided into the following sections:

What is ELS?

ELS is a monitoring system and an integral part of the device operating system. ELS manages the messages logged as a result of device activity. Use ELS commands to set up a configuration that sorts out only those messages you feel are important. You can then display the messages on the console terminal screen, log them to a remote workstation, or send the messages to a network management station using Simple Network Management Protocol (SNMP) traps.

The ELS system and the operational counters are the best troubleshooting tools you have to isolate problems in the device. A quick scan of the event messages will tell you whether the device has a problem and where to start looking for it.

In the ELS configuration environment, the commands are used to establish a default configuration. This default configuration does not take effect until the device reinitializes.

Occasionally, it is helpful to temporarily view messages using parameters other than was set up in the ELS configuration environment, without having to reinitialize the device. The ELS operating and monitoring environment is used to:

- Temporarily change the default ELS display settings
  - Changes made in the ELS console environment take effect immediately
  - Changes made in the operating/monitoring environment are not stored in nonvolatile configuration storage.
- View statistical information regarding ELS uses of dynamic RAM

Note: Specific ELS messages are described in the *Event Logging System Messages Guide*.

ELS is a subprocess that you access from the OPCON process.

Entering and Exiting the ELS Configuration Environment

The ELS configuration environment (available from the CONFIG process) is characterized by the `ELS Config>` prompt. Commands entered at this prompt create the ELS default state that takes effect after you restart the device. These commands are described in greater detail later in this chapter.

Configuration commands that have subsystem, group, or event as a parameter are executed in the following order:

- Subsystem
- Group
- Event

To set a basic ELS configuration, enter the **display subsystem all standard** command at the `ELS Config>` prompt. This command configures the ELS to display messages from all subsystems with the STANDARD logging level (that is, all errors and unusual informational comments).

Note: The device does not have a default ELS configuration. You must enter the ELS configuration environment and set the default state.

To enter the ELS configuration environment from OPCON:

1. Enter the **configuration** command. The console displays the CONFIG prompt (`Config>`). If the prompt does not appear when you first enter CONFIG, press **enter**.
2. At the CONFIG prompt, enter the following command to access ELS:

   ```
   Config> eve
   ```

   The console displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

Event Logging Concepts

This section describes how events are logged and how to interpret messages. Also described are the concepts of subsystem, event number, and logging level. A large part of ELS function is based on commands that accept the subsystem, event number, and logging level as parameters.

Causes of Events

Events occur continuously while the device is operating. They can be caused by any of the following reasons:

- System activity
- Status changes
- Service requests
- Data transmission and reception
- Data and internal errors

When an event occurs, ELS receives data from the system that identifies the source and nature of the event. Then ELS generates a message that uses the data received as part of the message.

Interpreting a Message

This section describes how to interpret a message generated by ELS. Figure 10 shows the message contents.

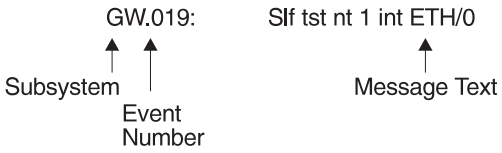

Figure 10. Message Generated by an Event

The information illustrated in Figure 10 as well as the ELS logging level information displayed with the **list subsystem** command is as follows:

Subsystem

Subsystem is a predefined short name for a device component, such as a protocol or interface. In Figure 10, **GW** identifies the subsystem through which this event occurred.

Other examples of subsystems include IP, TKR, and ATM. On a particular device, the actual subsystems present depend on the hardware and software configured for that device. You can use the **list subsystem** command described in this chapter to see a list of the subsystems on your device.

Enter the subsystem as a parameter to an ELS command when you want the command to affect the entire subsystem. For example, the ELS command **display subsystem GW** causes all events (except the events with 'debug' logging level) that occur through the GW subsystem to be displayed.

Event Number

Event Number is a predefined, unique, arbitrary number assigned to each message within a subsystem. In Figure 10, **019** is the event number within the GW subsystem. You can see a list of all the events within a subsystem by using the **list subsystem** command, where *subsystem* is the short name for the subsystem.

The event number always appears with a subsystem identifier, separated by a period. For example: **GW.019**. The subsystem and event number together identify an *individual* event. They are entered as a parameter to certain ELS commands. When you want a command to affect only the specified event, enter the subsystem and event number as a parameter for the ELS command.

Logging Level

Logging level is a predefined setting that classifies each message by the type of event that generated it. Use the **list subsystem** ELS console command to display the setting of the logging level. Table 17 on page 102 lists the logging levels and types. ERROR, INFO, TRACE, STANDARD, and ALL are aggregates of other

logging level types. STANDARD is the recommended default.

Table 17. Logging Levels

Logging Level	Type
UI ERROR	Unusual internal errors
CI ERROR	Common internal errors
UE ERROR	Unusual external errors
CE ERROR	Common external errors
ERROR	Includes all error levels above
UINFO	Unusual informational comment
CINFO	Common informational comment
INFO	Includes all comment levels above
STANDARD	Includes all error levels and all informational comment levels (default)
PTRACE	Per packet trace
UTRACE	Unusual operation Trace message
CTRACE	Common operation Trace message
TRACE	Includes all trace levels above
DEBUG	Message for debugging
ALL	Includes all logging levels

The logging level setting affects the operation of the following commands:

- **Display subsystem**
- **Nodisplay subsystem**
- **Trap subsystem**
- **Notrap subsystem**
- **Remote subsystem**
- **Noremote subsystem**

The logging level is set for a particular command when you specify it as a parameter to one of the above commands. For example:

```
display subsystem ETH ERROR
```

Including the logging level on the command line modifies the **display** command so that whenever an event with a logging level of either UI-ERROR or CI-ERROR occurs through subsystem TKR, the console displays the resulting message.

You cannot specify the logging level for operations affecting groups or events.

Message Text

Message Text appears in short form. In Figure 10 on page 101, `Slf tst nt 1 int ETH/0` is the message generated by this event. Variables, such as *source_address* or *network*, are replaced with actual data when the message displays on the console.

The variable *error_code* is referred to by some of the Event Logging System message descriptions (usually preceded by rsn or reason). They indicate the type of packet error detected. Table 18 on page 103 describes the error or packet completion codes. Packet completion codes indicate the disposition of the packets received by the device.

Table 18. Packet Completion Codes (Error Codes)

Code	Meaning
0	Packet successfully queued for output
1	Random, unidentified error
2	Packet not queued for output due to flow control reasons
3	Packet not queued because network is down
4	Packet not queued to avoid looping or bad broadcast
5	Packet not queued because destination host is down (only on networks where this can be detected)

ELS displays network information as follows:

`nt 1 int Eth/0` (or) `network 1, interface Eth/0,`

where:

- 1 is the network number (each network on the device is numbered sequentially from zero).
- 0 is the unit number (the interfaces of each hardware type are numbered sequentially from zero).

Ethernet and 802.5 hardware addresses appear as a long hexadecimal number.

IP (Internet Protocol) addresses are printed as 4 decimal bytes separated by periods, such as 18.123.0.16.

Groups

Groups are user-defined collections of events that are given a name, the group name. Like the subsystem, subsystem and event number, and logging level, use the group name as a parameter to ELS commands. However, there are no predefined group names. You must create a group before you can specify its name on the command line.

To create a group, use the **add** configuration command, specify the name you want to call the group, and then specify the events you want to be part of the group. The events you add to the group can be from different subsystems and have different logging levels.

After creating a group, use the group name to manipulate the events in the group as a whole. For example, to turn off display of all messages from events that have been added to a group named grouptwo, include the group name on the command line, as follows:

```
nodisplay group grouptwo
```

To delete a group, use the **delete** command.

Using ELS

To use ELS effectively, do the following:

- Know what you want before using the ELS system. Clearly define the problem or events that you want to see before using the MONITR process.
- Execute the command **nodisplay subsystem all all** to turn off all ELS messages.

- Turn on only those messages that relate to the problem you are experiencing.
- Use the *Event Logging System Messages Guide* to determine which messages are not normal.

When initially viewing ELS from the MONITR process, you will see a considerable amount of information. Because the device cannot buffer and display every packet under moderate to heavy loads the buffers are flushed. When this occurs the following message is displayed:

```
xx messages flushed
```

The device does not save these messages. When this message appears, tailor the ELS output to display only that information that is important to the current task you are monitoring, or use the advanced ELS commands to establish a message buffer. See “Using ELS Message Buffering” on page 113.

Managing ELS Message Rotation

It is also important to note that the ELS messages continually rotate through the device’s buffers. To stop and restart the displaying of ELS messages, use the following key combinations:

Ctrl-S to pause scrolling

Ctrl-Q to resume scrolling

Ctrl-P to go back to the last process

You may also want to capture the ELS output to a file. You can do this by starting a script file or log file from your location when Telneting to a device. You can also do this by attaching a PC to the device’s console port and starting a log file from within the terminal emulation package. This information is needed to help Customer Service diagnose a problem.

Capturing ELS Output Using a Telnet Connection on a UNIX Host

Use a Telnet connection on an AIX or UNIX host to capture the ELS messages on your screen to a file on the host. Before beginning, set up ELS for the messages you want to capture using the ELS console commands in “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 117.

To capture the ELS output to a file on an AIX or UNIX host, follow these steps:

1. From the host, enter **telnet** *device_ip_addr* **| tee** *local_file_name*
   - *device_ip_addr* is the IP address of the device
   - *local_file_name* is the name of the file on the host where you want the ELS messages to be saved.
   - The **tee** command displays the ELS messages on your screen and, at the same time, copies them to the local file.
2. From the OPCON prompt (*****), enter **t 2**. This accesses the MONITR process, which is the process that displays ELS messages on your screen. Depending on which ELS messages you configured, you should see ELS messages appearing on the screen.

   As long as you are in the MONITR process, all ELS messages will be written to the local file. When you exit the MONITR process (by entering **Ctrl-P**) or terminate the Telnet session, the logging of messages to the local file will stop.

You can also use remote logging instead of capturing ELS output on a UNIX Host. For more information about remote logging, see “Using and Configuring ELS Remote Logging” on page 106.

Configuring ELS So Event Messages Are Sent In SNMP Traps

ELS can be configured so that event messages are sent to a network management workstation in an SNMP enterprise-specific trap. These traps are useful for reporting status and diagnostic results, and are often used for remote monitoring of a IBM 8371. When ELS is configured appropriately, an SNMP trap will be generated each time the selected event occurs. For more information about SNMP, see *Protocols and Features*.

To tell ELS that a specific event should be activated to be sent as an SNMP trap, at the `ELS config>` prompt or at the `ELS>` prompt, using IP as an example, type:

```
trap event eth.007
```

Note: If you are at the `ELS config>` prompt, you will need to reboot.

To enable the ELS enterprise-specific trap, follow these steps:

1. At the `SNMP config>` prompt, using **public** as an example, type:

   ```
   SNMP config> add address public <network manager IP address>
   SNMP config> enable trap enterprise public
   SNMP config> set community access read_trap public
   ```

   Note: You need to reboot to activate these changes.
2. Enable your network management station to receive and properly display the enterprise-specific traps.

Follow these steps to trap groups, subsystems, and events.

Using ELS to Troubleshoot a Problem

If you are trying to troubleshoot a particular problem, display the messages related to the problem. For example, if experiencing a problem with bridging, turn on the bridging messages:

display subsystem br all

Initially, because of the rapid pace of messages scrolling across the screen, you may want to record the numbers you see and look them up in the *Event Logging System Messages Guide* manual. Once you become familiar with different types of messages being displayed for a particular protocol, you can turn on and turn off only those messages that contain the information that you require to troubleshoot a problem. The following sections list specific ELS examples. Keep in mind that different problems may require different steps.

ELS Example

Router cannot communicate with an IPX server on an Ethernet.

1. Enter the **talk** command and the PID for GWCON.

   ```
   * talk 5
   ```

   The console displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **Return**.

2. At the GWCON prompt (+), enter **IPX** to access the IPX console prompt (IPX>).
3. At the IPX console prompt, enter the **slist** command to verify that the server is listed. (See the section on monitoring IPX in the *Protocols and Features* for information on the **slist** command.)
4. Check the IPX configuration.
5. Enter the following:

```
* t 5
+ event
ELS> nodisplay subsystem all all
ELS> display subsystem IPX all
ELS> display subsystem eth all
ELS> Ctrl-P
* t 2
```

As the messages begin to scroll by, look for ELS message eth.001. This indicates that the server has a bad Ethernet type field.

Using and Configuring ELS Remote Logging

The remotely-logged ELS message contains all of the information that is contained in ELS messages found in the monitor queue, as viewed under talk 2, and also contains additional information as shown in Figure 11.

```
Date/Time         IP address      Sequence Number      Local Name      ELS Subsystem Name, &
                  assigned        used for detecting   assigned        Formatted message
                  by the user     missing messages     by the user

Nov 20 12:13:47   5.1.1.1         Msg [0444] from      ** IBM/8371 **  :els: MPC.011 Del ent ...
```

Figure 11. Syslog Message Description

Note the following differences in the remote log display:

- The month and day of month in addition to the time, which is always displayed as the time-of-day.
- An IP address, which is the user-specified source IP address. If a DNS server resolves the source IP address to a hostname, then the hostname will be displayed instead of the IP address.
- A Sequence number is added to the message by the source device to assist in detecting dropped messages. See “Remote Logging Output” on page 110 for an explanation of dropped messages. When the sequence number of the message reaches 9999, the next sequence number is 0001.
- A “Local Name” for the source device, to assist in distinguishing between messages from multiple sources. If you do not configure a local name, this field is blank.

Syslog Facility and Level

Remotely-logged ELS messages are transmitted over the network in UDP packets with the destination port number in the UDP header always equal to 514, the syslog port. To receive and process the UDP packets, the *syslog daemon* (syslogd) must be running in the remote workstation that is receiving and logging the ELS messages. See “Remote Workstation Configuration” on page 107 for details.

Although it is not displayed in the remotely-logged ELS message, every ELS message sent on the network in a UDP packet must be assigned a *syslog_facility* and a *syslog_level*. The syslog daemon uses the combination of facility and level to determine where to route the message. Typically, you want the ELS messages to be written to one or more files in the remote host. Other options include displaying the message on the console, sending the message to one or more users, or sending the message to another workstation.

The commands you use to specify the *syslog_facility* and *syslog_level* values, along with other remote-logging related console commands, are described in “ELS Monitoring Commands” on page 139 and “ELS Configuration Commands” on page 117. Review these commands before reading through the next section.

Remote Workstation Configuration

The following configuration assumes that a single 8371 is remote-logging to a single remote workstation. You can configure multiple 8371s to remote-log to the same remote workstation. However, a particular 8371 can log to one and only one remote workstation. The operating system used in this example is AIX 4.2. Your environment may be slightly different. For more information on syslog, refer to the documentation for your operating system.

To perform the configuration on an AIX workstation, you must log in as **root**. To configure the workstation:

1. Create or edit a syslog.conf file to specify where ELS messages with particular *syslog_facility* and *syslog_level* values are to be written. See the bottom of Figure 12 on page 108 for an example of how to specify the message destination. Note that the full pathname of the log files must be specified. The default location for the syslog configuration file is /etc/syslog.conf.
2. Create the files for logging syslog messages that you specified in the syslog.conf file.
3. Start the syslog daemon by entering **syslogd**. To start the syslog daemon from SRC (System Resource Controller), enter **startsrc -s syslogd**. If the pathname of the configuration file is not /etc/syslog.conf, then enter **syslogd -f** *pathname*. To start the syslog daemon in debug mode, enter **syslogd -d**.

   Note: Running multiple instances of the syslog daemon is not supported.
4. If the syslog daemon is already running when you create or modify the syslog.conf file, it must be restarted so that the daemon reinitializes the configuration from syslog.conf.
5. Verify the setup by using the **logger** command as follows:

   ```
   logger -p user.alert  THIS IS A TEST MESSAGE (user.alert)
   logger -p news.info  THIS IS A TEST MESSAGE (news.info)
   ```

   If the setup is correct, `THIS IS A TEST MESSAGE...` will be written to the files specified in syslog.conf.

```
# @(#)34       1.9 src/bos/etc/syslog/syslog.conf, cmdnet, bos411, 9428A410j 6/13/93 14:52:39
#
# COMPONENT_NAME: (CMDNET) Network commands.
#
# FUNCTIONS:
#
# ORIGINS: 27
#
# (C) COPYRIGHT International Business Machines Corp. 1988, 1989
# All Rights Reserved
# Licensed Materials - Property of IBM
#
# US Government Users Restricted Rights - Use, duplication or
# disclosure restricted by GSA ADP Schedule Contract with IBM Corp.
#
# /etc/syslog.conf - control output of syslogd
#
# Each line must consist of two parts:-
#
# 1) A selector to determine the message priorities to which the
#    line applies
# 2) An action.
#
# The two fields must be separated by one or more tabs or spaces.
#
# format:
#
# <msg_src_list>               <destination>
#
# where <msg_src_list> is a semicolon separated list of <facility>.<priority>
# where:
#
# <facility> is:
#      * - all (except mark)
#      kern,user,mail,daemon, auth, syslog, lpr, news, uucp, cron, authpriv, local0 - local7
#
# <priority or level> is one of (from high to low):
#      emerg,alert,crit,err(or),warn(ing),notice,info,debug
#      (meaning all messages of this priority or higher)
#
# <destination> is:
#      /filename - log to this file
#      username[,username2...] - write to user(s)
#      @hostname - send to syslogd on this machine
#      * - send to all logged in users
#
# example:
# "mail messages, at debug or higher, go to Log file. File must exist."
# "all facilities, at debug and higher, go to console"
# "all facilities, at crit or higher, go to all users"
#  mail.debug          /usr/spool/mqueue/syslog
#  *.debug             /dev/console
#  *.crit                      *

#   syslog messages with facilty / priority values of LOG_USER,   LOG_ALERT
user.alert            /tmp/syslog_user_alert

#   syslog messages with facilty / priority values of LOG_NEWS,  LOG_INFO
news.info           /tmp/syslog_news_info
```

Figure 12. syslog.conf Configuration File

Configuring the 8371 for Remote Logging

To configure a 8371:

1. In talk 6, configure the remote-logging facility as shown in Figure 13 on page 109. The IP address specified as the *source-ip-addr* should be an IP address that is configured in the 8371 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address resolves quickly into a hostname by the

name server or that the name server at least responds quickly with “address not found.” To determine whether this happens, issue the **host** command on your workstation as follows:

```
workstation> host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address which resolves more quickly.

2. In talk 6 configure events and subsystems for remote-logging, as shown in Figure 14 on page 110.
3. Write the configuration and reload the 8371.

```
ELS config>set remote source-ip-addr 5.1.1.1
Source IP Addr = 5.1.1.1

ELS config>set remote remote-ip-addr 192.9.200.1
Remote Log IP Addr = 192.9.200.1

ELS config>set remote local-id ** IBM/8371 **
Remote Log Local ID = ** IBM/8371 **

ELS config>set remote no-msgs-in-buffer 100
Number of messages in Remote Log Buffer must be 100-512
Number of Messages in Remote Buffer = 100

ELS config><B>set remote facility log_news
Default Syslog Facility = LOG_NEWS

ELS config>set remote level log_info
Default Syslog Level = LOG_INFO

ELS config>set remote on
Remote Logging is ON

ELS config>list remote

------------------   Remote Log Status  -----------------

Remote Logging is ON
Source IP Address = 5.1.1.1
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_NEWS
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log =  100
Remote Logging Local ID = ** IBM / 8371 **
ELS config>
```

Figure 13. Configuring the 8371 for Remote Logging

```
ELS config>display sub snmp all
ELS config>remote sub snmp all log_news log_info

ELS config>display event srt.017
ELS config>remote event srt.017 log_news log_info

ELS config>display event stp.016
ELS config>remote event stp.016 log_user log_info

ELS config>display event stp.026
ELS config>remote event stp.026 log_news log_info

ELS config>display event stp.024
ELS config>remote event stp.024 log_news log_info


ELS config>list status
Subsystem:    SNMP
Disp levels:  ERROR INFO TRACE
Trap levels:  none
Trace levels: none
Remote levels:  ERROR INFO TRACE
        Syslog Facility/Level: LOG_NEWS LOG_INFO

Event     Display Trap    Trace     Remote
SRT.017   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.016   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.026   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
STP.024   On      Unset   Unset     On
                                    Syslog Facility/Level: LOG_NEWS LOG_INFO
```

Figure 14. Configuring Subsystems and Events for Remote Logging

Remote Logging Output

Figure 15 on page 111 shows a sample from the /tmp/syslog_news_info file. Notice that the first message has a sequence number of 310. This means that the first 309 ELS messages were not sent from the source 8371. There are several reasons for this:

- The remote-logging facility had not completed initialization when the messages were first passed to ELS
- A route from the source 8371 to the remote workstation was not in the routing table
- The interface for the outbound UDP packet containing the ELS messages was not in the “Up” state

```
Nov 20 12:03:16 workstа01 root:  THIS IS A TEST MESSAGE  (news.info)
Nov 20 12:08:48 5.1.1.1 Msg [0310] from ** IBM / 8371 **: els:  IP.022: add nt 192.9.200.0 int 192.9.200.20
nt 0 int Eth/0

 1  ( messages 311, 312, and 313 did not get remote-logged due to ARP request outstanding - see
  explanation in the text)

 2  (messages 314 and 315 were logged to a separate
file - see explanation in the text)

Nov 20 12:08:48 5.1.1.1 Msg [0316] from ** IBM / 8371 **: els:  IP.068: routing cache cleared
Nov 20 12:08:48 5.1.1.1 Msg [0317] from ** IBM / 8371 **: els:  IP.022: add nt 5.0.0.0 int 5.1.1.1 nt 5 int Eth/4
Nov 20 12:08:48 5.1.1.1 Msg [0318] from ** IBM / 8371 **: els: SRT.017: Enabling SRT on port 5 nt 5 int Eth/4


(message 319 was logged to a separate file)

Nov 20 12:08:48 5.1.1.1 Msg [0320] from ** IBM / 8371 **: els:  IP.068: routing cache cleared

(120 messages not shown)

Nov 20 12:13:33 5.1.1.1 Msg [0441] from ** IBM / 8371 **: els:  GW.022: Nt fld slf tst nt 3 int Eth/3
Nov 20 12:13:33 5.1.1.1 Msg [0442] from ** IBM / 8371 **: els:  GW.022: Nt fld slf tst nt 6 int Eth/5
Nov 20 12:13:38 5.1.1.1 Msg [0443] from ** IBM / 8371 **: els:  GW.022: Nt fld slf tst nt 11 int ISDN/0


(messages 444 and 447 were logged to a separate file)


(messages 445 and 446 did not get remote-logged due to ARP request outstanding)

Nov 20 12:13:50 5.1.1.1 Msg [0448] from ** IBM / 8371 **: els:  GW.022: Nt fld slf tst nt 4 int PPP/0
Nov 20 12:13:50 5.1.1.1 Msg [0449] from ** IBM / 8371 **: els:  IP.068: routing cache cleared
Nov 20 12:13:50 5.1.1.1 Msg [0450] from ** IBM / 8371 **: els:  IP.058: del nt 4.0.0.0 rt via 0.0.0.4 nt 4 int PPP/0
```

Figure 15. Sample Contents from Syslog News Info File

If the initial ELS messages that are generated during and immediately after booting are of particular interest, then it is recommended that these messages also be displayed in the monitor queue, which is viewed with talk 2. Figure 16 on page 112 shows the talk 2 output including the initial messages that did not get remote-logged. Note that there is a message in the talk 2 output that indicates that the remote-logging facility is available. This does not indicate that a route exists to the remote workstation, nor that the associated interface is in the “Up” state. It simply provides a reference point before which no messages can be successfully remote-logged.

Also notice that you can account for the messages that were missing (indicated in Figure 15 with **2**) in the talk 2 output.

Using ELS

```
12:08:17 SNMP.024: generic trc (P2) at snmp_mg.c(766): Now 0 trap destinations
12:08:17 SNMP.012: comm public added
12:08:17 SNMP.012: comm public added
12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_device_if_info(): sr
rdrec failed

12:08:27 SNMP.022: ext err (Z1) at snmp_resconf.c(322): add_device_if_info(): sr
rdrec failed

12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:27 SNMP.028: err (E2) at snmp_moh.c(1583) : Duplicate
12:08:28   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:28   IP.022: add nt 4.0.0.0 int 4.1.1.1 nt 4 int PPP/0

     ( 297 messages not shown )                                    Corresponding Sequence
                                                                   Numbers in
12:08:43   GW.022: Nt fld slf tst nt 12 int PPP/2                   Remote-Logging Files :
12:08:43   GW.022: Nt fld slf tst nt 13 int PPP/3
12:08:48   IP.022: add nt 192.9.200.0 int 192.9.200.20 nt 0 int Eth/0   [0310] first message logged
12:08:48  SRT.017: Enabling SRT on port 1 nt 0 int Eth/0          -- not logged (ARP request) --
12:08:48  STP.016: Select as root TB-1, det topol chg            -- not logged (ARP request)--
12:08:48  STP.026: Root TB-1, strt hello tmr                     -- not logged (ARP request)--
12:08:48  ARP.002: Pkt in 1 1 800 nt 0 int Eth/0                 [0314]
12:08:48  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                 [0315]
12:08:48   IP.068: routing cache cleared                         [0316]


     ( 126 messages not shown )

12:13:38   GW.022: Nt fld slf tst nt 11 int ISDN/0               [0443]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                    [0444]
12:13:47  ARP.011: Del ent 1 3 nt 0 int Eth/0                    -- not logged (ARP request) --
12:13:47  ARP.002: Pkt in 1 1 800 nt 5 int Eth/4                 -- not logged (ARP request)--
12:13:47  ARP.002: Pkt in 2 1 800 nt 0 int Eth/0                 [0447]
12:13:50   GW.022: Nt fld slf tst nt 4 int PPP/0                 [0448]
```

Figure 16. Output from Talk 2

You can use the timestamp, which appears in both the remote-logging output file and the talk 2 output, to determine when the first ELS message is successfully remote-logged. To use the timestamp for this purpose, configure ELS such that the timestamp in the monitor queue displays the time-of-day.

Additional Considerations

ELS Messages Containing IP Addresses

ELS messages containing an IP address which matches the IP address of the remote workstation will not be remote-logged, even if configured for remote-logging, and may appear under talk 2. These messages are discarded instead of being remote-logged in order to prevent excessive UDP packets from being sent on the network.

Duplicate Logging

If a facility value is repeated in *syslog.conf*, for example:

```
user.debug        /tmp/syslog_user_debug
user.alert        /tmp/syslog_user_alert
```

The syslog daemon will log *user.debug* messages only to the */tmp/syslog_user_debug* file while user.alert messages will be logged to both the */tmp/syslog_user_debug* file and the */tmp/syslog_user_alert* file. This is consistent with the syslog design that logs the more severe conditions in multiple places.

To prevent this duplicate logging, it is recommended that different facility values be specified in the *syslog.conf* file. A total of 19 facility values are available.

Recurring Sequence Numbers in Syslog Output Files

Depending upon the configuration of your network, it is possible for duplicate UDP packets containing ELS messages to arrive at the remote host. It is also possible for the packets to arrive in a different order than they were transmitted. An example of this phenomenon is shown in Figure 17. Notice that the messages with sequence numbers 628 through 633 are logged twice. Also notice that after the first occurrence of sequence number 0630, sequence number 0629 occurs again, followed by the second occurrence of 0630.

```
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:48:33 0.0.0.0 Msg [0628] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0629] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:08 0.0.0.0 Msg [0630] from: RA22: : els: IPX.018: SAP gen rply sent nt 0 int TKR/0, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0631] from: RA22: : els: IPX.037: RIP resp sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:49:33 0.0.0.0 Msg [0632] from: RA22: : els: IPX.018: SAP gen rply sent nt 5 int TKR/1, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
Apr 01 10:50:08 0.0.0.0 Msg [0633] from: RA22: : els: IPX.037: RIP resp sent nt 0 int TKR/0, 1 pkts
```

Figure 17. Example of Recurring Sequence Numbers in Syslog Output

Because neither Syslog nor UDP has the ability to handle duplicate or out of sequence packets, it is important to recognize the possibility of duplicate sequence numbers occurring.

Using ELS Message Buffering

Message buffering is an advanced feature of ELS that can help you with problem determination. You can set up defaults that ELS will use for message buffering or change how messages are buffered while the device is operating. Message buffering can minimize the information lost because messages have wrapped in the default message buffers. Message buffering is accessible through the **advanced** configuration or monitoring command. It enables you to:

- Specify whether buffering is active.
- Specify what events are written to the message buffer.
- Stop buffering and free the memory allocated for buffering.
- Display the status of the message buffer.
- Specify an event that stops message buffering and what action the system takes when the event occurs.
- Send a formatted version of the buffer to a file at a remote server.
- View a specific number or all of the ELS messages in the buffer.
- Write the buffer to a hard drive if a hard drive is present.
- Read a file that contains a formatted ELS message buffer from the hard drive , if a hard drive is present.
- Send a file that contains a formatted ELS message buffer from the hard drive , if a hard drive is present.

For specifics about the commands, see “ELS Message Buffering Configuration Commands” on page 135 and “ELS Message Buffering Monitoring Commands” on page 164.

The following example shows how to configure ELS message buffering.

```
 MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

 *t 5 :Enter t 5 at the * prompt.

 CGW Operator Console

 +ev :Enter ev at the + prompt.
 Event Logging System user console
 ELS>a :Enter a for advanced at the ELS prompt.
 Advanced ELS Console
 ELS Advanced>li s :Enter li s to list status at the > prompt.
 ------------------Advanced ELS Configuration-----------------------
 Logging Status:  OFF  Wrap Mode:  ON   Logging Buffer Size: 0 KB
 Stop-Event:  NONE   Stop-String:   NONE
 Additional Stop-Action:  NONE
 ------------------------Run-Time Status----------------------------
 Has Stop Condition Occurred?   NO   Messages currently in buffer:  0

 ELS Advanced>s b :Enter s b to set buffer size.
 Enter buffer size of 0 KB or between 148 and 593 KB [148]?
 Buffer size set to 148 KB
 ELS Advanced>s s e gw.26 :Enter s s e to set stop event eg. gw.26
 Stop Event "GW.026" has been set
 ELS Advanced>ex :Enter ex to exit Advanced to list gw.26
 ELS>list ev gw.26
 Level: C-TRACE
 Message: Mnt nt %n int %s/%d
 Active:         Count: 742

 ELS>a :Enter a to get back to advanced.
 Advanced ELS Console
 ELS Advanced>s s s Mnt nt 5 :Enter s s s to set the stop string.
 Stop String set to "Mnt nt 5"
 ELS Advanced>s s a ? :Enter s s a ? to query available stop actions.
 NONE
 APPN-DUMP  :Only available if APPN active and in the load image.
 SYSTEM-DUMP
 ELS Advanced>s s a s :Enter s s a s to set SYSTEM-DUMP stop action.
 Stop Action has been set to SYSTEM-DUMP
 ELS Advanced>s w off to :Enter s w on to set wrap mode off.
 Advanced Wrap Mode set to OFF.

 ELS Advanced>log sub gw all :Enter to enable the whole gw subsystem
 ELS Advanced>s l on :Enter s l on to start the logging process.
 Advanced Logging set to ON.
 ELS Advanced>li s :Enter to list status of logging.
 ------------------Advanced ELS Configuration-----------------------
 Logging Status:  OFF  Wrap Mode: OFF  Logging Buffer Size: 148 KB
 Stop-Event:     GW.026   Stop-String:  Mnt nt 5
 Additional Stop-Action:  SYSTEM-DUMP


------------------------Run-Time Status----------------------------
 Has Stop Condition Occurred?   YES  Messages currently in buffer:  7

 ELS Advanced>v a n :Enter to view all messages in buffer. For this
                     trivial example any viewing command suffices.

  1  10:52:10   GW.026: Mnt nt 0 int Eth/0
  2  10:52:10   GW.026: Mnt nt 5 int Eth/1->This triggers stop action
  3  10:52:14   GW.026: Mnt nt 0 int Eth/0  Note that 5 more events
  4  10:52:14   GW.026: Mnt nt 5 int Eth/1  get logged before
  5  10:52:18   GW.026: Mnt nt 0 int Eth/0  logging stops and
  6  10:52:18   GW.026: Mnt nt 5 int Eth/1  the stop action occurs.
  7  10:52:22   GW.026: Mnt nt 0 int Eth/0

 Bughlt: Dump initiated by ELS Stop Action.

 BUGHLT+80; Dump initiated by ELS Stop Action.

 Note:
 In reality if the stop action is the SYSTEM-DUMP you will not be
```

```
able to list the final status as above nor view the buffer because
the router will be attempting to reload.
```

Using ELS

Chapter 13. Configuring and Monitoring the Event Logging System (ELS)

This chapter describes how to configure events logged by ELS and how to use the ELS commands. The information includes the following sections:

- "Accessing the ELS Configuration Environment"
- "ELS Configuration Commands"
- "Entering and Exiting the ELS Operating Environment" on page 138
- "ELS Monitoring Commands" on page 139

For more information on the Event Logging System and how to interpret ELS event messages, refer to "Chapter 12. Using the Event Logging System (ELS)" on page 99.

Accessing the ELS Configuration Environment

The ELS configuration environment is characterized by the `ELS config>` prompt. Commands entered at this prompt are described "Chapter 13. Configuring and Monitoring the Event Logging System (ELS)".

To enter the ELS configuration environment:

1. Enter **configuration**.

   The monitoring displays the `Config>` prompt. If the prompt does not appear, press **enter**.
2. At the `Config>` prompt, enter the following command to access ELS:

   ```
   event
   ```

   The monitoring displays the ELS configuration prompt (`ELS config>`). Now, you can enter ELS configuration commands.

To leave the ELS configuration environment, enter the **exit** command.

ELS Configuration Commands

Table 19 summarizes the ELS configuration commands. The remainder of this section describes each one in detail. After accessing the ELS configuration environment, you can enter ELS Configuration commands at the `ELS Config>` prompt.

Table 19. ELS Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds an event to an existing group or creates a new group.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Clears all ELS configuration information.
Default	Resets the display or trap setting of an event, group, or subsystem.

Table 19. ELS Configuration Command Summary (continued)

Command	Function
Delete	Deletes an event number from an existing group or deletes an entire group.
Display	Enables message display on the console monitor.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to a remote workstation.
Notrace	Controls disablement of packet trace events.
Notrap	Keeps messages from being sent out in SNMP traps.
Remote	Allows messages to be logged to a remote workstation.
Set	Sets the pin parameter and the timestamp feature options.
Trace	Controls enablement of packet trace events.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add an individual event to an existing group or to create a new group. Group names must start with a letter and are case sensitive. You cannot append an entire subsystem to a group.

Syntax:

add *group_name subsystem.event_number*

Note: If the specified group does not exist, the following prompt asks you to confirm the creation of a new group:

```
Group not found. Create new group? (yes or no)
```

Advanced

Use the **advanced** command to enter the advanced configuration environment. In this environment you configure message buffering.

Syntax:

advanced

Clear

Use the **clear** command to clear all of the ELS configuration information.

Syntax:

clear

Example:

```
clear

You are about to clear all ELS configuration information
Are you sure you want to do this (Yes or No):
```

Default

Resets the display or trap setting of an event, group, or subsystem back to a disabled state.

Syntax:

default	display
	trap
	remote

display *event* **or** *group* **or** *subsystem*
Controls the output of the display of messages to the monitoring.

trap *event* **or** *group* **or** *subsystem*
Controls the generation of traps to the network management station.

remote *event* **or** *group* **or** *subsystem*
Controls the generation of traps to the remote station.

Delete

Use the **delete** command to delete an event number from an existing group or to delete the entire group. If the specified event is the last event to be deleted in a group, you will be notified. If *all* is specified instead of *subsystem.event_number*, a prompt asks you to confirm the deletion of the entire group.

Syntax:

delete	*group_name subsystem.event_number*

Display

Use the **display** command to enable message displaying on the monitoring monitor for specific events, a range of events for a subsystem, groups, or subsystems.

Syntax:

display	event . . .
	group . . .
	range . . .
	subsystem . . .

event *subsystem.event#*
Displays messages of the specified event (*subsystem.event#*).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Displays messages associated with the specified subsystem. To find out which subsystems are on the device, type **list subsystems**.

Note: Although ELS supports all subsystems on the device, not all devices support all subsystems. See *Event Logging System Messages Guide* for a list of currently supported subsystems.

Filter

Use the **filter** command to access the filter configuration command environment. See "ELS Net Filter Configuration Commands" on page 132 for complete command details.

Syntax:

filter	net

List

Use the **list** command to get updated information regarding ELS settings and listings of selected messages.

Syntax:

list	all
	filter-status
	groups
	pin
	remote-log status
	status
	subsystem . . .
	subsystems all
	trace-status

all Lists information from all the **list** categories.

filter-status
Lists ELS net number filters.

groups
Lists the user-defined group names and contents.

pin Lists the current number of ELS event messages sent in SNMP traps (per second).

remote-log status
Lists the current values of remote logging options.

Example:

```
list r

Remote Logging is ON
Source IP Address = 192.67.38.2
Remote Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_DAEMON
Default Syslog Priority Level = LOG_CRIT
Number of Messages in Remote Log = 256
Remote Logging Local ID = MYHOSTNAME
```

status Lists the subsystems, groups, and events that have been modified by the **display**, **nodisplay**, **trap**, **notrap**, **trace**, **notrace**, **remote**, and **noremote** commands.

Example:

```
list status

Subsystem:              TKR
Disp Levels:            STANDARD
Trap levels:            none
Trace levels:           none
Remote levels:          ERROR INFO TRACE
Syslog Facility/Level: LOG_USER LOG_INFO

Group        Disp     Trap    Trace  Remote
Mygroup     Unset    Unset    Unset    On
                                      Syslog Facilty/Level: LOG_DAEMON LOG_CRIT

Event        Disp     Trap    Trace  Remote
IP.007      Unset    Unset    Unset    On
                                      Syslog Facility/Level: LOG_CRON LOG_NOTICE
```

Note: Not only is remote logging enabled, but the display includes the Syslog Facility/Level values for each subsystem, group, and event. Ranges of events are listed as individual events.

subsystem

Lists names, events, and descriptions of all subsystems.

(Example output from a **list subsystem** command can be found beginning on page 143.)

subsystem *subsystem*

Lists all events in a specified subsystem.

Example:

```
list subsystem gw


Event      Level      Message

GW.001     ALWAYS   Copyright 1984 Mass Institute of Technology
GW.002     ALWAYS   Portable CGW %s Rel %s strtd
GW.003     ALWAYS   Unus pkt len %d nt %d int %s/%d
GW.004     ALWAYS   Sys %s q adv alloc %d excd %d
GW.005     ALWAYS   Bffrs: %d avail %d idle   fair %d low %d
GW.006     C-INFO    Pkt frm nt %d int %s/%d for uninit prt, disc
GW.007     C-INFO    Ip err %x nt %d int %s/%d
GW.008     U-INFO    Ip ovfl nt %d int %s/%d, disc
GW.009     UI-ERROR  Nt dwn ip rstrt nt %d int %s/%d
GW.010     UI-ERROR  Ip q len %d no ip buf nt %d int %s/%d
GW.011     U-INFO    Op err %x hst %wo nt %d int %s/%d
GW.012     U-INFO    Op err cnt excd hst %wo nt %d int %s/%d
GW.013     U-INFO    Rtrns cnt excd hst %wo nt %d int %s/%d
GW.014     UI-ERROR  Nt dwn op rstrt nt %d int %s/%d
GW.015     UI-ERROR  Nt dwn to hst %wo nt %d int %s/%d
GW.016     U-INFO    Op ovfl to hst %wo nt %d int %s/%d
GW.017     UE-ERROR  Intfc hdw mssng nt %d int %s/%d
GW.018     U-TRACE   Strt nt slf tst nt %d int %s/%d
GW.019     C-INFO    Slf tst nt %d int %s/%d
GW.020     U-TRACE   Nt pss slf tst nt %d int %s/%d
GW.021     UE-ERROR  Nt up nt %d int %s/%d
GW.022     U-TRACE   Nt fld slf tst nt %d int %s/%d
```

subsystems all

Lists all events in all subsystems.

trace-status

Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay event. . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*

Suppresses the displaying of a specified event (*subsystem.event#*).

group *groupname*

Suppresses the displaying of messages that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*

Suppresses the displaying of messages associated with the specified subsystem.

Noremote

Use the **noremote** command to suppress the logging of events to a remote workstation based on event number, group, range of events, or subsystem.

Note: With the **noremote** command, there is usually no need to specify a *syslog_facility* and *syslog_level*, such as there is with the **remote** command. However, for **noremote subsystem** command, there exists the option of selectively suppressing specific message levels (for example, “error” only or “trace” only) rather than turning them all off. (If you do not specify any

particular message level, “all” is assumed). Additionally, with the **noremote subsystem** command, you can set a *syslog_facility* and *syslog_level* for any remaining message levels that have not been turned off.

Syntax:

noremote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.019, gw.020, gw.021, and gw.022

subsystem *subsystem.name [syslog_facility syslog_level]*
Suppresses the remote logging of messages associated with the specified subsystem (*subsystem.name*).

Example 1:

```
noremote subsystem tkr
```

Suppresses the remote logging of all “tkr” messages.

Example 2:

```
ELS config> noremote subsystem tkr info
ELS config> SYSLOG FACILITY[LOG_USER]?
ELS config> SYSLOG LEVEL[LOG_INFO]?
```

In this example, “LOG_USER” and “LOG_INFO” were the values last picked for subsystem TKR. The command specified turns off the remote logging for subsystem TKR only for messages coded for “info”. Because *syslog_facility* and *syslog_level* was not specified, the software prompts for *syslog_facility* and *syslog_level*. If you enter another value at the prompts, that value will replace *syslog_facility* and *syslog_level* for the remaining remote-logged messages for the TKR subsystem.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

For more information about *syslog_facility* and *syslog_level* see “Remote” on page 125.

Notrace

Disables packet trace for the specified event/range/subsystem/group.

Syntax:

notrace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of packet trace data for the specified event#

group *groupname*
Suppresses the sending of packet trace data that was previously added to the specified group (groupname).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
trace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname*
Suppresses the sending of packet trace data for the specified subsystem (subsystemname).

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*
Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname*
Suppresses the sending of messages in SNMP traps that are associated with the specified subsystem.

Remote

Use the **remote** command to select the events to be logged to a remote workstation by event number, range of events, group, or subsystem.

Syntax:

remote event . . .
range . . .
group . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*
Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert

log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM 8371. They are merely identifiers which are used by the syslog daemon on the remote workstation.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 125.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely on the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

group *group.name syslog_facility syslog_level*

Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 125.

subsystem *subsystem.name message_level syslog_facility syslog_level*

Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely at the files based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 125.

Message_level is a value such as “ALL,” “ERROR,” “INFO,” or “TRACE”. See “Logging Level” on page 101. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem TKR all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely based on log_user and log_info values at the remote host.

Use the **list all** or **list status** commands to display what you have set with the **noremote** and **remote** commands.

Set

Use the **set** command to set the maximum number of tags per second, the timestamp feature, or to set tracing options.

Syntax:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin *max_traps*

Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number (*max_traps*) is sent every tenth of a second.)

remote-logging

Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
no-msgs
remote_ip_addr . . .
source_ip_addr ...
local_id

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the 'remote' command will be prevented from being logged.

facility

Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon

log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

no-msgs
Specifies the number of messages in the buffer for the remote log before log wraps.

remote_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255. It represents the ip address of the remote host where the log files reside.

source_ip_addr
This is an ip address of the form xxx.xxx.xxx.xxx where xxx can be any integer 0 to 255.

You should use an IP address that is configured in the 8371 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

local_id
This is any character string of up to 32 characters, which is

included in the logged message at the remote file and can help identify which machine logged the message.

timestamp [timeofday or uptime or off]
Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the device was last initialized) appears next to each message. Set timestamp can also be turned off.

Use the **set timestamp** command to enable one of the following timestamp options.

timeofday
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

trace Use the **set trace** command to configure tracing options. If you configure tracing options from the monitoring environment, the changes take effect immediately. They return to their previously configured settings when the device is rebooted.

Note: Tracing should be used only under the direction of trained support personnel. Tracing, especially when used with disk-shadowing enabled, uses device resources and can impact overall performance and throughput.

Syntax:

set trace decode
default-bytes-per-pkt
disk-shadowing
max-bytes-per-pkt
memory-trace-buffer-size
off
on
reset
stop-event
wrap-mode

decode *off/on*
Turns packet decoding on or off. Packet decoding is not supported by all components.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing [[off or on] or record-size or time-limit or delete-file or max-file-size]

Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

[off or on]

Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it can no longer be viewed from the monitoring.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

disk-shadowing delete-file

Deletes the trace file.

disk-shadowing max-file-size *Mbytes*

Sets the maximum file size for the trace file.

Valid Values: 1 Mbyte to 16 Mbytes

Default Value: 10 Mbytes

disk-shadowing record-size *bytes*

Sets the record size for trace file records:

Valid Values 1024, 2048, or 4096 bytes

Default 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

disk-shadowing time-limit *hours*

Sets the maximum time for disk-shadowing of traces:

Valid Values 1 - 72 hours

Default 24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

max-bytes-per-pkt *bytes*

Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*

Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

wrap-mode [off or **on]**
Turns the trace buffer wrap mode on or off. If wrap mode is on and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Trace

Enables packet trace for the specified event/range/subsystem/group. When the **trace** command is used from the `ELS Config>` prompt, the changes become part of the configuration, and a reboot is required to activate the changes.

Syntax:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the device monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the device monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the device.

ELS Net Filter Configuration Commands

ELS net filters give you the capability of looking only at ELS messages with certain net numbers and discarding other ELS messages.

When you create a filter, you specify the subsystem, event, or range of events to which the filter applies. You also specify the queue (for example, “DISPLAY”, “TRAP”, “TRACE”, or “REMOTE-LOGGING”). Finally, you specify the net number (or range of net numbers) that you want to filter.

When you enable the filter, messages that have been turned on by the ELS commands are subject to filtering. The filter allows only messages with the specified net numbers. The filter causes the device to discard messages that do not contain the specified net numbers.

By reducing the number of ELS messages sent, you can more easily locate messages for the interfaces in which you are interested.

This section describes the commands to configure the ELS net filters. To configure these filters, enter the **filter net** command at the ELS> prompt. Then, enter the configuration commands at the `ELS Filter net>` prompt.

Table 20. ELS Net Filter Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Creates a filter and assigns it a number. A maximum of 64 filters is allowed.
Delete	Deletes a specified filter number or all filters.
Disable	Disables a specified filter number or all filters.
Enable	Enables a specified filter number or all filters.
List	Lists a specified filter number or all filters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **create** command to create an ELS net filter.

Syntax:

create ***queue*** event *event_name net#_start net#_end*
range *event_range net#_start net#_end*
subsystem *subsystem_name net#_start net#_end*

queue The queue for which you are setting the filter. The valid queues are:

Display
Trace
Trap
Remote

event *event_name net#_start net#_end*
Specifies the event and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **`create trap event GW.009 2 10`** filters traps for message GW.009 for net numbers 2 through 10.

range *event_range net#_start net#_end*
Specifies the range of ELS messages and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create remote range ipx 19 22 3 6** filters all ipx messages beginning with IPX.019 and ending with IPX.022 for net numbers 3 through 6 for remote logging.

subsystem *subsystem_name net#_start net#_end*
Specifies the subsystem and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **create display subsys ip 1 1**, filters all ELS messages for the ip subsystem that contain net number 1 to the display. All other ip subsystem messages are discarded.

Delete

Use the **delete** command to delete a specific ELS filter or all ELS filters.

Syntax:

delete all
filter *filter#*

all Deletes all currently configured filters.

filter *filter#*
Deletes the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to delete.

Disable

Use the **disable** command to disable a specific ELS filter or all ELS filters.

Syntax:

disable all
filter *filter#*

all Disables all currently configured filters.

filter *filter#*
Disables the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to disable.

Enable

Use the **enable** command to enable a specific ELS filter or all ELS filters.

Syntax:

enable all
filter *filter#*

all Enables all currently configured filters.

filter *filter#*
Enables the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to enable.

List

Use the **list** command to list a specific ELS filter or all ELS filters.

Syntax:

list all
filter *filter#*

all Lists all currently configured filters.

filter Lists the filter specified by *filter#.*

ELS Message Buffering Configuration Commands

Table 21 describes the commands available at the `ELS Config Advanced>` prompt.

Table 21. ELS Message Buffering Configuration Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Displays the configuration settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Config Advanced> list status
---------------------------------Configuration-----------------------------------
Logging Status:    OFF    Wrap Mode:   ON  Logging Buffer Size:    8500   Kbytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  NONE
```

See “Set” on page 137 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log event
group

range

subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event

group

range

subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Set

Use the **set** command to configure various ELS message buffering options.

Syntax:

set buffer-size *Kbytes*
logging [on or off]
stop action . . .
stop event *subsystem.event#*
stop string *text*
wrap on or off]

buffer-size *Kbytes*
Specifies the size, in kilobytes, of the message buffer that the system should allocate. The **mem** command displays this memory as Never Alloc. Setting this value too high could prevent the device from operating correctly after a reboot because of insufficient memory for protocols and features.

Valid values: 0 KB to 80% of the memory available on the device.

Default value: 0 (no message buffering)

Note: You must allocate a buffer with this command before you can set logging on.

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the “stop event” (and if specified, the “stop string”) occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard drive . If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

ELS Configuration Commands (Talk 6)

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified “stop action.”

Logging remains stopped until the next time you issue the **set logging on** command or reboot the device.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**
Specifies the string to be used in conjunction with the “stop event” to stop logging. If you have not specified a stop event, the system ignores the “stop string.”

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the “stop string.”

Default value: none

wrap [on or **off]**
Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Entering and Exiting the ELS Operating Environment

The ELS monitoring environment (available from the GWCON process) is characterized by the ELS> prompt. Commands entered at this prompt modify the current ELS parameter settings. These commands are described “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 117.

To enter the ELS monitoring environment from OPCON:

1. Enter the **console** command.

   ```
   * console
   ```

   The monitoring displays the GWCON prompt (+). If the prompt does not appear when you first enter GWCON, press **enter**.
2. At the GWCON prompt, enter the following command to access ELS:

   ```
   + event
   ```

   The monitoring displays the ELS monitoring prompt (ELS>). Now, you can enter ELS monitoring commands.

To leave the ELS monitoring environment, enter the **exit** command.

ELS Monitoring Commands

This section summarizes and then explains all the ELS monitoring commands. After accessing the ELS Monitoring environment, you can enter ELS monitoring commands at the ELS> prompt.

Table 22. ELS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Advanced	Places you in the advanced configuration environment in which you can configure message buffering.
Clear	Resets to zero the counts of messages associated with specified events, groups, or subsystems.
Display	Enables message display on the console.
Exit	Exits the ELS console process and returns the user to GWCON.
Filter	Filter ELS messages based upon the net number.
List	Lists information on ELS settings and messages.
Nodisplay	Disables message display on the console.
Noremote	Disables remote logging to file at remote workstation.
Notrace	Disables trace event display on the console.
Notrap	Keeps messages from being sent out in SNMP traps to the network management workstation.
Packet-trace	Provides an enhanced central environment for setting and listing active packet tracing parameters.
Remote	Allows messages to be logged at a file on a remote workstation.
Remove	Frees up memory by erasing stored information.
Restore	Clears current settings and reloads initial ELS configuration.
Retrieve	Reloads the saved ELS configuration.
Save	Stores the current configuration.
Set	Sets the pin parameter and the timestamp feature.
Statistics	Displays available subsystems and pertinent statistics.
Trace	Enables trace event display on the console.
Trap	Allows messages to be sent to a network management workstation in SNMP traps.
View	Allows viewing of traced packets.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Advanced

Use the **advanced** command to enter the advanced monitoring environment. In this environment you change message buffering operation.

Syntax:

advanced

Clear

Use the **clear** command to reset to zero the counts of the display, trace, trap, or remote commands as they relate to specific events, groups or subsystems.

Syntax:

clear event . . .
group . . .
subsystem . . .

event *subsystem. event#*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified event (*subsystem.event#*).

group *group.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified group (*group.name*).

subsystem *subsystem.name*
Resets the count of events to zero for displaying, trapping, tracing or remote logging of the specified subsystem (*subsystem.name*).

Display

Use the display command to enable the message display on the monitoring monitor for specific events.

Syntax:

display event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Displays messages for the specified event (subsystem.event#).

group *groupname*
Displays messages of a specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event in the specified event range.

Displays a range of messages for the specified subsystem.

Example:

```
display range gw 19 22
```

Displays events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Displays any messages associated with the specified subsystem (*logging level*). If you do not specify a logging level, all messages for that subsystem are turned on.

Files Trace TFTP

Use the **files trace tftp** command to retrieve trace files from the subdirectory associated with:

- The currently active bank (bank A or bank B on the hard disk)
- Bank A on the hard disk

- Bank B on the hard disk
- The trace file stored in the Network Subdirectory (if there is no active bank)

Syntax:

files trace tftp active-bank ...
bank-a ...
bank-b ...
net-subdir ...

You are prompted for the *remote server IP address* and the *remote path/file name*.

active-bank
Retrieves the traces file from the currently active bank

bank-a
Retrieves the trace file from bank A

bank-b
Retrieves the trace file from bank B

net-subdir
Retrieves the trace file stored in the Network Subdirectory (if there is no active bank)

Files

Use the **files** command to transfer trace files to another host on the network using TFTP.

Syntax:

files trace tftp *host_IP_addr filename*

host_IP_addr
Is the IP address of the host to which you are transferring the files.

filename
Is the target file name. For TFTP, the file name must be fully path specified, and the file name must already exist on the target host.

Filter

Use the **filter** command to access the filter configuration command environment. See “ELS Net Filter Monitoring Commands” on page 161 for complete command details.

Syntax:

filter net

List

Use the **list** command to get updated information regarding ELS settings and to get listings of selected messages.

Syntax:

list

- all
- active . . .
- event . . .
- filter-status
- groups . . .
- pin
- remote-log status
- subsystem . . .
- trace-status

all Lists all subsystems, defined groups, enabled subsystems, enabled events, and pins.

active *subsystem.name*
Displays the events that are active for a specific subsystem or have non-zero message counts.

Example:

```
list active ip
Event      Active  Count  Message

IP.007              2874  %I -> %I
IP.022                13  add nt %I int %I nt %n int %s/%d
IP.036              2874  rcv pkt prt %d frm %I
IP.058                23  del nt %I rt via %I nt %n int %s/%d
IP.068     D          37  routing cache cleared
D=Display on   T=Trap on   P=Packet Trace on   F=Filter on  R=Remote Logging on
A=Advanced on
```

If Remote logging is turned on, those events displayed as active for a subsystem will have an “R” next to their name.

event *subsystem.event#*
Displays the logging level, the message, and the count of the specified event.

Example:

```
list event ip.007

Level: p-TRACE
Message: source_ip_address -> destination_ip_address
Active:  Count: 84182
```

If Remote-logging had been activated for this event, and the *syslog_facility* and *syslog_level* values were log_daemon and log_crit, the last lines would look like:

```
Active:  R count:84182
Syslog Facility: log_daemon   Syslog Level: log_crit
```

filter-status
Lists ELS net number filters.

groups *group.name*
Displays the user-defined group names.

pin Lists the current number of ELS event messages sent per second in SNMP traps. This is a threshold value that can be used to reduce the amount of SNMP trap traffic.

Example:

```
list pin

Pin: 100 events/second
```

remote-log status

Lists the current values of the remote logging options set in the **set remote-logging** command.

Example:

```
list r

Remote Logging is On
Source Ip Address = 192.9.200.8
Remote  Log IP Address = 192.9.200.1
Default Syslog Facility = LOG_USER
Default Syslog Priority Level = LOG_INFO
Number of Messages in Remote Log = 256
Remote Logging Local ID =  SPHINX
```

subsystem *subsystem.name*

Lists event names, the total number of events that have occurred, and their descriptions.

Note: Although ELS supports all subsystems on the device, not all devices support all subsystems. See *ELS Messages* for a list of currently supported subsystems.

subsystem *subsystem.name*

Lists all events, logging levels, and messages for the specified subsystem.

Example:

```
list subsystem eth

Event      Level      Message
ETH.001    P-TRACE    brd rcv unkwn type packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.002    UE-ERROR   rcv unkwn typ packet_type source_Ethernet_address ->
                      destination_Ethernet_address nt network
ETH.010    C-INFO     LLC unk SAP DSAP source_Ethernet_address ->
                      destination_Ethernet_address nt network
```

subsystem all

Lists all events, logging levels, and messages for every event that has occurred on the device.

trace-status

Displays information on the status of packet tracing, including configuration and run-time information.

Example:

```
list trace-status

------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
------------------------ Run-time Status ---------------------------
Packets in RAM Trace Buffer:1   Free Trace Buffer Memory:99958
Trace Errors:0  First Packet:1  Last Packet:1
Trace Records Stored on HD:8  Trace Buffer File Size:16560
HD-Shadowing Time Exceeded? NO Elapsed Time:  0 hr,  0 min, 10 sec
Has Stop Trace Event Occurred? NO
```

- “Trace Status” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs.
- “HD Shadowing” in the LIST TRACE-STATUS display will indicate OFF when STOP-ON-EVENT action occurs or when Time Limit is exceeded.
- “Trace Buffer File Size” will display <wrapped> when a wraparound has occurred in the trace file.

- If disk-shadowing time limit is exceeded, but there has not been a trace record written since the time expired, then " HD-Shadowing Time Exceeded? NO < Next trace will turn it OFF>" will be displayed. When the next trace record has been written, then "HD-Shadowing Time Exceeded? YES" will be displayed.

ELS Config>**LIST TRACE** command under **talk 6** displays information similar to the following:

```
------------------------ Configuration -----------------------------
Trace Status:ON  Wrap Mode:ON  Decode Packets:ON  HD Shadowing:ON
RAM Trace Buffer Size:100000  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: TCP.013
Maximum Hours to HD Shadow:  1
```

Nodisplay

Use the **nodisplay** command to select and turn off messages displaying on the console.

Syntax:

nodisplay event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Suppresses the displaying of messages for the specified event.

group *group.name*
Suppresses the displaying of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the displaying of a range of messages for the specified subsystem.

Example:

```
nodisplay range gw 19 22
```

Suppresses the display of events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystem.name*
Suppresses the displaying of messages associated with the specified subsystem (*logging level*).

Noremote

Use the **noremote** command to select and turn off messages logging to a remote workstation.

Syntax:

noremote event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
Suppresses the remote logging of messages for the specified event.

group *group.name*
Suppresses the remote logging of messages that were previously added to the specified group (*group.name*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the remote logging of a range of messages for the specified subsystem.

Example:

```
noremote range gw 19 22
```

Suppresses the remote logging of events gw.19, gw.20, gw.21, and g.22

subsystem *subsystem.name*
Suppresses the remote logging of messages associated with the specified subsystem (*logging level*).

Example:

```
noremote subsystem tkr
```

Note: With noremote, there is no need to specify a Syslog Facility and Level, such as there is with Remote.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Notrace

Use the **notrace** command to stop display of selected trace events at the monitoring.

Syntax:

notrace

event . . .

group . . .

range . . .

subsystem . . .

event *subsystem.event#*
Suppresses the display of the specified tracing event.

group *groupname*
Suppresses the display of tracing events related to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Disables the sending of packet trace data for a range of messages for the specified subsystem.

Example:

```
notrace range gw 19 22
```

Suppresses the sending of packet trace data for events gw.19, gw.20, gw.21, and gw.22.

subsystem *subsystemname [logging-level]*

Suppresses the display of tracing events that are associated with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress tracing for all logging levels for the subsystem.

Example:

```
notrace subsystem frl error

notrace subsystem frl
```

Notrap

Use the **notrap** command to select and turn off messages so that they are no longer sent to a network management workstation in SNMP traps.

Syntax:

notrap event. . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*

Suppresses the sending of the specified message in an SNMP trap (*subsystem.event#*).

group *groupname*

Suppresses the sending of messages in SNMP traps that were previously added to the specified group (*groupname*).

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Suppresses the sending of messages for the events in the specified range for the specified subsystem in SNMP traps.

Example:

```
notrap range gw 19 22
```

Suppresses the sending of messages for events gw.19, gw.20, gw.21, and gw.22 in SNMP traps.

subsystem *subsystemname [logging-level]*

Suppresses the sending of messages in SNMP traps that are associated

with the specified subsystem and logging level. If you do not specify a *logging-level* you suppress trapping for all logging levels for the subsystem.

Example:

```
notrap subsystem eth error
```

Packet Trace

Use the **packet-trace** command to display/enable/disable packet tracing information for various subsystems.

Syntax:

packet-trace

Use the **Exit** command when you are finished using Packet Trace.

For complete command descriptions, see “Packet-trace Monitoring Commands” on page 159.

Remote

Use the **remote** command to select the events to be logged to a remote file by event number, range of events, group, or subsystem.

Syntax:

remote event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event# syslog_facility syslog_level*

Causes the specified event to be logged remotely.

Syslog facility and level values are used by the syslog daemon in the remote workstation to determine where to log the messages. This value overrides the default values that are set with the **set facility** and **set level** commands.

syslog_facility

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user
log_uucp
log_local0-7

syslog_level

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

These values do NOT have any particular association with any daemons on the IBM 8371. They are merely identifiers which are used by the syslog daemon on the remote workstation.

Example:

```
remote event gw.019 log_user log_info
```

group *group.name syslog_facility syslog_level*

Allows events belonging to the specified group to be logged remotely based on the *syslog_facility* and *syslog_level* values. See “the remote event command” on page 147.

range *subsystemname first_event_number last_event_number syslog_facility syslog_level*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the events in the specified range for the specified subsystem to be remotely logged based on the *syslog_facility* and *syslog_level*. See “the remote event command” on page 147.

Example:

```
remote range gw 19 22 log_user log_info
```

Causes the event gw.19, gw.20, gw.21, and gw.22 to be logged remotely to the files specified by the *syslog_facility* value of log_user and the *syslog_level* value of log_info.

subsystem *subsystem.name message_level syslog_facility syslog_level*

Where *subsystem.name* is the name of the subsystem and *message_level* is the level of messages selected in the subsystem.

Causes the events within the specified *subsystem.name* whose *message_level* agrees with the specified *message_level* to be logged remotely based on the *syslog_facility* and *syslog_level*. See “the remote event command” on page 147.

Message_level is a value such as ALL, ERROR, INFO, or TRACE. See “Logging Level” on page 101. The value specified in the **remote** command must agree with the value as coded on the particular event within the subsystem, or that event within the subsystem will not be remotely logged.

Example:

```
remote subsystem eth all log_user log_info
```

In the above example, all messages in subsystem TKR (“all” includes any messages coded for “error,” “info,” or “trace”) will be logged remotely to files specified by log_user and log_info at the remote host.

Use the **list event** and **list active** commands to verify what you set with the **remote** and **noremote** commands.

Remove

Use the **remove** command to free up memory by erasing stored information. If you have previously saved the current configuration with the **save** command, remove allows you to erase the saved configuration.

Syntax:

remove

Restore

Use the **restore** command to clear all current settings (except counters) and reload the initial ELS configuration. To retain the current settings, use the **save** command before restoring the initial configuration.

Syntax:

restore

Retrieve

Use the **retrieve** command to reload the saved ELS configuration. If you have previously saved the current configuration with the **save** command, use **retrieve** to reload it. **Retrieve** does not erase the saved configuration after it executes. To erase the saved configuration, use the **remove** command.

Syntax:

retrieve

Save

Use the **save** command to store the current configuration (except counters). **Save** does not affect the default configuration (the one you set with the configuration commands). Use **save** after modifying the configuration with the monitoring commands with the intention of saving this configuration over a restart. There can be only one saved configuration at a time. To reload the saved configuration, use the **retrieve** command.

Syntax:

save

Set

Use the **set** command to set the maximum number of traps per second, to set the timestamp feature, or to set the tracing options.

ELS Monitoring Commands (Talk 5)

Syntax:

set pin . . .
remote-logging . . .
timestamp . . .
trace . . .

pin Use the **set pin** command to set the pin parameter to the maximum number of traps that can be sent on a per-second basis. Internally, the pin resets every tenth of a second. (One tenth of the number *max_traps* is sent every tenth of a second.)

remote-logging
Use the **set remote-logging** command to configure remote logging options. When these options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set remote-logging on
off
facility . . .
level . . .
local_id
remote_ip_addr . . .
source_ip_addr ...

on Turns remote logging on. Remote logging is now enabled to allow any messages selected by the **remote** command to be actively logged.

off Turns remote logging off. All messages selected by the **remote** command will be prevented from being logged.

facility
Specifies a value that, in combination with the *level* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog facility values:

log_auth
log_authpriv
log_cron
log_daemon
log_kern
log_lpr
log_mail
log_news
log_syslog
log_user

log_uucp
log_local0-7

level Specifies a value that, in conjunction with the *facility* value, is used by the syslog daemon in the remote workstation to determine where to log messages. This value is used for all remotely-logged ELS messages unless you specify a different value for a particular ELS event, range, group, or subsystem with the **remote** command.

These are all possible syslog level values:

log_emerg
log_alert
log_crit
log_err
log_warning
log_notice
log_info
log_debug

local_id
Specifies a 1-32 character identifier that appears in the remote logging message that you can use to identify which machine logged a particular message.

remote_ip_addr
This is an IP address of the remote host where the log files reside.

source_ip_addr
Specifies the IP address of the machine that originated the message that is being remotely-logged.

You should use an IP address that is configured in the 8371 for easier identification when the IP address or the hostname is shown in the remotely-logged ELS message. You should also verify that this IP address is quickly resolved to a hostname by the name server, or at least that the name server responds quickly with "address not found."

To determine that the IP address resolves properly enter the **host** command on your workstation as shown:

```
workstation>host 5.1.1.1
host: address 5.1.1.1 NOT FOUND
workstation>
```

If the response takes more than 1 second, select an IP address that resolves more quickly.

timestamp
Allows you to turn on message timestamping so that either the time of day or uptime (number of hours, minutes, and seconds, but no date, since the device was last initialized) appears next to each message, or to turn off message timestamping.

Note: If you turn on timestamping, you must remember to go back into the CONFIG process and set the device's date and time using the time command. Otherwise, all messages will come out with 00:00:00, or negative numbers in the hours, minutes, and/or seconds, for example 00:-4:-5.

Use the **set timestamp** command to enable one of the following timestamp options:

timeofday
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 24-hour day.

uptime
Adds an HH:MM:SS prefix to each ELS message indicating the time of the occurrence during a 100-hour cycle of uptime for the device. After 100 hours of uptime, the uptime counter returns to zero to begin another 100-hour cycle.

off Turns off the ELS timestamp prefix.

Syntax:

set timestamp [timeofday or uptime or off]

trace Use the **set trace** command to configure tracing options. When tracing options are configured from the monitoring environment, the changes take effect immediately, and return to their previously configured settings when the device is rebooted.

Syntax:

set trace decode . . .
default-bytes-per-pkt . . .
disk-shadowing . . .
max-bytes-per-pkt . . .
memory-trace-buffer-size . . .
off
on
reset
stop-event . . .
wrap-mode . . .

decode . . .
Sets packet decode options. Packet decoding is not supported by all components.

exclude
Excludes the specified frame type for decode. The possible frame types for exclusion are:

lecontrol
LE Control

ip IP

arp ARP

ipx IPX

netbios
NetBIOS

bpdu BPDU

appletalk
AppleTalk

aarp AppleTalk ARP

hex Turns off printing of hexadecimal frame data.

summary
Turns off printing of a one-line summary decode. A complete decode is printed.

all Excludes all packet types from the trace. No frame types are decoded.

none Excludes no packet types from the trace. *exlcude all*.

include
Includes the specified frame type for decode. The possible frame types for inclusion are:

lecontrol
LE Control

ip IP

arp ARP

ipx IPX

netbios
NetBIOS

bpdu BPDU

appletalk
AppleTalk

aarp AppleTalk ARP

hex Turns on printing of hexadecimal frame data.

summary
Turns on printing of a one-line summary decode. A complete decode is not printed.

all Includes all packet types in the trace.

none Includes no packet types in the trace. This is the opposite of *include all*.

off Sets decoding off.

on Sets decoding on.

Note: The default setting is to print complete decode output for all frame types. Use the **list trace-status** command to see the current decode settings. See page 143.

default-bytes-per-pkt *bytes*
Sets the default number of bytes traced. This value is used if a value is not specified by the component doing the tracing.

disk-shadowing [[off or on] or [delete-file or *record-size* **or** *time-limit*]]
Turns disk shadowing on or off, sets the maximum trace file size, or sets the maximum time for disk-shadowing traces.

[off or on]

Turns disk shadowing on or off. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it can no longer be viewed from the monitoring.

Note: Disk shadowing should be set to OFF whenever the WRITE, TFTP software, RETRIEVE system dump, or COPY software commands are issued.

Turns disk shadowing on or off and sets the maximum trace file size. If disk shadowing is enabled, trace records are copied to the hard disk. Once a traced record is copied to the hard disk, it is no longer viewable through the monitoring.

record-size *bytes*

Sets the record size for trace file records:

Valid Values: 1024, 2048, or 4096 bytes

Default: 2048 bytes

Notes:

1. If a trace file already exists, “Cannot change Record Size without first deleting the existing Trace File” is displayed and record size is not changed.
2. If you configure a record size and a trace file already exists, the trace will use the record size of the existing file.

delete-file

Deletes the trace file (in the subdirectory associated with the active bank only).

Note: If disk shadowing is ON when the command is issued, “ Disk-shadowing must be set to OFF before trace file can be deleted” is displayed and the file is not deleted.

time-limit *hours*

Sets the maximum time for disk-shadowing of traces:

Valid Values:

1 - 72 hours:

Default

24 hours

Note: Disk shadowing stops (tracing continues) after this time has elapsed. The actual time is reset to 0 when disk shadowing is turned on again.

max-bytes-per-pkt *bytes*

Sets the maximum number of bytes traced for each packet.

memory-trace-buffer-size *bytes*

Sets the size, in bytes, of the RAM trace buffer.

Valid Values: 0, ≥10,000

Default Value: 0

off Disables packet tracing.

on Enables packet tracing.

reset Clears the trace buffer and resets all associated counters.

stop-event *event id*
Stops tracing when an event (event id) occurs. Enter either an ELS event id (for example: TCP.013) or “None”. “None” is the default. Tracing stops only if the display of the particular ELS event is enabled.

When a stop-event occurs, an entry is written to the trace buffer. The **view** command for this trace entry will display “Tracing stopped due to ELS Event Id: TCP.013”.

After tracing stops due to a stop-event, you must re-enable tracing with the **set trace on** command. (A restart will also re-enable tracing if enabled from the `ELS Config>` prompt.)

Example:

```
set trace stop-event TCP.013
```

wrap-mode *off/on*
Turns the trace buffer wrap mode on or off. When wrap mode is enabled and the trace buffer is full, previous trace records will be overwritten by new trace records as necessary to continue tracing.

Statistics

Use the **statistics** command to display a list of all of the available subsystems and their statistics.

Note: The following example may not match your display exactly. The output of the command depends on the version and release of the installed software.

Syntax:

statistics

Example:

```
statistics

Subsys  Vector  Exist   String  Active    Heap

  GW     105     101      3411     0         0
 FLT      20       7       184     0         0
 BRS      50       5       201     0         0
 ARP     150     142      7030     0         0
  IP     100     100      2463     2        20
ICMP      30      21       529     0         0
 TCP      60      57      2420     0         0
 UDP      10       6       179     0         0
 BTP      40      13       695     0         0
 RIP      30      22       474     0         0
OSPF      80      73      2859     0         0
MSPF      40      17       593     0         0
TFTP      35      29       819     0         0
SNMP      30      28       821     0         0
 DVM      30      21       589     0         0
  DN     140     115      5842     0         0
  XN      35      21       780     0         0
 IPX     110     110      4705     0         0
CLNP      80      58      1763     0         0
ESIS      40      24       716     0         0
ISIS      80      58      2422     0         0
DNAV      50      26      1314     0         0
```

```
 AP2      80      70      1755     0         0
ZIP2      60      51      1859     0         0
R2MP      50      38      1185     0         0
 VIN      90      79      3159     0         0
 SRT     120      94      5040     0         0
 STP      60      32      1590     0         0
  BR      50      30      1616     0         0
SRLY      30      28      1409     0         0
 ETH      60      47      1098     0         0
  SL      50      35       584     0         0
 TKR      60      45      2031     0         0
 X25      70      53      1909     0         0
FDDI      30      27      1155     0         0
SDLC     100      95      4263     0         0
 FRL     130      97      6068     0         0
 PPP     190     186      6394     0         0
X251      50      16       546     0         0
X252      50      34       996     0         0
X253      50      42      1649     0         0
ISDN      50      43      1994     0         0
IPPN      20       4       132     0         0
 WRS      40      33      1938     0         0
 LNM      70      60      3137     0         0
 LLC     170     168      9840     0         0
 BGP      80      74      2477     0         0
 MCF      15       9       244     0         0
 DLS     500     497     24340     0         0
 V25B     30      28      1058     0         0
 BAN      30      29      1223     0         0
 COMP     80      26      1050     0         0
 NBS     100      50      3029     0         0
 ATM     300     216     10808     0         0
 LEC     200     174      7258     0         0
APPN     100      28       467     0         0
ILMI     150      23       487     0         0
SAAL      30      26       621     0         0
 SVC      30      26       465     0         0
 LES     400     361     22333     0         0
LECS     150     145      5666     0         0

EVLOG      1       1       105     0         0
 NOT      25      15       508     0         0
NHRP     250     211      8193     0         0
 XTP      64      58      2271     0         0
 ESC     150      67      3122     0         0
 LCS      40      22       858     0         0
 LSA      70      61      3506     0         0
 MPC     130      30      1677     3        44
SCSP      40      34      1234     0         0
ALLC      50      36      1842     0         0
 NDR      50      38      1150     0         0
 MLP     100      93      4006     0         0
 SEC      50      30       688     0         0
ENCR     100       4       194     0         0
  PM      25       6       120     0         0
 DGW      20       9       238     0         0
QLLC      55      54      2411     0         0

Total   6490    4942    215805     5        64

Maximum:7976 vector, 155 subsystem
Memory:71784/620 vector+ 81256/217714 data+ 64 heap=371438Subsys
```

Subsys
Name of subsystem

Vector
Maximum size of subsystem

Exist Number of events defined in this subsystem

String Number of bytes used for message storage in this subsystem

Active Number of active (displayed, trapped, or counted) events in the subsystem

Heap Dynamic memory in use by subsystem

Trace

Use the **trace** command to select the trace events to be displayed on the system monitoring. This command provides function that is similar to the **packet trace** command described in “Packet-trace Monitoring Commands” on page 159.

Syntax:

trace event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified trace event (*subsystem.event#*) to be displayed on the system monitoring.

group *groupname*
Allows trace events that were previously added to the specified group to be displayed on the device monitoring.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_numbe*r is the number of the last event of the specified event range.

Causes the trace events in the specified range for the specified subsystem to be displayed on the system monitoring.

Example:

```
trace range gw 19 22
```

Causes the trace events gw.19, gw.20, gw.21, and gw.22 to be displayed on the system monitoring.

subsystem *subsystemname*
Allows trace events associated with the specified subsystem to be displayed on the device monitoring.

Trap

Use the **trap** command to select the message to be sent to the remote SNMP network management workstation. A remote SNMP network management workstation is an IP host in the network acting as an SNMP manager.

Syntax:

trap event . . .
group . . .
range . . .
subsystem . . .

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be sent to a network management workstation in an SNMP trap.

group *groupname*
Allows messages that were previously added to the specified group to be sent to a network management workstation in an SNMP trap.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be sent to a network management workstation in an SNMP trap.

Example:

```
trap range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be sent to a network management workstation in an SNMP trap.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be sent to a management station in an SNMP trap.

Note: Messages for the IP, ICMP, ARP and UDP subsystems cannot be sent in SNMP traps because these areas are or may be used in the process of sending the SNMP trap. This could lead to an infinite loop of traffic putting an undue strain on the device.

View

Use the **view** command to view traced packets.

Syntax:

view current
first
jump
last
next
prev
search ...

current
Displays the current trace packet. If the current packet is not valid, the first packet in the trace buffer is displayed.

first Displays the first traced packet in the trace buffer.

jump *n*
Displays the traced packet *n* packets ahead of or behind the current packet.

last Displays the last traced packet in the trace buffer.

next Displays the next traced packet.

prev Displays the previous traced packet.

search
Displays the next traced packet that contains the specified information. You can specify the search information by:

- Hexadecimal string
- IP address
- ASCII text

Packet-trace Monitoring Commands

This section describes the Packet-trace Monitoring commands. After accessing the Packet-trace Monitoring environment, you can enter Packet-trace Monitoring commands at the `ELS Packet Trace>` prompt.

Table 23. Packet Trace Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Off	Disables packet tracing.
On	Enables packet tracing. Prompts for memory trace buffer size if not previously set.
Reset	Clears the trace buffer and resets all associated counters.
Set	Configures tracing options.
Subsystems	Activates tracing for the subsystems that support packet tracing, or displays a summary.
Trace-status	Displays information on the status of packet tracing, including configuration and run-time.
View	Provides View Captured Packet Trace Buffers Console
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Off

Use the **off** command to disable packet tracing.

Syntax:

off

On

Use the **on** command to enable packet tracing.

Syntax:

on

Reset

Use the **reset** command to clear the trace buffer and reset all associated counters.

Syntax:

reset

Set

Use the **set** command to configure tracing options.

Syntax:

set	decode
	default-bytes-per-pkt
	disk-shadowing
	max-bytes-per-pkt
	memory-trace-buffer-size
	stop-event
	wrap-mode
	exit

For an explanation of the `set` command, see page 152.

Subsystems

Use the **subsystems** command to activate tracing for the subsystems that support packet tracing, or to display a summary.

Syntax:

subsystems	atm
	lec
	summary

Example:

```
subsystems atm
Network number? 0
ATM Interface is selected
on | off | list [list]? on
Note that SVC  uses VPI = 0, VCI = 5
and ILMI uses VPI = 0, VCI = 16
Beginning of VPI range [0]?
End of VPI range [0]?
Beginning of VCI range [0]? 16
End of VCI range [0]? 16
Tracing event ATM.88: ATM frames
```

Example:

```
subsystems lec
Network number? 1
ATM Emulated LAN is selected
on | off | list [list]? on
Trace which types of frames (data, control, both) [both]?
Tracing event LEC.11: data frames over ATM Forum LEC: interface 1
Tracing event LEC.12: control frames over ATM Forum LEC: interface 1
Note that if the user DISABLEs and TESTs this LEC interface,
the LEC trace settings from Talk 6 Config will take effect.

MAC Address packet filtering can be enabled under the LEC net
using the 'trace mac-address' command.
```

Example:

```
subsystems summary
Subsystems Being Traced

ATM        net number = 0, VPI Range:     0 -     0
                           VCI Range:    16 -    16
LEC        net number = 1
```

Trace-Status

Use the **trace-status** command to get updated information regarding packet trace.

Syntax:

trace-status

Example:

```
trace-status
------------------------ Configuration -----------------------------
Trace Status:OFF  Wrap Mode:OFF  Decode Packets:OFF  HD Shadowing:OFF
RAM Trace Buffer Size:0  Maximum Trace Buffer File Size:10000000
Max Packet Bytes Trace:256  Default Packet Bytes Traced:100
Trace File Record Size:2048  Stop Trace Event: None
Maximum Hours to HD Shadow:  24
----------------------- Run-time Status ---------------------------
Packets in RAM Trace Buffer:0   Free Trace Buffer Memory:0
Trace Errors:0  First Packet:0  Last Packet:0
Trace Records Stored on HD:0  Trace Buffer File Size:0
HD-Shadowing Time Exceeded? NO
Has Stop Trace Event Occurred? NO
```

View

Use the **view** command to enter the View Captured Packet Trace Buffers Monitoring.

For an explanation of the **view** commands, see “View” on page 158.

Syntax:

view	current
	first
	jump
	last
	next
	prev
	search
	exit

ELS Net Filter Monitoring Commands

This section describes explains the commands to manipulate ELS net filters. To enter the filter environment, enter the **filter net** command at the ELS> prompt. Enter the monitoring commands at the `ELS Filter net>` prompt.

Table 24. ELS Net Filter Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Create	Creates a filter and assigns it a number. A maximum of 64 filters is allowed.
Delete	Deletes a specified filter number or all filters.
Disable	Disables a specified filter number or all filters.
Enable	Enables a specified filter number or all filters.
List	Lists a specified filter number or all filters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Create

Use the **create** command to create an ELS net filter.

Syntax:

create *queue* event *event_name net#_start net#_end*

range *event_range net#_start net#_end*

subsystem *subsystem_name net#_start net#_end*

queue The queue for which you are setting the filter. The valid queues are:

Display

Trace

Trap

Remote

event *event_name net#_start net#_end*

Specifies the event and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **`create trap event GW.009 2 10`** filters traps for message GW.009 for net numbers 2 through 10.

range *event_range net#_start net#_end*

Specifies the range of ELS messages and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **`create remote range ipx 19 22 3 6`** filters all ipx messages beginning with IPX.019 and ending with IPX.022 for net numbers 3 through 6 for remote logging.

subsystem *subsystem_name net#_start net#_end*

Specifies the subsystem and net numbers that you are filtering.

If you specify *net#_start* and *net#_end* as the same number, you are filtering on a single net number.

The command **`create display subsys ip 1 1`**, filters all ELS messages for the ip subsystem that contain net number 1 to the display. All other ip subsystem messages are discarded.

Delete

Use the **delete** command to delete a specific ELS filter or all ELS filters.

Syntax:

delete all
filter *filter#*

all Deletes all currently configured filters.

filter *filter#*
Deletes the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to delete.

Disable

Use the **disable** command to disable a specific ELS filter or all ELS filters.

Syntax:

disable all
filter *filter#*

all Disables all currently configured filters.

filter *filter#*
Disables the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to disable.

Enable

Use the **enable** command to enable a specific ELS filter or all ELS filters.

Syntax:

enable all
filter *filter#*

all Enable all currently configured filters.

filter *filter#*
Enable the filter specified by *filter#*. Use the **list** command to obtain the number for the filter you want to enable.

List

Use the **list** command to list a specific ELS filter or all ELS filters.

Syntax:

list all
filter *filter#*

all Lists all currently configured filters.

filter *filter#*
Lists the filter specified by *filter#*.

ELS Message Buffering Monitoring Commands

Table 25 describes the commands available at the `ELS Config Advanced>` prompt.

Table 25. ELS Message Buffering Monitoring Commands

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Flush	Clears the message buffer and turns off logging to the message buffer.
List	Displays the operational settings for message buffering.
Log	Enables logging of selected messages to the message buffer.
Nolog	Turns off logging of selected messages to the message buffer.
Read-file	Reads a formatted message buffer from a file and displays it on the console.
Set	Sets the size of the message buffer, the wrapping mode, whether logging occurs, which event will end message buffering, and what the system does when message buffering is stopped by an event.
Tftp	Sends the ELS message buffer to a file at a remote host.
View	Displays all or a specific number of messages in the message buffer. You can also control how the messages scroll off the screen.
Write-buffer	Writes the ELS message buffer to the hard drive . The buffer is formatted before it is written. The file name on the hard drive is always ELSADV.LOG.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Flush

Use the **flush** command to set logging off, clear the messages from the buffer, and release the buffer memory for other use by the system.

Syntax:

flush buffer

List

Use the **list** command to list the ELS message buffering configuration.

Syntax:

list status

Example:

```
ELS Advanced> list status
-----------------------------------Configuration--------------------------------
Logging Status:    OFF       Wrap Mode:   ON    Logging Buffer Size:    8500 Kytes
Stop-Event:    APPN.2          Stop-String:     netdn for  intf 6
Additional Stop-Action:  APPN DUMP
-----------------------------------Run-Time Status------------------------------
Has Stop Condition Occurred ?     YES       Messages currently in buffer:         1222
```

See “Set” on page 166 for a description of the commands that change the values in the display.

Log

Use the **log** command to select which messages will be logged to the message buffer.

Syntax:

log event
group
range
subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem to be logged to the message buffer.

Nolog

Use the **nolog** command to remove messages from the defined list of messages that are logged to the message buffer.

Syntax:

nolog event
group
range
subsystem

event *subsystem.event#*
Causes the specified message (*subsystem.event#*) not to be logged to the message buffer.

group *groupname*
Allows messages that were previously added to the specified group not to be logged to the message buffer.

range *subsystemname first_event_number last_event_number*

Where *first_event_number* is the number of the first event in the specified event range, and *last_event_number* is the number of the last event of the specified event range.

Causes the messages that are in the specified range for the specified subsystem not to be logged to the message buffer.

Example:

```
log range gw 19 22
```

Causes the messages in events gw.19, gw.20, gw.21, and gw.22 not to be logged to the message buffer.

subsystem *subsystemname*
Allows messages associated with the specified subsystem not to be logged to the message buffer.

Read-file

Use the **read-file** command to read formatted ELS messages from a file on the hard drive , ELSADV.LOG, created by the **write-buffer** command.

Note: If you enter this command and a hard drive is not available, you will receive a message indicating the drive is unavailable.

Syntax:

read-file

Set

Use the **set** command to change configured ELS message buffering options.

Syntax:

set logging [on or off]
stop action . . .
stop event *subsystem.event#*
stop string *text*
wrap [on or off]

logging [on or **off]**
Specifies whether message buffering will occur. This command will not take affect until you allocate a buffer using the **set buffer-size** command. The default is off.

stop action [appn-dump or **disk-offload**or **none** or **system-dump]**
Specifies the additional action the system takes when the “stop event” (and if specified, the “stop string”) occurs. The actions are:

appn-dump
Dumps the APPN protocol, if it is active. The APPN dump will indicate that the dump was taken as the result of a stop action.

disk-offload
Writes a formatted version of the buffer to a file on the hard drive .

If the file already exists, the new file replaces it. You can then use the **tftp file** monitoring command to send the file to a remote host.

none No other action is taken after logging stops.

system-dump
Dumps the entire system. The system dump will indicate that the dump was taken as the result of a stop action.

Default value: none

stop event [*subsystem.event#* or **none]**
Specifies the event (*subsystem.event#*) that stops logging. If you have specified a stop string, the text in the stop string must also match. When the stop event occurs:

1. The next five ELS messages are logged.
2. Logging stops.
3. The system performs the specified “stop action.”

Logging remains stopped until the next time you issue the **set logging on** command or the device reboots.

If you do not specify the stop event when you enter the command, the system prompts you to enter the stop event. Specifying **none** disables the stop event function.

Default value: none

stop string *text* or **none**
Specifies the string to be used in conjunction with the “stop event” to stop logging. If you have not specified a stop event, the system ignores the “stop string.”

Text can be any ASCII string up to 32 characters in length. If you do not specify *text* when you enter the command, the system will prompt you for the string. Entering **none** clears the “stop string.”

Default value: none

wrap [on or **off]**
Specifies whether to stop the log when the buffer is full (off) or to log the new messages at the beginning of the buffer (on).

Default value: off

Tftp

Use the **tftp** command to send the ELS message buffer to a remote host as a formatted file.

Syntax:

tftp buffer [formatted] *dest_ip_address dest_filename*

file *dest_ip_address dest_filename*

buffer [formatted] *dest_ip_address dest_filename*
Specifies that the ELS message buffer is to be sent to the remote host indicated by *dest_ip_address* as file *dest_filename.* The buffer can be either formatted.

View

Use the **view** command to view all of the messages or a specific number of messages in the message buffer.

Syntax:

view all [scroll/noscroll]

last [scroll/noscroll *number*]

all *scroll/noscroll*

Displays all of the messages in the message buffer.

[scroll]

Specifies that the screen pauses until you hit the spacebar.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll

Specifies that the messages will scroll off the screen if the number of messages exceeds the screen length.

last *scroll/noscroll number*

Display the last *number* messages in the message buffer.

[scroll]

Specifies that the screen pauses after displaying a full screen of messages and waits for the user to hit the space bar to get the next screen.

Note: If you are displaying a large number of messages, specify scroll so you do not miss any critical messages.

noscroll

Specifies that the messages will continuously scroll off the screen with no scroll control until either all messages in the buffer (or the last number of messages requested) have been displayed.

number

Specify a number from 1 to the total number of messages in the message buffer. To display the total number of messages in the buffer, use the **list status** monitoring command.

Write-buffer

Use the **write-buffer** command to write formatted ELS messages to the hard drive .

Note: If you enter this command and a hard drive is not available, you will receive a message indicating the drive is unavailable.

Syntax:

write-buffer

Chapter 14. Configuring and Monitoring Performance

This chapter describes how to use the Performance configuration and monitor operating commands and includes the following sections:

Performance Overview

Configuring performance allows you to monitor your CPU load. In the idle (non-work load) state, performance reflects operations that the device continuously performs as a part of managing external interfaces. The CPU load registered in the idle state is dependent upon:

- Number of protocols running.
- Number of interfaces/cards installed.
- Type of interfaces installed.

The performance function can be used as a tool for trend analysis, bottleneck evaluation, and capacity planning. By collecting the CPU utilization information on the device, a network manager can monitor:

- CPU load versus time of day.
- CPU load versus location of the device in the network.
- CPU load versus traffic throughput.
- CPU load versus user load

Performance Reporting Accuracy

If you request a performance analysis when the 8371 first comes online, you will see values that reflect an initialization state that has little or no network traffic, so it is of little use in helping to balance your network load.

It is best to use performance reports that are generated under normal loads after approximately 2 minutes of operation.

Accessing the Performance Configuration Environment

Use the following procedure to access the Performance monitor configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, see "What is CONFIG?" on page 55.) For example:

```
* talk 6
Config>
```

After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the CONFIG prompt, enter the **perf** command to get to the `PERF Config>` prompt.

Performance Configuration Commands

To configure Performance, enter the commands at the `PERF Config>` prompt.

Table 26. PERF Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable cpu statistics

t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable cpu statistics

t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Accessing the Performance Monitoring Environment

Use the following procedure to access the Performance monitoring commands. This process gives you access to the Performance *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, see “Chapter 10. The Operating/Monitoring Process (GWCON - Talk 5) and Commands” on page 85.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the + prompt, enter the **perf** command to get you to the `PERF Console>` prompt.

   Example:

   ```
   + perf
   PERF Console>
   ```

Performance Monitoring Commands

This section describes the Performance monitoring commands.

Table 27. PERF Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Clear	Clear the CPU utilization high water statistics and resets the reporting period to a new cycle.
Disable	Disables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
Enable	Enables the collection of CPU utilization statistics or `Talk 2` ELS monitor output.
List	Lists the configuration.
Report	Displays a report of performance statistics.
Set	Sets the reporting period.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **disable** command to disable collection of CPU utilization statistics and disable the `talk 2` ELS monitor output.

Syntax:

disable	cpu statistics
	t2 output

Enable

Use the **enable** command to enable collection of CPU utilization statistics and enable the `talk 2` ELS monitor output.

Syntax:

enable	cpu statistics
	t2 output

List

Use the **list** command to display the performance monitor configuration.

Syntax:

list

Report

Use the **report** command to display performance monitor statistics.

Syntax:

report

Example:

```
PERF Console>report
-------------------------------------------------------------
KEY:  SW = Short Window = 9 seconds
KEY:  LW = Long Window =  9.0 minutes  (60 x SW)

  CPU UTIL :   Most recent SW                    = 38%
               Most recent LW                    = 33%
               Highest for all SW's              = 92%
               Highest for all LW's              = 52%
               % of time cpu util (SW) was > 60%  = 16%
               % of time cpu util (SW) was > 70%  = 15%
               % of time cpu util (SW) was > 80%  = 1%
               % of time cpu util (SW) was > 90%  = 0%
               % of time cpu util (SW) was > 95%  = 0%
-------------------------------------------------------------
```

Set

Use the **set** command to set the reporting period.

Syntax:

set *time*

time Specifies the short window time.

Valid Values: 2 - 30 seconds

Default Value: 2

Performance Monitoring Commands (Talk 5)

Part 2. Interfaces

Chapter 15. Using the 10/100 Mbps Ethernet Network Interface

This chapter describes how to use the 10/100 Mbps Ethernet interface. It includes the following section:

Displaying 10/100 Mbps Ethernet Statistics

You can use the **interface** command from the GWCON environment to display the following statistics.

```
+interface
                                                    Self-Test  Self-Test Maintenance
Net   Net'   Interface   Slot-Port                      Passed     Failed      Failed
0     0      Eth/0       Slot: 0   Port: 1               0          0           0
1     1      Eth/1       Slot: 0   Port: 2               0          0           0
2     2      Eth/2       Slot: 0   Port: 3               0          0           0
3     3      Eth/3       Slot: 0   Port: 4               0          0           0
4     4      Eth/4       Slot: 0   Port: 5               0          0           0
5     5      Eth/5       Slot: 0   Port: 6               0          0           0
6     6      Eth/6       Slot: 0   Port: 7               0          0           0
7     7      Eth/7       Slot: 0   Port: 8               0          0           0
8     8      Eth/8       Slot: 0   Port: 9               0          0           0
9     9      Eth/9       Slot: 0   Port: 10              0          0           0
10    10     Eth/10      Slot: 0   Port: 11              0          0           0
11    11     Eth/11      Slot: 0   Port: 12              0          0           0
12    12     Eth/12      Slot: 0   Port: 13              0          0           0
13    13     Eth/13      Slot: 0   Port: 14              0          0           0
14    14     Eth/14      Slot: 0   Port: 15              0          0           0
15    15     Eth/15      Slot: 0   Port: 16              0          0           0
16    16     Eth/16      Slot: 1   Port: 1               0          0           0
17    17     Eth/17      Slot: 1   Port: 2               0          0           0
18    18     Eth/18      Slot: 1   Port: 3               0          0           0
19    19     Eth/19      Slot: 1   Port: 4               0          0           0
20    20     Eth/20      Slot: 1   Port: 5               0          0           0
21    21     Eth/21      Slot: 1   Port: 6               0          0           0
22    22     Eth/22      Slot: 1   Port: 7               0          0           0
23    23     Eth/23      Slot: 1   Port: 8               0          0           0
24    24     Eth/24      Slot: 2   Port: 1               0          0           0
25    25     Eth/25      Slot: 2   Port: 2               0          0           0
26    26     Eth/26      Slot: 2   Port: 3               0          0           0
27    27     Eth/27      Slot: 2   Port: 4               0          0           0
28    28     Eth/28      Slot: 2   Port: 5               0          0           0
29    29     Eth/29      Slot: 2   Port: 6               0          0           0
30    30     Eth/30      Slot: 2   Port: 7               0          0           0
31    31     Eth/31      Slot: 2   Port: 8               0          0           0
32    32     NULL/0                                      0          0           0
33    33     NULL/1                                      0          0           0
34    34     NULL/2                                      0          0           0
35    35     NULL/3                                      0          0           0
36    36     ATM/0       Slot: 1   Port: 1               0          1           0
37    37     ATM/1       Slot: 1   Port: 2               0          1           0
38    38     ATM/2       Slot: 2   Port: 1               0          1           0
39    39     ATM/3       Slot: 2   Port: 2               0          1           0
40    40     Eth/32                                      0          1           0
41    41     Eth/33                                      0          0           0
42    42     Eth/34                                      0          0           0
43    43     Eth/35                                      0          0           0
44    44     Eth/36                                      0          0           0
45    45     Eth/37                                      0          0           0
46    46     Eth/38                                      0          0           0
47    47     Eth/39                                      0          0           0
48    48     Eth/40                                      0          0           0
50    50     Eth/42                                      0          0           0
51    51     Eth/43                                      0          0           0
52    52     Eth/44                                      0          0           0
53    53     Eth/45                                      0          0           0
54    54     Eth/46                                      0          0           0
55    55     Eth/47                                      0          0           0
56    56     Eth/48                                      0          0           0
```

```
57    57     Eth/49                                  0          0          0
58    58     Eth/50                                  0          0          0
59    59     Eth/51                                  0          0          0
60    60     Eth/52                                  0          0          0
61    61     Eth/53                                  0          0          0
62    62     Eth/54                                  0          0          0
63    63     Eth/55                                  0          0          0
+
```

These statistics have the following meaning:

Nt Global network number.

Nt′ This field is for the serial interface card. Disregard the output.

Interface
Interface name and its instance number.

Self-Test: Passed
Number of self-tests that succeeded.

Self-Test: Failed
Number of self-tests that failed.

Maintenance: Failed
Number of maintenance failures.

Physical address
The Ethernet address of the device currently in use. This may be the PROM address or an address overwritten by some other protocol.

PROM address
The permanent unique Ethernet address in the PROM for this Ethernet interface.

Actual address

Adapter level

Configured duplex
The value configured for duplex. Values can be Half Duplex, Full Duplex, or Auto-Negotiation.

Actual duplex
The value at which the adapter is presently operating. It might be different from the value configured, depending on the switch capability. If the adapter is not Up, the value displayed will be *Unknown*. Otherwise the value can be Half Duplex or Full Duplex.

Whenever the link partner (switch or hub) does not participate during the negotiation phase, "***" will follow the actual duplex mode value. When "***" is indicated the operational duplex value should be verified on the switch or hub for consistency.

Most hubs (unlike switches) can only support half-duplex mode, and are not capable of negotiation. As such the "***" indication will usually be displayed when the interface is connected to a hub.

A message will also be logged via the ELS system whenever a possibilty of a mis-match in duplex mode exists.

Note: If the link partner (switch or hub) to which the interface is connected does not respond during the negotiation phase, the two may result in operating in different duplex modes. That is, the interface may be operating in half-duplex, while the switch port is operating in full duplex mode. A mis-match in the duplex mode can result in severe

performance degradation. See “10/100 Mbps Ethernet Configuration Commands” on page 183 for important information regards speed and duplex configurations.

Configured speed
The value configured for speed. Values can be 10 Mbps, 100Mbps, or Auto-Negotiation.

Actual speed
The speed at which the adapter is presently operating.If the adapter is not Up, the value displayed will be *Unknown*. Otherwise the value can be 10 Mbps or 100 Mbps.

Input statistics:

failed, packet too long or failed, frame too long
The Failed, Packet Too Long counter increments when the interface receives a packet that is larger than the maximum size of 1518 bytes for an Ethernet frame. This data is exported via SNMP as the dot3StatsFrameTooLongs counter.

failed, CRC error or failed, FCS (Frame Check Sequence) error
The Failed, CRC (Cyclic Redundancy Check) Error counter increments when the interface receives a packet with a CRC error. This data is exported via SNMP as the dd3StatsFCSErrors counter.

failed, alignment error
The Failed, Framing Error counter increments when the interface receives a packet where the length in bits is not a multiple of eight.

failed, receive overflow
Overflow error indicates that the receiver has lost all or part of the incoming frame, due to an inability to move data from the receive FIFO into memory buffer before the internal FIFO overflowed.

receive collision
Indicates the total number of collisions encountered by the receiver support on the adapter.

Note: This counter cannot be cleared by the **clear statistics** command because it is maintained on the adapter. The **test network** command is the only way to reset this counter.

missed frame
Indicates the number of incoming receive frames lost due to unavailability of a receive buffer in the system. This error indicates that the system is not processing received frames as fast as they are being received from the local network.

Note: This counter cannot be cleared by the **clear statistics** command because it is maintained on the adapter. The **test network** command is the only way to reset this counter.

frames filtered
Indicates the number of incoming frames that were discarded by the adapter. This counter is updated only when bridging is enabled.

Note: This counter is maintained on the adapter, and is cleared every time it is read. This counter will be cleared by the **interface statistics** and the **test network** commands.

receive underrun
Indicates the number of times the adapter did not have a second buffer to store a long frame (requiring more than one buffer).

Output statistics:

one retry
Indicates that exactly one retry was needed to transmit a frame. This data is exported via SNMP as the dot3StatsDeferredTransmissions counter.

single collision
The Single Collision counter increments when a packet has a collision on the first transmission attempt, and then successfully sends the packet on the second transmission attempt. This data is exported via SNMP as the dot3StatsSingleCollisionFrames counter.

multiple collisions
The Multiple Collisions counter increments when a packet has multiple collisions before being successfully transmitted. This data is exported via SNMP as the dot3MultipleCollisionFrames counter.

failed, transmit underflow
Transmit underrun indicates that transmitter has truncated a message because it could not read data from the memory fast enough. It also indicates that the FIFO on the adapter has emptied out before the end of the frame was reached. IFO into memory buffer before the internal FIFO overflowed.

failed, excess collisions
The Failed, Excess Collisions counter increments when a packet transmission fails due to 16 successive collisions. This error indicates a high volume of network traffic or hardware problems with the network. This data is exported via SNMP as the dot3StatsExcessiveCollisions counter.

failed, loss of carrier
Loss of carrier is set when the carrier is lost during transmission. The adapter does not retry upon loss of carrier. It will continue to transmit the whole frame until done.

late collisions
A late collision indicates that a collision has occurred after the first channel slot time has elapsed. The adapter does not retry on late collisions.

more than one retry
More than one retry indicates that more than one retry was needed to transmit a frame.

buffer error
Buffer error occurs if there is a memory corruption problem in the system, or under certain FIFO underflow conditions on the adapter.

total collisions
The Total Collisions counter increments by the number of collisions a packet incurs.

excessive deferral
Excessive deferral indicates that the transmitter on the adapter has experienced Excessive Deferral on this a transmit frame, where Excessive Deferral is defined in the ISO 8802-3 (IEEE/ANSI 802.3) standard.

deferred
Deferred indicates the number of times the adapter had to defer while trying to transmit a frame. This condition occurs if the DMA channel is busy when the adapter is ready to transmit.

memory error
Memory errors occur when the adapter is not given access to the system interface bus within the programmable length of time. This error will normally occur during transmit operations, indicating transmit underrun.

Auto-negotiation on the 10/100 Mbps Ethernet Interface

Specifying values other than *auto* for speed or duplex on the 10/100 Ethernet interface or its link partner (switch port) can result in duplex mode mismatch or link activation failures.

Link activation failures due to configuration mismatches will occur on the IBM 8371 whenever the speed configured at both ends are not identical.

When either speed or duplex value is *auto-negotiate*, both speed and duplex will be negotiated with the link partner and its configured speed or duplex will be used.

Chapter 16. Configuring and Monitoring the 10/100 Mbps Ethernet Network Interface

This chapter describes the 10/100 Mbps Ethernet interface configuration and operational commands. It includes the following sections:

Accessing the Interface Configuration Process

Use the following procedure to access the configuration process. This process gives you access to an Ethernet interface's *configuration* process.

1. At the OPCON prompt, enter **configuration**. (For more detail on this command, refer to "What is the OPCON Process?" on page 43.) For example:

   ```
   * configuration
   Config>
   ```

   The CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter configuration, press **enter** again.

2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the device is currently configured.
3. Record the interface numbers.
4. Enter the **network** command and the number of the Ethernet interface you want to configure. For example:

   ```
   Config> network 0
   Ethernet 100 interface configuration
   ETH100 Config>
   ```

   The 10/100 Mbps Ethernet configuration prompt (`ETH100 Config>`), is displayed.

10/100 Mbps Ethernet Configuration Commands

This section describes the 10/100 Mbps Ethernet configuration commands. Enter the commands at the `ETH config>` prompt.

Table 28. 10/100 Mbps Ethernet Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Duplex	Sets the duplex mode.
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X'0800') or IEEE (802.3 with SNAP).
List	Displays the current connector-type, and IP encapsulation.
Physical-Address	Sets the physical MAC address.
Speed	Sets the link speed.

Table 28. 10/100 Mbps Ethernet Configuration Command Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Duplex

Use the **duplex** command to set the duplex mode.

Note: The default value of *auto* is recommended. The value **half duplex** or **full-duplex** should be specified only if auto-negotiation does not result in successful activation of the interface or desired duplex mode.

If a value other than *auto* is specified, ensure that the same value is configured on the switch port. After configuring the switch port to match the duplex specified on the 10/100 Mbps Ethernet interface, disable and test the interface.

Verify that the actual duplex mode shown on the interface status panel matches the operational value on the switch port.

The interface may enter the Up state with mis-matched duplex mode. Operating with mis-matched duplex modes on the interface and switch port can cause severe performance degradation.

Syntax:

duplex half_duplex
full_duplex
auto

Half_duplex
The interface will not transmit while receiving or receive while transmitting.

Full_duplex
The interface will transmit and receive simultaneously.

Auto The interface will automatically select half duplex or full duplex depending on the link partner’s capability.

IP-Encapsulation

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X’0800’) or IEEE 802.3 (Ethernet 802.3 with SNAP). Enter **e** or **i** for the type.

Syntax:

IP-encapsulation *type*

Example: `IP-encapsulation e`

List

Use the **list** command to display the current configuration for the 10/100 Mbps Ethernet interface.

Syntax:

list all

Example:

```
list all

The duplex is   HALF DUPLEX
The speed is   100Mb
IP Encapsulation:   Ether

MAC Address:        023456789A56
```

Physical-Address

Use the **physical-address** command to set the physical (MAC) address.

Syntax:

physical-address ***address***

physical-address

This command lets you indicate whether you want to define a locally administered address for the Ethernet interface's MAC sublayer address, or use the default burned-in address (indicated by all zeros). The MAC sublayer address is the address that the Ethernet interface uses to receive and transmit frames.

Note: Pressing **Enter** leaves the value the same. Entering **0** causes the device to use the burned-in address. The default is to use the burned-in address.

Valid Values: Any 12-digit hexadecimal address.

Default Value: burned-in address (indicated by all zeros).

Example:

```
physical-address
MAC address in 00:00:00:00:00:00 form []? 12:15:00:FA:00:FE
```

Speed

Use the **speed** command to set the speed used by this interface.

Note: The default value of *auto* is recommended. The values of **ten** and **hundred** should be specified only if auto-negotiation does not result in sucessful activation of the interface or desired speed.

If a value other than *auto* is specified, ensure that the same value is configured on the switch port. After configuring the switch port to match the speed specified on the 10/100 Mbps Ethernet interface, disable and test the interface.

If the interface and switch (or hub) port are not configured for identical speed, the interface will not attain the Up state.

See "Auto-negotiation on the 10/100 Mbps Ethernet Interface" on page 181 for information about auto-negotiation.

Syntax:

speed ten
hundred
auto

Ten The interface will operate at 10 Mbps.

Hundred
The interface will operate at 100 Mbps

Auto The interface will automatically select the speed (10 Mbps or 100 Mbps) depending on the link partner's capability.

Accessing the 10/100 Mbps Interface Monitoring Process

To monitor information related to the 10/100 Mbps Ethernet Network Interface, access the interface monitoring process by doing the following:

1. At the OPCON prompt, enter **console**. For example:

   ```
   * console
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter GWCON, press **enter** again.
2. At the GWCON prompt, enter the **configuration** command to see the protocols and networks for which the device is configured. For example:

   ```
   + configuration
   ```

   See "Configuration" on page 87 for sample output of the **configuration** command.
3. Enter the **network** command and the number of the Ethernet interface. In this example:

   ```
   + network 0
   ETH100>
   ```

   The 10/100 Mbps Ethernet monitoring prompt is displayed. You can now view information about the 10/100 Mbps Ethernet interface by entering monitoring commands.

10/100 Mbps Ethernet Interface Monitoring Commands

This section summarizes the 10/100 Mbps Ethernet monitoring commands. Enter commands at the ETH100> prompt. Table 29 lists the monitoring commands.

Table 29. Ethernet Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Collisions	Displays collision statistics for the specified Ethernet interface.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Collisions

This command displays the counts of transmissions for packets that incurred collisions before successful transmission. Counters are displayed for packets sent after 15 collisions. An increased number of packets transmitted with collisions and higher numbers of collisions per packet are signs of transmitting onto a busy Ethernet.

These counters are cleared by the OPCON **CLEAR** command. This data is exported via SNMP as the dot3CollTable counter.

Syntax:

collisions

Example:

```
Eth100> coll

Transmitted with  1 collisions:0
Transmitted with  2 collisions:0
Transmitted with  3 collisions:0
Transmitted with  4 collisions:0
Transmitted with  5 collisions:0
Transmitted with  6 collisions:0
Transmitted with  7 collisions:0
Transmitted with  8 collisions:0
Transmitted with  9 collisions:0
Transmitted with 10 collisions:0
Transmitted with 11 collisions:0
Transmitted with 12 collisions:0
Transmitted with 13 collisions:0
Transmitted with 14 collisions:0
Transmitted with 15 collisions:0
```

Chapter 17. Using ATM

This chapter describes how to use the ATM interface. It includes the following sections:

- "ATM and LAN Emulation"
- "How to Enter Addresses"
- "ATM-LLC Multiplexing" on page 190

ATM and LAN Emulation

LAN emulation provides support for virtual Token-Ring and Ethernet LANs over an ATM network. Refer to "How to Enter Addresses" for a discussion of ATM addressing.

How to Enter Addresses

Enter addresses in two ways, depending upon whether the address represents (1) an IP address, or (2) an ATM address, MAC address, or route descriptor, as follows:

1. IP address

   Enter IP addresses in dotted decimal format, a 4-byte field represented by four decimal numbers (0 to 255) separated by periods (.).

   Example of IP Address:

   01.255.01.00

2. ATM or MAC address or route descriptor

   Enter ATM addresses, MAC addresses, and route descriptors as strings of hexadecimal characters with or without optional separator characters between bytes. Valid separator characters are dashes (-), periods (.), or colons (:).

   Examples of ATM address, MAC address or route descriptor

   A1FF01020304
   or
   A1-FF-01-02-03-04
   or
   A1.FF.01.02.03.04
   or
   39.84.0F.00.00.00.00.00.00.00.00.00.03.10.00.5A.00.DE.AD.08
   or
   A1:FF:01:02:03:04
   or even
   A1-FF.01:0203:04

   Each type of address requires a different number of hexadecimal characters:

   ATM 40

   MAC 12

   ESI 12

   Route descriptor
   4

   This information applies to addresses entered for LAN emulation and MPOA.

ATM-LLC Multiplexing

Protocols that run natively over an ATM interface can use ATM-LLC multiplexing to share ATM addresses and both SVC and PVC channels between users. ATM-LLC is implicitly configured when the protocols are configured and can be monitored using the `ATM Config+` command prompt from **t 5**. There are no explicit configuration options for the ATM-LLC multiplexing function. For example, if two protocols which use ATM-LLC multiplexing are configured to use the same local ATM address (local endpoint), this implicitly configures ATM-LLC to use the same shared ATM address for both protocols.

See “ATM-LLC Monitoring Commands” on page 202 for additional information.

Sharing of ATM addresses or SVC/PVC channels is not possible between protocols that use the ATM-LLC multiplexing function and those that do not use the ATM-LLC multiplexing function (such as Classical IP). Currently, Server Cache Synchronization Protocol (SCSP) and APPN are the only two protocols that use the ATM-LLC multiplexing function.

Chapter 18. Configuring and Monitoring ATM

This chapter describe the ATM interface configuration and operational commands. It includes the following sections:

Accessing the ATM Interface Configuration Process

Use the following procedure to access the configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to "What is the OPCON Process?" on page 43.) For example:

   ```
   * talk 6
     Config>
   ```

   The CONFIG prompt (`Config>`) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the CONFIG prompt, enter the **list devices** command to display the network interface numbers for which the device is currently configured.
3. Enter the **network** command and the number of the ATM interface you want to configure. For example:

   The ATM configuration prompt (`ATM Config>`), is displayed.

ATM Configuration Commands

This section summarizes the ATM configuration commands. Enter the commands at the `ATM config>` prompt.

Table 30. ATM Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Interface	Displays the `ATM Interface Config>` prompt from which you can list, change, or configure the ATM Interface. • Add an ESI. • List the current configuration or list ESIs. • Remove an ESI. • Set parameters of the ATM network. • Enable or disable an ESI. • Exit

Table 30. ATM Configuration Command Summary (continued)

Command	Function
Le-client	Displays the `LE Client Config>` prompt from which you can list, change, or configure the LAN Emulation Client Interface as described in "Chapter 19. Using LAN Emulation Clients" on page 205. • Configure a LEC by network #. This command displays the `LE Config>` prompt, from which you can configure a specific LAN Emulation Client (LEC). • List LAN Emulation Clients (LECs).
Assign-lec	Assigns a specified LEC to an ATM interface.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

ATM Interface Configuration Commands

This section summarizes and then explains the commands for configuring a specific ATM interface.

Enter the commands at the `ATM INTERFACE>` prompt.

Table 31. ATM INTERFACE Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds an ESI.
List	Lists the current configuration or list ESIs.
Qos	Displays the `ATM I/F 0 QOS Config>` prompt from which you can configure Quality of Service as described in "QoS Configuration" on page 193.
Remove	Removes an ESI.
Set	Sets parameters of the ATM network.
Disable	Disables an ESI.
Enable	Enables an ESI.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Add

Use the **add** command to add an ESI to your ATM configuration.

Octets 14–19 of an ATM address are the End System Identifier (ESI). Each end system attached to the same switch must use a disjoint set of ESIs. When an end system activates, it attempts to register its ESIs with its ATM switch using ILMI. The switch forces all of its registered ESIs to be unique.

Syntax:

add esi *esi-address*

esi *esi-address*

Address of End System Identifier.

Valid Values: Any 12 hexadecimal digits

Default Value:

none

List

Use the **list** command to list the configuration of this ATM device or to list the set of configured ESIs.

Syntax:

list configuration

esi

configuration

Lists the ATM device configuration. For an explanation of the listed fields, see “Set” on page 194.

Example: `list con`

```
                        ATM Configuration

Interface (net) number =     36
Maximum VCC data rate Mbps   =      155
Maximum frame size    = 1664
Maximum number of callers =  209
Maximum number of calls =  1024
Maximum number of parties to a multipoint call =  512
Maximum number of Selectors that can be configured  =  200
UNI Version = UNI 3.0
Packet trace = OFF
ATM Network ID =    0
```

esi Lists the ESIs in the ATM configuration.

Example: `list esi`

```
ATM INTERFACE> list esi

         ESI                Enabled
------------------------   -------
000000000009                  YES
000000000100                  YES
```

QoS Configuration

Use the **qos-configuration** command to display the `ATM I/F 0 QOS Config>` prompt from which you can configure Quality of Service as described in “QoS Configuration”.

Syntax:

qos-configuration

Remove

Use the **remove** command to remove an ESI from your ATM configuration. All ATM components using this ESI should be reconfigured to use a different ESI. An ATM component that attempts to use a removed ESI may not activate on the next device restart.

Syntax:

remove esi *esi-address*

esi *esi-address*
Address of End System Identifier.

Valid Values: Any 12 hexadecimal digits

Default Value:
none

Set

Use the **set** command to specify ATM network parameters.

Syntax:

set max-callers
max-calls
max-config-selectors
max-data-rate
max-frame
max-mp-parties
network-id
trace
uni-version

max-callers
Sets the maximum number of entities on the device that use the ATM interface. Each LEC, Classical IP Client, and 1483 bridge interface qualifies as a user of the ATM interface. Increasing this parameter allows more users of the interface and uses more system memory.

Valid Values:
An integer in the range 64 – 1024

Default Value:
209

Example:

```
ATM INTERFACE> set max-callers 25
```

max-calls
Sets the maximum number of switched virtual circuits (SVCs) that can exist on this ATM device. Every point-to-point and point-to-multipoint SVC uses system resources. This parameter helps limit the system resources reserved for signaling and switched connections. Increasing this parameter will allow more simultaneous SVCs. However, more system memory will be required to manage these connections.

Valid Values:
An integer in the range 64 - 10500

Default Value:
1024

Example:

```
ATM INTERFACE> set max-calls 500
```

max-config-selectors

Sets the maximum number of selectors under your specific control.

The selector is used to distinguish different users on the same end system. VCC setup requests are routed in the following hierarchical fashion: ATM switches route to the destination ATM switch using the Network Prefix, the destination ATM switch routes to the destination end system using the ESI, and the end system notifies the destination user based on the selector.

Each ESI can have up to 255 associated selectors (0x00 through 0xff). The range of selectors is partitioned into two subranges, a configured selector range and an automatically assigned selector range. The ATM interface parameter max-configured-selector gives the upper bound on the configured selector range.

The relative sizes of the selector range can be modified to conform to the types and numbers of ATM users on the device.

Valid Values:

0 – 255 (0x00 – 0xFF)

Default Value:

200

Note: The selector is byte 20 of a 20-byte ATM address.

Example:

```
ATM INTERFACE> set max-config-selectors 225
```

max-data-rate *speed*

Sets the default and upper bound for VCC traffic parameters of most LANE and CIP connections. For example, this is the default PCR for best-effort VCCs initiated by LE Clients. Signaled SCRs and PCRs cannot exceed this limit. The default value should be satisfactory in most situations. An example of a situation where it is beneficial to change this value would be if the majority of the stations use 25–Mbps adapters. In this case, it may be desirable to limit the data rate on VCCs to 25 Mbps so that the lower speed stations are not overwhelmed with frames from the device. The units for this parameter are Mbps.

Valid Values:

25

100

155

Default Value:

155

Example:

```
ATM INTERFACE> set speed 155
```

max-frame

Sets the maximum number of octets permitted in any data frame sent or received on the ATM interface. System memory is allocated based upon this parameter. Increasing the max-frame requires more system memory, but allows processing of larger frames.

All device entities using the ATM interface must use a maximum frame size less than or equal to the max-frame-size of the ATM interface.

Valid Values:
An integer in the range 512 - 31000

Default Value:
9234

Example:

```
ATM INTERFACE> set max-frame 1000
```

max-mp-parties
Sets the maximum number of leaves on a point-to-multipoint connection initiated by the device. This parameter affects system memory allocation. Increasing this value is necessary if the device must set up point-to-multipoint connection(s) to a large number of destinations.

Valid Values:
An integer in the range 1 – 5000

Default Value:
512

Example:

```
ATM INTERFACE> set max-mp-parties 300
```

network-id
Sets the network id of the ATM interface. Multiple ATM interfaces should have the same network id if there is ATM connectivity between the interfaces.

Valid Values:
0 - 255

Default Value:
0

trace Sets the packet tracing parameters on the interface. Packet tracing can be enabled or disabled on a range of VPI/VCI values. Common VPI/VCI values to trace are:

- 0/5 for signalling packets
- 0/16 for ILMI packets.

Valid Values:
on, off

Default Value:
off

You are prompted for the VPI/VCI range you want to trace.

Beginning VPI Valid Values:
0 – 255

Default Value:
0

Ending VPI Valid Values:
0 - 255

Default Value:
255

Beginning VCI Valid Values:
0 - 65535

Default Value:
0

Ending VCI Valid Values:
0 - 65535

Default Value:
65535

Example:

```
ATM INTERFACE> set trace on
beginning of VPI range [0]? 0
end of VPI range [255]? 0
beginning of VCI range [0]? 5
end of VCI range [65535]? 5
```

uni-version

Sets the User Network Interface (UNI) version used by the ATM interface with communicating with the attached ATM switch. If the UNI versions are configured on the ATM switch and ATM device interface to a specific version (not AUTO-DETECT), the UNI versions must match.

If the UNI version is configured as AUTO, the ATM device attempts to learn the UNI version to use from the switch.

In UNI AUTO-DETECT mode, if the switch does not respond to the query for UNI version, the default is UNI 3.0. If the switch responds with a value other than UNI 3.0 or UNI 3.1, the default is UNI 3.1.

Valid Values:
[UNI 3.0|UNI 3.1|AUTO-DETECT|None]

Default Value:
UNI 3.0

Note: Must be compatible with the ATM switch.

Example:

```
ATM INTERFACE> set uni-version 3.0
```

Enable

Use the **enable** command to enable an ESI in the configuration of your ATM device. The ATM interface attempts to register only enabled ESIs when it activates.

Syntax:

enable esi *esi-address*

esi *esi-address*

Address of End System Identifiers.

Valid Values:
Any 12 hexadecimal digits

Default Value:
none

Example: `enable esi`

```
ATM INTERFACE> enable esi 00:00:00:00:00:09
```

Disable

Use the **disable** command to disable an ESI in the configuration. ATM components using disabled ESIs will not become active on the next device restart.

Syntax: disable esi *esi-address*

esi *esi-address*

Address of End System Identifiers.

Valid Values:

Any 12 hexadecimal digits

Default Value:

none

Example: `disable esi`

```
ATM INTERFACE> disable esi 00:00:00:00:00:09
```

Accessing the ATM Monitoring Process

Use the following procedure to access the ATM monitoring commands. This process gives you access to an ATM's *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to "What is the OPCON Process?" on page 43.) For example:

   ```
   * talk 5
   +
   ```

   The GWCON prompt (+) is displayed on the console. If the prompt does not appear when you first enter the console, press **Return** again.

2. Enter **interface** at the + prompt to display a list of configured interfaces.
3. Record the interface numbers.
4. Enter **network** followed by the number of the ATM interface.

   ```
   + network 36
   ATM+
   ```

   The ATM monitoring prompt (`ATM+`) is displayed.

ATM Monitoring Commands

This section summarizes the ATM monitoring commands for monitoring ATM interfaces. Enter the commands at the `ATM+` prompt.

Table 32. ATM monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Interface	Displays the `ATM Interface+` prompt from which you can monitor the ATM Interface, as described in "ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)" on page 199.
Atm-llc	Displays the `ATM LLC+` prompt from which you can monitor endpoints, a set of user clients, and a set of ATM channels.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Interface

Displays the `ATM Interface+` prompt, described in "ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)".

Syntax:

interface

ATM-LLC

Displays the `ATM-LLC+` prompt, described in "ATM-LLC Monitoring Commands" on page 202.

Syntax:

atm-llc

ATM Interface Monitoring Commands (ATM INTERFACE+ Prompt)

This section summarizes and then explains the commands for monitoring a specific ATM interface.

Enter the commands at the `ATM INTERFACE+` prompt.

Table 33. ATM INTERFACE monitoring command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
List	Lists ATM addresses and VCCs.
Trace	Starts/Stops packet tracing on a specified VPI/VCI range. Trace can be viewed by ELS.
Wrap	Starts/Stops a loopback test on the VCC.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

List

Use the **list** command to list various categories of ATM data.

Syntax:

list addresses
all
circuit
vccs
reserved-bandwidth

addresses

Lists the ATM addresses, along with a descriptive name, in use on the device.

Example:

```
ATM INTERFACE+ list addresses

                ATM Address                          Name
----------------------------------------  ------------------------------------
39999999999999000099990200000041347391804  LEC 1 'eth1'
39999999999999000099990200000041347391802  LES/BUS 'eth1'
```

all Lists all of the following:

- Addresses
- Circuit statistics
- VCCs
- Reserved Bandwidth

circuit Lists the statistics for a particular VCC by specifying the particular VCI-VPI pair. You can also specify the circuit on the command line; for example: list circuit 33.

Example:

```
ATM INTERFACE+ list circuit
VPI [0]?
VCI [32]?33

     Frames transmitted   =         2  Bytes transmitted   =       216
     Frames received      =         2  Bytes received      =       216
```

vccs Lists all the VCCs established by the device. The VCCs may be permanent (PVC) or switched (SVC), point-to-point or point-to-multipoint, and each is identified by a unique VPI/VCI. The trace command uses the VPI/VCI value for a VCC to perform packet tracing over a particular VCC.

Example:

P-P point to point VCC

P-MP point to multipoint VCC

ILMI Interim Local Management Interface VCC

SAAL signalling VCC

Bx-y Internally bound VCC to VPI x, VCI y

Sx-y Internally spliced VCC to VPI x, VCI y

reserved-bandwidth
Lists the reserved bandwidth on the ATM Interface.

Example:

```
ATM INTERFACE+ list reserved-bandwidth
Line Rate                    : 155000 Kbps
Peak Reserved Bandwidth      : None
Sustained Reserved Bandwidth : None
```

Trace

Use the **trace** command activate packet tracing over a specified range of VPI/VCI values. You can view trace data by using ELS as described in “View” on page 158.

Syntax:

trace list
on
off

list Displays the current packet tracing options on the ATM interface.

Example:

```
ATM Interface+ trace
on | off | list []? list
Packet trace is ON
Range of VPIs to be traced:       0 -       0
Range of VCIs to be traced:      32 -      39
```

on Starts packet tracing on all active VCCs within the specified VPI/VCI range.

Example:

```
ATM Interface+ trace on
beginning of VPI range [0]?
end of VPI range [0]?
beginning of VCI range [32]?
end of VCI range [65535]? 39
```

off Stops packet tracing on all VCCs.

Example:

```
ATM Interface+ trace off
ATM Interface+ trace list
Packet trace is OFF
```

Wrap

Use the **wrap** command to perform a loopback data test on the ATM interface of the adapter. Wrap can be issued on a per VC basis by specifying VPI-VCI pairs. Data is looped back internally.

You can selectively start a wrap, stop a wrap, or display the current wrap settings.

If you stop or display a wrap, the following statistics will be displayed:

- Wrap transmits
- Wrap receives
- Wrap transmit errors
- Wrap receive errors
- Wrap receive timeouts

For display, the current wrap statistics are displayed.

For stop, the final wrap statistics are displayed.

Syntax:

wrap display
start
stop

display
Displays the current wrap settings.

start Starts the wrap procedure and specifies the VPI-VCI length of pattern and the pattern itself.

Example:

```
ATM Interface+ wrap start
VPI [0]?
VCI [32]?
wrap pattern length [32]?
Enter 32-byte wrap pattern: [ABCDEFGHIJKLMNOPQRSTUVWXYZ123456]?
```

stop Stops the wrap procedure and displays final wrap statistics.

ATM-LLC Monitoring Commands

This section explains the commands for monitoring ATM LLC multiplexing.

Enter the commands at the `ATM-LLC+` prompt.

Table 34. ATM LLC Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists various options
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list various categories of ATM LLC monitoring data.

Syntax:

list endpoints

channels

endpoints

Lists the ATM addresses in use by protocols using the ATM-LLC multiplexing function on the device. The endpoint is displayed as the End System Identifier and the Selector.

Example: `list endpoints`

```
ATM-LLC+ list endpoints
```

channels

Lists the channels in use by protocols using the ATM-LLC multiplexing function on the device.

Example: `list channels`

```
ATM-LLC+ list channels
```

Assign-lec Configuration Command

Use the **assign-lec** command to assign a specified LEC to the ATM interface.

Syntax:

assign-lec

Select LEC to assign

Specifies the interface number of the LEC to be assigned to the ATM interface.

Note: The ATM interface is selected using the **net x** at the `Config>` prompt, where *x* is the physical ATM interface number.

Assign-lec Monitoring Command

Use the **assign-lec** command to dynamically assign a specified LEC to the ATM interface.

Syntax:

assign-lec

Select LEC to assign

Specifies the interface number of the LEC to be assigned to the ATM interface.

Note: The ATM interface is selected using the **net x** at the + prompt, where *x* is the physical ATM interface number.

ATM-LLC Monitoring Commands (Talk 5)

Chapter 19. Using LAN Emulation Clients

This chapter describes LAN Emulation Clients (LECs). It includes the following sections:

- "LAN Emulation Client Overview"

LAN Emulation Client Overview

On the router, LECs serve the purpose of "ports" or "interfaces" on traditional routers and bridges. The router bridges and routes traffic between ports by receiving and transmitting traffic through its LECs.

LEC has two prompt levels:

1. `LE Client Config>` lets you enter commands that control the environment of all your LECs. The commands for this prompt level are described in "Configuring LAN Emulation Clients" on page 207
2. One of the commands, **config**, gets you to another prompt level, `LEC Config>`, at which you can enter commands to configure a specific LEC.

An explanation of commands for LAN Emulation Clients follows.

Chapter 20. Configuring and Monitoring LAN Emulation Clients

This chapter describes how to configure LAN Emulation Clients (LECs). It includes the following sections:

Configuring LAN Emulation Clients

This section explains the commands for viewing, changing, and using the set of LE Clients on a particular ATM interface.

Enter the commands at the `LE Client Config>` prompt under the `ATM Config>` prompt, as described in "ATM Configuration Commands" on page 191.

To get to the `LE Client Config>` prompt, enter **le-c** at the ATM Config> prompt as described in "ATM Configuration Commands" on page 191.

Table 35. LAN EMULATION Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Config	Gets you to the `LEC Config>` prompt, from which you can configure a specific LAN Emulation Client as described in: • "Configuring an ATM Forum-Compliant LE Client" on page 208
List	Lists the LECs
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Config

Use the **config** command to get you to the `LEC Config>` prompt, from which you can configure the details of a specific LAN Emulation Client. Refer to "Configuring an ATM Forum-Compliant LE Client" on page 208.

Syntax:

config interface#

interface#

An integer number assigned by the device when the LEC was added to the configuration. Use the **list** command to determine the interface number assigned to the LEC.

Example:

```
LE Client Config> config 40
```

List

Use the **list** command to list the LAN emulation clients.

Syntax:

list

Example:

```
LE Client Config> list
                 ATM Emulated LANs
-------------------------------------------------------
  ATM interface number = 36
  LEC interface number = 40
  Emulated LAN type    = Ethernet Forum Compliant
  Emulated LAN name    =
```

Configuring an ATM Forum-Compliant LE Client

Use this process to access the appropriate `LEC Config>` prompt.:

1. Use the **config** command at the `LE Client Config>` prompt to access the appropriate LEC interface number, or use the **network** configuration command with the appropriate LEC interface number.
2. Enter the appropriate commands at the `Ethernet Forum Compliant LEC Config>` prompt.

This section explains the commands for configuring an ATM Forum-compliant LAN Emulation Client.

Table 36. LAN Emulation Client Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
ARP-Configuration	Allows you to configure the LE-ARP configuration for the ATM Forum-compliant client
IP-Encapsulation	Sets the IP encapsulation as Ethernet (type X’0800’) or IEEE (802.3 with SNAP). Applies only to Ethernet LECs.
List	Lists the LAN Emulation Client configuration.
QoS-Configuration	Gets you to the `LEC QoS Config` prompt from which you can configure Quality of Service as described in “LE Client QoS Configuration Commands” on page 237.
Set	Sets the LAN Emulation Client parameters.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

ARP Configuration

Use the **arp-configuration** command to configure the static LE-ARP entries for the ATM forum-compliant LAN Emulation Client.

Syntax:

arp-configuration

Example:

```
Token Ring Forum Compliant LEC Config> arp-configuration
ATM LAN Emulation Clients ARP configuration
```

Table 37. ATM LAN Emulation Client ARP Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an LE-ARP cache entry using a MAC or route descriptor ARP.
Config	Sets cache entry QoS parameter values.
List	Lists configured ARP cache entries.
Remove	Removes an ARP cache entry.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add an ARP cache entry using the MAC address or a route descriptor.

MAC addresses, and route descriptors are entered as strings of hexadecimal characters with or without optional separator characters between bytes. Valid separator characters are dashes (–), periods (.), or colons (:).

Syntax:

add mac

route-descriptor

Example 1:

```
ARP config for LEC>add mac
MAC address of LE ARP Entry []? 123456789098
ATM address in 00.00.00.00.00.00:... form []? 390f000000000000000000000000123456789098
Destination Type -  REMOTE or LOCAL [Remote]?
```

Example 2:

```
ARP config for LEC>add route 12.34
ATM address in 00.00.00.00.00.00:... form []? 390f000000000000000000001234567890988888
ARP config for LEC>
```

Config

Use the **Config** command to configure the permanent ARP cache entry QoS parameters for the ATM forum-specific LAN Emulation Client.

Syntax:

config *arp-entry-number*

Example:

```
ARP config for LEC> config
ARP entry number [1]
Configure LEC ARP entry
```

Table 38. ATM LAN Emulation Client ARP Config Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Set	Sets QoS parameter values.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Set:

Use the **Set** command to configure the permanent ARP cache entry QoS parameters for the ATM forum-specific LAN Emulation Client.

Syntax:

set max-reserved-bandwidth
traffic-type
peak-cell-rate
sustained-cell-rate
qos-class
max-burst-size

Example:

```
ARP entry 'identifier' config> set ?
 MAX-RESERVED-BANDWIDTH
 TRAFFIC-TYPE
 PEAK-CELL-RATE
 SUSTAINED-CELL-RATE
 QOS-CLASS
 MAX-BURST-SIZE
```

See “Chapter 21. Configuring and Monitoring Quality of Service (QoS)” on page 231 for detailed information about the QoS parameters.

List

Use the **list** command to display information about ARP configuration.

Remove

Use the **remove** command to remove an configured MAC address or Route Descriptor LE-ARP entry.

Select the ARP entry number to be removed from the list provided.

Syntax:

remove *arp-entry-number*

IP-Encapsulation (for Ethernet ATM Forum-Compliant LEC only)

Use the **IP-encapsulation** command to select Ethernet (Ethernet type X’0800’) or IEEE 802.3 (Ethernet 802.3 with SNAP). Specify either type **E**thernet or **I**EEE-802.3.

Syntax:

IP-encapsulation	Ethernet
	IEEE-802.3

List

Use the **list** command to list the LE client configuration.

Syntax:

list

QoS

Use the **qos-configuration** command to get you to the `LEC QoS Config>` prompt from which you can configure Quality of Service as described in “LE Client QoS Configuration Commands” on page 237.

Syntax:

qos-configuration

Set

Use the **set** command to set LE Client parameters.

Syntax:

set	arp-aging-time
	arp-cache-size
	arp-queue-depth
	arp-response-time
	auto-config
	best-effort-peakrate
	bus-connect-retries
	conn-completion-time
	control-timeout
	data-direct-timeout
	data-direct-vcc-mode
	elan-name
	esi-address
	flush-timeout
	forward-delay
	forward-disconnect-timeout
	frame-size
	initial-control-timeout

lecs-atm-address

les-atm-address

mac-address

multicast-send-avg

multicast-send-peak

multicast-send-type

multiplier-control-timeout

path-switch-delay

reconfig-delay-min

reconfig-delay-max

retry-count

selector

trace

unknown-count

unknown-time

vcc-timeout

arp-aging-time

Sets ARP aging time. This is the maximum time that a LEC will maintain an entry in its LE_ARP cache in the absence of a verification of that relationship. A larger aging time may result in a faster session setup time, but may also use more memory and reacts slower to changes in network configuration.

Valid Values:

An integer number of seconds in the range of 10 to 300.

Default Value:

300

Example:

```
LEC Config> set arp-aging-time 200
```

arp-cache-size

Sets the number of entries in the ARP cache. The size of the ARP cache limits the number of simultaneous data direct VCCs. Larger ARP caches require more memory, but permit the client to simultaneously converse with a larger number of destinations.

Valid Values:

An integer number in the range of 10 to 65535.

Default Value:

5000

Example:

```
LEC Config> set arp-cache-size 10
```

arp-queue-depth

Sets the maximum number of queued frames per ARP cache entry. The LEC enqueues frames when switching the data path from the Multicast Send VCC to a Data Direct VCC. Frames passed to the LEC for

transmission will be discarded if the queue is full. A larger queue requires more memory, but results in fewer discarded frames during the data path switch.

Valid Values:
An integer number in the range of 0 to 10.

Default Value:
5

Example:

```
LEC Config> set arp-queue-depth 10
```

arp-response-time
Sets expected ARP response time. This value controls how frequently an unanswered LE ARP request is retried. Larger values result in fewer LE ARPs, which causes less traffic and possibly increase the amount of time before a Data Direct VCC is established.

Valid Values:
An integer number of seconds in the range of 1 to 30.

Default Value:
1 second

Example:

```
LEC Config> set arp-response-time 20
```

auto-config
Specifies whether this LEC uses LECS auto-config mode. Specify YES or NO. The LEC may contact the LECS to obtain the address of its LES and various other configuration parameters.

Valid Values:
If YES, then you do not have to configure the ATM address of the LES.

If NO, then you *must* configure the ATM address of the LES using the **set les-atm-address** command as described on page 216.

Default Value:
NO

Example:

```
LEC Config> set auto-config yes
```

best-effort-peakrate
Sets the Best Effort Peak Rate. Used when establishing best effort multicast send connections.

The maximum peak rate depends on the maximum data rate of the ATM device.

Specify an integer from 1 to the maximum peak rate in Kbps (the definition is the maximum data rate) as follows:

- If ATM maximum data rate is 25 Mbps, the maximum peak rate is 25,000 Kbps.
- If ATM maximum data rate is 155 Mbps, the maximum peak rate is 155,000 Kbps.

Valid Values:
An integer number in the range of 1 - device maximum data rate.

Default Value:
155000

Example:

```
LEC Config> set best-effort-peakrate 24000
```

bus-connect-retries
This parameter sets the maximum number of times that the LEC will attempt to reconnect to the BUS before returning to the initial state.

Valid Values:
0 - 2

Default Value:
1

connection-completion-time
Sets the connection completion time. This is the time interval in which data or a READY_IND message is expected from a calling party.

When a Data Direct VCC is established to the client, the LEC expects data or a READY_IND message within this time period. The LEC will not transmit frames over a Data Direct VCC established to it until receiving data or a READY_IND. This parameter value controls the amount of time which passes before the LEC issues a READY QUERY (in hopes of receiving a READY_IND). Smaller values lead to faster response times, but also to unnecessary transmissions.

Valid Values:
An integer number of seconds in the range of 1 to 10.

Default Value:
4

Example:

```
LEC Config> set connection-completion-time 5
```

control-timeout
This parameter sets the maximum cumulative control timeout of a request.

A current timeout value is initialized to the value of ***initial-control-timeout***. If a response to a request is not received within the current timeout value, the current timeout is multiplied by the value of the ***multiplier-control-timeout*** and the request is reissued. Each time the current timeout value expires, this process is repeated until the current timeout value exceeds the value of ***control-timeout***.

Valid Values:
An integer number of seconds in the range of 10 to 300.

Default Value:
30

Example:

```
LEC Config> set control-timeout 100
```

data-direct-timeout
Specifies the timeout value for the data direct VCC. This parameter limits the time the Data Direct VCCs are left up without the LEC having a connection to the LES/BUS.

Valid Values:
10 - 300 seconds

Default Value:
30

data-direct-vcc-mode
Specifies whether persistant Data Direct VCC mode is enabled or disabled. When the Data Direct VCC mode is enabled, if the LEC loses its connection to the LES/BUS, the Data Direct VCCs are not dropped and the reconnect timeout timer is started.

Valid Values:
yes or no

Default Value:
no

elan-name
Specifies name of the ELAN that the LEC wishes to join. This is the ELAN name sent to the LECS in the configure request (if the LEC autoconfigures) or to the LES in the join request. The LECS or LES may return a different ELAN name in the response.

Valid Values:
Any character string length of 0 - 32 bytes.

Default Value:
Blank

Note: A blank name (0 length string) is valid.

Example:

```
LEC Config> set elan-name FUZZY
```

esi-address
Sets the ESI portion of the LEC's ATM address.

Specify the ESI portion (octets 13 through 19) of the LEC's ATM address. The ESI and selector combination of the LEC must be unique among all LAN emulation components on the device.

Valid Values:
Any 12 hexadecimal digits.

Default Value:
Burned-in ESI

Example:

```
set esi
Select ESI
   (1) Use burned in ESI
   (2) 11.22.33.44.55.66

Enter selection [1]?
```

flush-timeout
Sets the flush timeout. This is the time limit to wait to receive the LE_FLUSH_RESPONSE after the LE_FLUSH_REQUEST has been sent before taking recovery action. During recovery, any queued frames are dropped and a new flush request is sent.

When switching from the multicast send to a data direct data path, the client sends a flush request over the multicast send VCC. Until a flush response is received, or until the path switch delay expires, frames are queued for the destination.

Valid Values:

An integer number of seconds in the range of 1 to 4.

Default Value:

4

Example:

```
LEC Config> set flush-timeout 3
```

forward-delay

Sets the forward delay. Entries in the LE ARP cache must be periodically re-verified. The forward delay time is the maximum amount of time a remote entry may remain in the cache during a network topology change. Larger aging times may result in stale (invalid) entries, but also cause less re-verification traffic.

Valid Values:

An integer number of seconds in the range of 4 to 30.

Default Value:

15

Example:

```
LEC Config> set forward-delay 10
```

forward-disconnect-timeout

This parameter sets the amount of time that a LEC will wait after losing its last Multicast Forward VCC from the BUS before returning to the initial state. This delay permits the BUS to attempt to reconnect to the client without returning to the initial state.

Valid Values:

10 - 300 seconds

Default Value:

60

frame-size

Sets the frame size.

The value specified for frame-size must be equal to or less than the value specified for ATM max-frame using the ATM INTERFACE> **set max-frame** command as described on page 195.

Valid Values:

1516

4544

9234

18190

Default Value:

If the ELAN type is token ring, the default is 4544. If the ELAN type is Ethernet, the default is 1516.

Example:

```
LEC Config> set frame-size 4544
```

initial-control-timeout

This parameter sets the value of the initial control timeout used in the control timeout algorithm described in 214.

Valid Values:

1 - 10

Default Value:

5

Example:

```
LEC Config> set initial-control-timeout 10
```

lecs-atm-address

Specifies the ATM address of the LECS.

If the client is set to auto configure, it attempts to connect to a LECS. If it is unable to connect to a LECS, then it may try another LECS ATM address. The LECS ATM addresses that are tried, in order, are:

1. This configured LECS address
2. Any LECS address obtained through ILMI
3. The well-known LECS address defined by the ATM Forum.

No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
LEC Config> set lecs-atm-address
39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.01
```

les-atm-address

Sets the LES ATM address. This command may be optional or required depending upon the setting of lecs-auto-config as described in the **set auto-config** command on page 213.

- If auto-config is YES, the les-atm-address is not configurable.
- If auto-config is NO, then the les-atm-address is required.

Specify the ATM address of the LES. No default is provided.

Note: This command should be entered on one command line. It is shown here on two lines because of spacing.

Example:

```
LEC Config> set les-atm-address
      39.84.0F.00.00.00.00.00.00.00.00.00.01.10.00.5A.00.DE.AD.02
```

mac-address

Sets the MAC address for this LE client. You *may* specify that the client use the burned-in MAC address of the ATM interface, or you may specify a different MAC address. If you have two clients that are bridged together, they should use different MAC addresses.

This MAC address is registered with the LES when the client joins the ELAN.

Valid Values:
Any valid MAC address.

Default Value:
none

Example:

```
LEC Config> set mac-address
  Use adapter address for MAC? [No]
  MAC address []: 10.00.5a.00.00.01
```

multicast-send-avg
Sets the multicast send VCC average rate in Kbps. Used by the LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward sustained cell rate used when setting up a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-avg 4000
```

multicast-send-peak
Sets the multicast send peak rate in Kbps. Used by LEC for reserving bandwidth on the VCC to the BUS. It specifies the forward and backward peak cell rate used when establishing a reserved bandwidth multicast send VCC.

This parameter is only applicable when the multicast-send-type is reserved bandwidth. If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must be less than or equal to multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-avg and multicast-send-peak must be specified.

Example:

```
LEC Config> set multicast-send-peak 155
```

multicast-send-type
Sets the multicast send type. Specifies the method used by the LEC when establishing the multicast send VCC.

If multicast-send-avg equals multicast-send-peak, then a constant bit rate (CBR) multicast send is signalled. Otherwise, a variable bit rate (VBR) multicast send is signalled. Multicast-send-avg must at least equal multicast-send peak.

A reserved bandwidth multicast send VCC may improve data transfer rates in congested networks, but reserving bandwidth and not using it wastes network resources.

When the multicast-send-type is reserved, then multicast-send-no and multicast-send-peak must be specified.

Valid Values:
Best Effort or Reserved

Default Value:
Best Effort

Example:

```
LEC Config> set multicast-send-type best-effort
```

multiplier-control-timeout
This parameter sets the value of the control timeout multiplier used in the control timeout algorithm described on page 214.

Valid Values:
2 - 5

Default Value:
2

Example:

```
LEC Config> set multiplier-control-timeout 5
```

path-switch-delay
Sets the path switch delay.

The LEC must ensure that all frames sent through the BUS to a destination have arrived at the destination before it can start using a Data Direct VCC. This is accomplished using the flush protocol, or by waiting path-switch-delay seconds after sending the last packet to the BUS. Smaller values improve performance, but may result in out-of-order packets in a heavily congested network.

Valid Values:
An integer number of seconds in the range of 1 to 8.

Default Value:
6

Example:

```
LEC Config> set path-switch-delay 5
```

reconfig-delay-min
This parameter sets the minimum delay time when LEC returns to the initial state. This value must be ≤ ***reconfig-delay-max***.

Valid Values:
1 - the value of ***reconfig-delay-max***

Default Value:
1

Example:

```
LEC Config> set reconfig-delay-min  5
```

reconfig-delay-max

This parameter sets the maximum delay time when LEC returns to the initial state. This value must be ≥ ***reconfig-delay-min***.

Valid Values:

1 - 10

Default Value:

5

Example:

```
LEC Config> set reconfig-delay-max 9
```

retry-count

Sets the retry count. This is maximum number of times that the LEC retries an LE_ARP_REQUEST for a specific frame's LAN destination. If no ARP response is received after the specified number of retries, then the entry is purged from the LE ARP cache.

Valid Values:

0, 1, or 2

Default Value:

1

Example:

```
LEC Config> set retry-count 2
```

selector

Specifies the selector portion of the client's ATM address. The combination of ESI and selector must be unique among all LANE components on the device. By default, a unique selector is selected for the configured ESI.

Valid Values:

Any octet, in hexadecimal, that is not in use by another LANE component with the same ESI.

Example:

```
LEC Config> set selector 01
```

trace Enables tracing for the LEC. To perform packet tracing, three steps are required:

1. Enable packet tracing system (under ELS)
2. Enable tracing on the LEC subsystem (under ELS)
3. Enable packet tracing on the desired LECs (using this command).

Valid Values:

Yes or No

Default Value:

No

unknown-count

Sets the unknown frame count. This is the maximum number of frames for a specific unicast MAC address or route descriptor that may be sent to the BUS within the time specified by the unknown-time parameter. Larger values decrease the number of discarded frames while increasing the load on the BUS.

Valid Values:

An integer number of frames in the range of 1 to 255.

Default Value:
10

unknown-time
Sets the unknown frame time. This is the time interval during which the maximum number of frames for a specific unicast MAC address or route descriptor (specified by the unknown-count parameter) may be sent to the BUS. Larger values increase the number of discarded frames while decreasing the load on the BUS.

Valid Values:
An integer number of seconds in the range of 1 to 60.

Default Value:
1

Example:

```
LEC Config> set unknown-time 5
```

vcc-timeout
Sets the VCC timeout. Data direct VCCs over which no traffic has been sent for this period of time should be released.

Valid Values: 0 to 31536000 seconds (1 year).

Default Value: 1200

Note: This parameter is meaningful only for SVC connections.

Example:

```
LEC Config> set vcc-timeout 1000
```

Accessing the LEC Monitoring Environment

Use the following procedure to access the LEC monitoring commands. This process gives you access to the LEC *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to “What is the OPCON Process?” on page 43.) For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the console. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the + prompt, enter the **network ?** command to display the network interface numbers for which the device is currently configured, and enter the *interface number* for the LEC you wish to monitor. For example:

   ```
   + network ?
    1  : 1-port 10/100 Ethernet
    2  : 1-port 10/100 Ethernet
    3  : 1-port 10/100 Ethernet
   .
   .
   .
   30  : 1-port 10/100 Ethernet
   31  : 1-port 10/100 Ethernet
   36  : ATM
   37  : ATM
   38  : ATM
   39  : ATM
   40  : ATM Ethernet LAN Emulation: ELAN1
   41  : ATM Ethernet LAN Emulation: ELAN2
   ```

```
.
.
.
  LEC+
```

The LEC monitoring prompt (LEC+), is displayed.

If you know the interface number of the LEC you wish to monitor, enter the **network** command followed by the *interface number* of the LEC.

```
+ network 1
LEC+
```

LEC Monitoring Commands

This section summarizes and then explains the LEC monitoring commands. You can access LEC monitoring commands at the LEC+ prompt. Table 39 shows the commands.

Table 39. LE Client Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists: • LEC Address Resolution Table (ARP) • LEC configuration • Data Direct VCC information • Group addresses • RIF information • LEC statistics • VCC table.
MIB	Displays LEC MIB objects including: • LEC MIB Configuration Table • LEC MAC ARP Table • LEC Route Descriptor Table • LEC MIB Server VCC Tables • LEC MIB Statistics Table • LEC MIB Status Table
QoS	Gets you to the LEC x QoS+ prompt from which you can monitor Quality of Service as described in “Quality of Service Monitoring Commands” on page 245.
Trace	Sets packet tracing on or off or sets a trace address or trace mask.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the LEC Address Resolution Table (ART), list the LEC configuration, list Data Direct VCC information, or list LEC statistics.

Syntax:

list arp-table
configuration

data-direct-vccs

group

rif

statistics

vcc-table

arp Lists the LEC Address Resolution Table (entries in the ARP cache).

Example:

```
LEC+ list arp

         LEC Address Resolution (LE ARP Cache) Table

  Max Table Size          = 10
  Free Table Entries      = 10
  Current Mac Entries     = 0
  Current RD Entries      = 0
  Arp Aging Time          = 300
  Verify Sweep Interval   = 60

                              Xmit  BUS   Arp
                        Conn  Queue Frame Retry Aging
 MAC Address     Remote Handle Depth Count Count Timer  Destination ATM Ad
                                                                    dress
 ------------------------------------------------------------------------
 40.00.00.00.00.09 False 652   0     0     0     60     39.99.99.99.99.99.
                               99.00.00.99.99.30.02.40.00.00.00.00.09.81
```

Note: The Sweep Interval is always one-fifth of the ARP Aging Timer value.

Max Table Size
The total number of entries available

Free Table Entries
The number of free entries

Current MAC Entries

Current RD Entries
Route Descriptor ATM entries

ARP Aging Time
Time for an entry to be aged out

Verify Sweep Interval

MAC Address

Remote

Connection Handle

Queue Depth

Xmit Frame Count

BUS Retry Count

ARP Aging Timer

Destination ATM Address

configuration
Lists the LEC configuration.

data Lists the LEC Data Direct VCC information.

Example:

```
LEC+ list data

          LEC Data Direct VCC Table

   Max Table Size     = 1019    Max no of SVC connections
   Current Size       = 0       Currently used
   Inactivity Timeout = 1200    No Data Xfer Timeout before connection is
                                closed (seconds)
   Sweep Interval     = 60
      Conn              Inactive  User
      Handle  VPI  VCI   Timer    Count  Destination ATM Address
    ------------------------------------------------------------------------------

       652     0  7241    300       1    39.99.99.99.99.99.99.00.00.99.99.30.02.
                                          40.00.00.00.00.09.81


    ------------------------------------------------------------------------------
```

group Lists the group addresses in use by the LEC.

rif Lists the MAC address to Routing Information Field (RIF) mappings in use by the LEC.

statistics
Lists LEC statistics.

Example:

```
LEC+ list stat

          LEC Statistics

   In Octets.high     = 0       No of Bytes received
   In Octets.low      = 346
   In Discards        = 2       Packets discarded
   In Errors          = 0       Rx.Errors
   In Unknown Protos  = 0       Unknown protocols received
   Out Octets.high    = 0       No of Bytes xmitted.
   Out Octets.low     = 0
   Out Discards       = 0
   Out Errors         = 0       Tx.Errors
   In Frames          = 0
   Out Frames         = 0
   In Bytes           = 0
   Out Bytes          = 0
```

VCC table
Lists VCC table.

Example:

```
LEC+ list vcc
```

MIB

Use the **mib** command to display MIB objects.

Note: Some of this information may be displayed in a different format using the **list** command.

Syntax:

mib config-table

mac-arp-table

rd-arp-table

server-vcc-table

statistics-table

status-table

config Displays the LEC MIB Configuration Table.

Example:

```
LEC+ mib config

 lecConfigTable:
 lecConfigMode                 = Manual
 lecConfigLanType              = 802.3 - Ethernet
 lecConfigMaxDataFrameSize     = 1516
 lecConfigLanName              =
 lecConfigLesAtmAddress        = 39.84.0F.00.00.00.00.00.11.23.24.24.24.24.55.66.77.88.99.00
 lecControlTimeout             = 120
 lecMaxUnknownFrameCount       = 1
 lecMaxUnknownFrameTime        = 0
 lecVccTimeoutPeriod           = 1200
 lecMaxRetryCount              = 1
 lecAgingTime                  = 300
 lecForwardDelayTime           = 15
 lecExpectedArpResponseTime    = 1
 lecFlushTimeout               = 4
 lecPathSwitchingDelay         = 6
 lecLocalSegmentId             = 0
 lecMulticastSendType          = 1
 lecMulticastSendAvgRate       = 25000000
 lecMulticastSendPeakRate      = 25000000


 lecConnectionCompleteTimer    = 4
```

lecConfigMode
LEC config mode: AUTO or MANUAL. If AUTO, LEC Uses LECS to get the LES ATM address.

lecConfigLanType
LAN type, either Ethernet or token-ring

lecConfigMaxDataFrameSize
Maximum frame size

lecConfigLanName
ELAN Name

lecConfigLesAtmAddress
LE Server ATM address

lecControlTimeout
Timeout for request/response control frame

lecMaxUnknownFrameCount
Maximum number of unknown frames

lecMaxUnknownFrameTime
Period in which LEC will send a maximum of MaxUnknownFrameCount frames to the BUS for a given unicast LAN Destination, and it must also initiate the address resolution protocol to resolve that LAN Destination.

lecVccTimeoutPeriod
Inactivity timeout of SVC Data Direct VCCs

lecMaxRetryCount
LE ARP retry count

lecAgingTime
Life of unverified entry in the ARP table

lecForwardDelayTime

lecExpectedArpResponseTime
ARP Request/Response cycle time

lecFlushTimeout
LE Flush Request/Flush Reply timeout period

lecPathSwitchingDelay

lecLocalSegmentId
Segment ID of emulated LAN. Only for 802.5 clients

lecMulticastSendType
Signaling parameter used by LEC for multicast send VCC

lecMulticastSendAvgRate
Signaling parameter used by LEC for multicast send VCC

lecMulticastSendPeakRate
Signaling parameter used by LEC for multicast send VCC

lecConnectionCompleteTimer

mac Displays the LEC MAC ARP Table

rd Displays the LEC Route Descriptor Table

server Displays the LEC MIB Server VCC Tables

Example:

```
LEC+ mib server

lecServerVccTable:
   lecConfigDirectInterface      = 0
   lecConfigDirectVpi            = 0
   lecConfigDirectVci            = 0
   lecControlDirectInterface     = 1
   lecControlDirectVpi           = 0
   lecControlDirectVci           = 38
   lecControlDistributeInterface = 1
   lecControlDistributeVpi       = 0
   lecControlDistributeVci       = 37
   lecMulticastSendInterface     = 1
   lecMulticastSendVpi           = 0
   lecMulticastSendVci           = 34
   lecMulticastForwardInterface  = 1
   lecMulticastForwardVpi        = 0
   lecMulticastForwardVci        = 33
```

lecConfigDirectInterface
The interface associated with the Configuration Direct VCC

lecConfigDirectVpi
VPI which identifies the above VCC if it exists

lecConfigDirectVci
VCI which identifies the above VCC if it exists

lecControlDirectInterface
The interface associated with the Control Direct VCC

lecControlDirectVpi
VPI which identifies the above VCC if it exists

lecControlDirectVci
VCI which identifies the above VCC if it exists

lecControlDistributeInterface
The interface associated with the Control Distribute VCC

lecControlDistributeVpi
VPI which identifies the above VCC if it exists

lecControlDistributeVci
VCI which identifies the above VCC if it exists

lecMulticastSendInterface
The interface associated with the Multicast Send VCC

lecMulticastSendVpi
VPI which identifies the above VCC if it exists

lecMulticastSendVci
VCI which identifies the above VCC if it exists

lecMulticastForwardInterface
The interface associated with the Multicast Forward VCC

lecMulticastForwardVpi
VPI which identifies the above VCC if it exists

lecMulticastForwardVci
VCI which identifies the above VCC if it exists

statistics
Displays the LEC MIB Statistics Table.

Example:

```
LEC+ mib statistics

lecStatisticsTable:
   lecArpRequestsOut             = 1
   lecArpRequestsIn              = 0
   lecArpRepliesOut              = 0
   lecArpRepliesIn               = 1
   lecControlFramesOut           = 2
   lecControlFramesIn            = 2
   lecSvcFailures                = 1
```

lecArpRequestsOut
No. of LE ARP requests sent by this LEC

lecArpRequestsIn
No. of LE ARP requests received by this LEC

lecArpRepliesOut
No. of LE ARP responses sent by this LEC

lecArpRepliesIn
No. of LE ARP responses received by this LEC

lecControlFramesOut
No. of Control Packets sent by this LEC

lecControlFramesIn
No. of Control Packets received by this LEC

lecSvcFailures
The total number of:

- Outgoing LAN Emulation SVCs which this client tried but failed, to open
- Incoming LAN Emulation SVCs which this client tried, but failed to establish

- Incoming LAN Emulation SVCs which this client rejected for protocol or security reasons

status Lists MIB status.

Example:

```
LEC+ mib status

lecStatusTable:
   lecPrimaryAtmAddress          = 39.84.0F.00.00.00
   Client ATM address=           = 00.00.00.00.00.01.10.00.5A.00.DE.AD.03
   lecId                         = 1                    Assigned by LES
   lecInterfaceState             = Operational          State of the LEC
   lecLastFailureRespCode        = None                 Error code from last
                                                        failed Config/Join resp.
   lecLastFailureState           = Initial State        State of LEC when
                                                        updating above field.
   lecProtocol                   = 1                    Protocol specified by
                                                        LEC in Join requests.
   LecVersion                    = 1                    LEC Protocol Version
                                                        of above
   lecTopologyChange             = False
   lecConfigServerAtmAddress     = 00.00.00.00.00.00.

   lecConfigSource               = Did not use LECS
   lecActualLanType              = 802.3 - Ethernet     Frame format currently
                                                        used by LEC
   lecActualMaxDataFrameSize     = 1516
   lecActualLanName              = ETH                  Name of emulated LAN
                                                        that LEC joined.
   lecActualLesAtmAddress        = 39.84.0F.00.00.00.

   lecProxyClient                = False                Is LES acting like a
                                                        proxy ?
```

QoS Information

Use the **qos-information** command to get to the `LEC x QoS+` prompt from which you can monitor Quality of Service as described in “Quality of Service Monitoring Commands” on page 245.

Syntax:

qos-information

Trace

Use the **trace** command to turn packet tracing on or off on the LEC. See “Chapter 13. Configuring and Monitoring the Event Logging System (ELS)” on page 117 for more information.

Use the **trace mac-address** command to limit the data traced. A packet will only be traced if its destination or source MAC address logically ANDed with the trace MAC mask equals the trace MAC address logically ANDed with the trace MAC mask.

Syntax:

trace

Part 3. Features

Chapter 21. Configuring and Monitoring Quality of Service (QoS)

This chapter describes Quality of Service (QoS) configuration and operational commands for LAN and ELAN interfaces in the device. It contains the following sections:

Quality of Service Overview

The QoS feature leverages the benefits of ATM QoS capabilities for LAN Emulation Data Direct VCCs. This support is referred to as "Configurable QoS for LAN Emulation". The key attributes and the benefits of this feature are as follows:

- An LE Client makes use of configured QoS parameters for its Data Direct VCCs.
- QoS parameters can be configured for:
  - LE Client
  - ATM Interface
- The set of QoS parameters configured are for use with ATM Forum UNI 3.0/3.1 signaling. The parameters include the desired Peak Cell Rate, Sustained Cell Rate, QoS Class and Maximum Burst Size.
- Maximum Reserved Bandwidth per VCC can be configured to protect an LE Client from accepting/establishing VCCs whose traffic parameters it cannot support.
- The QoS Negotiation mechanism enables the participating LE Clients to be aware of each other's QoS parameters. A data-direct VCC is set up using the negotiated parameters.

Benefits of QoS

- Using QoS for the LE Client, ATM Interface, or Emulated LAN provides the following benefits for LANE Data Direct VCCs.
  - An LE Client can be configured with QoS if the QoS required by the client is different from the QoS required by other clients on the ELAN. For example, if an LE Client serves a file server, then the user may want to configure appropriate QoS parameters for all traffic to and from the file server.
  - An Emulated LAN can be configured with QoS if the user wishes to provide QoS for all traffic in that ELAN. For example, an ELAN carrying SNA traffic can be given priority by configuring QoS parameters for that ELAN.

– An ATM Interface can be configured with QoS if a user wants all LE Clients on that ATM interface to use the same set of parameters. For example, if an ATM Interface is connected at 25 Mbps, the user can configure appropriate parameters that are different from those at a 155-Mbps interface.

QoS Configuration Parameters

This section describes nine parameters that are used for QoS configuration. The following six parameters can be configured for an LE Client, ATM Interface, and an Emulated LAN:

1. max-reserved-bandwidth
2. traffic-type
3. peak-cell-rate
4. sustained-cell-rate
5. max-burst-size
6. qos-class

The following two parameters can be configured for an Emulated LAN and an LE Client:

1. *validate-pcr-of-best-effort-vccs*
2. *negotiate-qos*

The *accept-qos-parms-from-lecs* parameter can be configured only for an LE Client.

The first six parameters control the traffic characteristics of Data Direct VCCs established by the LE Client while the first parameter also applies to the calls received by the LE Client. The following characteristics are associated with all the Data Direct VCCs established by the LE Client:

- Bandwidth is not reserved for best-effort traffic.
- Traffic parameters apply to both forward and backward directions.
- When a reserved bandwidth connection is rejected due to the traffic parameters or QoS Class, the call is retried as a best-effort connection with the configured peak cell rate (cause codes on release or release-complete messages are used to determine why a VCC was released).
- When a best-effort connection is rejected due to the Peak Cell Rate (PCR), the call may be automatically retried with a lower PCR. Retries are performed under the following conditions:
  1. If the rejected PCR is greater than 100 Mbps, the call is retried with a PCR of 100 Mbps.
  2. Otherwise, if the rejected PCR is greater than 25 Mbps, the call is retried with a PCR of 25 Mbps.

Maximum Reserved Bandwidth (max-reserved-bandwidth)

The maximum reserved bandwidth acceptable for a Data Direct VCC. This parameter applies to both Data Direct VCC calls received by the LE Client and Data Direct VCC calls placed by the LE Client. For incoming calls, this parameter defines the maximum acceptable SCR for a Data Direct VCC. If SCR is not specified on the incoming call, then this parameter defines the maximum acceptable PCR for a Data Direct VCC with reserved bandwidth.

Calls received with traffic parameters specifying higher rates will be released. If SCR is specified on the incoming call, the call will not be rejected due to the PCR or Maximum Burst Size. The constraint imposed by this parameter is not applicable to best_effort connections. For outgoing calls, this parameter sets an upper bound on the amount of reserved bandwidth that can be requested for a Data Direct VCC. Therefore the traffic-type and sustained-cell-rate parameters are dependent upon this parameter.

Valid Values:
Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:
0

Traffic Type (traffic-type)

The desired traffic type for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the type of calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired type of traffic characteristics for Data Direct VCCs. When QoS parameters are negotiated, if either the source or target LEC desires a reserved bandwidth connection and both LECs support reserved bandwidth connections (that is, max-reserved-bandwidth > 0), then an attempt will be made to establish a reserved bandwidth Data Direct VCC between the two LECs. Otherwise, the Data Direct VCC will be a best-effort connection. Dependencies: max-reserved-bandwidth

Valid Values:
best_effort or reserved_bandwidth

Default:
best_effort

Peak Cell Rate (peak-cell-rate)

The desired peak cell rate for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the PCR traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired PCR traffic parameter for Data Direct VCCs. The minimum of the desired PCRs of the two LECs is used for negotiated best-effort VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired PCR of that LEC is used for the Data Direct VCC subject to the upper bound imposed by the line rate of the local ATM device. If both LECs request a reserved bandwidth connection, then the maximum of the desired PCRs of the LE Clients is used for the Data Direct VCC subject to the upper bound imposed the line rate of the local ATM device.

Valid Values:
An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:
Line speed of LEC ATM Device in Kbps.

Sustained Cell Rate (sustained-cell-rate)

The desired sustained cell rate for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the SCR traffic parameter for Data Direct

VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired SCR traffic parameter for Data Direct VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired SCR of that LEC is used for the Data Direct VCC (subject to the upper bound imposed by the max-reserved-bandwidth parameter of the other LEC). If both LECs request a reserved bandwidth connection, then the maximum of the desired SCRs of the LE Clients is used for the Data Direct VCC (subject to the upper bound imposed by the max-reserved-bandwidth parameters of both LECs). In any case (negotiation or not), if the SCR that is to be signaled equals the PCR that is to be signaled, then the call is signaled with PCR only.

Dependencies: max-reserved-bandwidth, traffic-type and peak-cell-rate. This parameter is applicable only when traffic-type is reserved_bandwidth.

Valid Values:

An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate, specified in Kbps

Default Value

None

Maximum Burst Size (max-burst-size)

The desired maximum burst size for Data Direct VCCs. If QoS parameters are not negotiated, then this parameter specifies the Maximum Burst Size traffic parameter for Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the desired Maximum Burst Size traffic parameter for Data Direct VCCs.

When a reserved bandwidth VCC is negotiated and only one of the LE Clients requests a reserved bandwidth connection, then the desired Maximum Burst Size of that LEC is used for the Data Direct VCC. If both LECs request a reserved bandwidth connection, then the maximum of the desired Maximum Burst Sizes of the LE Clients is used for the Data Direct VCC.

In any case (negotiation or not), the Maximum Burst Size is signaled only when SCR is signaled. Although this parameter is expressed in units of cells, it is configured as an integer multiple of the Maximum Data Frame Size (specified in LEC's C3 parameter) with a lower bound of 1.

Dependencies: This parameter is applicable only when traffic-type is reserved_bandwidth.

Valid Values:

An integer number of frames; must be greater than 0

Default:

1 frame

QoS Class (qos-class)

The desired QoS class for reserved bandwidth calls. If QoS parameters are not negotiated, then this parameter specifies the QoS Class to be used for reserved bandwidth Data Direct VCC calls placed by the LE Client. Otherwise, if QoS parameters are negotiated, this parameter specifies the QoS Class that is desired

for Data Direct VCCs. Unspecified QoS Class is always used on best-effort calls. Specified QoS Classes define objective values for ATM performance. Specified QoS Classes define objective values for ATM performance parameters such as cell loss ratio and cell transfer delay.

The UNI Specification states that:

Specified QoS Class 1
should yield performance comparable to current digital private line performance.

Specified QoS Class 2
is intended for packetized video and audio in teleconferencing and multimedia applications.

Specified QoS Class 3
is intended for interoperation of connection oriented protocols, such as Frame Relay.

Specified QoS Class 4
is intended for interoperation of connectionless protocols, such as IP or SMDS.

LECs must be able to accept calls with any of the above QoS Classes. When QoS parameters are negotiated, the configured QoS Classes of the two LECs are compared, and the QoS Class with the more stringent requirements is used.

Valid Values:
0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:
0 (Unspecified QoS Class)

Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs)

To validate Peak Cell Rate of Best-Effort VCCs. When FALSE, best-effort VCCs will be accepted without regard to the signaled forward PCR. When TRUE, best- effort VCCs will be rejected if the signaled forward PCR exceeds the line rate of the LE Client ATM device. Calls will not be rejected due to the backward PCR. The signaled backward PCR will be honored if it does not exceed the line rate; otherwise, transmissions to the caller will be at line rate.

Notes:

1. Accepting best-effort VCCs with forward PCRs that exceed the line rate can result in poor performance due to excessive retransmissions; however, rejecting these VCCs can result in interoperability problems.
2. The yes setting is useful when callers will retry with a lower PCR following call rejection due to unavailable cell rate.

Valid Values:
yes, no

Default Value:
no

Negotiate QoS (negotiate-qos)

Enable QoS parameter negotiation for Data Direct VCCs. This parameter should be enabled only when connecting to an IBM MSS LES. When this parameter is yes, the LE Client will include an IBM Traffic Parameter TLV in LE_JOIN_REQUEST and LE_ARP_RESPONSE frames sent to the LES. This TLV will include the values of max-reserved-bandwidth, traffic-type, peak-cell-rate, sustained-cell-rate, max-burst-size and qos-class. An IBM Traffic Parameter TLV may also be included in a LE_ARP_RESPONSE returned to the LE Client by the LES.

If there is no TLV in a LE_ARP_RESPONSE received by the LE Client, then the local configuration parameters must be used to setup the Data Direct VCC. If a TLV is included in a LE_ARP_RESPONSE, the LE Client must compare the contents of the TLV with the corresponding local values to determine the “negotiated” or “best” set of parameters acceptable to both parties before signalling for the Data Direct VCC.

Valid Values:
yes, no

Default Value:
no

Accept QoS Parms from LECS (accept-qos-parms-from-lecs)

This parameter gives the ability to configure an LE Client to accept/reject QoS parameters from a LECS. When this parameter is yes, the LE Client should use the QoS parameters obtained from the LE Clients in the LE_CONFIGURE_RESPONSE frames, that is, the QoS parameters from the LE Clients override the locally configured QoS parameters. If this parameter is no then the LE Client will ignore any QoS parameters received in an LE_CONFIGURE_RESPONSE frame from the LE Clients.

Valid Values:
yes, no

Default Value:
no

Accessing the QoS Configuration Prompt

Use the **feature** command from the CONFIG process to access the Quality of Service configuration commands. Enter **feature** followed by the feature number (6) or short name (QoS). For example:

```
Config> feature qos
Quality of Service - Configuration
QoS Config>
```

Once you access the `QoS Config>` prompt, you can configure the Quality of Service (QoS) of an LE Client, or an ATM Interface. To return to the `Config>` prompt at any time, enter the **exit** command at the `QoS Config>` prompt.

Alternatively, you can configure QoS parameters for an LE Client or an ATM Interface by accessing the entities as follows:

- LE Client
  1. At the `Config>` prompt, enter the **network** command and the LE Client interface number.

2. At the LE Client configuration> prompt enter **qos-configuration**.

   Example:

```
config> network 40
Ethernet Forum Compliant LEC Config> qos-configuration
elan-x LEC QoS Config>
```

- ATM Interface
  1. at the Config> prompt, enter the **network** command and the ATM interface number to get you to the ATM Config> prompt.
  2. Enter the **interface** parameter to get to the ATM Interface Config> prompt.
  3. At the ATM InterfaceConfig> prompt enter **qos-configuration**.

     Example:

```
config> network 36
ATM Config> interface
ATM Interface Config> qos-configuration
ATM-I/F 0 QoS>
```

Quality of Service Commands

This section summarizes the QoS configuration commands. Use the following commands to configure Quality of Service. Enter the commands from the QoS Config> prompt.

Table 40. Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
le-client	Gets you to the LE Client QoS configuration > prompt for the selected LE client.
atm-interface	Gets you to the ATM Interface QoS configuration> prompt for the selected ATM interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

LE Client QoS Configuration Commands

This section summarizes and explains the commands for configuring QoS for a specific LE Client.

Use the following commands at the LEC QoS config> prompt.

Table 41. LE Client Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists the current QoS configuration of the LE Client.
Set	Sets the QoS parameters of the LE Client.
Remove	Removes the QoS configuration of the LE Client.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the QoS configuration of this LE Client. QoS parameters are listed only if at least one has been specifically configured (see Example 1). Otherwise, no parameters are listed (see Example 2).

Syntax:

list

Example 1:

```
LEC QoS Config> list

           LE Client QoS Configuration for Data Direct VCCs
           ========================================
     (ATM interface number = 36,  LEC interface number = 40)

  Maximum Reserved Bandwidth for a Data-Direct VCC = 10000 Kbps
  Data-Direct VCC Type ........................... = Best-Effort
  Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
  Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
  Desired QoS Class of Reserved Connections ...... = 0
  Max Burst Size of Reserved Connections    ...... = 0 frames

  Validate Peak Rate of Best-Effort connections .. = No
  Enable QoS Parameter Negotiation ............... = Yes
  Accept QoS Parameters from LECS ................ = Yes

LEC QoS Config>
```

Example 2:

```
LEC QoS Config> list

   QoS has not been configured for this LEC.
   Please use the SET option to configure QoS.

LEC QoS Config>
```

Set

Use the **set** command to specify LE Client QoS parameters.

Syntax:

set	accept-qos-parms-from-lecs
	all-default-values
	max-burst-size
	max-reserved-bandwidth
	negotiate-qos
	peak-cell-rate
	qos-class
	sustained-cell-rate
	traffic-type
	validate-pcr-of-best-effort-vccs

accept-qos-parms-from-lecs
Use this option to enable/disable the LE Client to accept/reject the QoS

parameters received from an LECS as TLVs. See “Accept QoS Parms from LECS (accept-qos-parms-from-lecs)” on page 236 for a more detailed description of this parameter.

Valid Values:

yes, no

Default Value:

yes

Example:

```
LEC QoS Config> se acc y
LEC QoS Config>
```

all-default-values

Use this option to set the QoS parameters to default values. In the following example the default values are also listed.

Example:

```
LEC QoS Config> set all-default-values
   Failed to locate existing QoS configuration record!
   Using a new set of default values ...
   Initializing all parameters to default values
LEC Qos Config> list

              LE Client QoS Configuration for Data Direct VCCs
              ========================================
        (ATM interface number = 36,  LEC interface number = 40)

     Maximum Reserved Bandwidth for a Data-Direct VCC = 0 Kbps
     Data-Direct VCC Type ........................... = Best-Effort
     Data-Direct VCC Peak Cell Rate ................. = 155000 Kbps
     Data-Direct VCC Sustained Cell Rate ............ = 155000 Kbps
     Desired QoS Class of Reserved Connections ...... = 0
     Max Burst Size of Reserved Connections    ...... = 0 frames

     Validate Peak Rate of Best-Effort connections .. = No
     Enable QoS Parameter Negotiation ............... = No
     Accept QoS Parameters from LECS ................ = Yes

  LEC QoS Config>
```

max-burst-size

Sets the desired maximum burst size in frames. See “Maximum Burst Size (max-burst-size)” on page 234 for a more detailed description of this parameter.

Valid Values:

An integer number of frames; must be greater than 0

Default:

1 frame

Example:

```
LEC QoS Config> se ma
   Maximum Burst Size in Kbps [1]? 10000
   LEC QoS Config>
```

max-reserved-bandwidth

Use this option to set the maximum reserved bandwidth allowable per Data Direct VCC. See “Maximum Reserved Bandwidth (max-reserved-bandwidth)” on page 232 for a more detailed description of this parameter.

Valid Values:

Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:

0

Example:

```
LEC QoS Config> set max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]? 20000
LEC QoS Config>
```

negotiate-qos

Use this option to enable/disable the LE Client's participation in QoS negotiation. See "Negotiate QoS (negotiate-qos)" on page 236 for a more detailed description of this parameter.

Valid Values:

yes, no

Default Value:

no

Example:

```
LEC QoS Config> se neg y
LEC QoS Config>
```

peak-cell-rate

Sets the desired peak cell rate for Data Direct. See "Peak Cell Rate (peak-cell-rate)" on page 233 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:

Line speed of LEC ATM Device in Kbps.

Example:

```
LEC QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
LEC QoS Config>
```

qos-class

Sets the desired QoS Class for Data Direct VCCs. See "QoS Class (qos-class)" on page 234 for a more detailed description of this parameter.

Valid Values:

0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:

0 (Unspecified QoS Class)

Example:

```
LEC QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
LEC QoS Config>
```

sustained-cell-rate

Sets the desired sustained cell rate for Data Direct VCCs. See "Sustained Cell Rate (sustained-cell-rate)" on page 233 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate, specified in Kbps

Default Value

None

Example:

```
LEC QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
LEC QoS Config>
```

traffic-type

Sets the desired traffic for Data Direct VCCs. See “Traffic Type (traffic-type)” on page 233 for a more detailed description of this parameter.

Valid Values:

best effort or reserved bandwidth

Default:

best effort

Example:

```
LEC QoS Config>set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved-Bandwidth
Data Direct VCC Type [0]? 1
noTE: Peak Cell Rate has been reset to 1
      Sustained Cell Rate has been reset to 1
      Max Reserved Bandwidth has been reset to 1
      Please configure appropriate values.
LEC QoS Config>
```

validate-pcr-of-best-effort-vccs

Use this option to enable/disable validation of the Peak Cell Rate traffic parameter of the Data Direct VCC calls received by this LE Client. See “Validate PCR of Best-Effort VCCs (validate-pcr-of-best-effort-vccs)” on page 235 for a more detailed description of this parameter.

Valid Values:

yes, no

Default Value:

no

Example:

```
LEC QoS Config> se val y
LEC QoS Config>
```

Remove

Use the **remove** command to remove the QoS configuration of this LE Client.

Syntax:

remove

Example:

```
LEC QoS Config> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the LEC QoS configuration be deleted? [No]: yes
Deleted QoS configuration successfully
LEC QoS Config>
```

ATM Interface QoS Configuration Commands

Table 42. LE Client Quality of Service (QoS) Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists the current ATM Interface QoS configuration.
Set	Sets the ATM Interface QoS parameters.
Remove	Removes the QoS configuration of the ATM Interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the QoS configuration of this ATM Interface. QoS parameters are listed only if at least one parameter has been configured (see following example). Otherwise, no parameters are listed.

Syntax:

list

Example:

```
ATM-I/F 0 QoS> list

          ATM Interface 'Quality of Service' Configuration
          ================================================
                    (ATM interface number = 0  )

     Maximum Reserved Bandwidth for a VCC = 15000 Kbps
     VCC Type ........................... = RESERVED-BANDWIDTH
     Peak Cell Rate ..................... = 20000 Kbps
     Sustained Cell Rate ................ = 5000 Kbps
     QoS Class .......................... = 4
     Maximum Burst Size ................. = 5 frames
ATM-I/F 0 QoS>
```

Set

Use the **set** command to specify ATM Interface QoS parameters.

Syntax:

set max-burst-size
max-reserved-bandwidth
peak-cell-rate
qos-class
sustained-cell-rate
traffic-type

max-burst-size

Sets the desired maximum burst size in frames. See “Maximum Burst Size (max-burst-size)” on page 234 for a more detailed description of this parameter.

Valid Values:

An integer number of frames; must be greater than 0

Default:

1 frame

Example:

```
ATM-I/F 0 QoS Config> se ma
Maximum Burst Size in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

max-reserved-bandwidth

Use this option to set the maximum reserved bandwidth allowable for each Data Direct VCC. See “Maximum Reserved Bandwidth (max-reserved-bandwidth)” on page 232 for a more detailed description of this parameter.

Valid Values:

Integer in the range 0 to the line speed of ATM device in Kbps

Default Value:

0

Example:

```
ATM-I/F 0 QoS> se max-reserved-bandwidth
Maximum reserved bandwidth acceptable for a data-direct VCC (in Kbps) [0]?
15000
ATM-I/F 0 QoS>
```

peak-cell-rate

Sets the desired peak cell rate for Data Direct VCCs. See “Peak Cell Rate (peak-cell-rate)” on page 233 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the line speed of ATM device in Kbps

Default Value:

Line speed of LEC ATM Device in Kbps.

Example:

```
ATM-I/F 0 QoS Config> set peak-cell-rate
Data-Direct VCC Peak Cell Rate in Kbps [1]? 25000
ATM-I/F 0 QoS Config>
```

qos-class

Sets the desired QoS Class for Data Direct VCCs. See “QoS Class (qos-class)” on page 234 for a more detailed description of this parameter.

Valid Values:

0: for Unspecified QoS Class

1: for Specified QoS Class 1

2: for Specified QoS Class 2

3: for Specified QoS Class 3

4: for Specified QoS Class 4

Default Value:

0 (Unspecified QoS Class)

Example:

```
ATM-I/F 0 QoS Config> se qos
Desired QoS Class for Data Direct VCCs [0]? 1
ATM-I/F 0 QoS Config>
```

sustained-cell-rate

Sets the desired sustained cell rate for Data Direct VCCs. See “Sustained Cell Rate (sustained-cell-rate)” on page 233 for a more detailed description of this parameter.

Valid Values:

An integer value in the range 0 to the minimum of max-reserved-bandwidth and peak-cell-rate; specified in Kbps

Default Value

None

Example:

```
ATM-I/F 0 QoS Config> se sus
Data-Direct VCC Sustained Cell Rate in Kbps [1]? 10000
ATM-I/F 0 QoS Config>
```

traffic-type

Sets the desired traffic for Data Direct VCCs. See “Traffic Type (traffic-type)” on page 233 for a more detailed description of this parameter.

Valid Values:

best_effort or reserved_bandwidth

Default:

best_effort.

Example:

```
ATM-I/F 0 QoS> set traffic-type
  Choose from:
     (0): Best-Effort
     (1): Reserved Bandwidth
Traffic Type of VCCs [1]? 0
ATM-I/F 0 QoS>
```

Remove

Use the **remove** command to remove the QoS configuration of this ATM Interface.

Syntax:

remove

Example:

```
ATM-I/F 0 QoS> remove
WARNING: This option deletes the QoS configuration.
         To re-configure use any of the SET options.
Should the ATM Interface QoS configuration be deleted? [No]: yes
Deleted QoS SRAM record successfully
ATM-I/F 0 QoS>
```

Accessing the QoS Monitoring Commands

Use the **feature** command from the GWCON process to access the Quality of Service monitoring commands. Enter the **feature** followed by the feature number (6) or short name (QoS). For example:

```
+feature qos
Quality of Service (QoS) - User Monitoring
QoS+
```

Once you access the QoS monitoring prompt, you can select the monitoring of a particular LE Client. To return to the GWCON prompt at any time, enter the exit command at the QoS monitoring prompt.

Alternatively, you can access the QoS Monitoring of an LE Client as follows:

1. At the GWCON prompt (+), enter the network command and the LE Client interface number.
2. At the LE Client monitoring prompt enter **qos-information**.

   Example:

```
+network 40
ATM Emulated LAN Monitoring
LEC+qos information
LE Client QoS Monitoring
LEC 40 QoS+
```

Quality of Service Monitoring Commands

This section summarizes the QoS monitoring commands. Enter these commands at the QoS+ prompt.

Table 43. Quality of Service (QoS) Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
le-client	Gets you to the `LE Client QoS console +` prompt for the selected LE client.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

LE Client QoS Monitoring Commands

This section summarizes the LE Client QoS monitoring commands. Enter the commands from the `LEC num QoS+` prompt.

Table 44. LE Client QoS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
List	Lists the current LE Client QoS information. Options include: configuration parameters, TLVs, VCCs, and statistics.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to list the QoS related information of this LE Client.

Syntax:

list configuration-parameters
data-direct-VCCs (Detailed Information)
statistics
tlv-information
vcc-information

configuration-parameters

Lists the QoS configuration parameters. Because parameters can be configured for an LE Client, ATM Interface or the ELAN, these parameters are displayed along with a resolved set of parameters that are used by the LE Client.

le-client

The parameters configured for this LE Client which are obtained from the SRAM records. If the SRAM records contain an invalid set of parameters then this column will not display any parameters values.

ATM Interface

The parameters configured for the ATM Interface used by this LE Client. These parameters are obtained from the local SRAM records. If the SRAM records contain an invalid set of parameters then this column will not display any parameter values.

From LECS

The parameters received by this LE Client from the LE Configuration Server. The parameters are received as individual TLVs in the LE_CONFIGURE_RESPONSE control message.

used The resolved set of traffic parameters which are used by for its Data Direct VCCs. If none of the entities is configured with QoS parameters, then the USED parameters represent the default parameters. If parameters are configured for at least one entity, then they are resolved as follows:

- If only the LE Client or the ATM Interface is configured with parameters and either the accept-parms-from-lecs is FALSE or no parameters were received from the LECS, then the configured LE Client or the ATM Interface parameters are used.
- If both the LE Client and the ATM Interface have configured parameters, then the LE Client parameters are used.
- If the accept-parms-from-lecs is TRUE and parameters were received from the LECS, then the LE Client parameters (or the default if the LE Client is not configured) are combined with those received from the LECS to form a complete set of the first six QoS parameters described in “QoS Configuration Parameters” on page 232.
- If the set of the first six QoS parameters described in “QoS Configuration Parameters” on page 232 contains an invalid combination then the parameters from the LECS are rejected. Note that the two flags negotiate-qos and validate-pcr-of-best-effort-vccs are validated independently.

Example:

```
LEC 1 QoS+ list configuration parameters


                ATM LEC Configured QoS  Parameters
                ==================================

     QoS                                        |    LEC      ATM-IF    FROM

   PARAMETER                            USED    |    SRAM     SRAM      LECS

 ------------------------------------------------------------------------------
 Max Reserved Bandwidth (cells/sec) :    23584  |    23584        0     none
                       (Kbits/sec) :    10000  |    10000        0     none
 VCC Type ........................ :   ResvBW  |   ResvBW   BstEft        0
 Peak Cell Rate ........(cells/sec) :    18867  |    18867   365566   365566
```

```
                          (Kbits/sec) :     8000  |     8000   155000   155000
 Sustained Cell Rate ...(cells/sec) :    18867  |    18867   365566     none
                          (Kbits/sec) :     8000  |     8000   155000     none
 QoS Class ....................... :        4  |        4        0     none
 Max Burst Size .....(cells) :       95  |       95        0     none
                            (frames) :        1  |        1        0     none
 Validate PCR of Best-Effort VCCs . :       no  |       no      n/a     none
 Enable QoS Negotiation ........... :      yes  |      yes      n/a     none
 Accept QoS Parameters from LECS .. :      yes  |      yes      n/a      n/a
 ------------------------------------------------------------------------------
(BstEft = Best Effort, ResvBW = Reserved Bandwidth)
(n/a = not applicable, none = no value is specified)

LEC 1 QoS+
```

data-direct-vccs (Detailed Information)

This option lists the Data Direct VCC information of this LE Client. Similar information is also listed using **list vcc-information**.

Example:

```
LEC 1 QoS+ list data direct vccs

          LEC Data Direct VCCs - QoS Information
          ======================================

Conn Handle = 80, VPI = 0, VCI = 546
        Connection Type = RETRIED CONNECTION PARAMETERS
          TrafficType    = BEST EFFORT VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 58962 (25 Mbps)
          QoS Class      = 0
          Max Burst Size = 0

Conn Handle = 78, VPI = 0, VCI = 544
        Connection Type = PARAMETERS SET BY DESTINATION
          TrafficType    = RESERVED BANDWIDTH VCC
          PCR            = 58962 (25 Mbps)
          SCR            = 16509 (7 Mbps)
          QoS Class      = 1
          Max Burst Size = 95

LEC 1 QoS+
```

statistics

Counters are maintained for the following statistics:

Successful QoS Connections
Number of RESERVED-BANDWIDTH connections established by the LE Client.

Successful Best-Effort Connections
Number of BEST-EFFORT connections established by the LE Client.

Failed QoS Connections
Number of RESERVED-BANDWIDTH connection requests made by the LE Client that failed.

Failed Best-Effort Connections
Number of BEST-EFFORT connection requests made by the LE Client that failed.

QoS Negotiation Applied
Number of times the QoS negotiation extension was applied. Parameters are negotiated if the LE Client receives the destination LE Client's parameters in an LE_ARP_RESPONSE control message.

PCR Proposal (IBM) Applied
Number of times the IBM Peak Cell Rate Proposal was applied. This proposal recommends using specific rate parameters if signaling at 100 Mbps or 155 Mbps for BEST-EFFORT connections.

This allows other participating IBM products (for example, 25-Mbps ATM adapters) to reject a connection based on the signaled peak cell rates.

QoS Connections Accepted
Number of RESERVED-BANDWIDTH connections accepted by this LE Client.

Best-Effort Connections Accepted
Number of BEST-EFFORT connections accepted by this LE Client.

QoS Connections Rejected
Number of RESERVED-BANDWIDTH connection requests received by this LE Client that were rejected.

Best-Effort Connections Rejected
Number of BEST-EFFORT connection requests received by this LE Client that were rejected.

Rejected due to PCR Validation
Number of BEST-EFFORT connections rejected by the LE Client due to validation of Peak Cell Rate when the validate-pcr-of-best-effort-vccs parameter is TRUE.

Example:

```
LEC 1 QoS+ li stat

QoS Statistics: of Data Direct Calls Placed by the LEC
------------------------------------------------------
    Successful QoS Connections          = 0
    Successful Best-Effort Connections  = 1
    Failed QoS Connections              = 1
    Failed Best-Effort Connections      = 1
    Qos Negotiation Applied             = 0
    PCR Proposal (IBM) Applied          = 0

QoS Statistics: of Data Direct Calls Received by the LEC
--------------------------------------------------------
    QoS Connections Accepted            = 1
    Best-Effort Connections Accepted    = 0
    QoS Connections Rejected            = 0
    Best-Effort Connections Rejected    = 0
    Rejected due to PCR Validation      = 0

LEC 1 QoS+
```

tlv-information
Lists the IBM Traffic Information TLV that this LE Client registered with the LE Server. The TLV is registered only if the LE Client is participating in QoS Negotiation.

Example:

```
LEC 1 QoS+ list tlv

  Traffic Info TLV of the LEC (registered with the LES)
  =====================================================
    TLV Type .........................= 268458498
    TLV Length .......................= 24
    TLV Value:
           Maximum Reserved Bandwidth = 23584 cells/sec (10 Mbps)
           Data Direct VCC Type...... = RESERVED BANDWIDTH VCC
           Data Direct VCC PCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC SCR....... = 18867 cells/sec (8 Mbps)
           Data Direct VCC QoS Class  = 4
           Maximum Burst Size         = 95 cells (1 frames)

LEC 1 QoS+
```

vcc-information
Lists all active VCCs of the LE Client. The information includes the traffic parameters of the connections. For BEST-EFFORT connections, the

Sustained Cell Rate is displayed to be the same as the Peak Cell Rate, QoS Class and the Maximum Burst Size are displayed as 0.

The Parameter Descriptor entries are:

SrcParms
Parameters of a connection established by this LE Client.

DestParms
Parameters of a connection received by this LE Client.

NegoParms
Parameters of a connection established by the LE Client for which the QoS Negotiation was used.

RetryParms
Parameters of a connection established by this LE Client after failing at least once.

Example:

```
LEC 1 QoS+ li vcc

                          LEC VCC Table
                          =============

                                                                                Burst
Conn   Conn              Conn          VCC    PCR    SCR   QoS   Size    Parameters
Index  Handle VPI   VCI   Type  Status  Type  (kbps) (kbps) Class (cells) Descriptor
-------------------------------------------------------------------------------------
   2)     69    0   535  Cntrl  Ready  BstEft 155000 155000    0      0   SrcParms
   3)     71    0   537  Cntrl  Ready  BstEft      0      0    0      0   DestParms
   4)     72    0   538  Mcast  Ready  BstEft 155000 155000    0      0   SrcParms
   5)     74    0   540  Mcast  Ready  BstEft      0      0    0      0   DestParms
   6)     78    0   544  Data   Ready  ResvBW  25000   7000    1     95   DestParms

LEC 1 QoS+
```

Configuring Quality of Service (QoS)

Chapter 22. Self Learning IP

Self Learning IP is a feature that enables a LAN switch that is inserted between routers and their associated LANs to dynamically determine IP routing information. Once the LAN switch determines routing information, it assumes responsibility for routing all local IP unicast data and transparently passes data it cannot route to the attached router.

Self Learning IP works by snooping on the contents of ARP packets, identifying adjacent routers and building an IP forwarding table. The forwarding table includes the following information:

- IP address of the station
- MAC address of the station
- Interface through which the station can be accessed
- Type of LAN encapsulation used by the station
- MAC address of the station's default router
- Timeout value indicating when the IP forwarding table entry is to be aged-out

The Self Learning IP function does not rely on any routing protocol, so it works seamlessly in networks that use RIP, OSPF, or IGRP.

Note: The Self Learning IP and MPOA client functions are mutually exclusive since only one of these functions may be enabled at any given time.

Accessing the Self Learning IP Configuration Environment

Use the following procedure to access the Self Learning IP configuration process.

1. At the OPCON prompt, enter **talk 6**. For example:

```
* talk 6
Config>
```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.

2. At the CONFIG prompt, enter the **feature self** command to get to the `Self Learning IP Config>` prompt.

Self Learning IP Configuration Commands

Table 45. Self Learning IP Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Disable	Disables Self Learning IP.
Enable	Enables Self Learning IP in default mode.
One_to_one	Enables Self Learning IP in one-to-one mode.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

Disable

Use the **disable** command to disable Self Learning IP.

Syntax:

disable

Enable

Use the **enable** command to enable Self Learning IP in default mode.

Syntax:

enable

One-to-one

When this mode is enabled, the ports on the IBM 8371 are paired. Either of the ports of the dedicated pair may then be connected to a router port and the other port of the dedicated pair is connected to the router's LAN interface. In this mode, broadcast frames received at one port will be transmitted only on the other port of the pair.

To disable One-to-one mode, use the **enable** command to enable Self Learning IP in default mode.

Syntax:

one-to-one

Accessing the Self Learning IP Monitoring Environment

Use the following procedure to access the Self Learning IP monitoring process.

1. At the OPCON prompt, enter **talk 5**. For example:

```
* talk 5

CGW Operator Console

+
```

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter the monitoring environment, press **Return** again.

2. At the + prompt, enter the **feature self learning ip** command to get to the `Self Learning IP Console>` prompt.

Self Learning IP Monitoring Commands

Table 46. Self Learning IP Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Disable	Dynamically disables Self Learning IP.
Enable	Dynamically enables Self Learning IP.

Table 46. Self Learning IP Monitoring Command Summary (continued)

Command	Function
Hosts	Views the discovered hosts.
Routers	Views the discovered routers.
State	Displays the state of Self Learning IP.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **disable** command to dynamically disable Self Learning IP.

Syntax:

disable

Enable

Use the **enable** command to dynamically enable Self Learning IP.

Syntax:

enable

Hosts

Use the **hosts** command to display discovered hosts.

Syntax:

hosts

```
Self Learning IP Console> hosts

Host IP Addr. | Host MAC Address  | IF | EN |    Router MAC     | Ttl
--------------+-------------------+----+----+-------------------+-----
1.1.1.10      | 00:00:00:00:6E:00 | 00 | DX | 00:00:00:00:82:00 | 56 *
2.2.2.20      | 00:00:00:00:78:00 | 01 | SN | 00:00:00:00:82:01 | 56 *
```

Host IP Addr
Specifies the Host IP address.

Host MAC Address
Specifies the Host MAC address

IF Specifies the interface number on which the host has been found.

EN Specifies the encapsulation type. The encapsulation types are SN-LLC/SNAP and DX-DIX.

Router MAC
Specifies the MAC address of this host’s router.

Ttl Specifies the Time to Live for this host entry in this table.

***** Indicates that this entry has an active shortcut.

Routers

Use the **routers** command to display discovered routers.

Syntax:

routers

```
Self Learning IP Console> routers


IF │ Router MAC Address    │ State      │ Ttl
---+-----------------------+------------+-----
01 │ 00:00:00:00:78:00     │RESOLVED    │ 198
00 │ 00:00:00:00:6E:00     │RESOLVED    │ 199
03 │ 00:00:00:00:82:01     │RESOLVED    │ 199
02 │ 00:00:00:00:82:00     │RESOLVED    │ 199
```

IF Specifies the interface to which the router is attached.

Router MAC
Specifies the router MAC address.

State Specifies the interface state.

Ttl Specifies the Time to Live for this router entry in this table.

State

Use the **state** command to display the current state of Self Learning IP.

Syntax:

state

Example:

```
Self Learning IP Console> state
Self Learning IP Enabled Flag is ON
Current Microcode load           Self Learning IP
Self Learning IP Flag in SRAM is ON
Self Learning IP Operation Mode  Default
Number of Routers found          4
Number of Hosts found            10
Memory blocks allocated          32
Memory blocks freed              12
Self Learning IP Console>
```

Chapter 23. Remote Network Monitoring

Remote Network Monitoring (RMON)is a standardized traffic monitor based upon SNMP. For details on RMON MIB implementation, refer to the README files at the FTP site described in “SNMP Management” on page 317.

Accessing the RMON Configuration Environment

Use the following procedure to access the RMON *configuration* process.

1. At the OPCON prompt, enter **talk 6**. For example:

```
* talk 6
Config>
```

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear, press **Return** again.

2. At the CONFIG prompt, enter the **feature rmon** command to get to the `RMON Config>` prompt.

RMON Configuration Commands

Table 47. RMON Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Enable	Enables RMON, on reload. RMON defaults to *enabled*.
Disable	Disables RMON, on reload.
List	Displays RMON’s next state upon reload.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **disable** command to disable RMON upon the next reload.

Syntax:

disable

Enable

Use the **enable** command to enable RMON upon the next reload.

Syntax:

enable

List

Use the **list** command to display RMON’s next state upon reload.

Syntax:

RMON Configuration Commands (Talk 6)

list

```
RMON Config> list

RMON                        = Enabled
```

Accessing the RMON Monitoring Environment

Use the following procedure to access the RMON *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. For example:

   ```
   * talk 5
   +
   ```

   After you enter the **talk 5** command, the CONFIG prompt (+) displays on the terminal. If the prompt does not appear, press **Return** again.
2. At the + prompt, enter the **feature rmon** command to get to the `RMON Console>` prompt.

RMON Monitoring Commands

Table 48. RMON Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Enable	Dynamically enables RMON.
Disable	Dynamically disables RMON.
Memstats	Displays collected memory statistics.
List	Displays current RMON status.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Disable

Use the **disable** command to dynamically disable RMON.

Syntax:

disable

Enable

Use the **enable** command to dynamically enable RMON.

Syntax:

enable

Memstats

Use the **memstats** command to display statistics.

Syntax:

memstats

```
RMON Config> memstats

RMON memory size in use                = 170368 Bytes
RMON memory requests made              = 176
```

RMON memory size in use
Specifies the amount of memory currently in use for RMON.

RMON memory requests made
Specifies the number of requests made for memory.

List

Use the **list** command to display the current state of RMON.

Syntax:

list

```
RMON Config> list

RMON                       = Enabled
```

Part 4. Protocols

Chapter 24. Bridging Methods

This chapter describes the methods of bridging supported by the adaptive source routing transparent (ASRT) bridge. Each section gives an overview of a specific technology and is followed by a description of the data frames supported by that technology. The chapter includes the following sections:

- "Transparent Bridging"

Transparent Bridging

The transparent bridge is also commonly known as a spanning tree bridge (STB). The term *transparent* refers to the fact that the bridge silently forwards non-local traffic to attached LANs in a way that is *transparent* or unseen to the user. End station applications do not know about the presence of the bridge. The bridge learns about the presence of end stations by listening to traffic passing by. From this listening process it builds a database of end station addresses attached to its LANs.

For each frame it receives, the bridge checks the frame's destination address against the ones in its database. If the frame's destination is an end station on the same LAN, the frame is not forwarded. If the destination is on another LAN, the frame is forwarded. If the destination address is not present in the database, the frame is forwarded to all the LANs that are connected to the bridge except the LAN from which it originated.

All transparent bridges use the spanning tree protocol and algorithm. The spanning tree algorithm produces and maintains a loop-free topology in a bridged network that might contain loops in its physical design. In a mesh topology where more than one bridge is connected between two LANs, *looping* occurs. In such cases, data packets bounce back and forth between two LANs on parallel bridges. This creates a redundancy in data traffic and produces the phenomenon known as looping.

When looping occurs, you must configure the local and/or remote LAN to remove the physical loop. With spanning tree, a self-configuring algorithm allows a bridge to be added anywhere in the LAN without creating loops. When the new bridge is added, the spanning tree protocol automatically reconfigures all bridges on the LAN into a single loop-free *spanning tree*.

A spanning tree never has more than one active data route between two end stations, thus eliminating data loops. For each bridge, the algorithm determines which bridge ports can forward data and which ones must be blocked to form a loop-free topology. The features that spanning tree provides include:

- *Loop detection*. Detects and eliminates physical data link loops in extended LAN configurations.
- *Automatic backup of data paths*. The bridges connecting to the redundant paths enter backup mode automatically. When a primary bridge fails, a backup bridge becomes active.
- *User configurability*. Lets you tailor your network topology. Sometimes the default settings do not produce the desired network topology. You can adjust the bridge priority, port priority, and path cost parameters to shape the spanning tree to your network topology.

Bridging Methods

- *Seamless interoperability*. Allows LAN interoperability without configuration limitations caused by diverse communications environments.
- *Bridging of non-routing protocols*. Provides cost-effective bridging of non-routing protocols.

Network Requirements

Transparent Bridge implements a spanning tree bridge that conforms to the IEEE 802.1D standard. All transparent bridges on the network must be 802.1D spanning tree bridges. This spanning tree protocol is not compatible with bridges implementing the proprietary Digital Equipment Corporation spanning tree protocol used in some older bridges.

Transparent Bridge Operation

In a mesh topology where more than one bridge is connected between two LANs, a looping phenomenon can occur where two LANs bounce packets back and forth over parallel bridges. A loop is a condition where multiple data paths exist between two LANs. The spanning tree protocol operating automatically eliminates loops by blocking redundant paths.

During startup, all participating bridges in the network exchange Hello bridge protocol data units (BPDUs) which provide configuration information about each bridge. BPDUs include information such as the bridge ID, root ID, and root path cost. This information helps the bridges to unanimously determine which bridge is the root bridge and which bridges are the designated bridges for LANs to which they are connected.

Of all the information exchanged in the HELLO messages, the following parameters are the most important for computing the spanning tree:

- *root bridge ID*. The root bridge ID is the bridge ID of the bridge. The root bridge is the designated bridge for all the LANs to which it is connected.
- *Root Path Cost*. The sum total of the designated path costs to the root via this bridge's root port. This information is transmitted by both the root bridge and the designated bridges to update all bridges on path information if the topology changes.
- *bridge ID*. A unique ID used by the spanning tree algorithm to determine the spanning tree. Each bridge in the network is assigned a unique bridge identifier.
- *port ID*. The ID of the port from which the current HELLO BPDU message was transmitted.

With this information available, the spanning tree begins to determine its shape and direction and then creates a logical path configuration. This process can be summarized as follows:

1. A root bridge for the network is selected by comparing the bridge IDs of each bridge in the network. The bridge with the lowest ID (that is, highest value) wins.
2. The spanning tree algorithm then selects a designated bridge for each LAN. If more than one bridge is connected to the same LAN, the bridge with the smallest path cost to the root is selected as the designated bridge. In the case of duplicate path costs, the bridge with the lowest bridge ID is selected as the designated bridge.
3. The non-designated bridges on the LANs put each port that has not been selected as a root port into a BLOCKED state. In the BLOCKED state, a bridge

still listens to Hello BPDUs so that it can act on any changes that are made in the network (for example, designated bridge fails) and change its state from BLOCKED to FORWARDING (that is, it will be forwarding data).

Through this process, the spanning tree algorithm reduces a bridged LAN network of arbitrary topology into a single spanning tree. With the spanning tree, there is never more than one active data path between any two end stations, thus eliminating data loops. For each bridge on the network, the spanning tree determines which bridge ports to block from forming loops.

This new configuration is bounded by a time factor. If a designated bridge fails or is physically removed, other bridges on the LAN detect the situation when they do not receive Hello BPDUs within the time period set by the bridge maximum age time. This event triggers a new configuration process where another bridge is selected as the designated bridge. A new configuration is also created if the root bridge fails.

Shaping the Spanning Tree

When the spanning tree uses its default settings the spanning tree algorithm generally provides acceptable results. The algorithm, however, may sometimes produce a spanning tree with poor network performance. In this case you can adjust the bridge priority, port priority, and path cost to shape the spanning tree to meet your network performance expectations. The following examples explain how this is done.

Figure 18 on page 264 shows three LANs networked using three bridges. Each bridge is using default bridge priority settings for its spanning tree configuration. In this case, the bridge with the lowest physical address is chosen as the root bridge because the bridge priority of each bridge is the same. In this example, this is Bridge 2.

The newly configured spanning tree stays intact due to the repeated transmissions of Hello BPDUs from the root bridge at a preset interval (bridge hello time). Through this process, designated bridges are updated with all configuration information. The designated bridges then regenerate the information from the Hello BPDUs and distribute it to the LANs for which they are designated bridges.

Table 49. Spanning Tree Default Values

Bridge 1	**Bridge 2**	**Bridge 3**
Bridge Priority: 32768 Address: 00:00:90:00:00:10	Bridge Priority: 32768 Address: 00:00:90:00:00:01	Bridge Priority: 32768 Address: 00:00:90:00:00:05
Port 1 Priority: 128 Path Cost: 100	**Port 1** Priority: 128 Path Cost: 100	**Port 1** Priority: 128 Path Cost: 100
Port 2 Priority: 128 Path Cost: 17857	**Port 2** Priority: 128 Path Cost: 17857	**Port 2** Priority: 128 Path Cost: 17857
Port 3 Priority: 128 Path Cost: 17857	**Port 3** Priority: 128 Path Cost: 17857	**Port 3** Priority: 128 Path Cost: 17857

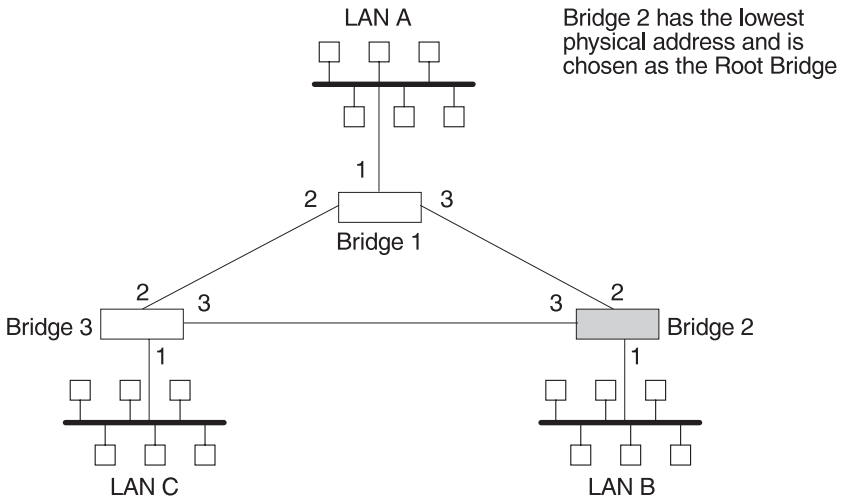

Figure 18. Networked LANs Before Spanning Tree

The spanning tree algorithm designates the port connecting Bridge 1 to Bridge 3 (port 2) as a backup port and blocks it from forwarding frames that would cause a loop condition. The spanning tree created by the algorithm using the default values in Table 49 on page 263 is shown in Figure 19 as the heavy lines connecting Bridge 1 to Bridge 2, and then Bridge 2 to Bridge 3. The root bridge is Bridge 2.

This spanning tree results in poor network performance because the workstations on LAN C can get to the file server on LAN A only indirectly through Bridge 2 rather than using the direct connection between Bridge 1 and Bridge 3.

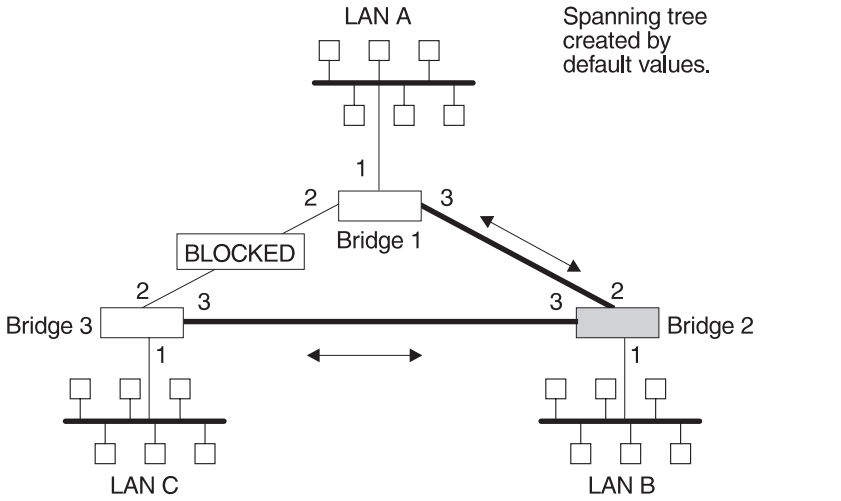

Figure 19. Spanning Tree Created With Default Values

Normally, this network uses the port between Bridge 2 and Bridge 3 infrequently. Therefore you can improve network performance by making Bridge 1 the root bridge of the spanning tree. You can do this by configuring Bridge 1 with the highest priority of 1000. The spanning tree that results from this modification is shown in Figure 20 on page 265 as the heavy lines connecting Bridge 1 to Bridge 3 and Bridge 1 to Bridge 2. The root bridge is now Bridge 1. The connection between Bridge 2 and Bridge 3 is now blocked and serves as a backup data path.

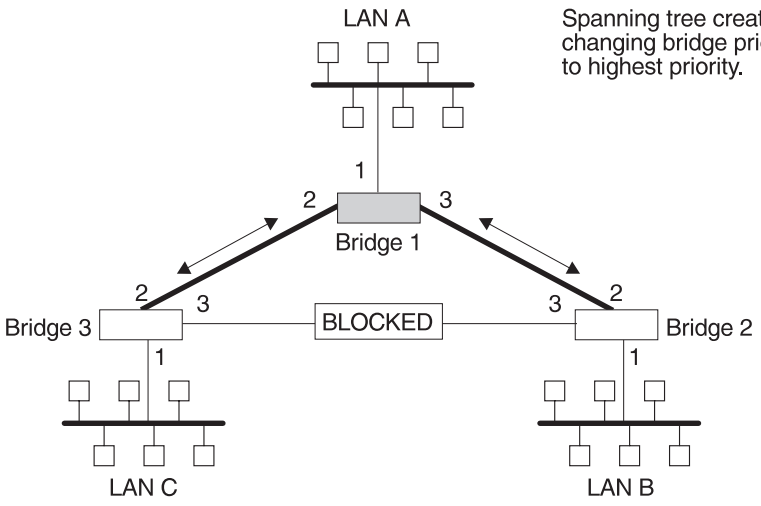

Figure 20. User-Adjusted Spanning Tree

Transparent Bridging and ATM

The ATM interface forwards transparent frames from Ethernet networks, provided bridging is enabled on the virtual channel connection (VCC).

Hello BPDUs are generated and transmitted for each LEC configured for transparent bridging. The spanning tree protocol causes ATM LECs that have not been designated as part of the active data path to be BLOCKED, thereby eliminating loops.

Transparent Bridge Terminology and Concepts

This section reviews the terms and concepts commonly used in transparent bridging.

Aging Time

The length of time (age) before a dynamic entry is removed from the filtering database when the port with the entry is in the forwarding state. If dynamic entries are not referenced by the aging time, they are deleted.

Bridge

A protocol-independent device that connects local area networks (LANs). These devices operate at the data link layer, storing and forwarding data packets between LANs.

Bridge Address

The least significant 6-octet part of the bridge identifier used by the spanning tree algorithm to identify a bridge on the network. The bridge address is set to the MAC address of the lowest-numbered port by default. You can override the default address by using the **set bridge** configuration command.

Bridge Hello Time

The bridge hello time specifies how often a bridge sends out Hello BPDUs (containing bridge configuration information) when it becomes the root bridge in the spanning tree. This value is useful only for the root bridge because it controls the hello time for all bridges in the spanning tree. Use the **set protocol bridge** command to set the bridge hello time.

Bridge Forward Delay

The amount of time a bridge port spends in the listening state as well as the learning state. The forward delay is the amount of time the bridge port listens in order to adjust the spanning tree topology. It is also the amount of time the bridge spends learning the source address of every packet that it receives while the spanning tree is configuring. This value is useful only for the root bridge because it controls the forward delay for all bridges in the spanning tree.

The root bridge conveys this value to all bridges. This time is set with the **set protocol bridge** command. The procedure for setting this parameter is discussed in the next chapter.

Bridge Identifier

A unique identifier that the spanning tree algorithm uses to determine the spanning tree. Each bridge in the network must have a unique bridge identifier.

The bridge identifier consists of two parts: a least-significant 6-octet bridge address and a most-significant 2-octet bridge priority. By default, the bridge address is set to the MAC address of the lowest-numbered port. You can override the default address with the **set bridge** configuration command.

Bridge Maximum Age

The amount of time that spanning tree protocol information is considered valid before the protocol discards the information and a topology changes. All the bridges in the spanning tree use this age to time out the received configuration information in their databases. This can cause a uniform timeout for every bridge in the spanning tree. Use the **set protocol bridge** command to set the bridge maximum age.

Bridge Priority

The most significant 2-octet part of the bridge identifier set by the **set protocol bridge** command. This value indicates the chances of each bridge becoming the root bridge of the network. In setting the bridge priority, the spanning tree algorithm chooses the bridge with the highest priority value to be the root bridge of the spanning tree. A bridge with the lowest numerical value has the highest priority value.

Designated Bridge

The bridge that claims to be the closest to the root bridge on a specific LAN. This closeness is measured according to the accumulated path cost to the root bridge.

Designated Port

The port ID of the designated bridge attached to the LAN.

Filtering and Permanent Databases

Databases that contain information about station addresses that belong to specific port numbers of ports connected to the LAN.

The filtering database is initialized with entries from the permanent database. These entries are permanent and survive power on/off or system resets. You can add or delete these entries through the spanning tree configuration commands. Entries in the permanent database are stored as static random access memory (SRAM) records, and the number of entries is limited by the size of SRAM.

Note: You can also add entries (static) by using the monitoring commands but these ***do not*** survive power on/off and system resets.

The filtering database also accumulates entries learned by the bridge (dynamic entries) which have an aging time associated with them. When entries are not referenced over a certain time period (age time), they are deleted. Static entries are ageless, so dynamic entries cannot overwrite them.

Entries in the filtering and permanent databases contain the following information:

- *Address*. The 6-byte MAC address of the entry
- *Port Map*. Specifies all port numbers associated with that entry
- *Type of Entry*. Specifies one of the following types:
  - Reserved Entries. Reserved by the IEEE 802.1d committee.
  - Registered Entries. Consist of unicast addresses belonging to communications hardware attached to the box or multicast addresses enabled by protocol forwarders.
  - Permanent Entries. Entered by the user in the configuration process. They survive power on/off and system resets.
  - Static Entries. Entered by the user in the monitoring process. They do not survive power on/off and system resets and are ageless.
  - Dynamic Entries. Dynamically learned by the bridge. They do not survive power on/off and system resets and have an associated age.
  - Free. Locations in database that are free to be filled by address entries.
- *Address Age (dynamic entries only)*. Resolution of time period at which address entries are ticked down before being discarded. You can set this value.

Make changes to the permanent database through the spanning tree configuration commands and make changes to the filtering database through the GWCON monitoring process.

Parallel Bridges

Two or more bridges connecting the same LANs.

Path Cost

Each port interface has an associated path cost which is the relative value of using this port to reach the root bridge in a bridged network. The spanning tree algorithm uses the path cost to compute a path that minimizes the cost from the root bridge to all other bridges in the network topology. The sum total of all the designated costs and the path cost of the root port is called the root path cost.

Port

The bridge's connection to each attached LAN or WAN. A bridge must have at least two ports to function as a bridge.

Port ID

A 2-octet port identifier. The most-significant octet represents the port priority and the least-significant octet represents the port number. Both port number and port priority are user-assignable. The port ID must be unique within the bridge.

Port Number

A user-assigned 1-octet part of the port ID whose value represents the attachment to the physical medium. A port number of zero is not allowed.

Port Priority

The second 1-octet part of the port ID. This value represents the priority of the port that the spanning tree algorithm uses in making comparisons for port selection and blocking decisions.

Resolution

The time factor by which dynamic entries are ticked down as they age within the database. The range is 1 to 60 seconds.

Root Bridge

The bridge selected as the *root* of the spanning tree because it possesses the highest priority bridge ID. This bridge is responsible for keeping the spanning tree intact by regularly emitting Hello BPDUs (containing bridge configuration information). The root bridge is the designated bridge for all the LANs to which it is connected.

Root Port

The port ID of a bridge's port that offers the lowest cost path to the root bridge.

Spanning Tree

A topology of bridges such that there is one and only one data route between any two end stations.

Transparent Bridging

This type of bridging involves a mechanism that is *transparent* to end stations applications. Transparent bridging interconnects local area network segments by bridges designated to forward data frames through a spanning tree algorithm.

Chapter 25. Bridging Features

This chapter describes bridging features that are available with the Adaptive Source Routing Transparent (ASRT) bridge. The chapter includes the following sections:

- "TCP/IP Host Services (Bridge-Only Management)"
- "Bridge-MIB Support"

TCP/IP Host Services (Bridge-Only Management)

The IBM 8371 also supports TCP/IP Host services, which let you configure and monitor a bridge . This option gives you the following capabilities:

- Management through SNMP
- Telnet server function
- Downloading and uploading of configurations through the TFTP protocol
- TFTP neighbor boot function
- IP diagnostic tools of ping and trace route
- Control of the device through SNMP sets and the telnet client

When viewed from the bridge's monitoring interface, TCP/IP Host Services is handled as a new protocol having its own configuration and monitoring prompts. These prompts are accessed via the **protocol** command in `talk 6` and `talk 5`.

Bridge-MIB Support

For Bridge Management via SNMP, the IBM 8371 supports the management information bases (MIBs) as specified by RFC 1493 and RFC 1525, ***except*** for the following MIBs:

- dot1dStaticTable
- dot1dTpFdbTable
- dot1dPortPairTable

Dynamic Protocol Filtering VLANs

Dynamic protocol filtering (DPF) VLANs are based on protocol and subnets, in addition to user-defined traffic types. For each configured vlan, the subset of bridge ports on which traffic for that vlan is received is the forwarding domain of that vlan. Dynamic protocol filtering (DPF) can partition the bridged network into:

- IP, IPX, and NetBIOS Protocol VLANs

  DPF monitors traffic on each bridge port and learns the location of traffic matching the configured protocols and subnets. Ports with matching inbound traffic are included in the forwarding domain of the corresponding VLAN.
- IP Multicast VLANs

  IP Multicast VLANs restrict IP multicast data to ports in the same IP multicast group and ports attached to multicast devices. IGMP Report frames are used to determine port inclusion in the forwarding domain for a particular IP Multicast VLAN. Also, ports receiving IGMP Query device frames are included in the forwarding domain of all IP Multicast VLANs to insure all IP multicast data is sent to the multicast devices.

Bridging Features

The purpose of DPF is to limit the proliferation of frames that are normally forwarded over all active spanning tree ports. DPF dynamically activates filters based upon the traffic on each bridge port. The bridged network can thus be dynamically partitioned into protocol-specific subnetworks.

DPF offers further benefits to increase performance, enhance security and facilitate moves and changes in the network.

For subnetted IP networks, DPF has an *IP-cut-through* facility that allows establishment of data-direct VCCs between IP workstations on different IP subnet VLANs. By enabling *IP-cut-through* and shortening the IP subnet mask in end-stations, the end-stations communicate directly with each other without involving an IP device. This significantly increases IP throughput in the network, reduces IP routing requirements, and isolates IP subnet broadcast traffic.

IP-cut-through can be enabled or disabled by an IP subnet or IP end-station. *IP-cut-through* can also be configured to allow cut-through in one direction but force a routed path in the reverse direction. This uni-directional cut-through can be used to force IP clients to go through an IP device for security but allow IP servers to “cut through” to the clients for maximum performance.

Since DPF automatically adjusts the forwarding domain of a VLAN based on traffic, it lets users move around the network without any changes to their configuration. This is especially useful for IP networks, because it eliminates the need for assigning new IP addresses when users move.

DPF is a bridging enhancement. All ports on the ASRT bridge environment must be the same type. VLANs can be configured for multiple IP subnets, multiple IPX networks, a single NetBIOS network, user-defined traffic types, and IP multicast groups.

Required Static Configurations

You must statically configure VLAN ports in the following situations:

- Ports with devices with low network utilization.

  Devices such as printers, servers or devices on a port could lose connectivity because of low network utilization. To prevent aging-out of a port that defines a VLAN to such a device, configure the port statically; specify **include** when prompted to configure the VLAN on the port. For example:
- A bridge port connected to IPX clients only.

  IPX clients do not know their network numbers. This prevents a VLAN from learning the association between the network number and the port number. Specify **include** when prompted to configure the VLAN for a bridge port connected to IPX clients only.

IP-Cut_Through Considerations

IP Cut-Through enables communication between stations on different IP subnets. IP Cut-Through is applicable in subnetted IP networks only. If stations are on different IP nets, then communication cannot be established between them and a device must be used to forward traffic between those stations.

To use IP Cut-Through, the subnet mask in end-stations (typically just servers) should be shortened. That is, a 255.255.255.255 subnet mask is shortened to

255.255.255.0 to imply a 3-byte subnet and a 255.255.0.0 subnet mask implies a 2-byte subnet. Shortening the subnet mask will cause the end-station to ARP for the destination and establish communication to the destination (or intermediate LAN switch), maximizing network throughput. However, this configuration can produce the following side effects:

1. A large number of ARP entries can be created in end-stations with a shortened mask which in turn can increase their CPU utilization. If these end-stations are ATM-attached, the number of ATM connections (data-direct VCCs) will also increase.

   Therefore, the need for faster network throughput must be balanced against increased CPU utilization in the end-stations and increased VCC utilization in the ATM switches.
2. An end-station with a shortened mask could ARP for a destination that is not directly connected. For example, this can happen if the destination is on a different type of LAN or behind a device firewall. The only way to reach this destination is through a device but devices normally do not propagate ARPs between networks. This scenario can work only when the Proxy ARP function is enabled in the device. This will cause the device to respond to the ARP and subsequent traffic will be sent to the device.

Answering Yes to the **Enable IP-Cut-Through from this VLAN?** question will allow forwarding of IP traffic from devices on this VLAN to devices on other VLANs that have IP-Cut-Through reception enabled.

Auto-created IP Multicast VLANs

Unlike other VLANs, IP Multicast VLANs can be automatically created and configured without user involvement. If auto-creation of IP Multicast VLANs is enabled, then the receipt of an IGMP Report frame (indicating a station's membership in an IP multicast group) causes an IP Multicast VLAN to be created for the group address indicated in the frame. Thus, IP Multicast groups can be configured on stations in the network without the need for VLAN configuration in the MSS bridge.

Auto-creation is enabled if an IP Multicast VLAN exists for the all IP hosts address of 224.0.0.1 and is enabled. If not already present, this VLAN is created and enabled during box initialization. It contains the initial port configuration, aging time, and MAC Address tracking status that will be applied to each new IP Multicast VLAN that is automatically created. To turn off auto-creation of IP Multicast VLANs, disable the VLAN for the 224.0.0.1 group address.

No IP Multicast VLANs can be auto-created or manually configured for the reserved multicast groups whose address is between 224.0.0.0 and 224.0.0.255, inclusive. This prevents potential problems in filtering frames necessary to several protocols that use these addresses.

Chapter 26. Configuring and Monitoring Bridging

This chapter describes how to configure the adaptive source routing transparent (ASRT) bridge protocol and how to use the ASRT configuration commands. The chapter includes the following sections:

- "Accessing the ASRT Configuration Environment"
- "ASRT Configuration Commands"

Accessing the ASRT Configuration Environment

To access the ASRT configuration environment, enter the **protocol asrt** command at the Config> prompt:

```
Config>protocol asrt
Adaptive Source Routing Transparent Bridge user configuration
ASRT config>
```

ASRT Configuration Commands

The ASRT configuration commands allow you to specify network parameters for the ASRT bridge and its network interfaces. These commands also allow you to enable and configure the NetBIOS, and ATM interface features.

The device must be restarted for the new configuration to take effect.

Enter the ASRT configuration commands at the ASRT config> prompt. Access the commands as follows:

- Enter the configuration commands for dynamic protocol filtering (Virtual LANs) at the VLAN config> prompt. The VLAN prompt is accessed by entering the **vlans** command explained later in this chapter.

Table 50 shows the ASRT configuration commands.

Table 50. ASRT Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds station address entries to the permanent database.
Delete	Deletes station address entries.
Disable	Disables the following functions: • Bridging • Propagation of Spanning Tree Explorer Frames • Transparent (spanning tree) bridging function on a given port
Enable	Enables the following functions: • Bridging • Propagation of Spanning Tree Explorer Frames • Transparent (spanning tree) bridging function on a given port
List	Displays information about the complete bridge configuration or about selected configuration parameters.

Table 50. ASRT Configuration Command Summary (continued)

Command	Function
Set	Sets the following parameters: • Aging time for dynamic address entries • Bridge address • Maximum frame size • Spanning tree protocol bridge and port parameters • Filtering database size • IPX Conversion Mode • Ethernet Preference
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add the following information to your bridging configuration:

- Station address entries to the permanent database
- LAN/WAN ports

Syntax:

add address . . .
dmac-addr
port . . .

address *addr-value*

Adds unique station address entries to the permanent database. These entries are copied into the filtering database as permanent entries when the bridge is restarted. The *addr-value* is the MAC address of the desired entry. It can be an individual address, multicast address, or broadcast address. You are also given the option to specify the outgoing forwarding port map for each incoming port. Permanent database entries are not destroyed by the power off/on process and are immune to the aging settings. Permanent entries cannot be replaced by dynamic entries.

Valid Values: X’0000 0000 0000’ to X’FFFF FFFF FFFF’

Default Value: none

The following sections present specific examples of how the **add address** command is used to manage address entries:

Adding an address

```
add address
Address (in 12-digit hex) []? 123456789013
    Exclude destination address from all ports?(Yes or [No]):
    Use same output port mapping for all input Ports?(Yes or [No]):
    Output port mapping:
       Input Port Number [1]?
       Bridge to all ports?(Yes or [No]):
       Bridge to  port 1  Yes or [No]:
       Bridge to  port 2  Yes or [No]:
       Bridge to  port 3  Yes or [No]:
       Bridge to  port 4  Yes or [No]:
       Bridge to  port 5  Yes or [No]:
       continue to another input port? (Yes or [No]): y
       Input Port Number [2]? 3
       Bridge to all ports?(Yes or [No]): y
       continue to another input port? (Yes or [No]): y
       Input Port Number [4]?
       Bridge to all ports?(Yes or [No]):
       Bridge to  port 1  Yes or [No]:
```

```
   Bridge to  port 2  Yes or [No]:
   Bridge to  port 3  Yes or [No]:
   Bridge to  port 4  Yes or [No]:
   Bridge to  port 5  Yes or [No]:
   continue to another input port? (Yes or [No]): n
Source Address Filtering Applies? (Yes or No): y
ASRT config>
```

Note: For any "Yes or No" question in the prompts, "No" is the default value. Press **Return** to accept the default value.

Exclude destination address ...
This prompt lets you set destination address filtering for that entry. Answering *yes* to the prompt causes filtering of any frames that contain this address as a destination address no matter which port it came from.

Use same output mapping...
Answering *yes* to this prompt lets you create one outgoing port map for all incoming ports rather than allowing for mapping to only specific ports. Answering *no* to this prompt causes further prompting (`Input Port Number [1]?`) to select each input port. From that specific input port prompt you can then create a unique port map for that input port.

Input Port 1, Port 2
Answering "No" to the previous prompt causes input port-by-input port prompting (`Input Port Number [1]?`) to select each input port and its associated outgoing bridge ports.

Bridge to all ports?
Answering *yes* to this prompt creates an outgoing port map that includes all ports. Thus, when a frame with this address as the destination address is received, it is forwarded to all outgoing forwarding ports except for the incoming port. The following are examples of how this is done according to the port map:

If a frame is received on *port 1* and the port map indicates 1 (for port 1), the frame is filtered.

If the same frame is received on *port 2* and the port map indicates 1 (for port 1), the frame is forwarded to port 1. If a frame is received on port 1 and the matching address entry's port map indicates 1, 2, or 3, the frame is forwarded to ports 2 and 3.

If the port map indicates no port (NONE/DAF), the frame is filtered. This is known as destination address filtering (DAF).

If no address entry is found to match the received frame, it is forwarded to all the forwarding ports except for the source port.

Bridge to Port 1, Port 2, etc.
This prompt lets you associate an address entry with that specific bridge port. Answering *yes* maps the address to the specified port so that the port is included in that address entry's port map. Answering *no* skips address mapping for that port.

continue to another bridge port?
This prompt lets you select the next input port to be configured.

Source address filtering
This allows for port-specific source address filtering (SAF). When SAF is applied (answer *yes* at the prompt), frames received with source addresses that match address entries in the filtering

database that have source address filtering enabled will be discarded. This mechanism allows a network manager to isolate an end station by prohibiting its traffic to be bridged.

Enabling Destination Address Filtering For Entry

This example shows how to answer the command prompts to select destination address filtering for an entry:

```
ASRT config>add address 000000334455
Exclude destination address from all ports?(Yes or [No]): y
Source Address Filtering Applies? (Yes or [No]): y
ASRT config>
```

After adding the address entry, you can verify its status by using the **list range** command. The following example shows that no port map exists for that entry (in bold) and that destination address filtering (DAF) has been turned on.

```
ASRT config>list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

00-00-00-22-33-44       PERMANENT       Input Port:  3
                                        Output ports: 1, 2
                                        Input Port:  4
                                        Output ports:  1, 2

00 00 00 33 44 55       PERMANENT       NONE/DAF
```

Output Port Map Created For Address Entry Having More Than One Input Port

This example shows how to answer the command prompts to create separate output port maps for an address entry that will have more than one input port.

```
ASRT config> add address 000000123456
Exclude destination address from all ports?(Yes or [No]):
Use same output port mapping for all input Ports?(Yes or [No]):
Input Port Number [1]? 1
Bridge to all ports ?(Yes or [No]):
Bridge to port 1 - Yes or [No]: y
Bridge to port 2 - Yes or [No]: y
Bridge to port 3 - Yes or [No]:
continue to another input port ? (Yes or [No]): y
Input Port Number [2]?
Bridge to all Ports?(Yes or [No]):
Bridge to Port 1 - Yes or [No]:
Bridge to port 2 - Yes or [No]:
Bridge to port 3 - Yes or [No]: y
continue to another input port ? (Yes or [No]):
Source Address Filtering Applies? (Yes or [No]):
ASRT config>
```

After adding the address entry, you can verify its status by using the **list range** command. The following example shows an entry (in bold) that has ports 1 and 2 as input ports and has separate port maps for both input ports. Source address filtering (SAF) has also been enabled.

```
ASRT config> list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF

00-00-00-12-34-56       PERM/SAF        Input Port:  1
```

```
Output ports: 1, 2
Input Port:  2
Output ports: 3
```

Single Output Port Map Created All Incoming Ports Associated With Address Entry

This example shows how to answer the command prompts to create a single output port map for all incoming ports associated with an address entry.

```
ASRT config> add address 000000556677
Exclude destination address from all ports?(Yes or [No]):
Use same output port mapping for all input Ports?(Yes or [No]): y
   Bridge to all ports?(Yes or [No]): n
   Bridge to  port 1 - Yes or [No]: y
   Bridge to  port 2 - Yes or [No]: y
   Bridge to  port 3 - Yes or [No]:
Source Address Filtering Applies? (Yes or [No]): y
ASRT config>
```

After adding the address entry, you can verify its status by using the **list range** command. The example below shows an entry (in bold) that has a single port map for all incoming ports. Source address filtering (SAF) has also been enabled.

```
ASRT config> list range
Start-Index [1]?
Stop-index [3]?
ADDRESS                 ENTRY TYPE      PORT MAP
=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF

00-00-00-55-66-77       PERM/SAF        Input Port:  ALL PORTS
                                        Output ports:  1, 2
```

port *interface# port#*

Adds a LAN/WAN port to the bridging configuration. This command associates a port number with the interface number and enables that port's participation in transparent bridging.

Port Number Valid Values: 1 to 254

Port Number Default Value: none

Example: add a port

```
ASRT config> add port
Interface Number [0]?
Port Number [5]?
```

See "ATM Commands" on page 287 for information about adding ATM ports.

Delete

Use the **delete** command to delete the following information from your bridging configuration:

- Station address entries to the permanent database

Syntax:

delete address

port . . .

address *addr-value*

Deletes an address entry from the permanent database. The address is the MAC address of the desired entry. Enter the addr-value (in 12-digit hexadecimal format) of the entry to be deleted and press **Return**. Reserved multicast addresses cannot be deleted. If you attempt to delete an address entry that does not exist, you will receive the message

```
Record matching that address not found
```

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: none

Example: `delete address`

port *port#*

Removes a port from a bridging configuration. Because the **enable bridge** command by default configures all LAN devices to participate in bridging, this command allows you to customize which devices should or should not participate in the bridging. The port number value normally is one greater than the interface number.

Example: `delete port 2`

Disable

Use the **disable** command to disable the following bridge functions:

- Bridging
- Propagation of Spanning Tree Explorer Frames
- Transparent (spanning tree) bridging function on a given port

Syntax:

disable bridge
stp
transparent . . .
tree

bridge

Disables bridging function entirely. This command does not remove previously configured bridging values, however.

Example: `disable bridge`

stp Disables the Spanning Tree Protocol on the bridge. The default is enabled.

Example: `disable stp`

transparent *port#*

Disables transparent bridging function on the given port.

Example: `disable transparent 2`

tree *port#*

Disables STP participation for the bridge on a per-port basis.

Example: `disable tree 1`

Note: Disabling STP on a per-port basis can produce network loops because of the existence of parallel bridges.

Enable

Use the **enable** command to enable the following bridging functions:

- Bridging
- Propagation of Spanning Tree Explorer Frames
- Transparent (Spanning Tree) bridging function on a given port

Syntax:

enable bridge . . .
stp
transparent . . .
tree

bridge
Enables transparent bridging function on all the LAN devices (interfaces) configured in the bridging device. The port numbers are assigned to each interface as the previous interface number plus 1. For example, if interface 0 is a LAN device its port number will be 1.

Example: `enable bridge`

stp Enables the spanning tree protocol on the bridge. This is the default.

Example: `enable stp`

transparent *port#*
Enables transparent bridging function on the given port. Under normal circumstances, this command is not necessary.

Example: `enable transparent`

```
Port Number [1]?
```

tree *port#*
Enables STP participation for the bridge on a per-port basis.

Example: `enable tree 1`

List

Use the **list** command to display information about the complete bridge configuration or to display information about selected configuration parameters.

Syntax:

list address
bridge
filtering . . .
permanent . . .
port . . .
protocol
range . . .

address *addr value*

Reads an address entry from the permanent database. The addr value is the MAC address of the required entry. It can be an individual address, multicast address, or broadcast address. Permanent databases are not destroyed by the power off/on process and are immune to the aging settings. Permanent entries cannot be replaced by dynamic entries.

Valid Values: X'0000 0000 0000' to X'FFFF FFFF FFFF'

Default Value: none

Example: `list address 000000123456`

```
0000-00-12-34-56    PERMANENT  Input Port:  1
                               Output ports:  1, 2
                               Input port:  2
                               Output ports:  3
ASRT config>
```

Address

Address entry in 12-digit hexadecimal format.

Entry Type

Permanent

Indicates that the entry is permanent in nature and will survive power on/offs or system resets.

Reserved

Indicates that the entry is reserved by the IEEE 802.1d committee for future use. Frames destined to reserved addresses are discarded.

Registered

Indicates that the entry is meant for the bridge itself.

SAF Appears after the entry type if source address filtering has been configured.

Input Port

Displays the numbers of the input port or ports associated with that address entry.

Output Port

Displays the numbers of the output port or ports associated with that address entry. Displays "NONE/DAF" to indicate that destination address filtering applies because no ports have been selected to be associated with that address entry.

bridge

Lists all general information regarding the bridge.

filtering *datagroup-option*

The following general data groups can be displayed under the **list filtering** command:

All Displays all filtering database entries.

Ethertype

Displays Ethernet protocol type filter database entries.

SAP Displays SAP protocol filter database entries.

SNAP Displays SNAP protocol identifier filter database entries.

The following examples illustrate each of the **list filtering** display options.

Example 1: `list filtering all`

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

Descriptors used in explaining how packets are communicated include:

Routed
Describes packets passed to routing forwarder to be forwarded.

Filtered
Describes packets that are administratively filtered setting protocol filters that you set.

Bridged and routed
This describes a protocol identifier for which there is a protocol entity within the system that is not a forwarder. For example a link level echo protocol. Unicast packets from this protocol are bridged or locally processed if being sent to a registered address. Multicast packets are forwarded and locally processed for a registered multicast address.

All of these descriptors also apply to ARP packets with this Ethertype.

Example 2:

`list filtering ethertype`

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

Example 3:

`list filtering sap`

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

Example 4:

`list filtering snap`

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

mapping *add-type type-field*
Lists specific address mapping for a given protocol.

Example: `list mapping SNAP`

```
PROTOCOL TYPE          GROUP ADDRESS          FUNCTIONAL ADDRESS
=============          =============          ==================
123456-7890            12-34-56-78-90-12      12:34:56:78:90:12
```

add-type
Choice of either DSAP, Ether (Ethernet), or SNAP.

type-field
Protocol type field:

- Destination Service Access Point (DSAP) protocol type is entered in the range 1–FE (hexadecimal).
- Ethernet (Ether) protocol type is entered in the range of 5DD–FFFF (hexadecimal).
- Subnetwork Access Protocol (SNAP) protocol type is entered in 10-digit hexadecimal format.

permanent
Displays the number of entries in the bridge's permanent database.

Example: `list permanent`

```
                    Number of Entries in Permanent Database:  17
```

port *port#*

Displays port information related to ports that are already configured. Port# selects the port you want to list. Specifying no number selects all ports.

Example: `list port`

```
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Port ID (dec)    : 128: 2, (hex): 80-02
Port State       : Enabled
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface  : 0  VPI  0  VCI:    78
Path Cost        : 0
```

Port ID

The ID consists of two parts: the port priority and the port number. In the example, 128 is the priority, and 1, 2, and 3 are the port numbers. In hexadecimal format, the low-order byte denotes the port number and the high-order byte denotes the priority.

Port state

Displays current state of the specified port or ports. This can be either ENABLED or DISABLED.

Port supports

Displays bridging method supported by that port (for example, transparent bridging).

Assoc interface

Displays interface number associated with the displayed port. Also displays the VPI/VCI or the destination ATM address if the port exists on an ATM interface.

Path Cost

Cost associated with the port which is used for possible root path cost. The range is 1 to 65535.

protocol

Displays bridge information related to the spanning tree protocol.

Note: Each of these bridge-related parameters is also described in detail in the previous chapter.

Bridge Identifier

8-byte value in ASCII format. If you did not set the bridge address prior to displaying this information, the low order 6 bytes will be displayed as zero, denoting that the default MAC address of a port is being used. When a bridge has been selected as the root bridge, the bridge max age and bridge hello time are transmitted by it to all the bridges in the network via the HELLO BPDUs.

Bridge-Max-Age

Maximum age (period of time) that should be used to time out spanning tree protocol-related information.

Bridge-Hello-Timer

Time interval between HELLO BPDUs.

Bridge-Forward-Delay

Time interval used before changing to another state (should this bridge become the root).

range *start-index stop-index*

Reads a range of address entries from the permanent database. To specify this, first determine the size of the database by using the **list permanent** command. From this value you can then determine a “start index” value for your entry range. The start index is in the range from 1 to the size of the database. You can then choose a “stop index” for displaying a limited number of entries. This input is optional. If you do not specify the stop index, the default value is the size of the database.

Address entries contain the following information:

Example: `list range`

```
Start-Index [1]? 1
Stop-index [17]? 6
ADDRESS                 ENTRY TYPE      PORT MAP

=======                 ==========      ========
01-80-C2-00-00-00       REGISTERED      Input Port:  ALL PORTS
                                        Output ports:

01-80-C2-00-00-01       RESERVED        NONE/DAF
01-80-C2-00-00-02       RESERVED        NONE/DAF
01-80-C2-00-00-03       RESERVED        NONE/DAF
01-80-C2-00-00-04       RESERVED        NONE/DAF
01-80-C2-00-00-05       RESERVED        NONE/DAF
```

Address

6-byte MAC address of the entry.

Type of Entry

Specifies one of the following types:

- Reserved - entries reserved by the IEEE 802.1d committee
- Registered - entries consist of unicast addresses belonging to proprietary communications hardware attached to the box or multicast addresses enabled by protocol forwarders
- Permanent - entries entered by the user in the configuration process which survive power on/offs or system resets
- Static - entries entered by the user in the monitoring process that do not survive power on/offs or system resets and are ageless
- Dynamic - entries “learned” by the bridge “dynamically” that do not survive power on/offs or system resets and that have an “age” associated with the entry
- Free - locations in database that are free to be filled by address entries

Port Map

Displays outgoing port map for all incoming ports.

Set

Use the **set** command to set certain values, functions, and parameters associated with the bridge configuration. These include:

- Aging time for dynamic address entries in the filtering database
- Bridge address
- MAC service data unit (MSDU) size
- Spanning tree protocol bridge and port parameters
- Size of the bridge filtering database

Syntax:

set

- age
- bridge
- filtering
- port
- protocol bridge
- protocol port . . .

age *seconds resolution*

Sets the time for aging out dynamic entries in the filtering database when the port with the entry is in the forwarding state. This age is also used for aging RIF entries in the adaptive database in the case of an SR-TB bridge personality.

Enter the required value after each prompt and press **Return**.

Aging Time Valid Values: 10 to 1000000

Aging Time Default Value: 30

The resolution value specifies how often dynamic entries in the filtering database should be scanned to determine if they have exceeded their age limit as set by the aging timer.

Resolution Valid Values: 1 to 60 seconds

Resolution Default Value: 5 seconds

Example: `set age`

```
seconds [300]  ?  400
resolution [5] ?  6
```

bridge *bridge-address*

Sets the bridge address. This is the low-order 6-octet bridge address found in the bridge identifier. By default, the bridge-addr-value is set to the medium access control (MAC) address of the lowest-numbered port at initialization time. You can use this command to override default address and enter your own unique address.

Note: Each bridge in the network must have a unique address for the spanning tree protocol to operate correctly.

Attention: In cases where a serial line interface is the lowest numbered port, it is mandatory to use this command so that the bridge will have a unique address when restarted. This process is necessary because serial lines do not have their own MAC address.

At the prompt, enter the bridge address in 12-digit hexadecimal format and press **Return**.

If you enter the address in the wrong format you will receive the message `Illegal Address`. If you enter no address at the prompt you will receive the message `Zero length address supplied` and the bridge will maintain its previous value. To return the bridge address to the default value, enter an address of all zeros.

Valid Values: 12 hexadecimal digits

Do not use dashes or colons to separate each octet. Each bridge in the network must have a unique address for the spanning tree protocol to operate correctly.

Default Value: 000000000000

Example: `set bridge`

```
Bridge Address (in 12-digit hex)[]?
```

filtering *database-size*

Sets the number of entries that can be held in the bridge filtering database.

Default Value: 1024 times the number of bridge ports.

For more information, see the **list filtering** command on page 280.

Example: `set filtering`

```
database-size [2048]?
```

port *block* **or** *disable*

Begins the port's participation in the spanning tree protocol. This is done by entering a status value of "block." This places the port in the "blocked" status as a starting point. The actual state of the port will later be determined by the spanning tree protocol as it determines its topology. Entering a status value of "disable" removes the port from participating in the spanning tree.

Example: `set port block`

```
Port Number [1]?
```

protocol *bridge* **or** *port*

Modifies the spanning tree protocol bridge or port parameters for a new configuration, or tunes the configuration parameters to suit a specific topology.

Enter "bridge" as the option to modify bridge parameters. The bridge-related parameters that can be modified with this command are described below.

When setting these values, make sure that the following relationships exist between the parameters or the input will be rejected:

2 X (Bridge Forward Delay - 1 second) ≥ Bridge Maximum Age
Bridge Maximum Age ≥ 2 X (Bridge Hello Time + 1 second)

Example: `set protocol bridge tb`

```
Bridge Max-Age [20]  25
Bridge Hello Time [2]   3
Bridge Forward Delay [15] 20
Bridge Priority [32768]    1
```

Bridge Maximum Age

Maximum age (period of time) that should be used to time out spanning tree protocol-related information.

When this bridging device is selected as the root bridge in a spanning tree, the value of this parameter specifies how long other active bridges are to store the configuration bridge protocol data units (BPDUs) they receive. When a BPDU reaches its maximum age limit without being replaced, the active bridges in the network discard it and assume that the root bridge has failed. A new root bridge is then selected.

Dependencies

The setting of this parameter may be affected by the setting of the Bridge Hello Time parameter. In addition, the setting of this parameter may affect the setting of the Bridge Forward Delay parameter.

Valid Values: 6 to 40 seconds

Default Value: 20 seconds

Bridge Hello Timer
Time interval between HELLO BPDUs.

When this bridging device is selected as the root bridge in a spanning tree, this parameter specifies how often this bridge transmits configuration bridge protocol data units (BPDUs). BPDUs contain information about the topology of the spanning tree and reflect changes to the topology.

Dependencies

The setting of this parameter may affect the setting of the Max age parameter.

Valid Values: 1 to 10 seconds

Default Value: 2

Bridge Forward Delay
Time interval used before changing to another state (should this bridge become the root).

When this bridging device is selected as the root bridge in a spanning tree, the value of this parameter specifies how long active ports in all bridges remain in a *listening state*. When the forward delay time expires, ports in the listening state go into the *forwarding state*. State changes occur as a result of changes in the topology of the spanning tree, such as when an active bridge fails or is shut down.

The root bridge conveys this value to all bridges. This process ensures that all bridges are consistent between changes.

Valid Values: 4 to 30 seconds

Default Value: 15

Bridge Priority
A high-order 2-octet bridge address found in the Bridge Identifier - either the MAC address obtained from the lowest-numbered port or the address set by the **Set Bridge** command.

The bridge priority indicates the chances that this bridge will become the root bridge of the spanning tree. The lower the numerical value of the bridge priority parameter, the higher the priority of the bridge and the more likely it is to be chosen. The spanning tree algorithm chooses the bridge with the lowest numerical value of this parameter to be the root bridge.

Valid Values: 0 to 65535

Default Value: 32768

Enter **port** as the option to modify the spanning tree protocol port parameters. Enter the desired value at each prompt and press **Return**.

Example: `set protocol port`

```
Port Number [1] ?
Port Path-Cost (0 for default) [0] ?   1
Port Priority [128] ?   1
```

Port Number

Bridge port number; selects the port for which the path cost and port priority will be changed.

Path Cost

Cost associated with the port, which is used for possible root path cost.

Each port interface has an associated path cost, which is the relative value of using the port to reach the root bridge in a bridged network. The spanning tree algorithm uses the path cost to compute a path that minimizes the cost from the root bridge to all other bridges in the network topology.

This parameter specifies the cost associated with passing frames through this port interface, should this bridging device become the root bridge. Factor this value in when determining spanning tree routes between any two stations. A value of 0 instructs the bridging device to automatically calculate a path cost for this port using its own formula.

Valid Values: 1 to 65535

Default Value: 0 (means the cost will be calculated automatically)

Port Priority

Identifies port priority for the specified port. This is used by the spanning tree algorithm in making comparisons for port selection (which port offers the lowest cost path to the root bridge) and blocking decisions.

Valid Values: 0 to 255

Default Value: 128

VLANS

Use the **vlans** command to access the VLAN configuration prompt. VLAN configuration commands are entered at this prompt. See “Dynamic Protocol Filtering (VLANS) Configuration Commands” on page 289 for an explanation of each of these commands.

Syntax:

vlans

ATM Commands

To enable bridging over the ATM interface, you must associate a VCC with a bridge port.

Once a bridge port is configured, all the function associated with bridge ports, including protocol filtering and address filtering are available.

You need to specify PVC or SVC support. For PVC support, you must specify the VPI and VCI of the PVC. For SVC support, you must provide the remote ATM address and the local selector byte.

At the `ASRT config>` prompt, use the following command to enable bridging on the ATM interface:

add port *interface# port# VCC-id*

interface#
The interface number of the ATM interface.

port# The unique bridge-specific number associated with the VCC.

Valid Range: 1 to 254

Default Value: none

Once the port has been added on the ATM interface, the port number will identify the port to the ATM ARP client and to the VCC associated with this port.

vcc-id To define a PVC, provide the VPI and VCI information. To define a SVC, provide the destaddr and selector information.

VPI The VPI of the PVC on which bridging is enabled.

VPI Valid Values: 0 to 255

VPI Default Value: 0

VCI The VCI of the PVC on which bridging is enabled.

VCI Valid Values: 0 to 65535

VCI Default Value: 0

destaddr
The destination ATM address of the SVC.

Destination ATM address Valid Values: any valid 20-byte ATM address

Destination ATM address Default Value: none

selector
The selector of the destination ATM address of the SVC.

Selector Valid Values: X'00' – X'FF'

Selector Default Value: X'00'

Example: add a port on an ATM interface (PVC)

```
ASRT config> add port
Interface number [0]?
Port number [1]?
Use PVC? [Yes]:
VPI, Range 0..255 [0]? 0
VCI, Range 0..65535 [0]? 795
```

Example: add a port on an ATM interface (SVC)

```
ASRT config> add port
Interface number [0]?
Port number [2]?
Use PVC? [Yes]:No
```

```
Destination ATM Address []? 391122334455667788990011223344556677889 9
Selector, Range 00..FF [00]? 0A
ASRT config>
```

Dynamic Protocol Filtering (VLANS) Configuration Commands

This section explains all of the VLAN configuration commands. These commands let you configure protocol and IP multicast VLANs.

See “Dynamic Protocol Filtering VLANs” on page 269 for additional information about VLANs.

Configuration commands for the ASRT bridge are entered at the `ASRT VLAN config>` prompt. This prompt is accessed by entering the **vlans** command at the `ASRT config>` prompt. The following table shows the VLAN filtering configuration commands.

Table 51. VLAN Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds the definition of a new VLAN filter
Change	Changes VLAN filtering parameters for an indicated VLAN
Delete	Deletes the selected VLAN filters
Disable	Disables VLAN filtering on the selected VLANs
Enable	Enables VLAN filtering on the selected VLANs
List	Displays all information associated with the selected VLAN filters
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **Add** command to define a new VLAN filter. See “Required Static Configurations” on page 270 for additional information.

Syntax:

add ip

ip-multicast

ipx

netbios

sliding-window

Example 1: add ip

```
IP Address [0.0.0.0]? 9.2.3.4
Subnet Mask [255.0.0.0]?
Configure this VLAN on Specific Ports? [No]:
Age (expiration in minutes,0=infinity) [10000]? 0
Enable IP-Cut-Through from this VLAN? [Yes]:
Enable IP-Cut-Through to this VLAN? [Yes]:
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) []? IP 9.x.x.x
VLAN 'IP 9.x.x.x' (IP subnet 9.0.0.0) successfully added
```

If some ports should not be configured as Auto-Detect and Include, then the port can be manually configured.

Example 2: add ip-multicast

```
IP Multicast Address [0.0.0.0]? 230.1.1.1
Configure Specific Ports? [No]:
Age (expiration in minutes,0=infinity) [10]? 0
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) []? IPmcast01
VLAN 'IPmcast01' (IP Multicast 230.1.1.1) successfully added
```

Example 3: add ipx

```
Network Number (in 8-digit hex) (1 - FFFFFFFE) [1]? 2FF
Configure this VLAN on Specific Ports? [No] y
Configure VLAN on port 1 (Include, Exclude, or Auto-Detect) [A]?
Configure VLAN on port 2 (Include, Exclude, or Auto-Detect) [A]? e
Age (expiration in minutes,0=infinity) [5000]?
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) []? IPX 2FF
VLAN 'IPX 2FF' (IPX network 0x2FF) successfully added
```

A description of each parameter follows:

IP Address
This prompt allows you to enter the IP address of the IP subnet whose traffic will be dynamically filtered to create this VLAN. This value, after the subnet mask is applied, is what will be saved and referenced in other VLAN commands.

Subnet Mask
This is the subnet mask that will be applied to the input IP Address to create the IP subnet value used to detect traffic for this VLAN.

IP Multicast address
This is the IP group address whose multicast traffic will be filtered to create this VLAN.

Note: A VLAN for 224.0.0.1 (the all IP hosts address) is created during initialization and is used to configure IP multicast VLANs that are auto-created when an IGMP report frame is detected and the 224.0.0.1 VLAN is enabled. See “Auto-created IP Multicast VLANs” on page 271 for additional information about auto-created IP multicast VLANs.

Valid Values: 224.0.1.0 - 239.255.255.255

Default Value: none

Network Number
This prompt allows you to enter the IPX network ID number whose traffic will be dynamically filtered to create this VLAN.

Sliding Window Filter Base
Determines whether the base for the offset is the first byte of the destination MAC address or the first byte of the frame’s information field.

Valid Values: mac or info

Default Value: mac

Sliding Window Filter Offset
Sets the byte offset into the frame where the comparison with the mask and value begins.

Valid Values: 0 - 255

Default Value: 0

Sliding Window Filter Value
The value used for comparing the sliding window filter.

A frame “matches” a sliding window filter if the octet pattern (whose start is determined by the *Sliding Window Filter Base* and *Sliding Window Filter Offset*) ANDED with the *Sliding Window Filter Mask* equals this *Sliding Window Filter Value* ANDED with the *Sliding Window Filter Mask*.

Valid Values: Any octet string of length 1 - 10

Default Value: None

Sliding Window Filter Mask
The mask used for comparing the sliding window filter.

Valid Values: Any octet string of length 1 - 10

Default Value: None

Configure

Answering “No” to this prompt causes all bridge ports to be set to the default value of Auto-Detect and Include. Answering *yes* to this prompt causes further prompting to select the desired port inclusion mode for each bridge port.

The modes are:

- Auto-Detect and Include (the default mode that requires that traffic from this vlan be received on the port before being included in the VLAN forwarding domain).
- Include Always (to always include this port in the forwarding domain regardless of received traffic)
- Exclude Always (to always exclude this port from the forwarding domain regardless of received traffic).

Age The amount of time, in minutes, that an Auto-Detect port will remain in the forwarding state in the absence of traffic received from that port for this VLAN. Entering a value of zero means that ports auto-detected will never expire and be removed from the forwarding domain.

If MAC address tracking is enabled for a VLAN, the aging time also determines when a MAC address is no longer considered a member of the VLAN in the absence of traffic received from that MAC address.

Valid Values: 0 to 4 294 967 295

Default Value

IP subnet
10 000 minutes

IP multicast
10 minutes

IPX Network
10 minutes

NetBIOS
5 000 minutes

Sliding Window
5000 minutes

Enable IP-Cut-Through Transmission Status
Answering *yes* will allow forwarding of IP traffic from devices on this VLAN to devices on other VLANs that have IP-Cut-Through reception enabled. See “IP-Cut_Through Considerations” on page 270 for additional information.

Enable IP-Cut-Through Reception Status
Answering *yes* will allow IP traffic to be forwarded to devices on this VLAN from devices on other VLANs that have IP-Cut-Through transmission enabled. See “IP-Cut_Through Considerations” on page 270 for additional information.

Track Active MAC Addresses
Answering *yes* causes source MAC addresses from transmissions on this VLAN to be saved. These learned addresses can be displayed with the **show-members** command. Learned addresses will be aged out with the aging timer for this VLAN.

VLAN Filter Status
Answering *yes* will enable dynamic filtering for this VLAN. Answering “No” means that no filtering will be done on traffic from members of this VLAN.

VLAN Name
This prompt lets you define a name for this VLAN that can be used with all VLAN commands. A VLAN name is required for MAC address, port-based, and sliding window VLANs.

This name must be unique among all VLANs of all types within the ASRT bridge. This name consists of up to 32 characters and can include spaces.

Change

Use the change command to change the configuration parameters associated with a particular VLAN. The VLAN to change can be chosen by explicitly specifying the subnet or by selecting the VLAN from a list with the *by-name* option. This command invokes the same prompts used with the add command. The current parameter values will be displayed as the default and can be maintained by simply pressing **Return**.

Syntax:

change by-name
ip subnet address
ip-multicast
ipx network number
netbios
sliding-window

Example: change ip

```
IP Address [9.0.0.0]?
Configure Specific Ports? [No]:
Age (expiration in minutes,0=infinity) [0]? 300
Enable IP-Cut-Through from this VLAN? [Yes]:
Enable IP-Cut-Through to this VLAN? [Yes]:
Track Active MAC Addresses on this VLAN? [No]:
Enable This Filter? [Yes]:
VLAN Name (32 chars max) [IP 9.x.x.x]?
VLAN 'IP 9.x.x.x' (IP subnet 9.0.0.0) successfully changed
```

Delete

Use the **delete** command to delete a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If you are deleting a single filter, you can choose the VLAN to be deleted by selecting the VLAN from a list using the *by-name* option.

Syntax:

delete	by-name
	ip all
	ip subnet *subnet address*
	ip-multicast all
	ip-multicast by-name
	ipx all
	ipx network *network-number*
	netbios
	sliding-window all
	sliding-window by-name
	all

Example 1: del ip subnet 9.0.0.0

```
VLAN 'IP 9.x.x.x' (IP subnet 9.0.0.0) deleted
```

Example 2: del ipx all

```
Are you sure you want to delete ALL IPX VLANS? [No]: y
All IPX VLANS deleted
```

Disable

Use the **disable** command to disable a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If disabling a single filter, the VLAN to be disabled can be chosen by selecting the VLAN from a list using the *by-name* option.

Syntax:

disable	by-name
	ip all
	ip subnet *subnet-address*
	ip-multicast all
	ip-multicast by-name

ipx all

ipx network *network-number*

netbios

sliding-window all

sliding-window by-name

all

Example: disable ip subnet 220.5.3.0

```
VLAN 'Building #4' (IP subnet 220.5.3.0) now disabled
```

Enable

Use the **enable** command to enable a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If you are enabling a single filter, you can choose the VLAN to be enabled by selecting the VLAN from a list using the *by-name* option.

Syntax:

enable by-name

ip all

ip subnet *subnet-address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network-number*

netbios

sliding-window all

sliding-window by-name

all

Example: enable by-name

```
 Choice of VLAN:
       VLAN type    Identifier         VLAN Name
       =========    ==========         =========
   (1) IP           9.0.0.0            IP 9.x.x.x
   (2) IP           220.5.3.0          Building #4
   (3) IPX          0x2FF              Ethernet A
   (4) IPX          0x3FF              Ethernet B
Enter Selection [1]? 3
VLAN 'Ethernet A' (IPX Network 0x2FF) now enabled
```

List

Use the **list** command to list the configuration information about a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If you are listing a single filter, you can choose the VLAN to be listed can be chosen by selecting the VLAN from a list using the *by-name* option.

Syntax:

list	by-name
	ip all
	ip subnet *subnet-address*
	ip-multicast all
	ip-multicast by-name
	ipx all
	ipx network *network-number*
	netbios
	sliding-window all
	sliding-window by-name
	all

Example 1: list ip subnet 9.0.0.0

```
Subnet Address              = 9.0.0.0
Subnet Mask                 = 255.0.0.0
Bridge Port 1 (Interface 0) = Auto-Detect and Include
Bridge Port 2 (Interface 1) = Always Exclude
Age (expiration in minutes) = 300
IP-Cut-Through Status:
   Transmit From This VLAN  = Enabled
   Reception By This VLAN   = Enabled
Tracking of MAC Addresses   = Disabled
VLAN Filter State           = Enabled
VLAN Name                   = IP 9.x.x.x
```

Example 2: list ipx all

```
----------- IPX VLANS -------------------------------
IPX Network Number          = 0x2FF
Bridge Port 1 (Interface 0) = Auto-Detect and Include
Bridge Port 2 (Interface 1) = Always Exclude
Age (expiration in minutes) = Never Expires
IP-Cut-Through Status:
   Transmit From This VLAN  = Enabled
   Reception By This VLAN   = Disabled
Tracking of MAC Addresses   = Disabled
VLAN Filter State           = Enabled
VLAN Name                   = Ethernet A
+++++++++++++++++++++++++++++++++++++++++++++++++++++++
IPX Network Number          = 0x3FF
Bridge Port 1 (Interface 0) = Auto-Detect and Include
Bridge Port 2 (Interface 1) = Auto-Detect and Include
Age (expiration in minutes) = 5000
IP-Cut-Through Status:
   Transmit From This VLAN  = Enabled
   Reception By This VLAN   = Enabled
Tracking of MAC Addresses   = Disabled
VLAN Filter State           = Disabled
VLAN Name                   = Ethernet B
```

Accessing the ASRT Monitoring Environment

To access the ASRT monitoring environment, enter the **protocol asrt** command at the + (GWCON) prompt:

```
+protocol asrt
ASRT>
```

ASRT Monitoring Commands

This section describes the ASRT monitoring commands. These commands allow you to view and modify parameters from the active monitoring. Information you modify with the monitoring commands is reset to the SRAM configuration when you restart the bridging device.

You can use these commands to temporarily modify the configuration without losing configuration information in the bridge memory. The ASRT> prompt is displayed for all ASRT monitoring commands.

Monitoring and dynamic reconfiguration VLANS commands are entered at the VLAN> monitoring prompt. The VLAN> command is accessed by entering the **VLANS** command explained later in this chapter.

Note: For commands requiring you to enter MAC Addresses, the addresses can be entered in the following formats:

IEEE 802 canonical bit order
00-00-00-12-34-56

IEEE 802 canonical bit order (shorthand format)
000000123456

Table 52 shows the ASRT monitoring commands.

Table 52. ASRT Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds permanent (static) address entries to the bridging device’s permanent database.
Cache	Displays cache entries for a specified port.
Delete	Deletes MAC addresses entries from the bridging device database.
Flip	Flips MAC address from canonical to 802.5 (noncanonical or IBM) bit order.
List	Displays information about the complete bridge configuration or about selected configuration options.
NetBIOS	Displays the NetBIOS monitoring prompt.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add static address entries and destination address filters to the bridging device’s database. These additions to the database are lost when you restart the device.

Syntax:

add static-entry

static-entry *mac_address input_port [output_ports]*
Adds static address entries to the bridging device’s permanent database. Enter the command followed by the MAC address of the static entry and

the input port number (an optional output port number may also be entered). To create a static entry with multiple port maps (1 per input port), use this command several times.

Example: `add static-entry`

```
MAC address [00-00-00-00-00-00]?  400000012345
Input port, 0 for all [0]? 2
Output port, 0 for none [0]? 3
Output port, 0 to end [0]?
```

Cache

Use the **cache** command to display the contents of a selected bridging-port routing cache. If the port does not possess a cache you will see the message `Port X does not have a cache`.

Syntax:

cache *port#*

Example: `cache`

```
Port number [1]? 3

MAC Address    MC*   Entry Type       Age  Port(s)

00-00-93-00-C0-D0   PERMANENT          0  3 (TKR/1)
00-00-00-11-22-33   STATIC             0  3 (TKR/1)
```

MAC Address
6-byte MAC address of the entry.

Entry Type
Specifies one of the following address entry types:

Reserved - entries reserved by the IEEE 802.1d Standard.

Registered - entries consist of unicast addresses belonging to proprietary communications hardware attached to the box or multicast addresses enabled by protocol forwarders.

Permanent - entries entered by the user in the configuration process which survive power on/offs or system resets.

Static - entries entered by the user in the monitoring process which do not survive power on/offs or system resets and are not effected by the aging timer.

Dynamic - entries “learned” by the bridge “dynamically” which do not survive power on/offs or system resets and which have an “age” associated with the entry.

Free - locations in database that are free to be filled by address entries.

Unknown - entry types unknown to the bridge. May be possible bugs and/or illegal addresses.

Age Age in seconds of each dynamic entry. Age is decremented at each resolution intervals.

port(s)
Specifies the port number associated with that entry and displays the interface name (this will always be that of the interface having the cache).

Delete

Use the **delete** command to delete station (including MAC) address entries from the device's permanent database.

Syntax:

delete mac-address

Example: `delete 00-00-93-10-04-15`

Flip

Use the **flip** command to view specific MAC addresses in the canonical and noncanonical format by "flipping" the address bit order. This command is useful for translating IEEE 802.5 addresses in their typical noncanonical format to the canonical format universally used by the bridge monitoring and ELS (and vice versa).

Syntax:

flip *MAC-address*

Example: `flip`

```
MAC address [00-00-00-00-00-00]? 00-00-00-33-44-55
IEEE 802 canonical bit order:    00-00-00-33-44-55
IBM Token-Ring native bit order: 00:00:00:CC:22:AA
```

List

Use the **list** command to display information about the bridging device configuration or to display information about selected configuration or bridging options.

Syntax:

list

- bridge . . .
- conversion . . .
- database . . .
- dmac
- filtering . . .
- port
- spanning-tree-protocol . . .
- transparent . . .

bridge

Lists all general information regarding the bridge device configuration.

Example: `list bridge`

Bridge ID

Unique ID used by the spanning tree algorithm in determining the spanning tree. Each bridge in the network is assigned a unique bridge identifier. The bridge priority is displayed in decimal followed by the hex address.

Bridge State
Indicates whether bridging is enabled or disabled.

Bridge Type
Displays the configured bridge type. This is displayed as NONE, TB, or ASRT.

Number of Ports
Displays the number of ports configured for that bridge.

Port Specifies a user defined number assigned to an interface by the Add Port command.

Interface
Identifies devices connected to a network segment through the bridge.

State Indicates the current state of the port. This is displayed as UP or DOWN.

MAC address
Displays the MAC address associated with that port in canonical bit order.

Modes
Displays the bridging mode for that port. T indicates transparent bridging. SR indicates source routing. A indicates adaptive bridging.

MSDU Specifies the maximum frame (data unit) size (including the MAC header but not the FCS field) the bridge can transmit and receive on this interface.

Segment
Displays the source routing bridge segment number assigned to that port (if any).

SR bridge number
Displays the user assigned source routing bridge number.

SR virtual segment
Displays the source routing bridge virtual segment number (if any).

Adaptive segment
Displays the number of the segment which is used in the source routing domain to route to the transparent domain (via conversion).

conversion *datagroup-option*

- Displays general information about the bridge's rules for converting frame formats based on the frame type. There are a number of general datagroups which may be displayed under the **list conversion** command. These include the following:
  - All - Displays all rules.
  - Ethertype - Displays rules for all Ethernet types or for a specific Ethernet type.
  - SAP - Displays rules for all SAP protocol identifiers or a specific 802.2 SAP type.
  - SNAP - Displays rules for all SNAP protocol identifiers or a specific 802.2 SNAP type.

  The following examples break down each of the list conversion display options.

Example: list conversion all

Example: list conversion ethertype

```
Ethernet type (in hexadecimal), 0 for all [0]?
```

Example: list conversion SAP

```
SAP (in hexadecimal), 100 for all [100]?
```

Example: list conversion SNAP

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
```

database *datagroup-option*

Lists the contents of transparent filtering databases. There are a number of datagroups which can be chosen to be displayed under the list database command. These include the following:

- All - Displays the entire transparent bridging database.
- Dynamic - Displays all dynamic (learned) address database entries.
- Local - Displays all local (reserved) address database entries.
- Permanent - Displays all permanent address database entries.
- Port - Displays address entries for a specific port.
- Range - Displays a range of database entries from the total transparent bridging filtering address database. A starting and ending MAC address is given to define the range. All entries falling within this range will be displayed.
- Static - Displays static entries from the address database.

The following examples break down the list database command options. The first example also shows the related output.

Example: `list database all`

Note: The following fields are displayed for all of the **list database** command options.

MAC Address
Specifies the address entry in 12-digit hex format (canonical bit order).

MC* An asterisk following an address entry indicates that the entry has been flagged as a multicast address.

Entry Type
Specifies one of the following types:

Reserved
Entries reserved by the IEEE 802.1d standard.

Registered
Entries consist of unicast addresses belonging to interfaces participating in the bridge or multicast addresses enabled by protocol forwarders

Permanent
Entries entered by the user in the configuration process which survive power on/offs or system resets

Static Entries entered by the user in the monitoring process which do not survive power on/offs or system resets and are ageless.

Dynamic
Entries "learned" by the bridge "dynamically" which do not survive power on/offs or system resets and which have an "age" associated with the entry

Free This type is not used and should not be normally be seen except in occasional "race" conditions between the monitoring and the bridge.

Unknown
Unknown entry type. May indicate a software bug. Report the hex entry type to Customer Service.

Age Refers to the age (in seconds) of each dynamic entry. Age is decremented at each resolution interval.

Port(s)
Specifies the outgoing port number(s) for that entry. Device type is also listed for single port entries.

Example: `list database dynamic`

Example: `list database local`

```
MAC Address    MC*  Entry Type       Age  Port(s)

00-00-93-B8-00-48   Registered            1 (TKR/1)
01-80-C2-00-00-00*  Registered            1
03-00-02-00-00-00*  Registered            1
ASRT>
```

Example: `list database permanent`

Example: `list database port` *port#*

Example: `list database static`

Example: `list database range`

```
First MAC address [00-00-00-00-00-00]? 00-00-93-00-C0-D0
Last MAC address [FF-FF-FF-FF-FF-FF]? 01-80-C2-00-00-00

MAC Address    MC*  Entry Type       Age  Port(s)
00-00-93-10-04-15   Registered            1 (Eth/2)
01-80-C2-00-00-00   Registered            1,3
```

filtering *datagroup-option*
Displays general information about the bridge's protocol filtering databases. There are a number of general datagroups which may be displayed under the **list filtering** command. These include the following:

- All - Displays all filtering database entries.
- Ethertype - Displays Ethernet protocol type filter database entries.
- SAP - Displays SAP protocol filter database entries.
- SNAP - Displays SNAP protocol identifier filter database entries.

The following examples break down each of the list filtering display options.

Example: `list filtering all`

```
Ethernet type 0800 is routed on ports 1
IEEE 802.2 destination SAP 42 is routed on ports 1
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

Descriptors used in explaining how packets are communicated include the following:

- Routed - Describes packets which are passed to routing forwarder to be forwarded
- Filtered- Describes packets which are administratively filtered by the user setting protocol filters
- Bridged and routed - This describes a protocol identifier for which there is a protocol entity within the system which is not a forwarder. An example of this would be a link level echo protocol. Unicast packets from this protocol are bridged or locally processed if being sent to a registered address. Multicast packets are forwarded and locally processed for a registered multicast address.

All of the descriptors just explained also apply to ARP packets with this Ethertype.

Example: `list filtering ethertype`

```
Ethernet type (in hexadecimal), 0 for all [0]? 0800
Ethernet type 0800 is routed on ports 1
```

Example: `list filtering SAP`

```
SAP (in hexadecimal), 100 for all [100]? 42
IEEE 802.2 destination SAP 42 is routed on ports 1
```

Example: `list filtering SNAP`

```
SNAP Protocol ID, return for all [00-00-00-00-00]?
IEEE 802 SNAP PID 00-00-00-08-00 is routed on ports 2-3
```

port *port#*

Displays port information.

Example: list port

```
Port Id (dec)    : 128: 3, (hex): 80-03
Port State       : Forwarding
STP Participation: Enabled
Port Supports    : Transparent Bridging Only
Assoc Interface #/name : 5/Eth/1
```

Port Specifies a user defined number assigned to an interface by the Add Port command.

Interface
Identifies devices connected to a network segment through the bridge.

State Indicates the current state of the port. This is displayed as UP or DOWN.

MAC address
Displays the MAC address associated with that port in canonical bit order.

Modes
Displays the bridging mode for that port. T indicates transparent bridging. SR indicates source routing. A indicates adaptive bridging.

MSDU Specifies the maximum frame (data unit) size (including the MAC header but not the FCS field) the bridge can transmit and receive on this interface.

Segment
Displays the source routing bridge segment number assigned to that port (if any).

spanning-tree protocol *datagroup-option*

- Displays spanning tree protocol information. The spanning tree protocol is used by the transparent bridge to form a loop-free topology. There are a number of general datagroup options which may be displayed under the **list spanning-tree-protocol** command. These include the following:
  - Configuration - Displays information concerning the spanning tree protocol.
  - Counters - Displays the spanning tree protocol counters.
  - State - Displays the current spanning tree protocol state information.
  - Tree - Displays the current spanning tree information including port, interface, and cost information.

  The following examples illustrate each of the list spanning-tree-protocol display options.

Example: `list spanning-tree-protocol configuration`

```
Bridge ID (prio/add):  32768/0000-93-00-84-EA
Bridge state:          Enabled
Maximum age:           20 seconds
Hello time:            2 seconds
Forward delay:         15 seconds
Hold time:             1 seconds
Filtering age:         320 seconds
Filtering resolution:  5 seconds

Port  Interface  Priority  Cost   State
  4   Eth/1      128    100     Enabled
128   Tunnel     128    65535   Enabled
```

Example: `list spanning-tree-protocol counters`

```
            Time since topology change (seconds)         0
            Topology changes:                            1
            BPDUs received:                              0
            BPDUs sent:                                14170

Port  Interface  BPDUs received  BDPU input overflow  Forward transitions

   1  TKR/1             0              0               1
```

Example: `list spanning-tree-protocol state`

```
       Designated root (prio/add):    32768/00-00-93-00-84-EA
       Root cost:                     0
       Root port:                     Self
       Current (root) maximum age:    20 seconds
       Current (root) hello time:     2 seconds
       Current (root) Forward delay:  15 seconds
       Topology change detected:      FALSE
       Topology change:               FALSE

       Port  Interface   State
         4  Eth/1       Forwarding
```

Example: `list spanning-tree-protocol tree`

```
       Port                Designated   Desig.         Designated   Des.
       No.  Interface           Root     Cost             Bridge   Port

        2  ATM/0:0:48  0/00-00-00-00-00-00    0     0/00-00-23-45-00-00 80-00
```

Dynamic Protocol Filtering (VLANS)

The VLAN monitoring commands are a superset of the VLAN configuration commands. However, instead of updating the SRAM configuration records immediately, they change the behavior of VLANs in real-time. Changes made

through the monitoring can be optionally saved to SRAM. Also, the configuration in SRAM can be loaded and used without requiring a reboot.

Monitoring commands for the ASRT bridge are entered at the ASRT VLAN> prompt. This prompt is accessed by entering the **vlans** command at the ASRT> prompt. The following table shows the VLAN monitoring commands.

Table 53. VLAN Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds the definition of a new VLAN filter
Change	Changes VLAN filtering parameters for an indicated VLAN
Delete	Deletes the selected VLAN filters
Disable	Disables VLAN filtering on the selected VLANs
Enable	Enables VLAN filtering on the selected VLANs
List	Displays all information associated with the selected VLAN filters
Load	Loads and uses the VLAN configuration currently in SRAM
Reset-Counters	Resets all counters associated with the selected VLAN filters
Save	Saves the current runtime configuration to SRAM
Show-members	Displays learned MAC addresses for a selected VLAN
Show-vlans	Lists the enabled VLANs of which a particular MAC address is a member
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

For a description of the **Add**, **Change**, **Delete**, **Disable**, and **Enable** commands, see "Dynamic Protocol Filtering (VLANS) Configuration Commands" on page 289.

List Use the list command to list the current real-time configuration for a particular VLAN filter, all VLAN filters of a particular type, or all defined VLAN filters. If listing a single filter, the VLAN to list can be chosen by selecting the VLAN from a list with the *by-name* option. The resulting output includes both configuration parameters and VLAN counters.

Syntax:

list

by-name

ip all

ip subnet *subnet address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network number*

netbios

sliding-window all

sliding-window by-name

all

Example:

```
vlans config>list ip subnet 9.0.0.0

   Subnet Address              = 9.0.0.0
   Subnet Mask                 = 255.0.0.0
   Port 1 (Interface 0) = Auto-Detect and Include, Forwarding
   Port 2 (Interface 1) = Always Exclude,          Not Forwarding
   Age (expiration in minutes) = 300
   IP-Cut-Through Status:
      Tx From This VLAN    = Enabled  Reception By This VLAN = Disabled
      Packets Transmitted  = 25       Packets Received       = 0
      Tx Packets Discarded = 0        Rx Packets Discarded   = 14
   Tracking of MAC Addresses  = Disabled
   VLAN Status                = Enabled
   Packets Processed          = 43
   Discards Due To Exclusion  = 13
   VLAN Name                   = IP 9.x.x.x
```

A description of the VLAN counters follows:

Packets Transmitted
Total number of IP packets successfully cut through from this VLAN.

Packets Received
Total number of IP packets successfully cut through to this VLAN.

Tx Packets Discarded
Number of IP packets that were intended to be cut through from this VLAN, but were discarded due to IP-Cut-Through transmission being disabled. Packets from ports configured as Always Exclude are not included in this count.

Rx Packets Discarded
Number of IP packets that were intended to be cut-through to this VLAN, but were discarded due to IP-Cut-Through reception being disabled.

Packets Processed
Total number of packets processed by this VLAN's forwarding logic. This includes all packets forwarded and discarded. For IP Multicast VLANs, this number includes IGMP Reports and matching IP Multicast frames. For the IP Multicast auto-creation VLAN (group 224.0.0.1), this counter indicates the number of received IGMP Query packets from multicast devices.

Discards Due To Exclusion
Number of packets received matching this VLAN on ports configured as Always Exclude for this VLAN.

Load Use the load command to load and immediately use the VLAN configuration stored in SRAM. This will overwrite any configuration changes that may have been made via monitoring since the last save. All timers and counters associated with VLANs will be reset.

Syntax: load

Example: load

```
Warning: This process will overwrite your current configuration.
Are you sure you want to load the VLAN configuration from SRAM? [No] y
VLAN configuration loaded
```

Reset-Counters
Use the reset-counters command to set all counters to zero for a particular VLAN filter, all VLAN filters for a particular protocol, or all defined VLAN filters. If you are resetting the counters in a single filter, you can choose the VLAN by specifying the subnet or by selecting the VLAN from a list with the by-name option.

Syntax:

reset-counters

by-name

ip all

ip subnet *subnet address*

ip-multicast all

ip-multicast by-name

ipx all

ipx network *network number*

netbios

sliding-window all

sliding-window by-name

all

Example: reset ipx network 3ff

```
VLAN 'Ethernet B' (IPX Network 0x3FF) counters reset
```

Save Use the **save** command to store the current runtime VLAN configuration into SRAM. This will overwrite the current SRAM configuration. This command does not affect the runtime behavior of VLANs or reset the timers or counters associated with VLANs.

Syntax: save

Example: save

```
Are you sure you want to save the VLAN configuration to SRAM? [No] y
VLAN configuration saved
```

Show-members

Use the **show-members** command to display all the learned MAC addresses for a particular VLAN that has MAC Address Tracking enabled. Addresses in this list have all transmitted broadcast frames within the configured aging time. The MAC addresses will be displayed along with the associated bridge port and interface and can be sorted by bridge port or increasing MAC address.

Syntax:

show-members

by-name

ip *subnet-address*

ip-multicast

ipx *network-number*

netbios

sliding-window

Example: show-members ip

```
Subnet Address [9.0.0.0]?

        Sort VLAN Members by Port (P) or Mac Address (M) [P]?
        Port Number to Show Membership (0=All) [0]?

        Current Members of Runtime VLAN 'IP 9.x.x.x' (IP Subnet 9.0.0.0):

           Port  1 (Interface  0),  Mac Address: 10.00.5A.00.64.00
           Port  2 (Interface  1),  Mac Address: 10.00.5A.00.65.00
```

Show-vlans

Use the **show-vlans** command to display all the enabled VLANs in which traffic from a particular MAC address has been observed since the last aging timer expiration.

Syntax:

Example: show-vlans

```
Enter Mac Address in Hex: []? 10005A006400

        List of VLANS with Mac Address 10.00.5A.00.64.00:

             VLAN Type    Identifier            VLAN Name
             =========    ==========            =========
          (1) IP           9.0.0.0               IP 9.x.x.x
```

ASRT Monitoring Commands (Talk 5)

Chapter 27. Configuring and Monitoring TCP/IP Host Services

This chapter describes how to configure the TCP/IP Host Services (TCP/IP Host) protocol and how to use the TCP/IP Host configuration commands. The chapter includes the following sections:

See "TCP/IP Host Services (Bridge-Only Management)" on page 269 if you want to know more about why you would use TCP/IP host services.

Accessing the TCP/IP Host Configuration Environment

To access the TCP/IP Host configuration environment, enter the following command at the Config> prompt:

```
Config> protocol hst
TCP/IP-Host Services user configuration
TCP/IP-Host Config>
```

Basic Configuration Procedures

The following sections describe the basic configuration procedures for enabling TCP/IP Host Services on your IBM 8371.

Setting the IP Address

To minimally configure TCP/IP Host services, assign the IBM 8371 an IP address by using the **set ip-host** command. This IP address is associated with the IBM 8371 as a whole, instead of being associated with a single interface.

Enabling TCP/IP Host Services

Use the **enable services** command to enable TCP/IP Host Services.

Adding a Default Gateway

The IBM 8371 uses its default gateway to communicate with hosts and gateways that are not on the bridged network to which the IBM 8371 is directly connected. The IBM 8371 can dynamically learn its default gateway using either ICMP Router Discovery (see the **enable router-discovery** command in this chapter) or RIP (see the **enable rip-listening** command in this chapter). You can also statically specify one or more default gateways by using the **add default gateway** command. The IBM 8371 uses only one default gateway at a time; any additional default gateways are used for backup.

To save the assigned IP address and default gateway information,

1. Exit from the `TCP/IP-Host config>` prompt to the `Config>` prompt.
2. Use the **write** command at the `Config>` prompt to write the current configuration to memory.
3. Enter **CTRL-P** to get to the OPCON prompt and use the **reload** OPCON command to load a new copy of the software.
4. After reloading the IBM 8371, return to the `TCP/IP-Host config>` prompt.

TCP/IP Host Configuration Commands

This section describes the TCP/IP Host configuration commands. The TCP/IP Host configuration commands allow you to specify network parameters for the TCP/IP Host bridge. Restart the device to activate the configuration commands. Enter the TCP/IP Host configuration commands at the `TCP/IP-Host config>` prompt. Table 54 shows the commands.

Table 54. TCP/IP Host Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a default-gateway.
Delete	Deletes a default-gateway.
Disable	Disables TCP/IP Host Services, router-discovery processes, and RIP listening.
Enable	Enables TCP/IP Host Services, router-discovery processes, and RIP listening.
List	Lists the current TCP/IP Host configuration.
Set	Sets the IBM 8371's IP address.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add default gateways (that is, routers) to your configuration.

Default gateways are used when trying to send packets to IP destinations that are off the local subnet. The routing table is then built up through redirect processing. An attempt is made to detect routers that disappear.

Syntax:

add default-gateway *def-gateway-IP-address*

Example: **`add default-gateway`**

```
Default-Gateway address [0.0.0.0]?  123.45.67.89
```

Delete

Use the **delete** command to delete default gateways from your IBM 8371 configuration. Enter the IP address of the default gateway you want to remove after the **delete** command.

Syntax:

delete default-gateway *def-gateway-IP-address*

Example: `delete default-gateway`

```
Enter address to be deleted [0.0.0.0]?  123.45.67.89
```

Disable

Use the **disable** command to disable the following TCP/IP functions:

- TCP/IP Host Services
- Router-discovery processes
- RIP listening

Syntax:

disable rip-listening
router-discovery
services

rip-listening
Disables the building of routing table entries that have been gathered by listening to the RIP protocol. By default, RIP-listening is disabled.

Example: `disable rip-listening`

router-discovery
Disables the ability to learn default gateways by receiving ICMP Router Discovery messages. By default, router discovery is enabled.

Example: `disable router-discovery`

services
Disables the TCP/IP Host Services protocol entirely. If IP routing is not enabled, TCP/IP Host Services is enabled by default.

Example: `disable services`

Enable

Use the **enable** command to enable the following TCP/IP functions:

- TCP/IP Host Services
- Router discovery processes
- RIP listening

Syntax:

enable rip-listening
router-discovery
services

rip-listening
Enables the building of routing table entries that have been gathered by the bridge “listening” to the RIP protocol. RIP-listening is disabled by default.

Example: `enable rip-listening`

router-discovery
Enables the learning of default gateways through reception of ICMP Router Discovery messages. By default, router discovery is enabled.

Example: `enable router-discovery`

services
Enables the TCP/IP Host Services protocol. If IP routing is not enabled, TCP/IP Host Services is enabled by default.

Example: `enable services`

List

Use the **list** command to display information about the current TCP/IP Host configuration.

Syntax:

list all

Example: `list all`

```
IP-Host IP address : 128.185.142.1
Address mask : 255.255.255.0

Default Gateway IP-address(es)
128.185.142.47

TCP/IP-Host Services Enabled.

RIP-LISTENING Disabled.

Router Discovery Enabled.
```

IP-Host IP address	Displays the current IP-Host IP address.
Address mask	Displays the current IP-Host IP subnet address mask.
Default Gateway IP-address(es)	Displays the current default gateway IP address.
TCP/IP Host Services	Displays whether TCP/IP Host Services is enabled or disabled.
RIP-LISTENING	Displays whether RIP-LISTENING is enabled or disabled.
Router Discovery	Displays whether Router Discovery is enabled or disabled.

Set

Use the **set** command to set the IBM 8371's IP address. You must assign the IBM 8371 an IP address before enabling TCP/IP Host Services.

Note: If the IP address is not already configured, it is set (by default) using boot information. This process applies only if the IBM 8371 is a network host operating as an IP host.

Syntax:

set ip-host address *IP-host-address*

Example: `set ip 123.45.67.89`

```
Address mask [255.255.0.0]?
IP-Host Address set.
```

Monitoring TCP/IP Host Services

This section describes how to monitor the TCP/IP Host Services on the IBM 8371.

Accessing the TCP/IP Host Monitoring Environment

To access the TCP/IP Host monitoring environment, enter the following command at the + (GWCON) prompt:

```
+ protocol hst
TCP/IP-Host>
```

TCP/IP Host Monitoring Commands

This section describes the TCP/IP Host monitoring commands. These commands allow you to view parameters and enter information requests from the active terminal. Enter these commands at the TCP/IP-Host> prompt. Table 55 shows the commands.

Table 55. TCP/IP Host Monitoring Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Dump	Displays the current IP routing table. One line is printed for each destination.
Interface	Displays the IBM 8371’s IP address.
Ping	Continuously pings a given destination, printing a line for each response received.
Traceroute	Displays the hop-by-hop route to a given destination.
Routers	Displays the list of all IP routers known to the IBM 8371.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Dump

Use the **dump** command to display the current IP routing table. One line is printed for each destination. Many of the entries that are displayed are the result of ICMP redirects.

Syntax:

dump

Example:

```
TCP/IP Host> dump
Type   Dest net         Mask      Cost     Age       Next hop(s)

Stat   0.0.0.0          00000000  0        51        128.185.142.47
 Dir*  128.185.142.0    FFFFFF00  1        50        BDG/0

Default gateway in use.
Type Cost     Age       Next hop
Stat 0        51        128.185.142.47

Routing table size: 768 nets (52224 bytes), 2 nets known
                    0 nets hidden, 0 nets deleted, 0 nets inactive
                    0 routes used internally, 766 routes free
```

Type — Route type which indicates how the route was derived:
- RIP - the route was learned through the RIP protocol.
- Stat - a statically configured route.
- Dir - a directly connected network or subnet.

Dest net — Displays the IP address of the destination network/subnet.

Mask — Displays the IP address mask.

Cost — Displays the Route Cost.

Age	For RIP routes displays the time, in seconds, since the route was refreshed. For other types of routes displays the time, in seconds, since the route was installed.
Next Hop	Displays the IP address of the next device on the path toward the destination host. Also displayed is the interface type used by the sending device to forward the packet.
Default gateway	Displays the IP address of the default gateway along with the route type, cost, age, and next hop information associated with that entry.
Routing table size	Displays the current size (in networks and bytes) of the current table. Also identifies the number of networks (nets) known to the host.

Interface

Use the **interface** command to display the IBM 8371's IP address. When TCP/IP Host Services are running over the bridge, a single address is displayed on the terminal as Bridge/0.

Syntax:

interface

Example:

```
TCP/IP Host> interface
Interface  IP Address(es)   Mask(s)
  BDG/0    128.185.142.16   255.255.255.0
```

Interface	Displays the type of interface. For TCP/IP Host Services, this is always BDG/0, indicating the bridge.
IP Address	Displays the IP address of the TCP/IP Host Services interface.
Mask	Displays the IP address subnet mask.

Ping

Use the **ping** command to make the device send ICMP Echo Requests to a given destination once a second ("pinging") and watch for a response. This command can be used to isolate trouble in an internetwork environment.

This process is done continuously, incrementing the ICMP sequence number with each additional packet. Matching received ICMP Echo responses are reported with their sequence number and the round trip time. The granularity (time resolution) of the round trip time calculation is platform-specific, and usually is around 20 milliseconds.

To stop the pinging process, type any character at the terminal. At that time, a summary of packet loss, round trip time, and number of unreachable ICMP destinations will be displayed.

When a multicast address is given as destination, there may be multiple responses printed for each packet sent, one for each group member. Each returned response is displayed with the source address of the responder.

The size of the ping (number of data bytes in the ICMP message, excluding the ICMP header), TTL value, and rate of pinging are all user-configurable. The default values are a size of 56 bytes, a TTL of 64, and a rate of 1 ping per second.

Syntax:

ping *destination source size ttl rate*

Example:

```
TCP/IP Host> ping
Destination IP address [0.0.0.0]? 128.185.142.11
Source IP address [128.185.142.16]?
Ping data size in bytes [56]?
Ping TTL [64]?
Ping rate in seconds [1]?
PING 128.185.142.16 -> 128.185.142.11: 56 data bytes, ttl=64, ... every 1 sec.
56 data bytes from 128.185.142.11: icmp_seq=0. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=1. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=2. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=3. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=4. ttl=254. time=0. ms
56 data bytes from 128.185.142.11: icmp_seq=5. ttl=254. time=0. ms

----128.185.142.11 PING Statistics----
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 0/0/0 ms
```

Traceroute

Use the **traceroute** command to display the entire path to a given destination, hop by hop. For each successive hop, the traceroute command sends out three probes and prints the IP address of the responder along with the round trip time associated with the response. If a particular probe receives no response, an asterisk (*) is printed. Each line in the display relates to this set of three probes, with the left-most number indicating the distance from the device executing the command (in network device hops).

The traceroute is complete when the destination is reached, an ICMP Destination Unreachable message is received, or the path length reaches 32 network device hops.

Syntax:

traceroute *destination source size probes wait ttl*

Example:

```
TCP/IP Host> traceroute
Destination IP address [0.0.0.0]? 128.185.144.239
Source IP address [128.185.142.16]?
Data size in bytes [56]?
Number of probes per hop [3]?
Wait time between retries in seconds [3]?
Maximum TTL [32]?
TRACEROUTE 128.185.142.16 -> 128.185.144.239: 56 data bytes
 1 128.185.142.11 16 ms 0 ms 0 ms
 2 128.185.143.33 16 ms 0 ms 0 ms
 3 128.185.144.239 16 ms 0 ms 0 ms
```

In the display:

TRACEROUTE	Displays the destination area address and the size of the packet being sent to that address.
1	The first trace showing the destination's NSAP and the round trip time it took the packet to reach the destination and return. The packet is traced three times.
Destination unreachable	Indicates that no route to the destination is available.
1 * * * 2 * * *	Indicates that the device is expecting some form of response from the destination, but the destination is not responding.

When a probe receives an unexpected result (see the previous output example), several indicators can be printed. These indicators are explained in the following table.

!N Indicates that an ICMP Destination Unreachable (net unreachable) has been received.
!H Indicates that an ICMP Destination Unreachable (host unreachable) has been received.
!P Indicates that an ICMP Destination Unreachable (protocol unreachable) has been received.
! Indicates that the destination has been reached, but the reply sent by the destination has been received with a TTL of 1. This usually indicates an error in the destination, prevalent in some versions of UNIX, whereby the destination is inserting the probe's TTL in its replies. This unfortunately leads to a number of lines consisting solely of asterisks before the destination is finally reached.

Routers

Use the **routers** command to display the list of all IP routers that are known to the IBM 8371. Routers can be learned through:

- Static configuration (using the **add default-gateway** command explained on page "Add" on page 310).
- Received ICMP redirects
- ICMP Router Discovery messages (if configured)
- RIP updates (if configured)

Each router is listed with its origin, its priority (used when selecting the default route), and its lifetime (the number of seconds before the router will be declared invalid unless it is heard from again).

Syntax:

routers

Example: `routers`

Chapter 28. Using SNMP

This chapter describes SNMP. It contains the following sections:

- "Network Management"
- "SNMP Management"

Network Management

Refer to the *Planning and Setup Guide* for information about Network Management.

SNMP Management

The IBM 8371 provides a Simple Network Management Protocol (SNMP) interface to network management platforms and applications, such as the Nways Campus Manager products.

SNMP is used for monitoring and managing IP hosts in an IP network and uses software called an SNMP agent to enable network hosts to read and modify some of the IBM 8371's operational parameters. In this way, SNMP establishes network management for the IP community.

You need to consider the following aspects of SNMP when you configure SNMP for your IBM 8371.

Community

The community allows you to define the IP address of the SNMP management station that is allowed to access the information in the SNMP agent's Management Information Base (MIB). You define a community name for use in accessing the MIB.

Authentication

The community name is used as an authentication scheme to prevent unauthorized users from learning information about an SNMP agent or modifying its characteristics.

This scheme involves defining one or more sets of MIB data (referred to as MIB views) and associating an access privilege (read-only, read-write), an IP mask, and a community name with each MIB view. The IP mask establishes which IP addresses can originate access requests for a given MIB view and the community name serves as a password that must be matched by the SNMP requests. The community name is included in each SNMP message and verified by the IBM 8371 SNMP agent. An SNMP request will be rejected if it does not provide the correct community name, does not match the IP mask, or attempts an access that is inconsistent with the assigned access privilege.

MIB Support

A MIB is a virtual information store that provides access to management information. This information is defined as MIB objects which can be accessed and, in some cases, be modified using network management tools.

Using SNMP

IBM 8371 provides a comprehensive set of standard MIBS, enterprise-specific MIBs for monitoring and managing resources, and Readme files.

You can find the Readme files documenting IBM 8371 MIB support by accessing the appropriate release directory on the World Wide Web at URL:

- **ftp://ftp.nways.raleigh.ibm.com/pub/netmgmt/8371/**

To receive a copy of a specific MIB, enter the **get** command with the name of the MIB. For example, the command,**get rfc1213.txt** places a copy of the specified MIB in the directory from which you connected to the FTP server.

You can access the following information from the ftp site:

- Standard MIBs
- Enterprise MIBs
- SNMP generic traps
- Enterprise-specific MIBs
- Settable values

SNMP generic traps, Enterprise MIBS, and settable values are located in the Readme files.

All MIB objects are implemented as READ-ONLY objects even if their access clause is defined as read-write or read-create, except those MIB objects identified in the Readme file that support SETs for objects that have their access clause defined as read-write or read-create.

Trap Messages

Trap messages are unsolicited messages sent from the SNMP agent in the device to an SNMP manager in response to a device or network condition, such as a device reload or network down.

Chapter 29. Configuring and Monitoring SNMP

This chapter describes the SNMP configuring and monitoring commands. It includes the following sections:

Accessing the SNMP Configuration Environment

To access the SNMP configuration environment, enter the following command at the `Config>` prompt:

```
Config> protocol snmp
SNMP user configuration
SNMP Config>
```

SNMP Configuration Commands

This section describes the SNMP configuration commands.

Table 56 lists the SNMP configuration commands. The SNMP configuration commands allow you to specify parameters that define the relationship between the SNMP agent and the network management station. The information you specify takes effect immediately after a restart or reload of the IBM 8371.

Enter the SNMP configuration commands at the `SNMP Config>` prompt.

Table 56. SNMP Configuration Commands Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
Add	Adds a community to the list of SNMP communities, an IP address with mask to a community, or a subtree to a MIB view.
Delete	Removes a community from the list of SNMP communities, an IP address with mask from a community, or a subtree from a MIB view.
Disable	Disables SNMP protocol and traps associated with named communities.
Enable	Enables SNMP protocol and traps associated with named communities.
List	Displays the current communities with their associated access modes, enabled traps, IP addresses, and views. Also displays all views and their associated MIB subtrees.
Set	Sets a community's access mode or view. A community's access mode is one of the following: Read and trap generation Read, write and trap generation Trap generation only This command is also used to set a trap UDP port.

Table 56. SNMP Configuration Commands Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add a community name to the list of SNMP communities, add an address to a community, or assign a portion of the MIB (subtree) to a view.

Syntax:

add community
address
sub_tree

community

Use the **add community** command to create a community. It will be created with a default access of read_trap, a view of all, all traps disabled, and all IP addresses allowed.

Note: To select access type or trap control, use the **set community access** command to assign access types to existing SNMP communities and use the **enable trap** or the **disable trap** command for trap control.

community name

Provides the community name used by the SNMP client. This community name is used when accessing the management information base (MIB) in the device from the host specified by the Community IP address parameter.

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

Example:

```
SNMP Config>  add community
Community Name  []? comm01
Community added successfully
```

address

Use the **add address** command to add to the community definition an address of a network management station in the network that should be allowed to communicate with this box. You must supply the name of the community and the network address (in standard a.b.c.d notation). You also may supply a net mask to restrict access to either an individual host (mask = 255.255.255.255) or to a network of hosts. More than one address can be added to a community; enter the command each time you want to add another address.

If you do not specify an address for a community, requests are handled from any host.

Addresses also specify hosts that receive the traps. If no address is specified, no trap is generated.

community name

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

IP address

Valid Values: Any valid IP address.

Default Value: 0.0.0.0

ip mask

You also may supply a mask to restrict access to either an individual host (mask = 255.255.255.255) or to a network of hosts.

Valid Values: 0.0.0.0 - 255.255.255.255

Default Value: 255.255.255.255

Example:

```
SNMP Config> add address
Community Name []?
IP Address [0.0.0.0]?
IP Mask [255.255.255.255]?
```

sub_tree

Use the **add sub_tree** command to add a portion of the MIB to a view or to create a new view. The default is the entire MIB. The **add sub_tree** command is used to manage MIB views. More than one subtree can be added to a view defined by <view_text_name>.

view name

Specifies the name of the view to be created.

Valid Values: Any alphanumeric character string up to 31 characters in length. Characters such as spaces, tabs, or <Esc> key sequences are not accepted.

Default Value: none

Note: You must assign a view to one or more communities using the **set community view** command to have it take effect. The subtree definitions are inclusive; that is, the subtree OID specified and any OID that is lexicographically greater than the specified OID is considered part of the MIB view.

If a community is added using the **add community** command, all supported MIB views are assigned to the community unless the **set community view** command is used to assign specific views to the community.

MIB OID name

Specifies the MIB Object ID for the sub_tree. This must be entered as a numeric value, not a symbolic value.

This parameter contains a MIB subtree name included in the view defined with the View name parameter. All children of a specified MIB subtree are also included in the view.

For example, to provide a view that would give access to the system group in MIB-II, specify **1.3.6.1.2.1.1**.

Valid Values:

An object identifier in the form of <element1>.<element2>.<element3>. . ., where:

- You need a minimum of 1 element. Since all MIB OIDs begin with *1.3.6.1*, the minimum number of elements that you need to be provide in order for the view to differ from *all* is 5 (1.3.6.1.X).
- You can define a maximum of 31 characters, including the . separators.
- All elements after the first four (*1.3.6.1*) are integers between 0 and 127.

Note: This value must be numeric in dotted notation, *not* a symbolic value.

Default Value: none

Example:

```
SNMP Config> add sub_tree
View Name  []? view01
MIB OID name []? 1.3.6.1.1
Subtree added successfully
```

Delete

Use the **delete** command to delete a community and all of its addresses, a specific address, or a subtree from a view.

Syntax:

delete community

address

sub_tree

community

Removes a community and its IP addresses.

community name

Specifies a community name used by the SNMP client. This community name is used when accessing the management information base (MIB) in the device from the host specified by the Community IP address parameter.

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

Example:

```
SNMP Config> delete community
Community Name []?
```

address

Removes an address from a community. You must supply the name.

community name

Specifies the name of the community from which an address is to be removed. This community name is used when accessing the management information base (MIB) in the device from the host specified by the Community IP address parameter.

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: public

IP address

Specifies the IP address to be removed.

Valid Values: Any valid IP address.

Default Value: none

Example:

```
SNMP Config>  delete address
Community Name []?
IP address []?
```

sub_tree

Removes a MIB or a portion of the MIB from a view. You must supply the name of the subtree. If all subtrees are deleted, the MIB view is also deleted and all references to it from any associated SNMP communities are removed.

view name

Specifies the view used by the community defined in the **community name** parameter. This view determines which MIB objects this community may access. If no view is specified, the community may access all objects known to the device's SNMP agent.

This parameter should be answered if you decide to restrict a community from accessing the entire MIB managed by the device's SNMP agent.

Default Value: none

MIB OID name

Specifies the MIB Object ID for the sub_tree. This must be entered as a numeric value, not a symbolic value.

This parameter contains a MIB subtree name included in the view defined with the View name parameter. All children of a specified MIB subtree are also included in the view.

Valid Values: An object identifier in the form of <element1>.<element2>.<element3>. . ., where:

- You need a minimum of 1 element. Since all MIB OIDs begin with *1.3.6.1*, the minimum number of elements that you need to be provide in order for the view to differ from *all* is 5 (1.3.6.1.X).
- You can define a maximum of 31 characters, including the . separators.
- All elements after the first four (*1.3.6.1*) are integers between 0 and 127.

Default Value:nne

Example:

```
SNMP Config> delete sub_tree
View name[]?
MIB OID[]?
```

Disable

Use the **disable** command to disable the SNMP protocol or specified traps on the device.

Syntax:

disable snmp

trap

snmp Disables SNMP.

Example: `disable snmp`

trap *trap type*
Disables specified traps or all traps.

trap type
Specifies the type of trap to be disabled. Valid trap types are shown in Table 57.

community name

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

Example:

```
SNMP Config> disable trap link_up
Community name []?
```

Table 57. SNMP Trap Types

Trap Type	Description
all	Specifies all traps in a specified community.
cold_start	A cold start trap means that the transmitting device is reinitializing and that the agent's configuration or the protocol entity implementation may be altered.
warm_start	A warm start trap means that the transmitting device is reinitializing, but the configuration or protocol implementation will remain the same. Specify the community name as part of the command line.
link_down	A link_down trap recognizes a failure in one of the communication links represented in the agent's configuration. The link_down trap-PDU contains the name and value of the ifIndex instance for the affected link as the first element of its variable-bindings.
link_up	A link_up trap recognizes that a previously inactive link in the network has come up. The link_up trap-PDU contains the name and value of the ifIndex instance for the affected link as the first element of its variable-bindings.
auth_fail	Authentication failure traps indicate that the sender of the SNMP request does not have the proper permission to talk to this box's SNMP agent.
enterprise	Enterprise specific traps indicate that some enterprise specific event has occurred. The specific-trap field identifies the particular trap that occurred. For example, when configured to do so, ELS event messages are sent in enterprise-specific traps.

Enable

Use the **enable** command to enable the SNMP protocol or specified traps on the device.

Syntax:

enable snmp

trap

snmp Enables SNMP

Example: `enable snmp`

trap *trap type*
Enables specified traps or all traps.

trap type
Specifies the trap type to be enabled. Valid trap types are shown in Table 57 on page 324.

community name

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

List

Use the **list** command to display the current configuration of SNMP communities, access modes, traps, network addresses, and views.

Syntax:

list all

community

views

list all Displays the current configuration of SNMP communities for Access, Traps, Address, and View. See the description of the **list community** command for details on the options.

Example: `list all`

```
SNMP Config>list all

   SNMP is enabled
   Trap UDP port: 162
   SRAM write is enabled

             Community Name                Access
   -------------------------------  -------------------
   oxnard                           Read, Write, Trap
   public                           Read, Trap


            Community Name             IP Address         IP Mask
   -------------------------------  ---------------  ---------------
   oxnard                           1.1.1.2          255.255.255.255
   public                           All              N/A


            Community Name                Enabled Traps
   -------------------------------  -------------------------------
   oxnard                           Link Down, Cold Restart
   public                           None


             Community Name                   View
   -------------------------------  -------------------------------
   oxnard                           mib2
```

```
public                          All

          View Name                          Sub-Tree
------------------------------  ------------------------------
mib2                            1.3.6.1.2
```

list community *option*

Displays the current attributes of an SNMP community. Options are access, address, traps, view.

Option	Description
Access	Displays the access modes for the community.
Address	Displays the network address for the community.
Traps	Displays the types of traps generated for the community.
View	Displays the MIB view for the community.

Example:

```
SNMP Config  list community access

            Community Name   Access
            public           Read, Write, Trap
            oxnard           Read, Trap
```

Example:

```
SNMP Config>  list community address

            Community Name   IP Address   IP Mask
            public           All          N/A
            oxnard           1.1.1.2      255.255.255.255
```

Example:

```
SNMP Config  list community traps

            Community Name   Enabled Traps
            public           Link Down, Cold Restart
            oxnard           NONE
```

Example:

```
SNMP Config>  list community view

             Community Name   View
            public           All
            oxnard           mib2
```

list views

Displays the current views for a specified SNMP community.

Example:

```
SNMP Config  list views

            View Name   Sub-Tree
            mib2        1.3.6.1.2.1
```

Set

Use the **set** command to assign a MIB view to a community, to set the SNMP UDP trap port number, or set the access mode of the community.

Syntax:

set community access

community view

trap_port

community access

Use the **set community access** command to assign one of three access types to a community. You must supply the name of the community and the access type.

options

Choose an option from the following list:

read_trap

Allows read access and trap generation to the named community.

write_read_trap

Allows write and read access and trap generation to the community specified.

trap_only

Indicates the community is used only when sending an SNMP trap.

comm_name

The **community name** has:

Valid Values: A string of 1 to 31 alphanumeric characters.

Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

Example: `set community access <options> comm_name`

community view

Use the **set community view** command to assign a MIB view to a community.

comm_name

Valid Values: A string of 1 to 31 alphanumeric characters. Characters such as spaces, tabs, or <ESC> key sequences are not supported.

Default Value: none

all Allows access to all MIB objects for the named community. All is the default.

view_text_name

Assigns a specified MIB view to the named community.

Example: `set community view comm_name <all` *or* `view_text_name>`

trap_port

Use the **set trap_port** command to specify a UDP port number, other than the default standard port 162, to send traps to.

Default Value: standard port

Example: `set trap_port udpport#`

UDP Port Number

Specifies a User Datagram Protocol port other than the standard UDP port.

Default Value: 162

Accessing the SNMP Monitoring Environment

To access the SNMP monitoring environment, enter the following command at the **+** (GWCON) prompt:

```
+ protocol snmp
SNMP>
```

SNMP Monitoring Commands

This section describes the SNMP monitoring commands.

Table 58 lists the SNMP monitoring commands. The SNMP monitoring commands allow you to view the parameters of the SNMP configuration and display some statistics relating to the SNMP agent.

Temporary changes to the runtime SNMP parameters can be made through the monitoring. If you want to make the temporary changes permanent, then use the SAVE command. If the original SNMP configuration needs to be restored, use the **revert** command. This command erases the specified changes and restores the settings to the values in the permanent SNMP configuration.

Enter the SNMP monitoring commands at the SNMP> prompt.

Table 58. SNMP Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds a community to the list of SNMP communities, an IP address with mask to a community, or a subtree to a MIB view.
Delete	Removes a community from the list of SNMP communities, an IP address with mask from a community, or a subtree from a MIB view.
Disable	Disables traps associated with named communities. Disabling SNMP or SRAM_write must be done using the SNMP Config> configuration environment.
Enable	Enables traps associated with named communities. Enabling SNMP or SRAM_write must be done using the SNMP Config> configuration environment.
List	Displays the current configuration of SNMP communities, views, access modes, traps, and network addresses.
Revert	Erases the specified changes and restores the settings to the values in the permanent SNMP configuration.
Save	Takes the specified changes and saves then permanently in the SNMP configuration.
Set	Sets a community’s access mode or view. A community’s access mode is one of the following: • Read and trap generation • Read, write and trap generation • Trap generation only Also allows setting of trap UDP port.
Statistics	Displays statistics about the SNMP agent.

Table 58. SNMP Monitoring Command Summary (continued)

Command	Function
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Add

Use the **add** command to add a community name to the list of SNMP communities, add an address to a community, or assign a portion of the MIB (subtree) to a view.

For information on using the **add** command, see “Add” on page 320.

Delete

Use the **delete** command to delete:

- A specific address.
- A community and all of its addresses.
- A subtree from a view.

For information on using the **delete** command, see “Delete” on page 322.

Disable

Use the **disable** command to disable specified traps on the device.

For information on using the **disable** command, see “Disable” on page 324.

Enable

Use the **enable** command to enable specified traps on the device.

For information on using the **enable** command, see “Enable” on page 324.

List

Use the **list** command to display the current configuration of SNMP communities, views, access modes, traps, and network addresses.

Syntax:

list	all
	community
	views

For information about using the **list** command, see “List” on page 325.

Revert

Use the **revert** command to erase the specified changes and restore the settings to the values in the permanent SNMP configuration.

Save

Use the **save** command to permanently save the specified changes.

Set

For information on using the **set** command, see “Set” on page 326.

Statistics

Use the **statistics** command to display statistics about the SNMP agent.

Syntax:

statistics

Example: `statistics`

```
              Max       Current    Current
             Alloc      Alloc       In Use

SNMP agent:  512000     181144     133120

SNMP MIBs:   1048576     57976      19712
```

The following information is displayed:

Max Alloc
The maximum amount of memory (in bytes) that is reserved for the SNMP component.

Current Alloc
As memory is needed, it is taken from the reserved pool (designated by MAX ALLOC) and moved in to an ″active″ memory pool. The size of this ″active″ memory pool size is indicated by the CURRENT ALLOC value.

Current In Use
This value represents the memory currently allocated from the ″active″ memory pool (designated by CURRENT ALLOC) that is in use by the SNMP component.

Chapter 30. Using MultiProtocol Over ATM (MPOA)

This chapter describes how to use Multiprotocol over ATM (MPOA) and includes the following section:

- "MPOA Overview"

MPOA Overview

The concept of virtual router, as shown in Figure 21, allows you to implement a conventional edge router function using MPOA servers, MPOA clients, and an ATM backbone network.

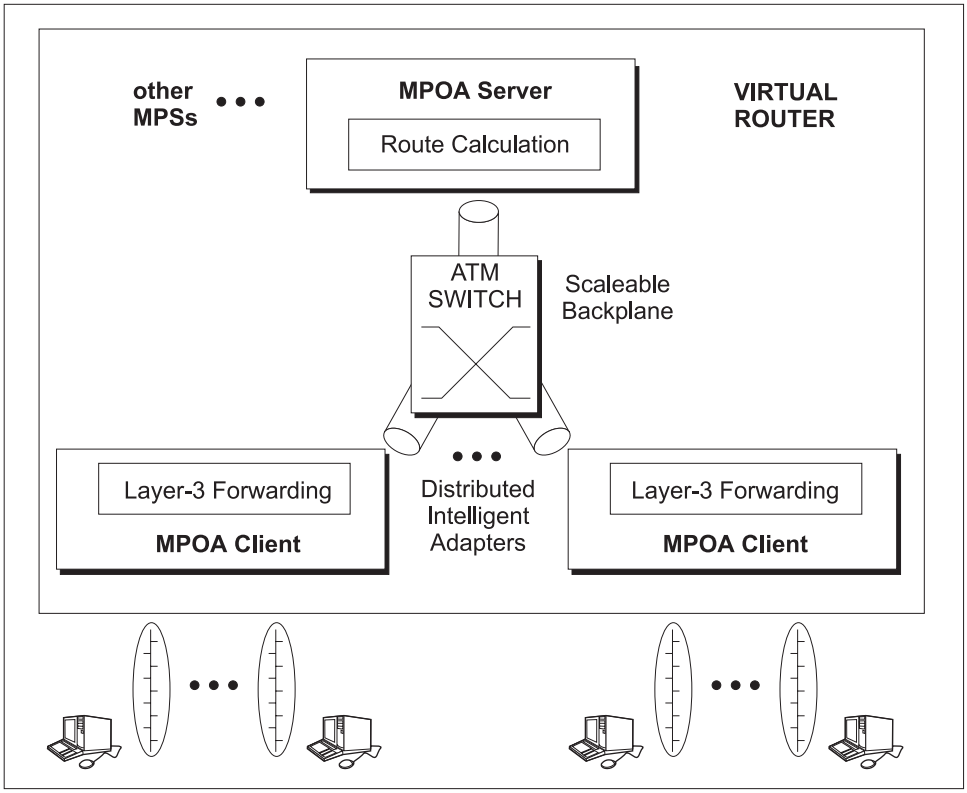

Figure 21. MPOA Virtual Router

MPOA uses networking technologies, such as bridging, LAN Emulation, and Next Hop Resolution Protocol, to implement the virtual router concept. As shown in Figure 22 on page 332, the virtual router model has:

- One router to manage
- One device participating in routing topology protocols, leading to simple edge devices
- Forwarding capacity of multiple devices

while a conventional edge router model has:

- Multiple routers to manage
- Multiple devices participating in routing topology protocols, leading to complex edge devices

- Forwarding capacity of multiple devices

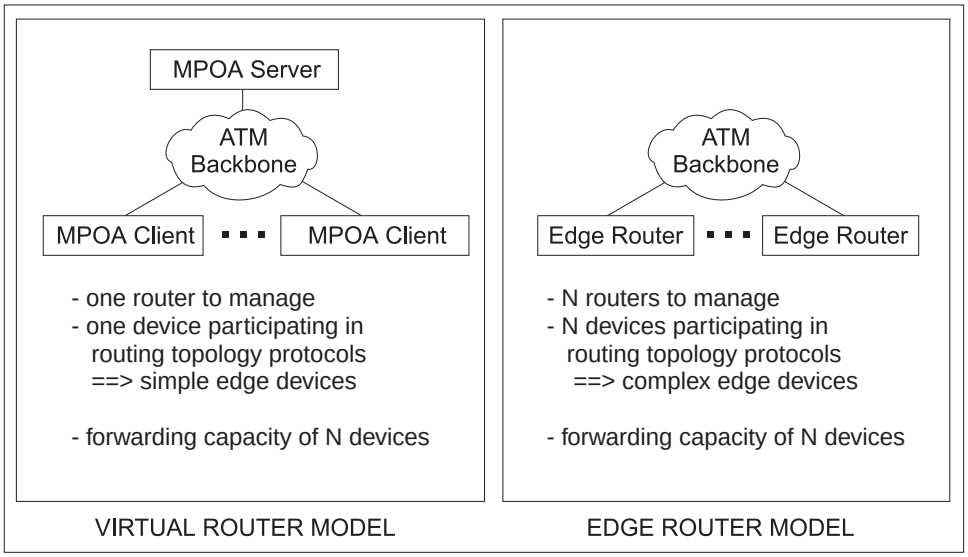

Figure 22. Comparison of Virtual Router and Edge Router Models

MPOA implements a virtual router with client/server protocols. MPOA clients (MPCs) issue requests to MPOA servers (MPSs). MPSs perform route calculations, while MPCs act as distributed intelligent adapters performing high-speed forwarding and the ATM network provides backplane throughput. MPSs are located with router functions and a NHRP server, while MPCs reside in MPOA hosts or MPOA edge devices, as shown in Figure 23 on page 333. The functions performed by a MPC in a MPOA host are very similar to those performed by a MPC in a MPOA edge device: establishing shortcut VCCs and forwarding intersubnet traffic over these VCCs to improve system performance. All MPOA devices include a LAN Emulation Client (LEC) that provides default path interconnection.

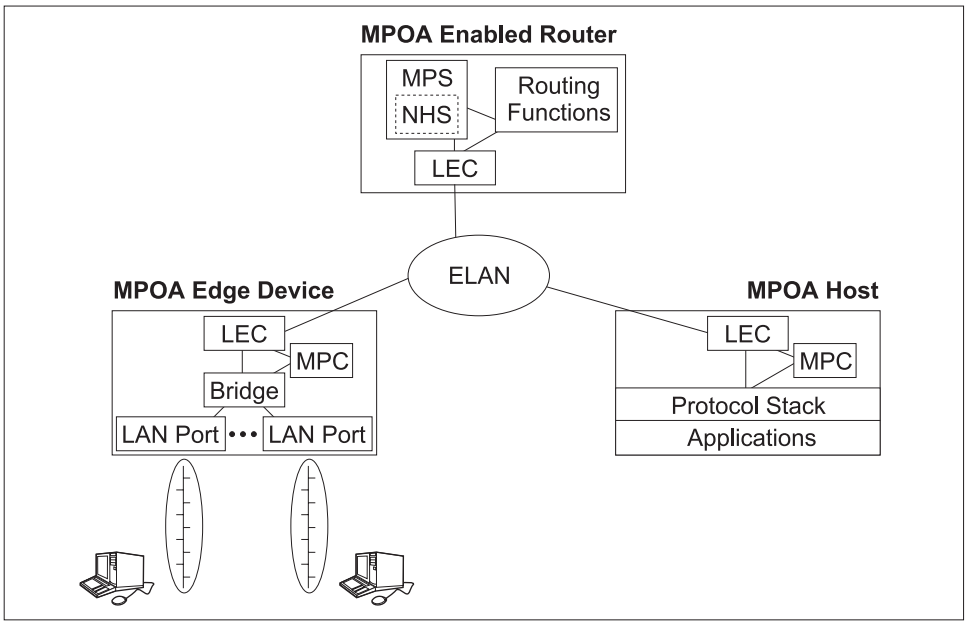

Figure 23. MPOA Components

MPOA and LAN Emulation

MPOA relies on LAN Emulation for three important functions:

- Auto-configuration
- Dynamic Device Discovery
- Intersubnet/default path connectivity

Auto-configuration allows MPOA configuration parameters to be stored and distributed from the LAN Emulation Configuration Server, or LECS. MPOA devices can obtain their configuration information from the LECS while they are being initialized, so that individual device configuration is reduced. See the chapter entitled “Configuring and Monitoring LAN Emulation Services” in the *8371 Interface Configuration and Software User’s Guide* for additional information about configuring LECS.

MPOA devices dynamically learn about neighbor components through the discovery protocol. MPOA devices attach special TLVs to LAN Emulation control messages and then inspect received TLVs to identify MAC addresses associated with other MPOA devices. Refer to the chapter entitled “Overview of LAN Emulation” in the *8371 Interface Configuration and Software User’s Guide* for additional information about LAN Emulation TLVs.

MPOA clients bridge intrasubnet traffic over ELANs. Since most MPOA edge devices include LAN switching hardware capabilities, intrasubnet traffic is handled with end-to-end switching. This use of bridging, coupled with dynamic device discovery, enables the MPC to be independent of router topology while maintaining the change management benefits provided by VLANs. For example, a station can be moved from a segment behind one MPC to a segment behind another MPC without any reconfiguration.

MPOA and Shortcut Establishment

MPOA clients are responsible for initiating shortcut establishment. The MPC discovers the MAC addresses of the MPS routers and the corresponding ATM addresses. MPC then monitors traffic flow to these MAC addresses, and when the flow exceeds a configured threshold, MPC initiates shortcut establishment by sending a MPOA resolution request to the associated MPS.

The MPOA implementation supports shortcuts for IP and IPX traffic.

Chapter 31. Configuring and Monitoring MPOA

This chapter describes how to use the MPOA configuration and operating commands and includes the following sections:

- "Accessing the MPOA Configuration Environment"
- "MPC Configuration Commands"
- "Accessing the MPOA Monitoring Environment" on page 341
- "MPC Monitoring Commands" on page 342

Accessing the MPOA Configuration Environment

Use the following procedure to access the MPOA configuration process.

1. At the OPCON prompt, enter **talk 6**. (For more detail on this command, refer to *The OPCON Process and Commands* in the 8371 Interface Configuration and Software User's Guide.)

   After you enter the **talk 6** command, the CONFIG prompt (`Config>`) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the CONFIG prompt, enter the **protocol mpoa** command to get to the `MPOA Config>` prompt.

MPOA Configuration Commands

The MPOA main menu includes the following commands.

Table 59. MPOA Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
MPC	Enters the MPC configuration environment. for the MPC instance defined over a specified ATM device. See "MPC Configuration Commands" for additional information.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

MPC Configuration Commands

To access the MPC *configuration* process, enter **mpc** *device#* at the `MPOA Config>` prompt to access the `MPC Config>` prompt. If you do not enter the *device#*, you will be prompted to supply the ATM device number.

Enter the following commands at the `MPC Config>` prompt. These commands apply to the MPC instance defined over the ATM device number supplied when you entered the `MPOA Config>` **mpc** *device#* command.

MPOA Configuration Commands (Talk 6)

Table 60. MPC Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Add	Adds an MPC instance with default parameter values.
List	Lists the enabled/disabled status of the MPC instance.
Config	Allows explicit configuration of MPC parameters.
Remove	Removes a MPC configuration.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Note: The MPOA client does not have to be explicitly configured in order to start functioning at startup. If no explicit configuration of the MPC has been done under `talk 6`, an MPOA client is automatically created in the *enabled* state with a default set of parameter values and begins MPOA operation including shortcut initiation. You should explicitly configure any non-default configuration parameters. To prevent the MPOA client function from automatically being activated, you should use the **config** command to access the `MPC Configuration>` prompt and then use the **disable** command to create an MPC instance with a status of *disabled*.

Add

Use the **add** command to add a MPC instance with default parameters.

The **add** option requires that an ATM interface has been previously added.

The added MPC defaults to ***enabled***.

Note: When an MPC is created, it is automatically associated with all LECs on the ATM device that have a bridge port configured on them. There is no explicit configuration to associate particular LECs to the MPC. Further, this association is formed during startup time and not during configuration. Thus, even if no bridge ports have been defined at the time the MPC is added and configured, the MPC will still be associated with all LECs that have a bridge port associated with them at startup time. You cannot dynamically disable association of the MPC with a particular LEC at runtime.

Syntax:

add MPC

Remove

Use the **remove** command to remove a MPC configuration.

Syntax:

remove MPC

List

Use the **list** command to display the existing MPC instance.

Syntax:

list

Config

Use the **config** command to access the `MPC Configuration>` prompt and perform explicit configuration of the MPC parameters.

Syntax:

config

To configure MPC parameters explicitly, enter the following commands at the `MPC Configuration>` prompt.

Table 61. MPC Explicit Configuration Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
Enable	Enables the MPC instance.
Disable	Disables the MPC instance. This command can also be used to create an MPC instance with a status of ***disabled***.
Set	Sets explicit values for MPC configuration parameters.
List	Displays all the configuration information associated with the MPC instance.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Enable

Use the **enable** command to enable an MPC instance.

Syntax:

enable

Disable

Use the **disable** command to disable an MPC instance.

This command can also be used to create an MPC instance with a status of ***disabled***.

Note: An MPC instance will be automatically created at startup, even if no MPC has been explicitly added. Use the **disable** command to disable this MPC instance if you do not want to configure MPC.

Syntax:

disable

Set

Use the **set** command to explicitly configure MPC parameters.

Syntax:

set frame-count
frame-time
initial-retry-time

maximum-retry-time

hold-down-time

vcc-timeout

accept-config-from-lecs

fragmentation-mode

esi

selector

pcr

max-reserved-bandwidth

shortcuts

ip-protocol

ipx-protocol

frame-count

Controls the rate of traffic required before the MPC will initiate a shortcut to a given protocol destination. The MPC will initiate a shortcut when at least this many frames are forwarded to the same protocol destination for a period of ***frame-time*** seconds.

Valid Values: 1 to 65535 frames

Default Value: 10

frame-time

Controls the rate of traffic required before the MPC will initiate a shortcut to a given protocol destination. The MPC will initiate a shortcut when at least ***frame-count*** frames are forwarded to the same protocol destination for a period of this number of seconds.

Valid Values: 1 to 60 seconds

Default Value: 1

initial-retry-time

Specifies the initial value of the retry timer when the MPC sends a request. If a corresponding reply is not received before the expiration of the retry timer, the request is retried if the retry timer is less than ***maximum-retry-time*** and the retry timer is then doubled. This process will repeat until a reply is received or until the retry timer ≥ ***maximum-retry-time***.

Valid Values: 1 to 300 seconds

Default Value: 5

maximum-retry-time

Specifies the maximum value of the retry timer when the MPC sends a request. If a corresponding reply is not received before the expiration of the retry timer, the request is retried if the retry timer is less than this value and the retry timer is then doubled. This process will repeat until a reply is received or until the retry timer ≥ this value.

Valid Values: 10 to 300 seconds

Default Value: 40

hold-down-time
Specifies the minimum time to wait before re-initiating a failed resolution request.

Valid Values: 30 to 1200 seconds

Default Value: 160

vcc-timeout
Specifies the length of time after which either inactive control or inactive data connections will be cleared.

Valid Values: 1 to 10080 minutes

Default Value: 20

accept-config-from-lecs
Specifies whether configuration parameters received from the LECS will be accepted by the MPC.

Valid Values: yes or no

Default Value: yes

fragmentation-mode
Controls the manner that the ingress MPC handles IP packet fragmentation.

When this parameter is set to ***maximize-shortcut-usage***, frames requiring fragmentation will be sent to the MPOA server, while smaller frames will be sent over the shortcut. A potential consequence of using ***maximize-shortcut-usage*** is that packets can get out of order.

When this parameter is set to ***maximize-inorder-usage***, usage of a particular shortcut will be suspended for the ***hold-down-time*** if a frame requiring fragmentation is received, causing all frames for the destination to be sent to the MPOA server.

When this parameter is set to ***perform-fragmentation***, IP frames requiring fragmentation are fragmented by the MPC and then sent over the shortcut. Both shortcut usage and inorder delivery are maximized.

Note: A single flow requiring fragmentation can impact the performance of all flows.

Valid Values: maximize-shortcut-usage, maximize-inorder-packet-delivery, or perform-fragmentation

Default Value: perform-fragmentation

esi Specifies the ESI that is to be used as the ESI component of the MPC's ATM address. The MPC implementation uses a single ATM address for control as well as data VCCs, so this ATM address refers to both the control and data ATM addresses of the MPC.

Valid Values:

- Burned-in
- One of the set of enabled ESI definitions for the MPC ATM device

Default Value: Burned-in

selector
Specifies the selector value that is to be used in combination with the esi to create a value that is unique among all protocol components using the MPC ATM device.

Valid Values: any single valid octet value that has not already been used

Default Value: automatically created

pcr Specifies the desired peak cell rate for connections established by the MPC over the associated ATM device.

All connections established by the MPC are best-effort connections.

Valid Values: 0 - line speed of the ATM device (integer Kbps)

Default Value: line speed of the ATM device

max-reserved-bandwidth
Specifies the maximum amount of reserved bandwidth acceptable on incoming calls received over the associated ATM device.

Valid Values: 0 - line speed of the ATM device (integer Kbps)

Default Value: 0

shortcuts
Specifies whether the MPC should establish shortcuts to LANE devices over the associated ATM device.

Valid Values: yes or no

Default Value: yes

If the value of this parameter is *yes*, you will be prompted for the following additional information:

Choice of source address for LANE shortcuts
Specifies what source MAC address is to be used in frames transmitted on LANE shortcut VCCs.

Valid Values:

- The MAC address burned into the MPC's ATM device
- A locally-administered MAC address
- The MAC address provided in the MPOA resolution reply

Default Value: Burned-in MAC address

If you choose to provide a locally-administered MAC address, you will be prompted for the value to be used.

Valid Values: 12 hexadecimal digits in the range of X'400000000000' and X'7FFFFFFFFFFF'

Default Value: None

ip-protocol
Permits enabling or disabling of the MPOA protocol for IP traffic.

Valid Values: Yes or No

Default Value: Yes

ipx-protocol
Permits enabling or disabling of the MPOA protocol for IPX traffic.

Valid Values: Yes or No

Default Value: Yes

List

Use the **list** command to display configuration information about the existing MPC instance.

Syntax:

list

```
MPC Configuration> list
   MPC Configuration
   -----------------
   STATUS:                              ENABLED
   Shortcut Setup Frame Count:           10 (sec)
   Shortcut Setup Frame Time:            1  frame (sec)
   Initial Retry Time:                   5  (sec)
   Maximum Retry Time:                   40 (sec)
   Hold Down Time:                       160(sec)
   VCC Timeout Period:                   20 (min)
   Accept Config Parms from LECS         YES
   Fragmentation Mode                    Maximize Shortcut Usage

   Interface:                            36
   ESI:                                  Burned In ESI
   Selector:                             3
   Desired PCR:                          155000 (Kbps)
   Maximum Reserved Bandwidth:           10000 (Kbps)
   Line Rate:                            155 Mbps
   Enable LANE Shortcuts:                Yes
   Source MAC Address for Shortcuts:     Burned In
   IP-Protocol:                          Enabled
   IPX-Protocol:                         Disabled
```

Accessing the MPOA Monitoring Environment

Use the following procedure to access the MPOA monitoring commands. This gives you access to the MPOA *monitoring* process.

1. At the OPCON prompt, enter **talk 5**. (For more detail on this command, refer to *The OPCON Process and Commands* in the 8371 Interface Configuration and Software User's Guide.)

   After you enter the **talk 5** command, the GWCON prompt (+) displays on the terminal. If the prompt does not appear when you first enter configuration, press **Return** again.
2. At the + prompt, enter the **protocol MPOA** command to get you to the `MPOA>` prompt.

MPOA Monitoring Commands

The MPOA main menu includes the following commands.

Table 62. MPOA Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.

Table 62. MPOA Monitoring Command Summary (continued)

Command	Function
MPC	Enters the MPC monitoring environment of the MPC instance defined on the specified ATM device. See “MPC Monitoring Commands” for additional information.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

MPC Monitoring Commands

To access the MPC *monitoring* process, enter **mpc** *device#* at the `MPOA>` prompt to access the `MPC Console>` prompt. Enter these commands at the `MPC Console>` prompt.

Table 63. MPC Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
atm-interface	Accesses the `MPC-ATM>` command prompt from which information about the ATM interface can be displayed.
mpc-base	Accesses the `MPC-BASE>` command prompt from which information about the overall MPC status can be displayed.
neighbor-mps	Accesses the `MPC-MPS>` command prompt from which information about the MPOA servers (MPS) that have been discovered by the MPC can be displayed.
VCCs	Accesses the `MPC VCC>` command prompt from which information about the VCCs being used by the MPC can be displayed.
ingress-cache	Accesses the `MPC Ingress>` command prompt from which information about the MPC’s ingress cache can be displayed.
egress-cache	Accesses the `MPC egress>` command prompt from which information about the MPC’s egress cache can be displayed.
configure	Accesses the `MPC Configure>` command prompt from which MPC configuration parameters can be dynamically changed.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Monitoring Commands for the MPC ATM-Interface

Enter the following commands at the `MPC-ATM>` command prompt.

Table 64. MPC ATM-Interface Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
display-interface-state	Provides information about the state of the MPC’s ATM interface and ATM address registration.
interface-statistics	Displays statistics about the ATM interface.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

Display-Interface-State

Use the **display-interface-state** command to provide information about the state of the MPC's ATM interface and ATM address registration.

Syntax:

display-interface-state

Example:

```
MPC ATM>display
  MPOA Client Configured on ATM Interface  36:
  ========================================

  1. ATM Interface Up/Down ?:              UP
  2. ATM Address Activated By Switch ?:    TRUE
  3. LLC Call Sap Ready ?:                 TRUE
  4. LANE Call Sap Ready ?:                TRUE
  5. Local ATM address :
       39.84.0F.00.00.00.00.00.00.00.00.02.10.00.5A.01.9C.00.03
```

Interface-Statistics

Use the **interface-statistics** command to display statistics such as the total number of address activation attempts and the number of times the ATM interface has been down.

Syntax:

interface-statistics

Example:

```
MPC ATM>inter
ATM Interface Statistics For This MPC:
--------------------------------------
Total Address Registration Timeouts:    0
Total Address Registration Failures:    0
Total Address Deactivations :           0
Total Net Downs:                        0
```

MPC Base Monitoring Commands

Enter the following commands at the MPC-BASE> command prompt.

Table 65. MPC BASE Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
list-config	Displays the current MPC configuration parameters.
LECs	Displays a list of local LAN Emulation Clients that are currently associated with the MPC.
state	Displays the current state of the MPC and the time since the last state change.
mpc-statistics	Displays a set of statistics for the MPC as a whole.
Enable-mpc	Dynamically starts a disabled MPC instance.
Enable-protocol	Dynamically starts a disabled MPC instance over IP or IPX.
Disable-protocol	Dynamically deactivates the MPC instance over IP or IPX.
Disable-mpc	Dynamically deactivates the MPC instance.

Table 65. MPC BASE Monitoring Command Summary (continued)

Command	Function
Create-mpc	Dynamically creates a new MPC instance.
Delete-mpc	Deletes the MPC instance.
clear-statistics	Resets all the statistics maintained for the MPC instance to their initial values.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List-config

Use the **list-config** command to display the current configuration parameters of the MPC.

Syntax:

list-config

Example:

Note: This command displays the parameters that are configurable through `talk 6` as well as some parameters, such as the *ATM address packet trace filter* value that can only be configured through `talk 5` (in the CONFIGURE menu).

```
MPC Base>list
   MPOA Client Configuration:
==========================

Status:                           ENABLED
Shortcut Setup Frame Count:       1
Shortcut Setup Frame Time:        1      (sec)
Initial Retry Time:               5      (sec)
Maximum Retry Time:               40     (sec)
Hold Down Time:                   160    (sec)
VCC Timeout Period:               20     (min)
Accept Config From LECS:          Yes
Fragmentation Mode:               Maximize Shortcut Usage
Interface:                        0
ESI:                              Burned In ESI
Selector:                         3
Desired PCR:                      155000   (kbps)
Maximum Reserved Bandwidth:       155000   (kbps)
Line Rate:                        155      (Mbps)
Enable LANE Shortcuts:            TRUE
Source MAC Address for Shortcuts: Burned In

Packet Trace Filtering Parameters:
==================================

ATM Address Pkt Trace Filter Value
 00000000000000000000000000000000000000000000
 ATM Address Pkt Trace Filter Mask
 00000000000000000000000000000000000000000000
LAN Pkt Trace Filter Value
 000000000000
LAN Pkt Trace Filter Mask
 000000000000
```

LECs

Use the **LECs** command to display a list of local LAN Emulation Clients (LECs) that are currently associated with the MPC. For each LEC, the interface number, ELAN ID, ELAN type, and bridge port type are displayed.

Syntax:

lecs

Example:

```
LECs Associated w/  MPOA Client (interface 36):
===============================================

     1) LEC Interface Number: 40
ELAN Type: ETHRNET      ELAN ID: x0
Bridge Port Type: TB PORT

Lan Destinations Registered by this LEC:
----------------------------------------
```

State

Use the **state** command to display the current state of the MPC and the time since the last state change.

Syntax:

state

Example:

```
MPC Base>state
MPOA Client State:
==================

ATM Interface Number:                 36
State:                                MPC UP STATE
Time Since Last State Change (h:m:s):  00:33:40
Last (internal) error code:           0
  Network-layer Protocols enabled:      IP IPX
```

MPC-Statistics

Use the **mpc-statistics** command to display aggregate statistics for the MPC instance.

Syntax:

mpc-statistics

Example:

Note: This command is basically a combination of the **statistics** commands in each of the other submenus.

```
MPC Base>mpc
MPOA Client Statistics (interface 36):
======================================
  Ingress MPC Statistics For This MPC:
  ------------------------------------
```

```
Total Resolution Requests Sent:         7
Total Refresh Res. Requests Sent:       6
Total Res. Rqst Retransmissions:        1
Total Res. Rqst Timeouts:               0
Total Res. Reply Successes:             7
Total Res. Reply NAKs:                  0
Total Res. Replies Discarded:           0
Total MPS Purges Recvd:                 0
Total MPS Purged Mappings:              0
Total MPS Purges Discarded:             0
Total Triggers Recvd:                   0
Total Triggers Discarded:               0
Total Keep Alives Recvd:                218
Total Inactive Mappings Deleted:        0
Total Frames Forwarded On Shortcuts:    2174
Total Data Plane Purges Recvd:          0
Total Data Plane Purged Mappings:       0
Total Data Plane Purges Discarded:      0
Total NHRP Purge Replies Transmitted:   0



  Egress MPC Statistics For This MPC:
  -----------------------------------
Total Imposition Requests Recvd:        8
Total Imposition Rqsts NAKed:           0
Total Imposition Updates Received:      7
Total Imposition Purges Received:       0
Total Imposition Purged Mappings:       0
Total E-MPC Purge Rqsts Sent To MPSs:   0
Total E-MPC Purge Rqst Retransmissions: 0
Total E-MPC Purge Rqst Timeouts:        0
Tot. Frames Recvd & Fwded (Software):   2286
Total Recvd Frames Discarded:           0
Total Data Plane Purge Rqsts Sent:      0
Total Data Plane Purge Rqst Retransmits:0
Total Data Plane Purge Rqst Timeouts:   0
Total Egress Cache Entries Aged Out:    0


  VCC Statistics For This MPC:
  ----------------------------
Total Call Setup Failures:              0
Total Incoming Calls Rejected:          0
Total Connections Released Locally:     0
Total Calls Placed Successfully:        1
Total Calls Received Successfully:      1
Total Remote Hangups (Normal):          0
Total Remote Hangups (Error):           0


  ATM Interface Statistics For This MPC:
  --------------------------------------
Total Address Registration Timeouts:    0
Total Address Registration Failures:    0
Total Address Deactivations :           0
Total Net Downs:                        0


  Additional Misc. Stats
  ----------------------
Total Error Indication Frames Received: 0
Total Error Indication Frames Txmtd:    0
Total Invalid Frames Received:          0
Total Keep-Alives Discarded:            0
Total OAM Frames Received:              0
```

Enable-MPC

Use the **enable-mpc** command to dynamically start operation of a disabled MPC instance. When the MPC instance is enabled, existing configuration parameters are used, and the MPC statistics are not reset to their initial values. Use **create-mpc** to start an MPC instance using the configuration parameters saved in the SRAM and to reset all statistics.

Syntax:

enable-mpc

Enable-protocol

Use the **enable-protocol** command to dynamically enable the MPC over IP or IPX.

Syntax:

enable-protocol	ip
	ipx

Disable-protocol

Use the **disable-protocol** command to dynamically disable the MPC over IP or IPX.

Syntax:

disable-protocol	ip
	ipx

Disable-MPC

Use the **disable-mpc** command to dynamically deactivate the MPC instance. Once the MPC has been disabled, all packets follow the normal routed path and no shortcut data forwarding occurs.

Syntax:

disable-mpc

Create-MPC

Use **create-mpc** to start an MPC instance using the configuration parameters saved in the SRAM and to reset all statistics.

Syntax:

create-mpc

Delete-MPC

Use the **delete-mpc** command to delete an existing MPC instance. The MPC ceases operation immediately.

Syntax:

delete-mpc

Clear-statistics

Use the **clear-statistics** command to reset all the statistics maintained for the MPC instance to their initial values.

Syntax:

clear-statistics

MPC Neighbor MPS Monitoring Commands

Enter the following commands at the MPC-MPS> command prompt.

Table 66. MPC Neighbor MPS Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
list	Displays a current list of all the MPSs that have been discovered by the MPC (all the MPSs for which the MPC may perform forwarding functions).
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to produce a current list of all the MPSs for which the MPC may perform forwarding functions. The displayed information includes a list of MAC addresses for which the MPC is performing flow detection, the interface number of the LEC associated with each MAC address, and the control ATM address of the MPS.

Syntax:

list

Example:

```
MPC MPS>list
List of Neighbor MPSs for MPOA Client (36):
=================================================
  1) Control ATM: 39.84.0F.00.00.00.00.00.00.00.00.01.10.00.5A.01.A4.00.05

1 MAC Address(es) Learnt For This MPS:

  1) MAC Addr: x10.00.5A.01.A4.00   Associated LEC Intf #:  42
```

MPC VCC Monitoring Commands

Enter the following commands at the MPC-VCC> command prompt.

Table 67. MPC VCC Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
list	Displays all the VCCs that are currently associated with the MPC.
list-vcc	Displays detailed information about a particular MPC VCC.

Table 67. MPC VCC Monitoring Command Summary (continued)

Command	Function
delete-vcc	Deletes a VCC associated with the MPC.
vcc-statistics	Displays aggregated statistics related to all VCCs associated with the MPC, including VCCs that may no longer be active).
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to display all of the VCCs that are currently associated with the MPC. This display includes fully operational VCCs and those that are not completely operational.

Syntax:

list

Example:

```
MPC VCC>list
SVCs For MPC On ATM Interface 36 (total    2):
============================================
    1) VPI/VCI 0/38    State: OPERATIONAL
Remote ATM: 39.84.0F.00.00.00.00.00.00.00.00.01.10.00.5A.01.A4.00.05
    2) VPI/VCI 0/39    State: OPERATIONAL
Remote ATM: 39.84.0F.00.00.00.00.00.00.00.00.03.10.00.5A.01.9A.00.04
```

List-VCC

Use the **list-vcc** command to display detailed information about a particular MPC VCC.

Syntax:

list-vcc *vpi vci*

Example:

```
MPC VCC>list-v
VPI, Range 0..255 [0]?
VCI, Range 0..65535 [0]? 39

  VPI/VCI: 0/39     State: OPERATIONAL    Calling Party: FALSE
  Hold Down Cause:  N/A   Cause Code: N/A   Fwd/Bak SDU:4388/4388
  Remote ATM Addr: 39.84.0F.00.00.00.00.00.00.00.00.03.10.00.5A.01.9A.00.04
  Conn Type: P2P     VCC Type: B. EFFORT     Encaps. Type: LLC 1483
  H/W Path Valid: FALSE    Ref. Frame Cnt: 4810
  Frames Tx/Rx: 2754/2754     Bytes Tx/Rx: 275400/275400


(Direct) Shortcut Routes Using This VCC:
----------------------------------------
     1) Address/Mask: 3.4.1.8/255.255.255.255    Shortcut State: RESOLVED
```

Delete-VCC

Use the **delete-vcc** command to delete a VCC associated with the MPC. ATM signalling closes the VCC. Because of on-going traffic, the VCC may be re-established shortly after deletion, giving the appearance that it was never deleted.

MPOA Monitoring Commands (Talk 5)

Syntax:

delete-vcc *vpi vci*

VCC-Statistics

Use the **vcc-statistics** command to display aggregated statistics related to all VCCs associated with the MPC, including VCCs that may no longer be active.

Syntax:

vcc-statistics

Example:

```
MPC VCC>vcc
VCC Statistics For This MPC:
----------------------------
Total Call Setup Failures:              0
Total Incoming Calls Rejected:          0
Total Connections Released Locally:     0
Total Calls Placed Successfully:        1
Total Calls Received Successfully:      1
Total Remote Hangups (Normal):          0
Total Remote Hangups (Error):           0
```

MPC Ingress Cache Monitoring Commands

Enter the following commands at the `MPC-Ingress>` command prompt.

Table 68. MPC Ingress Cache Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
list	Displays all the IP entries in the MPC’s ingress cache.
list-ipx	Displays all the IPX entries in the MPC’s ingress cache. This command may be shortened to **xlist**.
list-entries	Displays detailed information about specific IP ingress cache entries.
list-entries-ipx	Displays detailed information about specific IPX ingress cache entries. This command may be shortened to **xshow-entries**.
delete-entries	Deletes specified IP ingress cache entries.
delete-entries-ipx	Deletes specified IPX ingress cache entries. This command may be shortened to **xdelete-entries**.
ingress-statistics	Displays aggregated statistics for all of the MPC’s ingress cache entries.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

List

Use the **list** command to display a list of all the IP entries in the MPC ingress cache. Use **list-entries** to display more detailed information.

Syntax:

list

Example:

```
MPC INGRESS>list
Ingress Cache For MPC on ATM Interface 36
=========================================


Ingress Cache Entries for Direct Host Routes:
---------------------------------------------
1)  Protocol Address: 3.4.1.8    Shortcut State: RESOLVED

Ingress Cache Entries for Direct Network Routes:
------------------------------------------------

Ingress Cache Entries for Derived Host Routes:
----------------------------------------------
```

List-ipx

Use the **list-ipx** command to display a list of all the IPX entries in the MPC ingress cache. Use **list-entries-ipx** to display more detailed information.

This command may be shortened to **xlist**.

Syntax:

list-ipx

Example:

```
MPC INGRESS>list-ipx
Ingress Cache For MPC on ATM Interface 36
=========================================


Ingress Cache Entries for Direct Host Routes:
---------------------------------------------

Ingress Cache Entries for Direct Network Routes:
------------------------------------------------
 1) Network Number (in hex): 35508661   Shortcut State: RESOLVED

Ingress Cache Entries for Derived Host Routes:
----------------------------------------------
1) Network Number/Host Number (in hex): 35508661/00.00.00.00.00.01  Shortcut State:
RESOLVED
Derived From: 35508661
```

List-entries

Use **list-entries** to display more detailed information about IP entries.

You will be prompted for a destination IP address and address mask. Detailed information is displayed for all entries in the MPC's ingress cache which match the specified address/mask combination. The information displayed for each destination includes:

- State of the entry
- Destination ATM address (if resolved)
- Statistics on frames sent to the MPS and those sent over the shortcut
- Remaining age values
- MTU of the destination

- Shortcut VCC being used for this entry, if any, and the type of encapsulation being used on the VCC
- Whether this is a local shortcut
- Data link layer header information returned in the resolution reply
- Control ATM address of the MPS which provided the address resolution

Syntax:

list-entries *destination-protocol-address mask*

Example:

```
MPC INGRESS>list-en
Destination Protocol Address [0.0.0.0]? 3.4.1.8
Destination Protocol Address Mask [255.255.255.255]?
Host Route Entries matching 3.4.1.8/255.255.255.255
---------------------------


Direct Host Routes :

1) Address: 3.4.1.8  Shortcut State: RESOLVED
Hold Down Cause: N/A   CIE Code: x0
Dest ATM: 39.84.0F.00.00.00.00.00.00.00.00.03.10.00.5A.01.9A.00.04
Remaining Age (mins:secs): 3:12      Last Request ID: xB
Destn MTU: 4376       Encaps. Type: TAGGED
LANE Encaps. Hdr: xN/A
Tag Value: x1
Shortcut VCC (VPI/VCI):    0/  39   Local Shortcut ?: FALSE
MPS: 39.84.0F.00.00.00.00.00.00.00.00.01.10.00.5A.01.A4.00.05

Derived Host Routes :

Network Route Entries matching 3.4.1.8/255.255.255.255
------------------------------

None found!
```

List-entries-ipx

Use **list-entries-ipx** to display more detailed information about IPX entries.

You will be prompted for a destination network number and destination node number. Detailed information is displayed for all entries in the MPC's ingress cache which match the specified network number/node number combination. The information displayed for each destination includes:

- State of the entry
- Destination ATM address (if resolved)
- Remaining age values
- MTU of the destination
- Shortcut VCC being used for this entry, if any, and the type of encapsulation being used on the VCC
- Whether this is a local shortcut
- Data link layer header information returned in the resolution reply
- Control ATM address of the MPS which provided the address resolution.

This command may be shortened to **xshow-entries**.

Syntax:

list-entries-ipx *destination-network-number destination-node-number*

Example:

```
MPC INGRESS>list-entries-ipx
Destination Network Number (in 8-digit hex) (1 - FFFFFFFE) [0]? 35508661
 Destination Node Number (in hex) (0x000000000000 for network destination):[00.00.00.00.00.00]?

Host Route Entries matching 35508661/000000000000
-----------------------------

      Direct Host Routes :

      Derived Host Routes:

1) Network Number (in hex) 35508661  Shortcut State:  RESOLVED
      Hold Down Cause: N/A  CIE Code:  x0
      Dest ATM: 39.99.99.99.99.99.99.00.00.99.99.01.01.12.34.12.34.12.34.03
           Remaining Age  (mins:secs) : 17:17    Last Request ID: x0
      Destn MTU:  4381       Encaps. Type: TR 802.2-IPX-LANE
      LANE Encaps. Hdr: x0000004008005a6c3b778004ac47390d06a000110020
      Tag Value: N/A
      Shortcut VCC (VPI/VCI):    0/ 211   Local Shortcut ?: FALSE
      MPS: 39.99.99.99.99.99.99.00.00.99.99.01.01.00.04.AC.47.39.06.06

   Network Route Entries matching 35508661
   -----------------------------

   1) Network Number (in hex) 35508661  Shortcut State:  RESOLVED
      Hold Down Cause: N/A  CIE Code:  x0
      Destn: 39.99.99.99.99.99.99.00.00.99.99.01.01.12.34.12.34.12.34.03
           Remaining Age  (mins:secs) : 17:17    Last Request ID: x0
      Destn MTU:  4381       Encaps. Type: TR 802.2-IPX-LANE
      LANE Encaps. Hdr: x0000004008005a6c3b778004ac47390d06a000110020
      Tag Value: N/A
      Shortcut VCC (VPI/VCI):    0/ 211   Local Shortcut ?: FALSE
      MPS: 39.99.99.99.99.99.99.00.00.99.99.01.01.00.04.AC.47.39.06.06
```

Delete-entries

Use the **delete-entries** command to delete specific IP ingress cache entries.

Syntax:

delete-entries*destination-protocol-address mask*

You will be prompted for a destination protocol address and address mask. All ingress cache entries which match this address/mask combination are then deleted.

Note: Because of ongoing traffic, an ingress cache entry for a particular destination may immediately get recreated after it has been deleted using this command, giving the appearance that the entry had not been deleted.

Delete-entries-ipx

Use the **delete-entries-ipx** command to delete specific IPX ingress cache entries.

This command may be shortened to **xdelete-entries**.

Syntax:

delete-entries-ipx *destination-network-number destination-node-number*

You will be prompted for a destination network number and destination node number. All ingress cache entries which match this network number/node number combination are then deleted.

Note: Because of ongoing traffic, an ingress cache entry for a particular destination may immediately get recreated after it has been deleted using this command, giving the appearance that the entry had not been deleted.

Ingress-statistics

Use the **ingress-statistics** command to display aggregated statistics for all the MPC's ingress cache entries.

Syntax:

ingress-statistics

Example:

```
MPC INGRESS>ingress
Ingress MPC Statistics For This MPC:
-----------------------------------
Total Resolution Requests Sent:         14
Total Refresh Res. Requests Sent:       13
Total Res. Rqst Retransmissions:        1
Total Res. Rqst Timeouts:               0
Total Res. Reply Successes:             14
Total Res. Reply NAKs:                  0
Total Res. Replies Discarded:           0
Total MPS Purges Recvd:                 0
Total MPS Purged Mappings:              0
Total MPS Purges Discarded:             0
Total Triggers Recvd:                   0
Total Triggers Discarded:               0
Total Keep Alives Recvd:                443
Total Inactive Mappings Deleted:        0
Total Frames Forwarded On Shortcuts:    4414
Total Data Plane Purges Recvd:          0
Total Data Plane Purged Mappings:       0
Total Data Plane Purges Discarded:      0
Total NHRP Purge Replies Transmitted:   0
```

MPC Egress Cache Monitoring Commands

Enter the following commands at the `MPC-Egress>` command prompt.

Table 69. MPC Egress Cache Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See "Getting Help" on page 10.
list	Displays all the IP entries in the MPC's egress cache.
list-ipx	Displays all the IPX entries in the MPC's egress cache. This command may be shortened to **xlist**.
list-entries	Displays detailed information about specific IP egress cache entries.
list-entries-ipx	Displays detailed information about specific IPX egress cache entries. This command may be shortened to **xshow-entries**.
purge-entries	Purges specified IP egress cache entries.
purge-entries-ipx	Purges specified egress IPX cache entries. This command may be shortened to **xpurge-entries**.

Table 69. MPC Egress Cache Monitoring Command Summary (continued)

Command	Function
egress-statistics	Displays aggregated statistics for all of the MPC's egress cache entries.
Exit	Returns you to the previous command level. See "Exiting a Lower Level Environment" on page 11.

List

Use the **list** command to display a list of all the IP entries in the MPC egress cache. Use **list-entries** to display more detailed information.

Syntax:

list

Example:

```
MPC EGRESS>list
Egress Cache For MPC on ATM Interface 36
========================================

Egress Cache Entries w/ MPOA-Tag Encapsulation:
-----------------------------------------------

    1) Protocol Address/Mask: 5.4.1.5/255.255.255.255     State:     ACTIVE


Egress Cache Entries w/ Native 1483 Encapsulation (Host Routes):
----------------------------------------------------------------


Egress Cache Entries w/ Native 1483 Encapsulation (Netwk Routes):
----------------------------------------------------------------
```

List-ipx

Use the **list-ipx** command to display a list of all the IPX entries in the MPC egress cache. Use **list-entries-ipx** to display more detailed information.

This command may be shortened to **xlist**.

Syntax:

list-ipx

Example:

```
MPC EGRESS>list-ipx
Egress Cache For MPC on ATM Interface 36
========================================


Egress Cache Entries w/ MPOA-Tag Encapsulation:
-----------------------------------------------

Egress Cache Entries w/ Native 1483 Encapsulation (Host Routes):
----------------------------------------------
    1) Net/Host Num (in hex): 3/00.00.00.01.A2.00 State :   Active

Egress Cache Entries w/Native 1483 Encapsulation (Netwk Routes):
----------------------------------------------
```

List-entries

Use **list-entries** to display detailed information about all the IP entries in the MPC egress cache.

You will be prompted for a destination protocol address and mask. Detailed information is then displayed for all egress cache entries which match this address/mask combination. The information includes:

- ATM addresses of the source and the imposing MPS
- Type of the entry
- Identity of the egress LEC corresponding to the imposition request
- Cache ID of the entry
- Its remaining age
- Statistics on received data packets
- Tag value, if applicable
- Data link layer header information
- Information on the different types of LANE extensions returned in the last MPOA Cache Imposition reply for this entry

Syntax:

list-entries *destination-protocol-address mask*

Example:

```
MPC EGRESS>list-en
Destination Protocol Address [0.0.0.0]? 5.4.1.5
Destination Protocol Address Mask [255.255.255.255]?

      Egress Cache Entries matching 5.4.1.5/255.255.255.255 :

 1) Address/Mask: 5.4.1.5/255.255.255.255   Entry Type: TAG
    LEC #:  2    Cache ID: x1   State: ACTIVE
    MPS: 39.84.0F.00.00.00.00.00.00.00.00.01.10.00.5A.01.A4.00.05
    Source: 39.84.0F.00.00.00.00.00.00.00.00.03.10.00.5A.01.9A.00.04
    Remaining Age (mins:secs): 13:37
    Recvd Octets: 463900
    Recvd Frames Forwarded: 4639
    Recvd Frames Discarded: 0
    Tag Value: x1       Local Shortcut: FALSE
    DLL Header: x0040000000019f0090005a01a40006a08b884b40aaaa030000000800
    LANE Extensions in last Imposition reply:  None
```

List-entries-ipx

Use **list-entries-ipx** to display more detailed information about IPX entries.

You will be prompted for a destination network number and destination node number. Detailed information is displayed for all entries in the MPC's egress cache which match the specified network number/node number combination. The information displayed for each destination includes:

- State of the entry
- Destination ATM address (if resolved)
- Statistics on frames sent to the MPS and those sent over the shortcut
- Remaining age values
- MTU of the destination

- Shortcut VCC being used for this entry, if any, and the type of encapsulation being used on the VCC
- Whether this is a local shortcut
- Data link layer header information returned in the resolution reply
- Control ATM address of the MPS which provided the address resolution.

This command may be shortened to **xshow-entries** or **xs**.

Syntax:

list-entries-ipx *destination-network-number destination-node-number*

Example:

```
MPC EGRESS>list-entries-ipx
Destination Network Number (in 8-digit hex) (1 - FFFFFFFE) [0]? 3
Destination Node Number (in hex) (0x000000000000 for network destination):[00.00.00.00.00.00]?

Egress Cache Entries matching 3/000000000000

1) IPX Net/Host Num: 3/00000001a200 Entry Type: 1483 (Host,Direct)
Lec#: 1  Cache IP: x1  State: ACTIVE
MPS: 39.84.0F.00.00.00.00.00.00.00.00.00.04.10.00.5A.01.AC.00.05
Source: 39.84.0F.00.00.00.00.00.00.00.00.00.024.10.00.5A.01.9C.00.03
Remaining Age (mins:secs): 5:5
Recvd Octets: N/A
Recvd Frames Forwarded: N/A
Recvd Frames Discarded: N/A
Tage Value: N/A    Local Shortcut: FALSE
DLL Header: x0040000000001a20090005a00999906a00a2a0a10e0e003
LANE Extensions in last Imposition reply: Formats 7, 11, 13, 17
```

Purge-entries

Use the **purge-entries** command to purge specified IP egress cache entries.

You will be prompted for a destination protocol address and mask. All egress cache entries which match this address/mask combination are purged. This is done using the MPOA egress MPC-initiated egress cache purge request.

Note: Because of ongoing traffic, an egress cache entry for a destination may immediately get recreated after it has been purged, giving the appearance that the purge command may not have been successful.

Syntax:

purge-entries *destination-protocol-address mask*

Purge-entries-ipx

Use the **purge-entries-ipx** command to purge specified egress cache entries.

You will be prompted for a destination network number and destination node number. All egress cache entries which match this network number/node number combination are purged. This is done using the MPOA egress MPC initiated egress cache purge request.

Note: Because of ongoing traffic, an egress cache entry for a destination may immediately get recreated after it has been purged, giving the appearance that the purge command may not have been successful.

This command may be shortened to **xpurge-entries** or **xp**.

Syntax:

purge-entries *destination-network-number destination-node-number*

Egress-statistics

Use the **egress-statistics** command to display aggregated statistics for all the MPC's egress cache entries.

Syntax:

egress-statistics

Example:

```
MPC EGRESS>egr
Egress MPC Statistics For This MPC:
-----------------------------------
Total Imposition Requests Recvd:        18
Total Imposition Rqsts NAKed:           0
Total Imposition Updates Received:      17
Total Imposition Purges Received:       0
Total Imposition Purged Mappings:       0
Total E-MPC Purge Rqsts Sent To MPSs:   0
Total E-MPC Purge Rqst Retransmissions: 0
Total E-MPC Purge Rqst Timeouts:        0
Tot. Frames Recvd & Fwded (Software):   5510
Total Recvd Frames Discarded:           0
Total Data Plane Purge Rqsts Sent:      0
Total Data Plane Purge Rqst Retransmits:0
Total Data Plane Purge Rqst Timeouts:   0
Total Egress Cache Entries Aged Out:    0
```

MPC Configure Monitoring Commands

Enter the following commands at the `MPC-Configure>` command prompt to dynamically change values of the MPC configuration parameters. The changes occur immediately and are temporary. The changes are applied to the running MPC instance and are not saved.

The commands for setting various configuration parameters are very similar to the corresponding commands using `talk 6`. Under `talk 5`, however, there are separate explicit commands for setting each parameter that can be dynamically configured, while under `talk 6`, all parameters are configured under the **set** command.

Note: Dynamic enabling/ disabling or creation/deletion of an MPOA client can also be done and the commands are under the MPC-BASE menu.

Two additional sets of configuration parameters available using the `talk 5` **config** that do not have any `talk 6` counterparts are the **atm-packet-trace-filter** and **lan-packet-trace-filter** commands. You can configure a mask for an ATM address or MAC address respectively. MPOA client packets are only traced if the remote

ATM address of the VCC on which the packet is being sent or received or the destination MAC address of the packet if on a legacy LAN interface matches the configured mask.

The first example will result in only those MPOA client packets being traced on the ATM interface that are being sent/received over VCCs to a remote ATM address with the last two bytes being X'05'.

Example:

```
MPC CONFIGURE>atm
    ATM Address Pkt Trace Filter Value (40 hex digits)
     [0000000000000000000000000000000000000000]?
     0000000000000000000000000000000000000005
    ATM Address Pkt Trace Filter Mask (40 hex digits)
     [0000000000000000000000000000000000000000]?
     00000000000000000000000000000000000000ff
```

The following example will result in MPOA client packet tracing on the legacy LAN interfaces of only those packets for which the destination MAC address has a ′40’ as the first byte.

Example:

```
MPC CONFIGURE>lan
    LAN Pkt Trace Filter Value (12 hex digits)
     [000000000000]? 400000000000
    LAN Pkt Trace Filter Mask (12 hex digits)
     [000000000000]? ff0000000000
```

See page 338 for a description of each command.

Table 70. MPC Configure Monitoring Command Summary

Command	Function
? (Help)	Displays all the commands available for this command level or lists the options for specific commands (if available). See “Getting Help” on page 10.
list	Displays the current values of all the dynamically configurable parameters.
reset	Resets all the dynamically configurable parameters to the values configured at the `talk 6` prompt. See “MPC Configuration Commands” on page 335 for more information.
pcr	Dynamically sets the peak cell rate for the MPC instance.
max-reserved-bandwidth	Dynamically sets the maximum reserved bandwidth for the MPC instance.
enable-lane-shortcuts	Dynamically enables LANE shortcuts for the MPC instance.
lane-shortcuts-src-mac	Dynamically sets the source MAC address to be used in frames transmitted on LANE shortcut VCCs.
configured-src-mac	Dynamically sets locally administered MAC address to be used as the source MAC address in frames transmitted on LANE shortcut VCCs..
frame-count	Dynamically sets the frame count used to control the rate of traffic required before the MPC will initiate a shortcut to a given protocol destination.

Table 70. MPC Configure Monitoring Command Summary (continued)

Command	Function
frame-time	Dynamically sets frame time used to control the rate of traffic required before the MPC will initiate a shortcut to a given protocol destination.
init-retry-time	Dynamically sets the value of the retry timer used to determine if a request is to be retried when there is no response in a specified amount of time.
max-retry-time	Dynamically sets the maximum value of the retry timer used to determine if a request is to be retried when there is no response in a specified amount of time.
hold-down-time	Dynamically sets the minimum time to wait before reinitiating a failed resolution attempt.
vcc-timeout	Dynamically sets the time after which VCCs will be cleared when there has been no activity.
accept-config-from-lecs	Dynamically specifies whether any configuration parameters received from the LECS will be accepted by the MPC.
fragmentation-mode	Dynamically controls the manner that the ingress MPC handles IP packet fragmentation.
atm-packet-trace-filter	Allows the user to restrict packet tracing to specific VCCs.
lan-packet-trace-filter	Allows the user to restrict packet tracing to and from LAN ports.
Exit	Returns you to the previous command level. See “Exiting a Lower Level Environment” on page 11.

MPC Packet Tracing

MPOA client packet traces can be activated from the Event Logging System (ELS) which is an integral part of the device operating system. See the chapter entitled “Using the Event Logging System” and the chapter entitled “Configuring and Monitoring the Event Logging System” in *8371 Interface Configuration and Software User’s Guide* for additional information about ELS.

Note: Packet tracing for the MPOA server function is separate from that of the MPOA client function and is accessed as part of NHRP packet tracing.

For MPOA client packet tracing, use the MPOA ELS subsystem. MPOA client packet tracing supports the **set trace decode on** option. This option enables the MPOA output to be interpreted for viewing. For details on using the trace facility, see the description of the trace command in the chapter entitled “Configuring and Monitoring the Event Logging System” in *8371 Interface Configuration and Software User’s Guide*

MPOA client packets are identified by three different events under the MPOA ELS subsystem.

- Event 61 traces all MPOA client control frames
- Event 62 traces all MPOA client data frames
- Event 63 traces all MPOA client frames on legacy LAN interfaces.

Sample Trace Output 1:

```
#1 Dir:INCOMING  Time:2.10.16.85  Trap:7611
Comp:MPOA  Type:UNKNOWN  Port:0  Circuit:0x000000  Size:245
-------------------------------------------------------------
** MPC MPOA/NHRP Frame on 1483 VCC **
AddressFamily:ATM_NSAP  ProtocolType:IPv4  HopCount:64  PacketSize:237
```

```
Checksum:0x6F02  ExtensionOffset:0x0044  Version:1
PktType:MpoaCacheImpositionR
equest
SrcAddrTL:20  SrcSubAddrTL:0  SrcProtoLen:4  DstProtoLen:4
ReqID:26
Src NBMA:39840F0000000000000000000310005A019A0004
Src Protocol Addr: 5.4.2.0  Dest Protocol Addr: 5.4.1.5
0040: 00 FF 00 00 11 18 03 C0  00 00 00 00 10 01 00 00    | ................ |
0050: 10 02 00 04 D0 00 00 5A  00 08 00 08 08 00 5A 00    | .......Z......Z. |
0060: 00 01 00 06 00 08 00 1C  08 00 5A 00 00 01 00 0A    | ..........Z..... |
0070: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
0080: 00 00 00 00 00 08 00 34  08 00 5A 00 00 01 00 0C    | .......4..Z..... |
0090: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
00A0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
00B0: 00 00 00 00 00 00 00 00  00 00 00 00 00 08 00 08    | ................ |
00C0: 08 00 5A 00 00 01 00 10  90 00 00 25 00 00 00 02    | ..Z........%.... |
00D0: 00 00 00 00 1C 00 40 00  00 00 01 9F 00 90 00 5A    | ......@........Z |
00E0: 01 A4 00 06 20 4B 48 8B  80 AA AA 03 00 00 00 08    | .... KH......... |
00F0: 00 80 00 00 00
```

Sample Trace Output 2:

```
#3 Dir:OUTGOING  Time:2.10.16.85  Trap:7611
Comp:MPOA  Type:UNKNOWN  Port:0  Circuit:0x000000  Size:269
----------------------------------------------------------------
** MPC MPOA/NHRP Frame on 1483 VCC **
AddressFamily:ATM_NSAP  ProtocolType:IPv4  HopCount:255  PacketSize:261
Checksum:0x0DBE  ExtensionOffset:0x0058  Version:1
PktType:MpoaCacheImpositionR
eply
SrcAddrTL:20  SrcSubAddrTL:0  SrcProtoLen:4  DstProtoLen:4
ReqID:26
Src NBMA:39840F0000000000000000000310005A019A0004
Src Protocol Addr: 5.4.2.0  Dest Protocol Addr: 5.4.1.5
0040: 00 20 00 00 11 18 03 C0  14 00 00 FF 39 84 0F 00    | . ..........9... |
0050: 00 00 00 00 00 00 00 00  02 10 00 5A 01 9C 00 03    | ...........Z.... |
0060: 10 01 00 04 00 00 00 01  10 02 00 04 00 00 D0 00    | ................ |
0070: 00 08 00 08 08 00 5A 00  00 01 00 06 00 08 00 1C    | ......Z......... |
0080: 08 00 5A 00 00 01 00 0A  00 00 00 00 00 00 00 00    | ..Z............. |
0090: 00 00 00 00 00 00 00 00  00 00 00 00 00 08 00 34    | ..............4 |
00A0: 08 00 5A 00 00 01 00 0C  00 00 00 00 00 00 00 00    | ..Z............. |
00B0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
00C0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00    | ................ |
00D0: 00 00 00 00 00 08 00 08  08 00 5A 00 00 01 00 10    | ..........Z..... |
00E0: 90 00 00 25 00 00 00 02  00 00 00 00 1C 00 40 00    | ...%..........@. |
00F0: 00 00 01 9F 00 90 00 5A  01 A4 00 06 20 4B 48 8B    | .......Z.... KH. |
```

Sample Configuration

Example Configuration of an MPOA client

Notes:

1 Enter the MPOA client configuration menus.

2 First add an MPC.

3 Confirm that an MPC has been added, then go into the config option for configuring this MPC.

4 List the current configuration. Since we just added the MPC, all the configuration parameters have been set to the default values.

4a Some of the parameters displayed cannot be configured but are displayed simply for convenience. For instance the interface indicated refers to the ATM interface number on which the MPC is being configured.

5 If we would like the MPC to be in disabled state on bringup, use the **disable** command. The MPC can be dynamically activated from the monitoring console (talk 5).

6 Use the **set** command to configure various MPC parameters. Check the list of parameters which can be set using this command as shown below.

7 The *frame-count* parameter can be configured as shown (setting it to 1 will effectively result in the MPC making shortcut attempts to every destination for which a packet is encountered, while setting it to a very large value will result in shortcuts only to destinations to which extremely heavy traffic is being sent).

8 Configure the ESI portion of the ATM address of the MPC (the MPC uses a single ATM address as both its control and data ATM address). Two ESIs have already been administered under the ATM interface configuration menus.

9 Configure the selector byte to be used along with the ESI as part of the MPC's ATM address.

10 Configure parameters related to the use of LAN emulation shortcuts.

Note: If LANE shortcuts are enabled, you are prompted for the choice of source MAC address to be used in the layer 2 header of LANE shortcut packets. Further, if option 2 (*locally configured MAC address* is chosen, then you are also prompted for the MAC address desired.

11 Confirm the new configuration using the **list** command.

```
  MOS Operator Console

For help using the Command Line Interface, press ESCAPE, then '?'

*t 6
Gateway user configuration
Config>p mpoa        1
Next Hop Resolution Protocol/Multi Protocol Over ATM user configuration
MPOA config>mpc 36

MPOA Client user configuration
MPC >?
ADD
LIST
CONFIG
REMOVE
EXIT

MPC >add         2

     MPC added on interface 36
MPC >list        3
    LIST OF CONFIGURED MPOA CLIENTS
       ---------------------------------
       Interface                  Status
       ---------------------------------
          36                      ENABLED

MPC >config

MPC Configuration> ?
ENABLE
DISABLE
SET
LIST
EXIT
```

```
       MPC Configuration> list        4

MPC Configuration
-----------------
STATUS: ENABLED
Shortcut Setup Frame Count:       10    (frames)
Shortcut Setup Frame Time:        1     (sec)
Initial Retry Time:               5     (sec)
Maximum Retry Time:               40    (sec)
Hold Down Time:                   160   (sec)
VCC Timeout Period:               20    (min)
Accept Config From LECS:          Yes
Fragmentation Mode:               Maximize Shortcut Usage

Interface:                       36

ESI:                              Burned In ESI
Selector:                         0x 2
Desired PCR:                      155000 (kbps)
Maximum Reserved Bandwidth:       155000 (kbps)
Line Rate:                        155 (Mbps)
Enable LANE Shortcuts:            TRUE
Source MAC Address for Shortcuts: Burned In

 4a

MPC Configuration> disable         5
Disable MPC?  [Yes]?y
    MPC set to DISABLED

MPC Configuration> set ?       6
FRAME-COUNT (FOR SHORTCUTS)
FRAME-TIME (FOR SHORTCUTS)
INITIAL-RETRY-TIME
MAXIMUM-RETRY-TIME
HOLD-DOWN-TIME
VCC-TIMEOUT-PERIOD
ACCEPT-CONFIG-FROM-LECS
FRAGMENTATION-MODE
ESI
SELECTOR
PCR
MAX-RESERVED-BANDWIDTH
SHORTCUTS


MPC Configuration> set frame-count    7
Frame Count for Shortcut Setup (in frames):  [10]? 1

MPC Configuration> set esi       8
[1] Burned in ESI
[2] 12.34.56.78.9A.BC
[3] 12.12.12.12.12.12
 ESI:  [1]? 2

MPC Configuration> set selector      9
Selector Byte (in hex) [2]? 10
MPC Configuration> set short    10
Enable LANE Shortcuts?  [Yes]? y

  Choices for Source MAC Address for LANE Shortcuts:
   [1] Burned in ESI
   [2] Locally Configured MAC Address
   [3] MAC Address from the Resolution Reply

MAC Address Type for LANE Shortcuts:  [1]? 2
MAC Address for LANE Shortcuts:  [00.00.00.00.00.00]?42.42.42.42.42.42
```

MPOA Monitoring Commands (Talk 5)

```
MPC Configuration> list      11

MPC Configuration
-----------------
STATUS: DISABLED
Shortcut Setup Frame Count:       1     (frames)
Shortcut Setup Frame Time:        1     (sec)
Initial Retry Time:               5     (sec)
Maximum Retry Time:               40    (sec)
Hold Down Time:                   160   (sec)
VCC Timeout Period:               10    (min)
Accept Config From LECS:          Yes
Fragmentation Mode:               Maximize Shortcut Usage

Interface:                       36

ESI:                              12.34.56.78.9A.BC
Selector:                         0x10
Desired PCR:                      155000 (kbps)
Maximum Reserved Bandwidth:       155000 (kbps)
Line Rate:                        155 (Mbps)
Enable LANE Shortcuts:            TRUE
Source MAC Address for Shortcuts: Locally Configured
  42.42.42.42.42.42
```

Part 5. Appendixes

Appendix. Abbreviations

AAL ATM Adaptation Layer

AAL-5 ATM Adaptation Layer 5

AARP AppleTalk Address Resolution Protocol

ABR area border router

ack acknowledgment

AIX Advanced Interactive Executive

AMA arbitrary MAC addressing

AMP active monitor present

ANSI American National Standards Institute

AP2 AppleTalk Phase 2

APPN Advanced Peer-to-Peer Networking

ARE all-routes explorer

ARI ATM real interface

ARI/FCI
address recognized indicator/frame copied indicator

ARP Address Resolution Protocol

AS autonomous system

ASBR autonomous system boundary router

ASCII American National Standard Code for Information Interchange

ASN.1 abstract syntax notation 1

ASRT adaptive source routing transparent

ASYNC
asynchronous

ATCP AppleTalk Control Protocol

ATM Asynchronous Transfer Mode

ATMARP
ARP in Classical IP

ATP AppleTalk Transaction Protocol

AUI attachment unit interface

AVI ATM virtual interface

ayt are you there

BAN Boundary Access Node

BBCM Bridging Broadcast Manager

BCM BroadCast Manager

BECN backward explicit congestion notification

BGP Border Gateway Protocol

BGP Border Growth Protocol

BNC bayonet Niell-Concelman

BNCP Bridging Network Control Protocol

BOOTP
BOOT protocol

BPDU bridge protocol data unit

bps bits per second

bandwidth reservation

BSD Berkeley software distribution

BTP BOOTP relay agent

BTU basic transmission unit

BUS Broadcast and Unknown Server

CAM content-addressable memory

CCITT Consultative Committee on International Telegraph and Telephone

CD collision detection

CGWCON
Gateway Console

CIDR Classless Inter-Domain Routing

CIP Classical IP

CIPC Classical IP Client

CIR committed information rate

CLNP Connectionless-Mode Network Protocol

CPU central processing unit

CRC cyclic redundancy check

CRS configuration report server

CTS clear to send

CUD call user data

DAF destination address filtering

DB database

DBsum
database summary

DCD data channel received line signal detector

DCE data circuit-terminating equipment

DCS directly connected server

DDLC dual data-link controller

DDN Defense Data Network

DDP Datagram Delivery Protocol

DDT Dynamic Debugging Tool

DHCP Dynamic Host Configuration Protocol

dir directly connected

DL data link

DLC data link control

DLCI data link connection identifier

DLS data link switching

DLSw data link switching

DMA direct memory access

DNA Digital Network Architecture

DNCP DECnet Protocol Control Protocol

DNIC Data Network Identifier Code

DoD Department of Defense

DOS Disk Operating System

DR designated router

DRAM Dynamic Random Access Memory

DSAP destination service access point

DSE data switching equipment

DSE data switching exchange

DSR data set ready

DSU data service unit

DTE data terminal equipment

DTR data terminal ready

Dtype destination type

DVMRP
Distance Vector Multicast Routing Protocol

E1 2.048 Mbps transmission rate

EDEL end delimiter

EDI error detected indicator

EGP Exterior Gateway Protocol

EIA Electronics Industries Association

ELAN Emulated Local Area Network

ELAP EtherTalk Link Access Protocol

ELS Event Logging System

ESI End System Identifier

EST Eastern Standard Time

Eth Ethernet

fa-ga functional address-group address

FCS frame check sequence

FECN forward explicit congestion notification

FIFO first in, first out

FLT filter library

FR Frame Relay

FRL Frame Relay

FTP File Transfer Protocol

GMT Greenwich Mean Time

GOSIP
Government Open Systems Interconnection Profile

GTE General Telephone Company

GWCON
Gateway Console

HDLC high-level data link control

HEX hexadecimal

HST TCP/IP host services

HTF host table format

IBD Integrated Boot Device

ICMP Internet Control Message Protocol

ICP Internet Control Protocol

ID identification

IDP Initial Domain Part

IDP Internet Datagram Protocol

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Engineering Task Force

Ifc# interface number

IGP interior gateway protocol

ILMI Interim Local Management Interface

InARP Inverse Address Resolution Protocol

IP Internet Protocol

IPCP IP Control Protocol

IPPN IP Protocol Network

IPX Internetwork Packet Exchange

IPXCP IPX Control Protocol

ISDN integrated services digital network

ISO International Organization for Standardization

Kbps kilobits per second

LAN local area network

LAPB link access protocol-balanced

LAT local area transport

LCP Link Control Protocol

LE LAN Emulation

LEC LAN Emulation Client

LED light-emitting diode

LECS LAN Emulation Configuration Server

LES LAN Emulation Server

LES-BUS
LAN Emulation Server - Broadcast and Unknown Server

LF largest frame; line feed

LIS Logical IP subnet

LLC logical link control

LLC2 logical link control 2

LMI local management interface

LRM LAN reporting mechanism

LS link state

LSA link state advertisement

LSB least significant bit

LSI LANE Shortcuts Interface

LSreq link state request

LSrxl link state retransmission list

LU logical unit

MAC medium access control

Mb megabit

MB megabyte

Mbps megabits per second

MBps megabytes per second

MC multicast

MCF MAC filtering

MIB Management Information Base

MIB II Management Information Base II

MILNET
military network

MOS Micro Operating System

MOSDDT
Micro Operating System Dynamic Debugging Tool

MOSPF
Open Shortest Path First with multicast extensions

MSB most significant bit

MSDU MAC service data unit

MSS Multiprotocol Switched Services

MTU maximum transmission unit

nak not acknowledged

NBMA Non-Broadcast Multiple Access

NBP Name Binding Protocol

NBR neighbor

NCP Network Control Protocol

NCP Network Core Protocol

NetBIOS
Network Basic Input/Output System

NHRP Next Hop Resolution Protocol

NIST National Institute of Standards and Technology

NPDU Network Protocol Data Unit

NRZ non-return-to-zero

NRZI non-return-to-zero inverted

NSAP Network Service Access Point

NSF National Science Foundation

NSFNET
National Science Foundation NETwork

NVCNFG
nonvolatile configuration

OPCON
Operator Console

OSI open systems interconnection

OSICP
OSI Control Protocol

OSPF Open Shortest Path First

OUI organization unique identifier

PC personal computer

PCR peak cell rate

PDN public data network

PING Packet internet groper

PDU protocol data unit

PID process identification

P-P Point-to-Point

PPP Point-to-Point Protocol

PROM programmable read-only memory

PU physical unit

PVC permanent virtual circuit

QoS Quality of Service

RAM random access memory

RD route descriptor

REM ring error monitor

REV receive

RFC Request for Comments

RI ring indicator; routing information

RIF routing information field

RII routing information indicator

RIP Routing Information Protocol

RISC reduced instruction-set computer

RNR receive not ready

ROM read-only memory

ROpcon
Remote Operator Console

RPS ring parameter server

RTMP Routing Table Maintenance Protocol

RTP RouTing update Protocol

RTS request to send

Rtype route type

rxmits retransmissions

rxmt retransmit

SAF source address filtering

SAP service access point

SAP Service Advertising Protocol

SCR sustained cell rate

SCSP Server Cache Synchronization Protocol

sdel start delimiter

SDLC SDLC relay, synchronous data link control

SDU Service Data Unit

SGID server group id

seqno sequence number

SGMP Simple Gateway Monitoring Protocol

SL serial line

SLIP Serial Line IP

SMP standby monitor present

SMTP Simple Mail Transfer Protocol

SNA Systems Network Architecture

SNAP Subnetwork Access Protocol
SubNetwork Attachment Point

SNMP Simple Network Management Protocol

SNPA subnetwork point of attachment

SPF OSPF intra-area route

SPE1 OSPF external route type 1

SPE2 OSPF external route type 2

SPIA OSPF inter-area route type

SPID service profile ID

SPX Sequenced Packet Exchange

SQE signal quality error

SRAM static random access memory

SRB source routing bridge

SRF specifically routed frame

SRLY SDLC relay

SRT source routing transparent

SR-TB
source routing-transparent bridge

STA static

STB spanning tree bridge

STE spanning tree explorer

STP shielded twisted pair; spanning tree protocol

SVC switched virtual circuit

SVN Switched Virtual Networking

TB transparent bridge

TCN topology change notification

TCP Transmission Control Protocol

TCP/IP
Transmission Control Protocol/Internet Protocol

TEI terminal point identifier

TFTP Trivial File Transfer Protocol

TKR token ring

TLV Type/Length/Value

TMO timeout

TOS type of service

TSF transparent spanning frames

TTL time to live

TTY teletypewriter

TX transmit

UA unnumbered acknowledgment

UDP User Datagram Protocol

UI unnumbered information

UNI User-Network Interface

UTP unshielded twisted pair

VCC Virtual Channel connection

VINES VIrtual NEtworking System

VIR variable information rate

VL virtual link

VNI Virtual Network Interface

VR virtual route

WAN wide area network

WRS WAN restoral

X.25 packet-switched networks

X.251 X.25 physical layer

X.252 X.25 frame layer

X.253 X.25 packet layer

XID exchange identification

XNS Xerox Network Systems

XSUM checksum

ZIP AppleTalk Zone Information Protocol

ZIP2 AppleTalk Zone Information Protocol 2

ZIT Zone Information Table

Glossary

This glossary includes terms and definitions from:

- The *American National Standard Dictionary for Information Systems* , ANSI X3.172-1990, copyright 1990 by the American National Standards Institute (ANSI). Copies may be purchased from the American National Standards Institute, 11 West 42nd Street, New York, New York 10036. Definitions are identified by the symbol (A) after the definition.
- The ANSI/EIA Standard—440-A, *Fiber Optic Terminology* Copies may be purchased from the Electronic Industries Association, 2001 Pennsylvania Avenue, N.W., Washington, DC 20006. Definitions are identified by the symbol (E) after the definition.
- The *Information Technology Vocabulary* developed by Subcommittee 1, Joint Technical Committee 1, of the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC JTC1/SC1). Definitions of published parts of this vocabulary are identified by the symbol (I) after the definition; definitions taken from draft international standards, committee drafts, and working papers being developed by ISO/IEC JTC1/SC1 are identified by the symbol (T) after the definition, indicating that final agreement has not yet been reached among the participating National Bodies of SC1.
- The *IBM Dictionary of Computing* , New York: McGraw-Hill, 1994.
- Internet Request for Comments: 1208, *Glossary of Networking Terms*
- Internet Request for Comments: 1392, *Internet Users' Glossary*
- The *Object-Oriented Interface Design: IBM Common User Access Guidelines* , Carmel, Indiana: Que, 1992.

The following cross-references are used in this glossary:

Contrast with:
This refers to a term that has an opposed or substantively different meaning.

Synonym for:
This indicates that the term has the same meaning as a preferred term, which is defined in its proper place in the glossary.

Synonymous with:
This is a backward reference from a defined term to all other terms that have the same meaning.

See: This refers the reader to multiple-word terms that have the same last word.

See also:
This refers the reader to terms that have a related, but not synonymous, meaning.

A

AAL. ATM Adaptation Layer, the layer that adapts user data to/from the ATM network by adding/removing headers and segmenting/reassembling the data into/from cells.

AAL-5. ATM Adaptation Layer 5, one of several standard AALs. AAL-5 was designed for data communications, and is used by LAN Emulation and Classical IP.

abstract syntax. A data specification that includes all distinctions that are needed in data transmissions, but that omits (abstracts) other details such as those that depend on specific computer architectures. See also *abstract syntax notation 1 (ASN.1)* and *basic encoding rules (BER)*.

abstract syntax notation 1 (ASN.1). The Open Systems Interconnection (OSI) method for abstract syntax specified in the following standards:

- ITU-T Recommendation X.208 (1988) | ISO/IEC 8824: 1990
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1994

See also *basic encoding rules (BER)*.

ACCESS. In the Simple Network Management Protocol (SNMP), the clause in a Management Information Base (MIB) module that defines the minimum level of support that a managed node provides for an object.

acknowledgment. (1) The transmission, by a receiver, of acknowledge characters as an affirmative response to a sender. (T) (2) An indication that an item sent was received.

active monitor. In a token-ring network, a function performed at any one time by one ring station that initiates the transmission of tokens and provides token error recovery facilities. Any active adapter on the ring has the ability to provide the active monitor function if the current active monitor fails.

address. In data communication, the unique code assigned to each device, workstation, or user connected to a network.

address mapping table (AMT). A table, maintained within the AppleTalk router, that provides a current mapping of node addresses to hardware addresses.

address mask. For internet subnetworking, a 32-bit mask used to identify the subnetwork address bits in the host portion of an IP address. Synonymous with *subnet mask* and *subnetwork mask*.

address resolution. (1) A method for mapping network-layer addresses to media-specific addresses. (2) See also *Address Resolution Protocol (ARP)* and *AppleTalk Address Resolution Protocol (AARP)*.

Address Resolution Protocol (ARP). (1) In the Internet suite of protocols, the protocol that dynamically maps an IP address to an address used by a supporting metropolitan or local area network such as Ethernet or token-ring. (2) See also *Reverse Address Resolution Protocol (RARP)*.

addressing. In data communication, the way in which a station selects the station to which it is to send data.

adjacent nodes. Two nodes connected together by at least one path that connects no other node. (T)

Administrative Domain. A collection of hosts and routers, and the interconnecting networks, managed by a single administrative authority.

alert. A message sent to a management services focal point in a network to identify a problem or an impending problem.

all-stations address. In communications, synonym for *broadcast address*.

American National Standards Institute (ANSI). An organization consisting of producers, consumers, and general interest groups, that establishes the procedures by which accredited organizations create and maintain voluntary industry standards in the United States. (A)

analog. (1) Pertaining to data consisting of continuously variable physical quantities. (A) (2) Contrast with *digital*.

AppleTalk. A network protocol developed by Apple Computer, Inc. This protocol is used to interconnect network devices, which can be a mixture of Apple and non-Apple products.

AppleTalk Address Resolution Protocol (AARP). In AppleTalk networks, a protocol that (a) translates AppleTalk node addresses into hardware addresses and (b) reconciles addressing discrepancies in networks that support more than one set of protocols.

AppleTalk Transaction Protocol (ATP). In AppleTalk networks, a protocol that provides client/server request and response functions for hosts accessing the Zone Information Protocol (ZIP) for zone information.

APPN network. See *Advanced Peer-to-Peer Networking (APPN) network*.

APPN network node. See *Advanced Peer-to-Peer Networking (APPN) network node*.

arbitrary MAC addressing (AMA). In DECnet architecture, an addressing scheme used by DECnet Phase IV-Prime that supports universally administered addresses and locally administered addresses.

area. In Internet and DECnet routing protocols, a subset of a network or gateway grouped together by definition of the network administrator. Each area is self-contained; knowledge of an area's topology remains hidden from other areas.

asynchronous (ASYNC). Pertaining to two or more processes that do not depend upon the occurrence of specific events such as common timing signals. (T)

ATM. Asynchonous Transfer Mode, a connection-oriented, high-speed networking technology based on cell switching.

ATMARP. ARP in Classical IP.

attachment unit interface (AUI). In a local area network, the interface between the medium attachment unit and the data terminal equipment within a data station. (I) (A)

authentication failure. In the Simple Network Management Protocol (SNMP), a trap that may be generated by an authentication entity when a requesting client is not a member of the SNMP community.

autonomous system. In TCP/IP, a group of networks and routers under one administrative authority. These networks and routers cooperate closely to propagate network reachability (and routing) information among themselves using an interior gateway protocol of their choice.

autonomous system number. In TCP/IP, a number assigned to an autonomous system by the same central authority that also assigns IP addresses. The autonomous system number makes it possible for automated routing algorithms to distinguish autonomous systems.

B

BCM. BroadCast Manager, an IBM extension to LAN Emulation designed to limit the effects of broadcast frames.

backbone. (1) In a local area network multiple-bridge ring configuration, a high-speed link to which the rings are connected by means of bridges or routers. A backbone may be configured as a bus or as a ring. (2) In a wide area network, a high-speed link to which nodes or data switching exchanges (DSEs) are connected.

backbone network. A central network to which smaller networks, normally of lower speed, connect. The backbone network usually has a much higher capacity than the networks it helps interconnect or is a wide-area network (WAN) such as a public packet-switched datagram network.

backbone router. (1) A router used to transmit data between areas. (2) One in a series of routers that is used to interconnect networks into a larger internet.

Bandwidth. The bandwidth of an optical link designates the information-carrying capacity of the link and is related to the maximum bit rate that a fiber link can support.

basic transmission unit (BTU). In SNA, the unit of data and control information passed between path control components. A BTU can consist of one or more path information units (PIUs).

bootstrap. (1) A sequence of instructions whose execution causes additional instructions to be loaded and executed until the complete computer program is in storage. (T) (2) A technique or device designed to bring itself into a desired state by means of its own action, for example, a machine routine whose first few instructions are sufficient to bring the rest of itself into the computer from an input device. (A)

baud. In asynchronous transmission, the unit of modulation rate corresponding to one unit interval per second; that is, if the duration of the unit interval is 20 milliseconds, the modulation rate is 50 baud. (A)

Border Gateway Protocol (BGP). An Internet Protocol (IP) routing protocol used between domains and autonomous systems. Contrast with *Exterior Gateway Protocol (EGP)*.

border router. In Internet communications, a router, positioned at the edge of an autonomous system, that communicates with a router that is positioned at the edge of a different autonomous system.

bridge. A functional unit that interconnects multiple LANs (locally or remotely) that use the same logical link control protocol but that can use different medium access control protocols. A bridge forwards a frame to another bridge based on the medium access control (MAC) address.

bridge identifier. An 8-byte field, used in a spanning tree protocol, composed of the MAC address of the port with the lowest port identifier and a user-defined value.

bridging. In LANs, the forwarding of a frame from one LAN segment to another. The destination is specified by the medium access control (MAC) sublayer address encoded in the destination address field of the frame header.

broadcast. (1) Transmission of the same data to all destinations. (T) (2) Simultaneous transmission of data to more than one destination. (3) Contrast with *multicast*.

broadcast address. In communications, a station address (eight 1's) reserved as an address common to all stations on a link. Synonymous with *all-stations address*.

BUS. Broadcast and Unknown Server, a LAN Emulation Service component responsible for the delivery of multicast and unknown unicast frames.

C

cache. (1) A special-purpose buffer storage, smaller and faster than main storage, used to hold a copy of instructions and data obtained from main storage and likely to be needed next by the processor. (T) (2) A buffer storage that contains frequently accessed instructions and data; it is used to reduce access time. (3) An optional part of the directory database in network nodes where frequently used directory information may be stored to speed directory searches. (4) To place, hide, or store in a cache.

call request packet. (1) A call supervision packet that a data terminal equipment (DTE) transmits to ask that a connection for a call be established throughout the network. (2) In X.25 communications, a call supervision packet transmitted by a DTE to ask for a call establishment through the network.

canonical address. In LANs, the IEEE 802.1 format for the transmission of medium access control (MAC) addresses for token-ring and Ethernet adapters. In canonical format, the least significant (rightmost) bit of each address byte is transmitted first. Contrast with *noncanonical address*.

carrier. An electric or electromagnetic wave or pulse train that may be varied by a signal bearing information to be transmitted over a communication system. (T)

carrier detect. Synonym for *received line signal detector (RLSD)*.

carrier sense. In a local area network, an ongoing activity of a data station to detect whether another station is transmitting. (T)

carrier sense multiple access with collision detection (CSMA/CD). A protocol that requires carrier sense and in which a transmitting data station that detects another signal while transmitting, stops sending,

sends a jam signal, and then waits for a variable time before trying again. (T) (A)

channel. (1) A path along which signals can be sent, for example, data channel, output channel. (A) (2) A functional unit, controlled by the processor, that handles the transfer of data between processor storage and local peripheral equipment.

channel service unit (CSU). A unit that provides the interface to a digital network. The CSU provides line conditioning (or equalization) functions, which keep the signal's performance consistent across the channel bandwidth; signal reshaping, which constitutes the binary pulse stream; and loopback testing, which includes the transmission of test signals between the CSU and the network carrier's office channel unit. See also *data service unit (DSU)*.

checksum. (1) The sum of a group of data associated with the group and used for checking purposes. (T) (2) In error detection, a function of all bits in a block. If the written and calculated sums do not agree, an error is indicated. (3) On a diskette, data written in a sector for error detection purposes; a calculated checksum that does not match the checksum of data written in the sector indicates a bad sector. The data are either numeric or other character strings regarded as numeric for the purpose of calculating the checksum.

CIP. Classical IP.

CIPC. Classical IP Client.

Classical IP. An IETF standard for ATM-attached hosts to communicate using IP over ATM.

Classical IP Client. A Classical IP component that represents users of the Logical IP Subnet.

circuit switching. (1) A process that, on demand, connects two or more data terminal equipment (DTEs) and permits the exclusive use of a data circuit between them until the connection is released. (I) (A) (2) Synonymous with *line switching*.

class A network. In Internet communications, a network in which the high-order (most significant) bit of the IP address is set to 0 and the host ID occupies the three low-order octets.

class B network. In Internet communications, a network in which the two high-order (most significant and next-to-most significant) bits of the IP address are set to 1 and 0, respectively, and the host ID occupies the two low-order octets.

class of service (COS). A set of characteristics (such as route security, transmission priority, and bandwidth) used to construct a route between session partners. The class of service is derived from a mode name specified by the initiator of a session.

client. (1) A functional unit that receives shared services from a server. (T) (2) A user.

client/server. In communications, the model of interaction in distributed data processing in which a program at one site sends a request to a program at another site and awaits a response. The requesting program is called a client; the answering program is called a server.

clocking. (1) In binary synchronous communication, the use of clock pulses to control synchronization of data and control characters. (2) A method of controlling the number of data bits sent on a telecommunication line in a given time.

collision. An unwanted condition that results from concurrent transmissions on a channel. (T)

collision detection. In carrier sense multiple access with collision detection (CSMA/CD), a signal indicating that two or more stations are transmitting simultaneously.

Committed information rate. The maximum amount of data in bits that the network agrees to deliver.

community. In the Simple Network Management Protocol (SNMP), an administrative relationship between entities.

community name. In the Simple Network Management Protocol (SNMP), a string of octets identifying a community.

compression. (1) The process of eliminating gaps, empty fields, redundancies, and unnecessary data to shorten the length of records or blocks. (2) Any encoding to reduce the number of bits used to represent a given message or record.

configuration. (1) The manner in which the hardware and software of an information processing system are organized and interconnected. (T) (2) The devices and programs that make up a system, subsystem, or network.

configuration file. A file that specifies the characteristics of a system device or network.

configuration parameter. A variable in a configuration definition, the values of which can characterize the relationship of a product to other products in the same network or can define characteristics of the product itself.

configuration report server (CRS). In the IBM Token-Ring Network Bridge Program, the server that accepts commands from the LAN Network Manager (LNM) to get station information, set station parameters, and remove stations on its ring. This server also collects and forwards configuration reports generated by stations

on its ring. The configuration reports include the new active monitor reports and the nearest active upstream neighbor (NAUN) reports.

congestion. See *network congestion*.

control point (CP). (1) A component of an APPN or LEN node that manages the resources of that node. In an APPN node, the CP is capable of engaging in CP-CP sessions with other APPN nodes. In an APPN network node, the CP also provides services to adjacent end nodes in the APPN network. (2) A component of a node that manages resources of that node and optionally provides services to other nodes in the network. Examples are a system services control point (SSCP) in a type 5 subarea node, a network node control point (NNCP) in an APPN network node, and an end node control point (ENCP) in an APPN or LEN end node. An SSCP and an NNCP can provide services to other nodes.

control point management services (CPMS). A component of a control point, consisting of management services function sets, that provides facilities to assist in performing problem management, performance and accounting management, change management, and configuration management. Capabilities provided by the CPMS include sending requests to physical unit management services (PUMS) to test system resources, collecting statistical information (for example, error and performance data) from PUMS about the system resources, and analyzing and presenting test results and statistical information collected about the system resources. Analysis and presentation responsibilities for problem determination and performance monitoring can be distributed among multiple CPMSs.

control point management services unit (CP-MSU). The message unit that contains management services data and flows between management services function sets. This message unit is in general data stream (GDS) format. See also *management services unit (MSU)* and *network management vector transport (NMVT)*.

D

D-bit. Delivery-confirmation bit. In X.25 communications, the bit in a data packet or call-request packet that is set to 1 if end-to-end acknowledgment (delivery confirmation) is required from the recipient.

daemon. A program that runs unattended to perform a standard service. Some daemons are triggered automatically to perform their task; others operate periodically.

data carrier detect (DCD). Synonym for *received line signal detector (RLSD)*.

data circuit. (1) A pair of associated transmit and receive channels that provide a means of two-way data communication. (I) (2) In SNA, synonym for *link connection*. (3) See also *physical circuit* and *virtual circuit*.

Notes:

1. Between data switching exchanges, the data circuit may include data circuit-terminating equipment (DCE), depending on the type of interface used at the data switching exchange.
2. Between a data station and a data switching exchange or data concentrator, the data circuit includes the data circuit-terminating equipment at the data station end, and may include equipment similar to a DCE at the data switching exchange or data concentrator location.

data circuit-terminating equipment (DCE). In a data station, the equipment that provides the signal conversion and coding between the data terminal equipment (DTE) and the line. (I)

Notes:

1. The DCE may be separate equipment or an integral part of the DTE or of the intermediate equipment.
2. A DCE may perform other functions that are usually performed at the network end of the line.

data link connection identifier (DLCI). The numeric identifier of a frame-relay subport or PVC segment in a frame-relay network. Each subport in a single frame-relay port has a unique DLCI. The following table, excerpted from the American National Standards Institute (ANSI) Standard T1.618 and the International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) Standard Q.922, indicates the functions associated with certain DLCI values:

DLCI Values	Function
0	in-channel signaling
1–15	reserved
16–991	assigned using frame-relay connection procedures
992–1007	layer 2 management of frame-relay bearer service
1008–1022	reserved
1023	in-channel layer management

data link control (DLC). A set of rules used by nodes on a data link (such as an SDLC link or a token ring) to accomplish an orderly exchange of information.

data link control (DLC) layer. In SNA, the layer that consists of the link stations that schedule data transfer over a link between two nodes and perform error control for the link. Examples of data link control are SDLC for serial-by-bit link connection and data link control for the System/370 channel.

Note: The DLC layer is usually independent of the physical transport mechanism and ensures the integrity of data that reaches the higher layers.

data link layer. In the Open Systems Interconnection reference model, the layer that provides services to transfer data between entities in the network layer over a communication link. The data link layer detects and possibly corrects errors that may occur in the physical layer. (T)

data link level. (1) In the hierarchical structure of a data station, the conceptual level of control or processing logic between high level logic and the data link that maintains control of the data link. The data link level performs such functions as inserting transmit bits and deleting receive bits; interpreting address and control fields; generating, transmitting, and interpreting commands and responses; and computing and interpreting frame check sequences. See also *packet level* and *physical level*. (2) In X.25 communications, synonym for *frame level*.

data link switching (DLSw). A method of transporting network protocols that use IEEE 802.2 logical link control (LLC) type 2. SNA and NetBIOS are examples of protocols that use LLC type 2. See also *encapsulation* and *spoofing*.

data packet. In X.25 communications, a packet used for the transmission of user data on a virtual circuit at the DTE/DCE interface.

data service unit (DSU). A device that provides a digital data service interface directly to the data terminal equipment. The DSU provides loop equalization, remote and local testing capabilities, and a standard EIA/CCITT interface.

data set ready (DSR). Synonym for *DCE ready*.

data switching exchange (DSE). The equipment installed at a single location to provide switching functions, such as circuit switching, message switching, and packet switching. (I)

data terminal equipment (DTE). That part of a data station that serves as a data source, data sink, or both. (I) (A)

data terminal ready (DTR). A signal to the modem used with the EIA 232 protocol.

data transfer rate. The average number of bits, characters, or blocks per unit time passing between corresponding equipment in a data transmission system. (I)

Notes:

1. The rate is expressed in bits, characters, or blocks per second, minute, or hour.
2. Corresponding equipment should be indicated; for example, modems, intermediate equipment, or source and sink.

datagram. (1) In packet switching, a self-contained packet, independent of other packets, that carries information sufficient for routing from the originating data terminal equipment (DTE) to the destination DTE without relying on earlier exchanges between the DTEs and the network. (I) (2) In TCP/IP, the basic unit of information passed across the Internet environment. A datagram contains a source and destination address along with the data. An Internet Protocol (IP) datagram consists of an IP header followed by the transport layer data. (3) See also *packet* and *segment*.

Datagram Delivery Protocol (DDP). In AppleTalk networks, a protocol that provides network connectivity by means of connectionless socket-to-socket delivery service on the internet layer.

DCE ready. In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that the local data circuit-terminating equipment (DCE) is connected to the communication channel and is ready to send data. Synonymous with *data set ready (DSR)*.

DECnet. A network architecture that defines the operation of a family of software modules, databases, and hardware components typically used to tie Digital Equipment Corporation systems together for resource sharing, distributed computation, or remote system configuration. DECnet network implementations follow the Digital Network Architecture (DNA) model.

default. Pertaining to an attribute, condition, value, or option that is assumed when none is explicitly specified. (I)

designated router. A router that informs end nodes of the existence and identity of other routers. The selection of the designated router is based upon the router with the highest priority. When several routers share the highest priority, the router with the highest station address is selected.

destination node. The node to which a request or data is sent.

destination port. The 8-port asynchronous adapter that serves as a connection point with a serial service.

destination service access point (DSAP). In SNA and TCP/IP, a logical address that allows a system to route data from a remote device to the appropriate communications support. Contrast with *source service access point (SSAP)*.

device. A mechanical, electrical, or electronic contrivance with a specific purpose.

digital. (1) Pertaining to data that consist of digits. (T) (2) Pertaining to data in the form of digits. (A) (3) Contrast with *analog*.

Digital Network Architecture (DNA). The model for all DECnet hardware and software implementations.

direct memory access (DMA). The system facility that allows a device on the Micro Channel bus to get direct access to the system or bus memory without the intervention of the system processor.

directory. A table of identifiers and references to the corresponding items of data. (I) (A)

directory service (DS). An application service element that translates the symbolic names used by application processes into the complete network addresses used in an OSI environment. (T)

directory services (DS). A control point component of an APPN node that maintains knowledge of the location of network resources.

disable. To make nonfunctional.

disabled. (1) Pertaining to a state of a processing unit that prevents the occurrence of certain types of interruptions. (2) Pertaining to the state in which a transmission control unit or audio response unit cannot accept incoming calls on a line.

domain. (1) That part of a computer network in which the data processing resources are under common control. (T) (2) In Open Systems Interconnection (OSI), a part of a distributed system or a set of managed objects to which a common policy applies. (3) See *Administrative Domain* and *domain name*.

domain name. In the Internet suite of protocols, a name of a host system. A domain name consists of a sequence of subnames separated by a delimiter character. For example, if the fully qualified domain name (FQDN) of a host system is `ralvm7.vnet.ibm.com`, each of the following is a domain name:

- `ralvm7.vnet.ibm.com`
- `vnet.ibm.com`
- `ibm.com`

domain name server. In the Internet suite of protocols, a server program that supplies name-to-address translation by mapping domain names to IP addresses. Synonymous with *name server*.

Domain Name System (DNS). In the Internet suite of protocols, the distributed database system used to map domain names to IP addresses.

dotted decimal notation. The syntactical representation for a 32-bit integer that consists of four 8-bit numbers written in base 10 with periods (dots) separating them. It is used to represent IP addresses.

dump. (1) Data that has been dumped. (T) (2) To copy the contents of all or part of virtual storage for the purpose of collecting error information.

dynamic reconfiguration (DR). The process of changing the network configuration (peripheral PUs and LUs) without regenerating complete configuration tables or deactivating the affected major node.

Dynamic Routing. Routing using learned routes rather than routes statically configured at initialization.

E

echo. In data communication, a reflected signal on a communications channel. For example, on a communications terminal, each signal is displayed twice, once when entered at the local terminal and again when returned over the communications link. This allows the signals to be checked for accuracy.

EIA 232. In data communication, a specification of the Electronic Industries Association (EIA) that defines the interface between data terminal equipment (DTE) and data circuit-terminating equipment (DCE), using serial binary data interchange.

ELAN. Emulated Local Area Network, a LAN segment implemented with ATM technology.

Electronic Industries Association (EIA). An organization of electronics manufacturers that advances the technological growth of the industry, represents the views of its members, and develops industry standards.

encapsulation. (1) In communications, a technique used by layered protocols by which a layer adds control information to the protocol data unit (PDU) from the layer it supports. In this respect, the layer encapsulates the data from the supported layer. In the Internet suite of protocols, for example, a packet would contain control information from the physical layer, followed by control information from the network layer, followed by the application protocol data. (2) See also *data link switching*.

encode. To convert data by the use of a code in such a manner that reconversion to the original form is possible. (T)

end node (EN). (1) See *Advanced Peer-to-Peer Networking (APPN) end node* and *low-entry networking (LEN) end node*. (2) In communications, a node that is frequently attached to a single data link and cannot perform intermediate routing functions.

entry point (EP). In SNA, a type 2.0, type 2.1, type 4, or type 5 node that provides distributed network management support. It sends network management data about itself and the resources it controls to a focal point for centralized processing, and it receives and executes focal-point initiated commands to manage and control its resources.

ESI. End System Identifier, a 6-byte component of an ATM address.

Ethernet. A 10-Mbps baseband local area network that allows multiple stations to access the transmission medium at will without prior coordination, avoids contention by using carrier sense and deference, and resolves contention by using collision detection and delayed retransmission. Ethernet uses carrier sense multiple access with collision detection (CSMA/CD).

exception. An abnormal condition such as an I/O error encountered in processing a data set or a file.

exception response (ER). In SNA, a protocol requested in the form-of-response-requested field of a request header that directs the receiver to return a response only if the request is unacceptable as received or cannot be processed; that is, a negative response, but not a positive response, can be returned. Contrast with *definite response* and *no response*.

exchange identification (XID). A specific type of basic link unit that is used to convey node and link characteristics between adjacent nodes. XIDs are exchanged between link stations before and during link activation to establish and negotiate link and node characteristics, and after link activation to communicate changes in these characteristics.

explicit route (ER). In SNA, a series of one or more transmission groups that connect two subarea nodes. An explicit route is identified by an origin subarea address, a destination subarea address, an explicit route number, and a reverse explicit route number. Contrast with *virtual route (VR)*.

explorer frame. See *explorer packet*.

explorer packet. In LANs, a packet that is generated by the source host and that traverses the entire source routing part of a LAN, gathering information on the possible paths available to the host.

exterior gateway. In Internet communications, a gateway on one autonomous system that communicates with another autonomous system. Contrast with *interior gateway*.

Exterior Gateway Protocol (EGP). In the Internet suite of protocols, a protocol, used between domains and autonomous systems, that enables network reachability information to be advertised and exchanged. IP network addresses in one autonomous system are advertised to another autonomous system by means of EGP-participating routers. Contrast with *Border Gateway Protocol (BGP)*.

F

File Transfer Protocol (FTP). In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

flow control. (1) In SNA, the process of managing the rate at which data traffic passes between components of the network. The purpose of flow control is to optimize the rate of flow of message units with minimum congestion in the network; that is, to neither overflow the buffers at the receiver or at intermediate routing nodes, nor leave the receiver waiting for more message units. (2) See also *pacing*.

fragment. See *fragmentation*.

fragmentation. (1) The process of dividing a datagram into smaller parts, or fragments, to match the capabilities of the physical medium over which it is to be transmitted. (2) See also *segmenting*.

frame. (1) In Open Systems Interconnection architecture, a data structure pertaining to a particular area of knowledge and consisting of slots that can accept the values of specific attributes and from which inferences can be drawn by appropriate procedural attachments. (T) (2) The unit of transmission in some local area networks, including the IBM Token-Ring Network. It includes delimiters, control characters, information, and checking characters. (3) In SDLC, the vehicle for every command, every response, and all information that is transmitted using SDLC procedures.

frame level. Synonymous with *data link level*. See *link level*.

Frame Relay. (1) An interface standard describing the boundary between a user's equipment and a fast-packet network. In frame-relay systems, flawed frames are discarded; recovery comes end-to-end rather than hop-by-hop. (2) A technique derived from the integrated services digital network (ISDN) D channel standard. It assumes that connections are reliable and dispenses with the overhead of error detection and control within the network.

G

gateway. (1) A functional unit that interconnects two computer networks with different network architectures. A gateway connects networks or systems of different architectures. A bridge interconnects networks or systems with the same or similar architectures. (T) (2) In the IBM Token-Ring Network, a device and its associated software that connect a local area network to another local area network or a host that uses different logical link protocols. (3) In TCP/IP, synonym for *router*.

general data stream (GDS). The data stream used for conversations in LU 6.2 sessions.

general data stream (GDS) variable. A type of RU substructure that is preceded by an identifier and a length field and includes either application data, user control data, or SNA-defined control data.

H

header. (1) System-defined control information that precedes user data. (2) The portion of a message that contains control information for the message such as one or more destination fields, name of the originating station, input sequence number, character string indicating the type of message, and priority level for the message.

heap memory. The amount of RAM used to dynamically allocate data structures.

Hello. A protocol used by a group of cooperating, trusting routers to allow them to discover minimal delay routes.

hello message. (1) A message sent periodically to establish and test reachability between routers or between routers and hosts. (2) In the Internet suite of protocols, a message defined by the Hello protocol as an Interior Gateway Protocol (IGP).

heuristic. Pertaining to exploratory methods of problem solving in which solutions are discovered by evaluation of the progress made toward the final result.

high-level data link control (HDLC). In data communication, the use of a specified series of bits to control data links in accordance with the International Standards for HDLC: ISO 3309 Frame Structure and ISO 4335 Elements of Procedures.

hop. (1) In APPN, a portion of a route that has no intermediate nodes. It consists of only a single transmission group connecting adjacent nodes. (2) To the routing layer, the logical distance between two nodes in a network.

hop count. (1) A metric or measure of distance between two points. (2) In Internet communications, the number of routers that a datagram passes through on its way to its destination. (3) In SNA, a measure of the number of links to be traversed in a path to a destination.

host. In the Internet suite of protocols, an end system. The end system can be any workstation; it does not have to be a mainframe.

hysteresis. The amount the temperature must change past the set alert threshold before the alert condition is cleared.

I

I frame. Information frame.

IETF. Internet Engineering Task Force, an organization that produces Internet specifications.

ILMI. Interim Local Management Interface, SNMP-based procedures for managing the User-Network Interface (UNI).

information (I) frame. A frame in I format used for numbered information transfer.

input/output channel. In a data processing system, a functional unit that handles transfer of data between internal and peripheral equipment. (I) (A)

integrated services digital network (ISDN). A digital end-to-end telecommunication network that supports multiple services including, but not limited to, voice and data.

Note: ISDNs are used in public and private network architectures.

interface. (1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics, as appropriate. The concept includes the specification of the connection of two devices having different functions. (T) (2) Hardware, software, or both, that links systems, programs, or devices.

interior gateway. In Internet communications, a gateway that communicates only with its own autonomous system. Contrast with *exterior gateway*.

Interior Gateway Protocol (IGP). In the Internet suite of protocols, a protocol used to propagate network reachability and routing information within an autonomous system. Examples of IGPs are Routing Information Protocol (RIP) and Open Shortest Path First (OSPF).

intermediate node. A node that is at the end of more than one branch. (T)

intermediate session routing (ISR). A type of routing function within an APPN network node that provides session-level flow control and outage reporting for all sessions that pass through the node but whose end points are elsewhere.

International Organization for Standardization (ISO). An organization of national standards bodies from various countries established to promote development of standards to facilitate international exchange of goods and services, and develop cooperation in intellectual, scientific, technological, and economic activity.

International Telecommunication Union (ITU). The specialized telecommunication agency of the United Nations, established to provide standardized communication procedures and practices, including frequency allocation and radio regulations worldwide.

internet. A collection of networks interconnected by a set of routers that allow them to function as a single, large network. See also *Internet*.

Internet. The internet administered by the Internet Architecture Board (IAB), consisting of large national backbone networks and many regional and campus networks all over the world. The Internet uses the Internet suite of protocols.

Internet address. See *IP address*.

Internet Architecture Board (IAB). The technical body that oversees the development of the Internet suite of protocols that are known as TCP/IP.

Internet Control Message Protocol (ICMP). The protocol used to handle errors and control messages in the Internet Protocol (IP) layer. Reports of problems and incorrect datagram destinations are returned to the original datagram source. ICMP is part of the Internet Protocol.

Internet Control Protocol (ICP). The VIrtual NEtworking System (VINES) protocol that provides exception notifications, metric notifications, and PING support. See also *RouTing update Protocol (RTP)*.

Internet Engineering Task Force (IETF). The task force of the Internet Architecture Board (IAB) that is responsible for solving the short-term engineering needs of the Internet.

Internet Protocol (IP). A connectionless protocol that routes data through a network or interconnected networks. IP acts as an intermediary between the higher protocol layers and the physical network. However, this protocol does not provide error recovery and flow control and does not guarantee the reliability of the physical network.

Internetwork Packet Exchange (IPX). (1) The network protocol used to connect Novell's servers, or any workstation or router that implements IPX, with other workstations. Although similar to the Internet Protocol (IP), IPX uses different packet formats and terminology. (2) See also *Xerox Network Systems (XNS)*.

interoperability. The capability to communicate, execute programs, or transfer data among various functional units in a way that requires the user to have little or no knowledge of the unique characteristics of those units. (T)

intra-area routing. In Internet communications, the routing of data within an area.

Inverse Address Resolution Protocol (InARP). In the Internet suite of protocols, the protocol used for locating a protocol address through the known hardware address. In a frame-relay context, the data link connection identifier (DLCI) is synonymous with the known hardware address.

IP address. The 32-bit address defined by the Internet Protocol, standard 5, Request for Comments (RFC) 791. It is usually represented in dotted decimal notation.

IP datagram. In the Internet suite of protocols, the fundamental unit of information transmitted through an internet. It contains source and destination addresses, user data, and control information such as the length of the datagram, the header checksum, and flags indicating whether the datagram can be or has been fragmented.

IP router. A device in an IP internet that is responsible for making decisions about the paths over which network traffic will flow. Routing protocols are used to gain information about the network and to determine the best route over which the datagram should be forwarded toward the final destination. The datagrams are routed based on IP destination addresses.

IPXWAN. A Novell protocol that is used to exchange router-to-router information before exchanging standard Internetwork Packet Exchange (IPX) routing information and traffic over wide area networks (WANs).

L

LAN bridge server (LBS). In the IBM Token-Ring Network Bridge Program, the server that keeps statistical information about frames forwarded between two or more rings (through a bridge). The LBS sends these statistics to the appropriate LAN managers through the LAN reporting mechanism (LRM).

LAN Emulation (LE). An ATM Forum standard that supports legacy LAN applications over ATM networks.

LAN Emulation Client (LEC). A LAN Emulation component that represents users of the Emulated LAN.

LAN Emulation Configuration Server (LECS). A LAN Emulation Service component that centralizes and disseminates configuration data.

LAN Emulation Server (LES). A LAN Emulation Service component that resolves LAN Destinations to ATM Addresses.

LAN Network Manager (LNM). An IBM licensed program that enables a user to manage and monitor LAN resources from a central workstation.

LAN segment. (1) Any portion of a LAN (for example, a bus or ring) that can operate independently, but that is connected to other parts of the network by means of bridges. (2) A ring or bus network without bridges.

layer. (1) In network architecture, a group of services that is complete from a conceptual point of view, that is

one out of a set of hierarchically arranged groups, and that extends across all systems that conform to the network architecture. (T) (2) In the Open Systems Interconnection reference model, one of seven conceptually complete, hierarchically arranged groups of services, functions, and protocols, that extend across all open systems. (T) (3) In SNA, a grouping of related functions that are logically separate from the functions in other groups. Implementation of the functions in one layer can be changed without affecting functions in other layers.

LE. LAN Emulation.

LEC. LAN Emulation Client.

LECS. LAN Emulation Configuration Server.

LES. LAN Emulation Server.

line switching. Synonym for *circuit switching*.

link. The combination of the link connection (the transmission medium) and two link stations, one at each end of the link connection. A link connection can be shared among multiple links in a multipoint or token-ring configuration.

link access protocol balanced (LAPB). A protocol used for accessing an X.25 network at the link level. LAPB is a duplex, asynchronous, symmetric protocol, used in point-to-point communication.

link-attached. (1) Pertaining to devices that are connected to a controlling unit by a data link. (2) Contrast with *channel-attached*. (3) Synonymous with *remote*.

link connection. (1) The physical equipment providing two-way communication between one link station and one or more other link stations; for example, a telecommunication line and data circuit-terminating equipment (DCE). (2) In SNA, synonymous with *data circuit*.

link level. (1) A part of Recommendation X.25 that defines the link protocol used to get data into and out of the network across the full-duplex link connecting the subscriber's machine to the network node. LAP and LAPB are the link access protocols recommended by the CCITT. (2) See *data link level*.

link-state. In routing protocols, the advertised information about the usable interfaces and reachable neighbors of a router or network. The protocol's topological database is formed from the collected link-state advertisements.

link station. (1) The hardware and software components within a node representing a connection to an adjacent node over a specific link. For example, if node A is the primary end of a multipoint line that connects to three adjacent nodes, node A will have three link stations representing the connections to the adjacent nodes. (2) See also *adjacent link station (ALS)*.

LIS. Logical IP Subnet, an IP subnet implemented with ATM technology Virtual Networking (SVN) framework.

local. (1) Pertaining to a device accessed directly without use of a telecommunication line. (2) Contrast with *remote*. (3) Synonym for *channel-attached*.

local area network (LAN). (1) A computer network located on a user's premises within a limited geographical area. Communication within a local area network is not subject to external regulations; however, communication across the LAN boundary may be subject to some form of regulation. (T) (2) A network in which a set of devices are connected to one another for communication and that can be connected to a larger network. (3) See also *Ethernet* and *token ring*. (4) Contrast with *metropolitan area network (MAN)* and *wide area network (WAN)*.

local bridging. A function of a bridge program that allows a single bridge to connect multiple LAN segments without using a telecommunication link. Contrast with *remote bridging*.

local management interface (LMI). See *local management interface (LMI) protocol*.

local management interface (LMI) protocol. In NCP, a set of frame-relay network management procedures and messages used by adjacent frame-relay nodes to exchange line status information over DLCI X'00'. NCP supports both the American National Standards Institute (ANSI) and International Telegraph and Telephone Consultative Committee (ITU-T/CCITT) versions of LMI protocol. These standards refer to LMI protocol as *link integrity verification tests (LIVT)*.

locally administered address. In a local area network, an adapter address that the user can assign to override the universally administered address. Contrast with *universally administered address*.

logical channel. In packet mode operation, a sending channel and a receiving channel that together are used to send and receive data over a data link at the same time. Several logical channels can be established on the same data link by interleaving the transmission of packets.

logical link. A pair of link stations, one in each of two adjacent nodes, and their underlying link connection, providing a single link-layer connection between the two nodes. Multiple logical links can be distinguished while they share the use of the same physical media connecting two nodes. Examples are 802.2 logical links used on local area network (LAN) facilities and LAP E logical links on the same point-to-point physical link between two nodes. The term logical link also includes the multiple X.25 logical channels that share the use of the access link from a DTE to an X.25 network.

logical link control (LLC). The data link control (DLC) LAN sublayer that provides two types of DLC operation for the orderly exchange of information. The first type is connectionless service, which allows information to be sent and received without establishing a link. The LLC sublayer does not perform error recovery or flow control for connectionless service. The second type is connection-oriented service, which requires establishing a link prior to the exchange of information. Connection-oriented service provides sequenced information transfer, flow control, and error recovery.

logical link control (LLC) protocol. In a local area network, the protocol that governs the exchange of transmission frames between data stations independently of how the transmission medium is shared. (T) The LLC protocol was developed by the IEEE 802 committee and is common to all LAN standards.

logical link control (LLC) protocol data unit. A unit of information exchanged between link stations in different nodes. The LLC protocol data unit contains a destination service access point (DSAP), a source service access point (SSAP), a control field, and user data.

logical unit (LU). A type of network accessible unit that enables users to gain access to network resources and communicate with each other.

loopback test. A test in which signals from a tester are looped at a modem or other network element back to the tester for measurements that determine or verify the quality of the communications path.

low-entry networking (LEN). A capability of nodes to attach directly to one another using basic peer-to-peer protocols to support multiple and parallel sessions between logical units.

low-entry networking (LEN) end node. A LEN node receiving network services from an adjacent APPN network node.

low-entry networking (LEN) node. A node that provides a range of end-user services, attaches directly to other nodes using peer protocols, and derives network services implicitly from an adjacent APPN network node, that is, without the direct use of CP-CP sessions.

M

Management Information Base (MIB). (1) A collection of objects that can be accessed by means of a network management protocol. (2) A definition for management information that specifies the information available from a host or gateway and the operations allowed. (3) In OSI, the conceptual repository of management information within an open system.

management station. In Internet communications, the system responsible for managing all, or a portion of, a network. The management station communicates with network management agents that reside in the managed node by means of a network management protocol, such as the Simple Network Management Protocol (SNMP).

mapping. The process of converting data that is transmitted in one format by the sender into the data format that can be accepted by the receiver.

mask. (1) A pattern of characters used to control retention or elimination of portions of another pattern of characters. (I) (A) (2) To use a pattern of characters to control retention or elimination of portions of another pattern of characters. (I) (A)

maximum transmission unit (MTU). In LANs, the largest possible unit of data that can be sent on a given physical medium in a single frame. For example, the MTU for Ethernet is 1500 bytes.

medium access control (MAC). In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determining when a device has access to the transmission medium.

medium access control (MAC) protocol. In a local area network, the protocol that governs access to the transmission medium, taking into account the topological aspects of the network, in order to enable the exchange of data between data stations. (T)

medium access control (MAC) sublayer. In a local area network, the part of the data link layer that applies a medium access method. The MAC sublayer supports topology-dependent functions and uses the services of the physical layer to provide services to the logical link control sublayer. (T)

metric. In Internet communications, a value, associated with a route, which is used to discriminate between multiple exit or entry points to the same autonomous system. The route with the lowest metric is preferred.

metropolitan area network (MAN). A network formed by the interconnection of two or more networks which may operate at higher speed than those networks, may cross administrative boundaries, and may use multiple access methods. (T) Contrast with *local area network (LAN)* and *wide area network (WAN).*

MIB object. Synonym for *MIB variable*.

MIB variable. In the Simple Network Management Protocol (SNMP), a specific instance of data defined in a MIB module. Synonymous with *MIB object*.

MIB view. In the Simple Network Management Protocol (SNMP), the collection of managed objects, known to the agent, that is visible to a particular community.

MILNET. The military network that was originally part of ARPANET. It was partitioned from ARPANET in 1984. MILNET provides a reliable network service for military installations.

modem (modulator/demodulator). (1) A functional unit that modulates and demodulates signals. One of the functions of a modem is to enable digital data to be transmitted over analog transmission facilities. (T) (A) (2) A device that converts digital data from a computer to an analog signal that can be transmitted on a telecommunication line, and converts the analog signal received to data for the computer.

modulo. (1) Pertaining to a modulus; for example, 9 is equivalent to 4 modulo 5. (2) See also *modulus*.

modulus. A number, such as a positive integer, in a relationship that divides the difference between two related numbers without leaving a remainder; for example, 9 and 4 have a modulus of 5 (9 - 4 = 5; 4 - 9 = -5; and 5 divides both 5 and -5 without leaving a remainder).

monitor. (1) A device that observes and records selected activities within a data processing system for analysis. Possible uses are to indicate significant departure from the norm, or to determine levels of utilization of particular functional units. (T) (2) Software or hardware that observes, supervises, controls, or verifies operations of a system. (A) (3) The function required to initiate the transmission of a token on the ring and to provide soft-error recovery in case of lost tokens, circulating frames, or other difficulties. The capability is present in all ring stations.

MSS. Multiprotocol Switched Services, a component of IBM's Switched Virtual Networking (SVN) framework.

multicast. (1) Transmission of the same data to a selected group of destinations. (T) (2) A special form of broadcast in which copies of a packet are delivered to only a subset of all possible destinations.

multiple-domain support (MDS). A technique for transporting management services data between management services function sets over LU-LU and CP-CP sessions. See also *multiple-domain support message unit (MDS-MU)*.

multiple-domain support message unit (MDS-MU). The message unit that contains management services data and flows between management services function sets over the LU-LU and CP-CP sessions used by multiple-domain support. This message unit, as well as the actual management services data that it contains, is in general data stream (GDS) format. See also *control point management services unit (CP-MSU)*, *management services unit (MSU)*, and *network management vector transport (NMVT)*.

N

Name Binding Protocol (NBP). In AppleTalk networks, a protocol that provides name translation function from the AppleTalk entity (resource) name (character string) into an AppleTalk IP address (16-bit number) on the transport layer.

name resolution. In Internet communications, the process of mapping a machine name to the corresponding Internet Protocol (IP) address. See also *Domain Name System (DNS)*.

name server. In the Internet suite of protocols, synonym for *domain name server*.

nearest active upstream neighbor (NAUN). In the IBM Token-Ring Network, the station sending data directly to a given station on the ring.

neighbor. A router on a common subnetwork that has been designated by a network administrator to receive routing information.

NetBIOS. Network Basic Input/Output System. A standard interface to networks, IBM personal computers (PCs), and compatible PCs, that is used on LANs to provide message, print-server, and file-server functions. Application programs that use NetBIOS do not need to handle the details of LAN data link control (DLC) protocols.

network. (1) A configuration of data processing devices and software connected for information interchange. (2) A group of nodes and the links interconnecting them.

network accessible unit (NAU). A logical unit (LU), physical unit (PU), control point (CP), or system services control point (SSCP). It is the origin or the destination of information transmitted by the path control network. Synonymous with *network addressable unit*.

network address. According to ISO 7498-3, a name, unambiguous within the OSI environment, that identifies a set of network service access points.

network addressable unit (NAU). Synonym for *network accessible unit*.

network architecture. The logical structure and operating principles of a computer network. (T)

Note: The operating principles of a network include those of services, functions, and protocols.

network congestion. An undesirable overload condition caused by traffic in excess of what a network can handle.

network identifier. (1) In TCP/IP, that part of the IP address that defines a network. The length of the network ID depends on the type of network class (A, B, or C). (2) A 1- to 8-byte customer-selected name or an 8-byte IBM-registered name that uniquely identifies a specific subnetwork.

Network Information Center (NIC). In Internet communications, local, regional, and national groups throughout the world who provide assistance, documentation, training, and other services to users.

network layer. In Open Systems Interconnection (OSI) architecture, the layer that is responsible for routing, switching, and link-layer access across the OSI environment.

network management. The process of planning, organizing, and controlling a communication-oriented data processing or information system.

network management station. In the Simple Network Management Protocol (SNMP), a station that executes management application programs that monitor and control network elements.

network management vector transport (NMVT). A management services request/response unit (RU) that flows over an active session between physical unit management services and control point management services (SSCP-PU session).

network manager. A program or group of programs that is used to monitor, manage, and diagnose the problems of a network.

network node (NN). See *Advanced Peer-to-Peer Networking (APPN) network node*.

Next Hop Resolution Protocol (NHRP). A routing protocol, specified in Internet Draft Version 10 which has been submitted for RFC status. The Next Hop Resolution Protocol defines a method for a source station to determine the Non-Broadcast Multi-Access (NBMA) address of the "NBMA next hop" towards a destination. The NBMA next hop may be the destination itself or the router in the NBMA network that is "nearest" to the destination. The source station can then establish an NBMA virtual circuit directly with the destination or the router and reduce the number of routing hops through the NBMA network.

network user address (NUA). In X.25 communications, the X.121 address containing up to 15 binary code digits.

NHRP. Next Hop Resolution Protocol

node. (1) In a network, a point at which one or more functional units connect channels or data circuits. (I) (2) Any device, attached to a network, that transmits and receives data.

noncanonical address. In LANs, a format for the transmission of medium access control (MAC) addresses for token-ring adapters. In noncanonical format, the most significant (leftmost) bit of each address byte is transmitted first. Contrast with *canonical address*.

nonseed router. In AppleTalk networks, a router that acquires network number range and zone list information from a seed router attached to the same network.

O

Open Shortest Path First (OSPF). In the Internet suite of protocols, a function that provides intradomain information transfer. An alternative to the Routing Information Protocol (RIP), OSPF allows the lowest-cost routing and handles routing in large regional or corporate networks.

Open Systems Interconnection (OSI). (1) The interconnection of open systems in accordance with standards of the International Organization for Standardization (ISO) for the exchange of information. (T) (A) (2) The use of standardized procedures to enable the interconnection of data processing systems.

Note: OSI architecture establishes a framework for coordinating the development of current and future standards for the interconnection of computer systems. Network functions are divided into seven layers. Each layer represents a group of related data processing and communication functions that can be carried out in a standard way to support different applications.

Open Systems Interconnection (OSI) architecture. Network architecture that adheres to that particular set of ISO standards that relates to Open Systems Interconnection. (T)

Open Systems Interconnection (OSI) reference model. A model that describes the general principles of the Open Systems Interconnection, as well as the purpose and the hierarchical arrangement of its seven layers. (T)

origin. An external logical unit (LU) or application program from which a message or other data originates. See also *destination*.

orphan circuit. A non-configured circuit whose availability is learned dynamically.

P

pacing. (1) A technique by which a receiving component controls the rate of transmission of a sending component to prevent overrun or congestion.

(2) See also *flow control*, *receive pacing*, *send pacing*, *session-level pacing*, and *virtual route (VR) pacing*.

packet. In data communication, a sequence of binary digits, including data and control signals, that is transmitted and switched as a composite whole. The data, control signals, and, possibly, error control information are arranged in a specific format. (I)

packet internet groper (PING). (1) In Internet communications, a program used in TCP/IP networks to test the ability to reach destinations by sending the destinations an Internet Control Message Protocol (ICMP) echo request and waiting for a reply. (2) In communications, a test of reachability.

packet mode operation. Synonym for *packet switching*.

packet switching. (1) The process of routing and transferring data by means of addressed packets so that a channel is occupied only during transmission of a packet. On completion of the transmission, the channel is made available for transfer of other packets. (I) (2) Synonymous with *packet mode operation*. See also *circuit switching*.

parallel bridges. A pair of bridges connected to the same LAN segment, creating redundant paths to the segment.

parallel transmission groups. Multiple transmission groups between adjacent nodes, with each group having a distinct transmission group number.

path. (1) In a network, any route between any two nodes. A path may include more than one branch. (T) (2) The series of transport network components (path control and data link control) that are traversed by the information exchanged between two network accessible units. See also *explicit route (ER)*, *route extension*, and *virtual route (VR)*.

path control (PC). The function that routes message units between network accessible units in the network and provides the paths between them. It converts the basic information units (BIUs) from transmission control (possibly segmenting them) into path information units (PIUs) and exchanges basic transmission units containing one or more PIUs with data link control. Path control differs by node type: some nodes (APPN nodes, for example) use locally generated session identifiers for routing, and others (subarea nodes) use network addresses for routing.

path cost. In link-state routing protocols, the sum of the link costs along the path between two nodes or networks.

path information unit (PIU). A message unit consisting of a transmission header (TH) alone, or a TH followed by a basic information unit (BIU) or a BIU segment.

pattern-matching character. A special character such as an asterisk (*) or a question mark (?) that can be used to represent one or more characters. Any character or set of characters can replace a pattern-matching character. Synonymous with *global character* and *wildcard character*.

permanent virtual circuit (PVC). In X.25 and frame-relay communications, a virtual circuit that has a logical channel permanently assigned to it at each data terminal equipment (DTE). Call-establishment protocols are not required. Contrast with *switched virtual circuit (SVC)*.

physical circuit. A circuit established without multiplexing. See also *data circuit*. Contrast with *virtual circuit*.

physical layer. In the Open Systems Interconnection reference model, the layer that provides the mechanical, electrical, functional, and procedural means to establish, maintain, and release physical connections over the transmission medium. (T)

physical unit (PU). (1) The component that manages and monitors the resources (such as attached links and adjacent link stations) associated with a node, as requested by an SSCP via an SSCP-PU session. An SSCP activates a session with the physical unit in order to indirectly manage, through the PU, resources of the node such as attached links. This term applies to type 2.0, type 4, and type 5 nodes only. (2) See also *peripheral PU* and *subarea PU*.

ping command. The command that sends an Internet Control Message Protocol (ICMP) echo-request packet to a gateway, router, or host with the expectation of receiving a reply.

Point-to-Point Protocol (PPP). A protocol that provides a method for encapsulating and transmitting packets over serial point-to-point links.

polling. (1) On a multipoint connection or a point-to-point connection, the process whereby data stations are invited, one at a time, to transmit. (I) (2) Interrogation of devices for such purposes as to avoid contention, to determine operational status, or to determine readiness to send or receive data. (A)

port. (1) An access point for data entry or exit. (2) A connector on a device to which cables for other devices such as display stations and printers are attached. (3) The representation of a physical connection to the link hardware. A port is sometimes referred to as an adapter; however, there can be more than one port on an adapter. There may be one or more ports controlled by a single DLC process. (4) In the Internet suite of protocols, a 16-bit number used to communicate between TCP or the User Datagram Protocol (UDP) and a higher-level protocol or application. Some protocols, such as File Transfer Protocol (FTP) and Simple Mail Transfer Protocol (SMTP), use the same well-known

port number in all TCP/IP implementations. (5) An abstraction used by transport protocols to distinguish among multiple destinations within a host machine. (6) Synonymous with *socket*.

port number. In Internet communications, the identification of an application entity to the transport service.

problem determination. The process of determining the source of a problem; for example, a program component, machine failure, telecommunication facilities, user or contractor-installed programs or equipment, environmental failure such as a power loss, or user error.

program temporary fix (PTF). A temporary solution or bypass of a problem diagnosed by IBM in a current unaltered release of the program.

protocol. (1) A set of semantic and syntactic rules that determine the behavior of functional units in achieving communication. (I) (2) In Open Systems Interconnection architecture, a set of semantic and syntactic rules that determine the behavior of entities in the same layer in performing communication functions. (T) (3) In SNA, the meanings of, and the sequencing rules for, requests and responses used for managing the network, transferring data, and synchronizing the states of network components. Synonymous with *line control discipline* and *line discipline*. See *bracket protocol* and *link protocol*.

protocol data unit (PDU). A unit of data specified in a protocol of a given layer and consisting of protocol control information of this layer, and possibly user data of this layer. (T)

R

Rapid Transport Protocol (RTP) connection. In high-performance routing (HPR), the connection established between the endpoints of the route to transport session traffic.

reachability. The ability of a node or a resource to communicate with another node or resource.

read-only memory (ROM). Memory in which stored data cannot be modified by the user except under special conditions.

reassembly. In communications, the process of putting segmented packets back together after they have been received.

receive not ready (RNR). In communications, a data link command or response that indicates a temporary condition of being unable to accept incoming frames.

receive not ready (RNR) packet. See *RNR packet*.

received line signal detector (RLSD). In the EIA 232 standard, a signal that indicates to the data terminal equipment (DTE) that it is receiving a signal from the remote data circuit-terminating equipment (DCE). Synonymous with *carrier detect* and *data carrier detect (DCD)*.

Recognized Private Operating Agency (RPOA). Any individual, company, or corporation, other than a government department or service, that operates a telecommunication service and is subject to the obligations undertaken in the Convention of the International Telecommunication Union and in the Regulations; for example, a communication common carrier.

reduced instruction-set computer (RISC). A computer that uses a small, simplified set of frequently used instructions for rapid execution.

remote. (1) Pertaining to a system, program, or device that is accessed through a telecommunication line. (2) Synonym for *link-attached*. (3) Contrast with *local*.

remote bridging. The function of a bridge that allows two bridges to connect multiple LANs using a telecommunication link. Contrast with *local bridging*.

Remote Execution Protocol (REXEC). A protocol that allows the execution of a command or program on any host in the network. The local host receives the results of the command execution.

Request for Comments (RFC). In Internet communications, the document series that describes a part of the Internet suite of protocols and related experiments. All Internet standards are documented as RFCs.

reset. On a virtual circuit, reinitialization of data flow control. At reset, all data in transit are eliminated.

reset request packet. In X.25 communications, a packet transmitted by the data terminal equipment (DTE) to the data circuit-terminating equipment (DCE) to request that a virtual call or a permanent virtual circuit be reset. The reason for the request can also be specified in the packet.

ring. See *ring network*.

ring network. (1) A network in which every node has exactly two branches connected to it and in which there are exactly two paths between any two nodes. (T) (2) A network configuration in which devices are connected by unidirectional transmission links to form a closed path.

ring segment. A section of a ring that can be isolated (by unplugging connectors) from the rest of the ring. See *LAN segment*.

rlogin (remote login). A service, offered by Berkeley UNIX-based systems, that allows authorized users of one machine to connect to other UNIX systems across an internet and interact as if their terminals were connected directly. The rlogin software passes information about the user's environment (for example, terminal type) to the remote machine.

RNR packet. A packet used by a data terminal equipment (DTE) or by a data circuit-terminating equipment (DCE) to indicate a temporary inability to accept additional packets for a virtual call or permanent virtual circuit.

root bridge. The bridge that is the root of a spanning tree formed between other active bridges in the bridging network. The root bridge originates and transmits bridge protocol data units (BPDUs) to other active bridges to maintain the spanning tree topology. It is the bridge with the highest priority in the network.

route. (1) An ordered sequence of nodes and transmission groups (TGs) that represent a path from an origin node to a destination node traversed by the traffic exchanged between them. (2) The path that network traffic uses to get from source to destination.

route bridge. A function of an IBM bridge program that allows two bridge computers to use a telecommunication link to connect two LANs. Each bridge computer is connected directly to one of the LANs, and the telecommunication link connects the two bridge computers.

route extension (REX). In SNA, the path control network components, including a peripheral link, that make up the portion of a path between a subarea node and a network addressable unit (NAU) in an adjacent peripheral node. See also *explicit route (ER)*, *path*, and *virtual route (VR)*.

router. (1) A computer that determines the path of network traffic flow. The path selection is made from several paths based on information obtained from specific protocols, algorithms that attempt to identify the shortest or best path, and other criteria such as metrics or protocol-specific destination addresses. (2) An attaching device that connects two LAN segments, which use similar or different architectures, at the reference model network layer. (3) In OSI terminology, a function that determines a path by which an entity can be reached. (4) In TCP/IP, synonymous with *gateway*. (5) Contrast with *bridge*.

routing. (1) The assignment of the path by which a message is to reach its destination. (2) In SNA, the forwarding of a message unit along a particular path through a network, as determined by parameters carried in the message unit, such as the destination network address in a transmission header.

routing domain. In Internet communications, a group of intermediate systems that use a routing protocol so that the representation of the overall network is the same within each intermediate system. Routing domains are connected to each other by exterior links.

Routing Information Protocol (RIP). In the Internet suite of protocols, an interior gateway protocol used to exchange intradomain routing information and to determine optimum routes between internet hosts. RIP determines optimum routes on the basis of route metrics, not link transmission speed.

routing loop. A situation that occurs when routers circulate information among themselves until convergence occurs or until the networks involved are considered unreachable.

routing protocol. A technique used by a router to find other routers and to remain up to date about the best way to get to reachable networks.

routing table. A collection of routes used to direct datagram forwarding or to establish a connection. The information is passed among routers to identify network topology and destination feasibility.

Routing Table Maintenance Protocol (RTMP). In AppleTalk networks, a protocol that provides routing information generation and maintenance on the transport layer by means of the AppleTalk routing table. The AppleTalk routing table directs packet transmission through the internet from source socket to destination socket.

RouTing update Protocol (RTP). The VIrtual NEtworking System (VINES) protocol that maintains the routing database and allows the exchange of routing information between VINES nodes. See also *Internet Control Protocol (ICP)*.

rsh. A variant of the rlogin command that invokes a command interpreter on a remote UNIX machine and passes the command-line arguments to the command interpreter, skipping the login step completely.

S

SDU. Service Data Unit, data as it appears at the interface between a layer and the layer immediately above.

seed router. In AppleTalk networks, a router that maintains configuration data (network range numbers and zone lists, for example) for the network. Each network must have at least one seed router. The seed router must be initially set up using the configurator tool. Contrast with *nonseed router*.

segment. (1) A section of cable between components or devices. A segment may consist of a single patch cable, several patch cables that are connected, or a combination of building cable and patch cables that are connected. (2) In Internet communications, the unit of

transfer between TCP functions in different machines. Each segment contains control and data fields; the current byte-stream position and actual data bytes are identified along with a checksum to validate received data.

segmenting. In OSI, a function performed by a layer to map one protocol data unit (PDU) from the layer it supports into multiple PDUs.

sequence number. In communications, a number assigned to a particular frame or packet to control the transmission flow and receipt of data.

server. A functional unit that provides shared services to workstations over a network; for example, a file server, a print server, a mail server. (T)

service access point (SAP). (1) In Open Systems Interconnection (OSI) architecture, the point at which the services of a layer are provided by an entity of that layer to an entity of the next higher layer. (T) (2) A logical point made available by an adapter where information can be received and transmitted. A single service access point can have many links terminating in it.

Service Advertising Protocol (SAP). In Internetwork Packet Exchange (IPX), a protocol that provides the following:

- A mechanism that allows IPX servers on an internet to advertise their services by name and type. Servers using this protocol have their name, service type, and IP address recorded in all file servers running NetWare.
- A mechanism that allows a workstation to broadcast a query to discover the identities of all servers of all types, all servers of a specific type, or the nearest server of a specific type.
- A mechanism that allows a workstation to query any file server running NetWare to discover the names and addresses of all servers of a specific type.

session. (1) In network architecture, for the purpose of data communication between functional units, all the activities which take place during the establishment, maintenance, and release of the connection. (T) (2) A logical connection between two network accessible units (NAUs) that can be activated, tailored to provide various protocols, and deactivated, as requested. Each session is uniquely identified in a transmission header (TH) accompanying any transmissions exchanged during the session.

Simple Network Management Protocol (SNMP). In the Internet suite of protocols, a network management protocol that is used to monitor routers and attached networks. SNMP is an application layer protocol. Information on devices managed is defined and stored in the application's Management Information Base (MIB).

SLIP. Serial Line IP, an IETF standard for running IP over serial communication links.

SNA management services (SNA/MS). The services provided to assist in management of SNA networks.

SNAP. (1) SubNetwork Access Protocol. (2) SubNetwork Attachment Point.

socket. An endpoint for communication between processes or application programs.

source route bridging. In LANs, a bridging method that uses the routing information field in the IEEE 802.5 medium access control (MAC) header of a frame to determine which rings or token-ring segments the frame must transit. The routing information field is inserted into the MAC header by the source node. The information in the routing information field is derived from explorer packets generated by the source host.

source routing. In LANs, a method by which the sending station determines the route the frame will follow and includes the routing information with the frame. Bridges then read the routing information to determine whether they should forward the frame.

source service access point (SSAP). In SNA and TCP/IP, a logical address that allows a system to send data to a remote device from the appropriate communications support. Contrast with *destination service access point (DSAP)*.

spanning tree. In LAN contexts, the method by which bridges automatically develop a routing table and update that table in response to changing topology to ensure that there is only one route between any two LANs in the bridged network. This method prevents packet looping, where a packet returns in a circuitous route back to the sending router.

sphere of control (SOC). The set of control point domains served by a single management services focal point.

sphere of control (SOC) node. A node directly in the sphere of control of a focal point. A SOC node has exchanged management services capabilities with its focal point. An APPN end node can be a SOC node if it supports the function to exchange management services capabilities.

split horizon. A technique for minimizing the time to achieve network convergence. A router records the interface over which it received a particular route and does not propagate its information about the route back over the same interface.

spoofing. For data links, a technique in which a protocol initiated from an end station is acknowledged and processed by an intermediate node on behalf of the final destination. In IBM 6611 data link switching, for example, SNA frames are encapsulated into TCP/IP

packets for transport across a non-SNA wide area network, unpacked by another IBM 6611, and passed to the final destination. A benefit of spoofing is the prevention of end-to-end session timeouts.

standard MIB. In the Simple Network Management Protocol (SNMP), a MIB module that is located under the management branch of the Structure of Management Information (SMI) and that is considered a standard by the Internet Engineering Task Force (IETF).

static route. The route between hosts, networks, or both that is manually entered into a routing table.

station. An input or output point of a system that uses telecommunication facilities; for example, one or more systems, computers, terminals, devices, and associated programs at a particular location that can send or receive data over a telecommunication line.

StreetTalk. In the VIrtual NEtworking System (VINES), a unique network-wide naming and addressing system that allows users to locate and access any resource on the network without knowing the network topology. See also *Internet Control Protocol (ICP)* and *RouTing update Protocol (RTP)*.

Structure of Management Information (SMI). (1) In the Simple Network Management Protocol (SNMP), the rules used to define the objects that can be accessed by means of a network management protocol. (2) In OSI, the set of standards relating to management information. The set includes the *Management Information Model* and the *Guidelines for the Definition of Managed Objects*

subarea. A portion of the SNA network consisting of a subarea node, attached peripheral nodes, and associated resources. Within a subarea node, all network accessible units (NAUs), links, and adjacent link stations (in attached peripheral or subarea nodes) that are addressable within the subarea share a common subarea address and have distinct element addresses.

subnet. (1) In TCP/IP, a part of a network that is identified by a portion of the IP address. (2) Synonym for *subnetwork*.

subnet address. In Internet communications, an extension to the basic IP addressing scheme where a portion of the host address is interpreted as the local network address.

subnet mask. Synonym for *address mask*.

subnetwork. (1) Any group of nodes that have a set of common characteristics, such as the same network ID. (2) Synonymous with *subnet*.

Subnetwork Access Protocol (SNAP). In LANs, a 5-byte protocol discriminator that identifies the non-IEEE standard protocol family to which a packet belongs. The SNAP value is used to differentiate between protocols that use `$AA` as their service access point (SAP) value.

SubNetwork Attachment Point (SNAP). An LLC header extension that identifies the protocol type of a frame.

subnetwork mask. Synonym for *address mask*.

subsystem. A secondary or subordinate system, usually capable of operating independently of, or asynchronously with, a controlling system. (T)

SVN. Switched Virtual Networking, the name of IBM's framework for building and managing switch-based networks.

switched virtual circuit (SVC). An X.25 circuit that is dynamically established when needed. The X.25 equivalent of a switched line. Contrast with *permanent virtual circuit (PVC)*.

synchronous. (1) Pertaining to two or more processes that depend upon the occurrence of specific events such as common timing signals. (T) (2) Occurring with a regular or predictable time relationship.

Synchronous Data Link Control (SDLC). (1) A discipline conforming to subsets of the Advanced Data Communication Control Procedures (ADCCP) of the American National Standards Institute (ANSI) and High-level Data Link Control (HDLC) of the International Organization for Standardization, for managing synchronous, code-transparent, serial-by-bit information transfer over a link connection. Transmission exchanges may be duplex or half-duplex over switched or nonswitched links. The configuration of the link connection may be point-to-point, multipoint, or loop. (I) (2) Contrast with *binary synchronous communication (BSC)*.

SYNTAX. In the Simple Network Management Protocol (SNMP), a clause in the MIB module that defines the abstract data structure that corresponds to a managed object.

system configuration. A process that specifies the devices and programs that form a particular data processing system.

system services control point (SSCP). A component within a subarea network for managing the configuration, coordinating network operator and problem determination requests, and providing directory services and other session services for users of the network. Multiple SSCPs, cooperating as peers with one another, can divide the network into domains of control, with each SSCP having a hierarchical control relationship to the physical units and logical units within its own domain.

Systems Network Architecture (SNA). The description of the logical structure, formats, protocols,

and operational sequences for transmitting information units through, and controlling the configuration and operation of, networks. The layered structure of SNA allows the ultimate origins and destinations of information, that is, the users, to be independent of and unaffected by the specific SNA network services and facilities used for information exchange.

T

Telnet. In the Internet suite of protocols, a protocol that provides remote terminal connection service. It allows users of one host to log on to a remote host and interact as directly attached terminal users of that host.

threshold. (1) In IBM bridge programs, a value set for the maximum number of frames that are not forwarded across a bridge due to errors, before a "threshold exceeded" occurrence is counted and indicated to network management programs. (2) An initial value from which a counter is decremented to 0, or a value to which a counter is incremented or decremented from an initial value.

throughput class. In packet switching, the speed at which data terminal equipment (DTE) packets travel through the packet switching network.

time to live (TTL). A technique used by best-effort delivery protocols to inhibit endlessly looping packets. The packet is discarded if the TTL counter reaches 0.

timeout. (1) An event that occurs at the end of a predetermined period of time that began at the occurrence of another specified event. (I) (2) A time interval allotted for certain operations to occur; for example, response to polling or addressing before system operation is interrupted and must be restarted.

TLV. Type/Length/Value, a generalized information element in a LAN Emulation packet.

token. (1) In a local area network, the symbol of authority passed successively from one data station to another to indicate the station temporarily in control of the transmission medium. Each data station has an opportunity to acquire and use the token to control the medium. A token is a particular message or bit pattern that signifies permission to transmit. (T) (2) In LANs, a sequence of bits passed from one device to another along the transmission medium. When the token has data appended to it, it becomes a frame.

token ring. (1) According to IEEE 802.5, network technology that controls media access by passing a token (special packet or frame) between media-attached stations. (2) A FDDI or IEEE 802.5 network with a ring topology that passes tokens from one attaching ring station (node) to another. (3) See also *local area network (LAN)*.

token-ring network. (1) A ring network that allows unidirectional data transmission between data stations, by a token passing procedure, such that the transmitted data return to the transmitting station. (T) (2) A network that uses a ring topology, in which tokens are passed in a circuit from node to node. A node that is ready to send can capture the token and insert data for transmission.

topology. In communications, the physical or logical arrangement of nodes in a network, especially the relationships among nodes and the links between them.

trace. (1) A record of the execution of a computer program. It exhibits the sequences in which the instructions were executed. (A) (2) For data links, a record of the frames and bytes transmitted or received.

transceiver (transmitter-receiver). In LANs, a physical device that connects a host interface to a local area network, such as Ethernet. Ethernet transceivers contain electronics that apply signals to the cable and that sense collisions.

Transmission Control Protocol (TCP). A communications protocol used in the Internet and in any network that follows the U.S. Department of Defense standards for internetwork protocol. TCP provides a reliable host-to-host protocol between hosts in packet-switched communications networks and in interconnected systems of such networks. It uses the Internet Protocol (IP) as the underlying protocol.

Transmission Control Protocol/Internet Protocol (TCP/IP). A set of communications protocols that support peer-to-peer connectivity functions for both local and wide area networks.

transparent bridging. In LANs, a method for tying individual local area networks together through the medium access control (MAC) level. A transparent bridge stores the tables that contain MAC addresses so that frames seen by the bridge can be forwarded to another LAN if the tables indicate to do so.

transport layer. In the Open Systems Interconnection reference model, the layer that provides a reliable end-to-end data transfer service. There may be relay open systems in the path. (T) See also *Open Systems Interconnection reference model*.

trap. In the Simple Network Management Protocol (SNMP), a message sent by a managed node (agent function) to a management station to report an exception condition.

tunneling. To treat a transport network as though it were a single communication link or LAN. See also *encapsulation*.

T1. In the United States, a 1.544-Mbps public access line. It is available in twenty-four 64-Kbps channels. The

European version (E1) transmits 2.048 Mbps. The Japanese version (J1) transmits 1.544 Mbps.

U

UNI. User-Network Interface, the interface between user equipment and an ATM switch network.

universally administered address. In a local area network, the address permanently encoded in an adapter at the time of manufacture. All universally administered addresses are unique. Contrast with *locally administered address*.

User Datagram Protocol (UDP). In the Internet suite of protocols, a protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process. UDP uses the Internet Protocol (IP) to deliver datagrams.

V

V.24. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE).

V.25. In data communication, a specification of the CCITT that defines the automatic answering equipment and parallel automatic calling equipment on the General Switched Telephone Network, including procedures for disabling of echo controlled devices for both manually and automatically established calls.

V.35. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at various data rates.

V.36. In data communication, a specification of the CCITT that defines the list of definitions for interchange circuits between data terminal equipment (DTE) and data circuit-terminating equipment (DCE) at rates of 48, 56, 64, or 72 kilobits per second.

VCC. Virtual Channel Connection, a connection between parties.

VINES. VIrtual NEtworking System.

virtual circuit. (1) In packet switching, the facilities provided by a network that give the appearance to the user of an actual connection. (T) See also *data circuit*. Contrast with *physical circuit*. (2) A logical connection established between two DTEs.

virtual link. In Open Shortest Path First (OSPF), a point-to-point interface that connects border routers that are separated by a non-backbone transit area. Because area routers are part of the OSPF backbone, the virtual link connects the backbone. The virtual links ensure that the OSPF backbone does not become discontinuous.

Virtual Local Area Network (VLAN). A logical grouping of one or more LANs based on protocol and subnet and used to isolate network traffic within these groups.

VIrtual NEtworking System (VINES). The network operating system and network software from Banyan Systems, Inc. In a VINES network, virtual linking allows all devices and services to appear to be directly connected to each other, when they may actually be thousands of miles apart. See also *StreetTalk*.

virtual route (VR). (1) In SNA, either (a) a logical connection between two subarea nodes that is physically realized as a particular explicit route or (b) a logical connection that is contained wholly within a subarea node for intranode sessions. A virtual route between distinct subarea nodes imposes a transmission priority on the underlying explicit route, provides flow control through virtual route pacing, and provides data integrity through sequence numbering of path information units (PIUs). (2) Contrast with *explicit route (ER)*. See also *path* and *route extension (REX)*.

W

wide area network (WAN). (1) A network that provides communication services to a geographic area larger than that served by a local area network or a metropolitan area network, and that may use or provide public communication facilities. (T) (2) A data communication network designed to serve an area of hundreds or thousands of miles; for example, public and private packet-switching networks, and national telephone networks. (3) Contrast with *local area network (LAN)* and *metropolitan area network (MAN)*.

wildcard character. Synonym for *pattern-matching character*.

X

X.21. An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for a general-purpose interface between data terminal equipment and data circuit-terminating equipment for synchronous operations on a public data network.

X.25. (1) An International Telegraph and Telephone Consultative Committee (CCITT) recommendation for the interface between data terminal equipment and packet-switched data networks. (2) See also *packet switching*.

Xerox Network Systems (XNS). The suite of internet protocols developed by the Xerox Corporation. Although

similar to TCP/IP protocols, XNS uses different packet formats and terminology. See also *Internetwork Packet Exchange (IPX)*.

Z

zone. In AppleTalk networks, a subset of nodes within an internet.

Zone Information Protocol (ZIP). In AppleTalk networks, a protocol that provides zone management service by maintaining a mapping of the zone names and network numbers across the internet on the session layer.

zone information table (ZIT). A listing of network numbers and their associated zone name mappings in the internet. This listing is maintained by each internet router in an AppleTalk internet.

Index

Numerics

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W

Readers' Comments — We'd Like to Hear from You

8371 Networking Multilayer Ethernet Switch
Software User's Guide
and Configuration Reference

Publication No. GC30-9688-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	☐	☐	☐	☐	☐

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	☐	☐	☐	☐	☐
Complete	☐	☐	☐	☐	☐
Easy to find	☐	☐	☐	☐	☐
Easy to understand	☐	☐	☐	☐	☐
Well organized	☐	☐	☐	☐	☐
Applicable to your tasks	☐	☐	☐	☐	☐

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name _____ Address _____

Company or Organization _____

Phone No. _____

Readers' Comments — We'd Like to Hear from You
GC30-9688-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

IBM Corporation
Design & Information Development
Department CGF/Bldg. 656
PO Box 12195
Research Triangle Park, NC 27709-9990

Fold and Tape **Please do not staple** Fold and Tape

GC30-9688-00

Cut or Fold
Along Line

Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GC30-9688-00

Spine information:

8371 Networking Multilayer
Ethernet Switch

8371 Interface Configuration