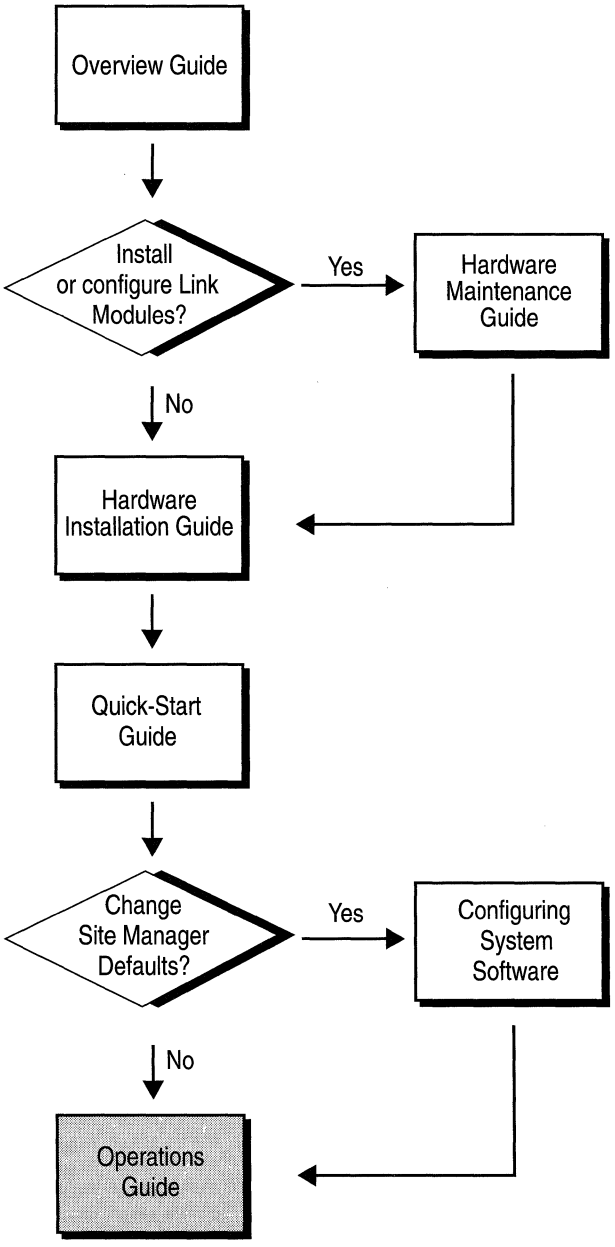
Operations Guide: Site Manager

Software Version 7.50, Site Manager Version 1.50

Reading Path



Part Number: 105545, Revision A

Wellfleet Communications, Inc., 15 Crosby Drive, Bedford, MA 01730

Software License

This license governs the licensing of all Wellfleet software (Software) provided to licensee for use with Wellfleet equipment (Equipment). Licensee is provided with Software in machine-readable form and related documentation. The Software provided under this license is proprietary to Wellfleet and to third parties from whom Wellfleet has acquired license rights. Wellfleet does not grant any Software license whatsoever, either explicitly or implicitly, except by acceptance of an order for either a Software license or for a Wellfleet product that is packaged with Software. Each such license is subject to the following restrictions:

1. Licensee is granted a license to use the Software when payment for the license fee is made. Upon receipt of payment, licensee is granted a personal, nontransferable, nonexclusive license to use the Software with the specific item of Equipment with which or for which it was originally acquired, including use at any of licensee's facilities to which the Equipment may be transferred, for the useful life of the Equipment unless earlier terminated by default or cancellation. Use of the Software shall be limited to such specific item of Equipment and to such facility. Software which is licensed for use on hardware not offered by Wellfleet (e.g. Site Manager) is not subject to restricted use on any Equipment, however, unless otherwise specified in the Documentation, each licensed copy of such Software may only be installed on one item of hardware at any time.
2. Licensee may use the Software with the backup Equipment only if the Equipment with which or for which it was acquired in inoperative.
3. Licensee may make a single copy of the Software (but not firmware) for safekeeping (archives) or backup purposes.
4. Licensee may modify Software (but not firmware), or combine it with other software, subject to the provision that those portions of the resulting software which incorporate licensed Software are subject to the restrictions of this license. Licensee shall not make the resulting software available for use by any third party.
5. Wellfleet and third parties from whom Wellfleet has acquired license rights shall at all times retain title to and ownership of their respective portions of the Software including new versions, new releases, updates and modifications provided to licensee. Licensee agrees and acknowledges that licensee will obtain only such rights to a license or sublicense for the Software as are specifically provided herein.

Software License (continued)

6. Licensee shall not provide, or otherwise make available, any Software, in whole or in part, in any form, to any third party. Third parties do not include consultants, subcontractors or agents of licensee who have licensee's permission to use the Software at licensee's facility, and who have agreed in writing to use the Software only in accordance with the restrictions of this license.

7. Third party owners from whom Wellfleet has acquired license rights to software that is incorporated into Wellfleet products shall have the right to enforce the provisions of this license against licensee.

8. Licensee shall not remove or obscure any copyright, patent, trademark, trade secret or similar intellectual property or restricted rights notice within or affixed to any Software and shall reproduce and affix such notice on any backup copy of Software or copies of software resulting from modification or combination performed by licensees as permitted by this license.

9. Notwithstanding any foregoing terms to the contrary, if Customer licenses the Product "Site Manager", Customer may duplicate and install the Site Manager Software as specified in the Documentation. This right is granted solely as necessary for use of the Site Manager Software on hardware installed within Customer's network. [Note: For licensees in the European Community, the Software Directive enacted by the Council of European Communities Directive dated 14 May 1991 shall apply for interoperability purposes. Licensee must notify Wellfleet in writing of any such intended examination of the Software and Wellfleet may provide review and assistance.]

10. Licensee shall not reverse assemble, reverse compile, or in any way reverse engineer the Software.

11. This license will automatically terminate upon improper handling of Software, such as by disclosure, or Wellfleet may terminate this license by written notice to licensee if licensee fails to comply with any of the material provisions of this license and fails to cure such failure within thirty (30) days after the receipt of written notice from Wellfleet. Upon termination of this license, licensee shall discontinue all use of the Software and return the Software and related documentation, including all copies, to Wellfleet.

12. Licensee's obligations under this license shall survive expiration or termination of this license.

FCC Compliance Notice: Radio Frequency Notice

The following notice regarding compliance with Federal Communications Rules pertain to the Backbone Node.

This equipment generates, uses, and can radiate radio-frequency energy. If you do not install and use this equipment according to the instruction manual, this product may interfere with radio communications. This product has been tested and found to comply with the limits for a Class A computing device, pursuant to Subpart J of Part 15 of FCC Rules; compliance with these limits provides reasonable protection against radio interference when such equipment is operated in a commercial environment. Operating this equipment in a residential area is likely to interfere with radio communications; in which case, the user, as his/her own expense, must correct the interference.

Wellfleet shielded cables must be used with this unit to ensure compliance with the Class A limits.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (the Backbone Node) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique (le Feeder Node, le Link Node, et le Concentrator Node) n'émet pas de bruits radioélectriques dépassant les limites applicables au appareils numériques de Classe A prescrites dans Le Réglement sur Le Brouillage Radioélectrique Édité par Le Ministère des Communications du Canada.

SITE MANAGER SOFTWARE

SITE MANAGER SOFTWARE IS AVAILABLE FOR INSTALLATION ON EITHER SUN SPARCSTATIONS OR DOS-BASED PERSONAL COMPUTERS (PCs). SITE MANAGER MAY BE INSTALLED ON AN UNLIMITED NUMBER OF CUSTOMER SUN SPARCSTATIONS. HOWEVER, SITE MANAGER FOR DOS PCs INCLUDES DISTINCT CORPORATION'S IP RUNTIME SOFTWARE WHICH CAN BE COPIED AND INSTALLED ON UP TO 15 PCs PER NETWORK IN CONJUNCTION WITH WELLFLEET SITE MANAGER FOR DOS PCs.

Table of Contents

Chapter 3

Managing the File System

Chapter 4

Displaying Statistics

Chapter 5

System Administration

Appendix A

Utilities

About this Guide

Audience and Scope

This guide is written for experienced network operators who are using the Site Manager to operate the Wellfleet Backbone Node (BN). This guide assumes that the reader has a technical understanding of data communications.

This guide describes how to use the Site Manager to perform day-to-day operations. The Site Manager is the primary tool for configuration, monitoring, event management, and control of the Wellfleet router. This guide describes how to start up the Site Manager, boot the BN, reset individual slots in the BN, and manage BN events, traps, files, and statistics.

How to Use this Guide

Refer to the following table for instructions on how to use this guide.

For Instructions on How to:	Refer to:
Start up the BN	*Introduction to the Site Manager*
Display and respond to events and traps	*Managing Events and Traps*
Display BN filenames, copy or delete BN files, transfer files between the Site Manager and the BN, and compact and format BN volumes	*Managing the File System*
Transfer data link layer and network layer statistics from the BN and display them	*Displaying Statistics*
Display the Site Manager and BN software versions, boot the BN, and reset a slot on the BN	*System Administration*
Convert configuration files to ASCII for viewing	*Utilities*

Document Set

The following guides complete this documentation set:

Overview Guide

Describes the user interface, called the Site Manager application, the system software, and the router hardware.

Hardware Installation Guide

Describes how to physically install the router hardware.

Quick-Start Guide

Describes how to configure the router's initial IP network interface, install the Site Manager application software, and remotely create a pilot configuration for the Wellfleet router using the Site Manager.

Configuring System Software, Volumes I and II

Describes how to use the Site Manager's Configuration Manager application to set Wellfleet router parameters in one of three modes: local, remote, or dynamic.

Hardware Maintenance Guide

Describes how to access the interior of the Wellfleet router, replace the hardware, and how to read the LEDs.

If you are missing any guides, contact Wellfleet Customer Support at 1-800-2LANWAN.

Conventions

This document set uses the following conventions:

Convention:	Denotes:
filename	Italics denote file and directory names.
command	Bold text denotes text the user needs to enter.
Events/Log Files	The slash character (/) separates menu and option names in instructions; this example identifies the Log Files option in the Events menu.

Chapter 1

Introduction to the Site Manager

List of Figures

List of Tables

Introduction to the Site Manager

About this Chapter

This chapter describes how to start up the Site Manager and its associated management applications to perform monitoring, event management, and control functions. This chapter also describes how to establish or change the Site Manager or management application connection to the Wellfleet router (IP address), and how to send an Internet Control Message Protocol echo request (ping) to a remote IP address.

This chapter assumes the following:

- The Wellfleet router is installed (refer to the *Hardware Installation Guide* for instructions).
- The Wellfleet router is configured (refer to the *Quick-Start Guide* and *Configuring System Software* guide for instructions).
- The Site Manager is installed on your SPARC station (refer to the *Release Notes* for instructions).
- You have read the *Site Manager User Interface* chapter in the *Configuring System Software* guide.

Starting Up

The instructions that follow describe how to start the Site Manager from the PC and from the SPARCstation.

The Site Manager includes four management applications: Configuration Manager, Events Manager, File Manager, and Statistics Manager. You can start up these management applications from within the Wellfleet Site Manager Window, or from the windows application you are running. The sections that follow also provide instructions for starting these management applications.

Note: Refer to the *Quick-Start Guide* for installation instructions and for the System Requirements.

System Capacity

Assuming memory is available on the Site Manager workstation, you can run the following Site Manager applications simultaneously:

- One Statistics Manager application with up to eight Statistics Manager options.
- One local mode or remote mode Configuration Manager application, with any number of dynamic mode Configuration Manager applications until the Config/Dynamic option is grayed out.
- One File System Manager application.
- Eight Events Manager applications.
- One Trap Monitor application.

Starting Up the Site Manager on the PC

You start up the Site Manager on the PC as follows:

1. Ensure Windows is up. To start Windows, enter the following after the DOS (*C:*) prompt:

   win

2. Select the Wellfleet menu.
3. Double-click the PC Site Manager icon.

The Wellfleet Site Manager Window appears (see Figure 1-1). This window displays the IP address and community name of the Wellfleet router which it is ready to manage.

Starting Up the Site Manager on the SPARC

You start up the Site Manager on the SPARCstation as follows:

1. Ensure OpenWindows is up. To start OpenWindows, enter the following after the UNIX prompt:

   openwin

2. Click in the cmdtool window.

Note: The Site Manager uses the directory from it is started as the default file storage location.

3. Enter the directory in the cmdtool window where you want the configuration files, log files, and transferred files to be stored.
4. Enter the following in the cmdtool window to start the Site Manager:

   wfsm &

The Wellfleet Site Manager Window appears (see Figure 1-1). This window displays the IP address and community name of the Wellfleet router it is ready to manage.

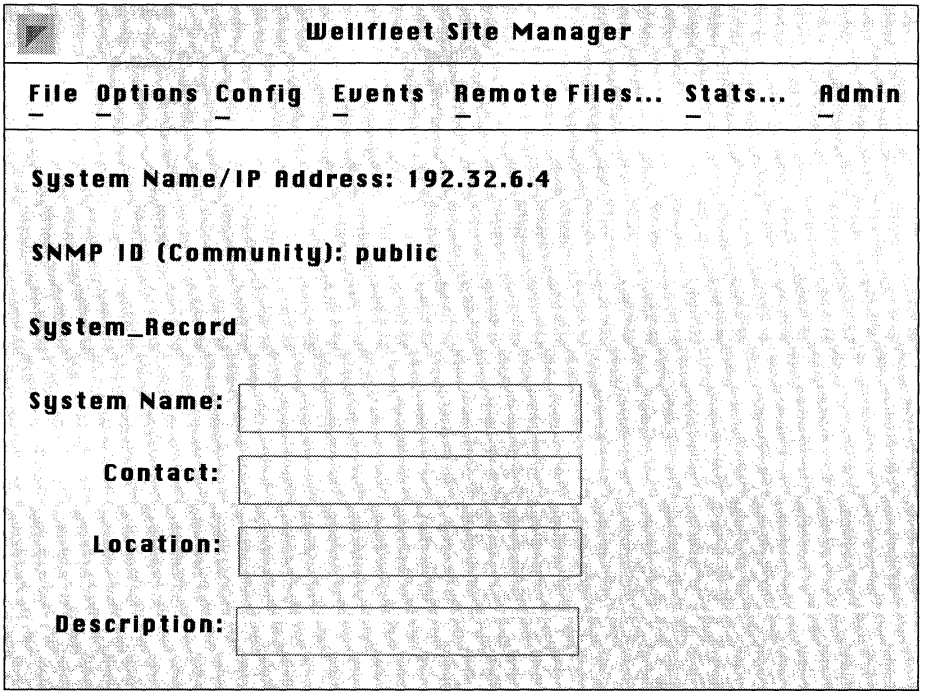


Figure 1-1. Wellfleet Site Manager Window

Starting Up Management Applications

The management applications associated with the Site Manager are as follows:

- Configuration Manager. Three options are displayed when you click on the Config option: Local, Remote, and Dynamic. Refer to the *Configuring System Software* guide for configuration instructions.
- Events Manager. Two options are displayed when you click on the Events option: Trap Monitor and Log Files. The Trap Monitor option starts the Trap Monitor application, which displays traps sent by the Wellfleet router. The Log Files options starts the Events Manager application, which allows you to transfer and display the log file from the Wellfleet router, save the file on the workstation, and read and display a log file on the workstation.
- File Manager. The Remote Files option starts the File Manager application, which establishes a connection with the Wellfleet router and displays a list of the files stored on its active volume. The file manager allows you to display the filenames stored on other volumes in the Wellfleet router; transfer, copy, and delete files; and format and compact a Wellfleet router volume.
- Statistics Manager. The Stats option starts the Statistics Manager application, which establishes a connection with the Wellfleet router and allows you to display protocol and circuit statistics.

You can start up the management applications by selecting the menu options displayed in the Site Manager window, or you can start them up from the windows application installed on your system.

Table 1-1 shows the Site Manager startup commands you enter to start the management applications from the windows application. Table 1-2 lists options you can enter when using these startup commands. The sections that follow, *Starting Up Management Applications on the PC* and *Starting Up Management Applications on the SPARC* provide instructions for using the commands and options listed in these tables.

Note: Tables 1-1, 1-2, and the sections *Starting Up Management Applications on the PC* and *Starting Up Management Applications on the SPARC* are optional.

Table 1-1. Site Manager Startup Commands

Command	Function
wfsm	Starts the Site Manager, which establishes a connection with the Wellfleet router. You can use the Site Manager to establish a connection to another Wellfleet router, start management applications, and issue administrative commands.
wfcfg	Starts the Configuration Manager, which establishes a connection with the Wellfleet router.
wflog	Starts the Events Manager, which establishes a connection with the Wellfleet router.
wftraps	Starts the Trap Monitor, which establishes a connection with the Wellfleet router.
wfrfs	Starts the File Manager, which establishes a connection with the Wellfleet router.
<xx>mon	Starts the **<xx>** Statistics Manager, which establishes a connection with the Wellfleet router. (**Note:** You must specify the SNMP agent IP address using the -a <SNMP Agent IP Address> startup option.) You may enter one of the following: **atmon** starts the AppleTalk Statistics Manager **cctmon** starts the Circuit Statistics Manager **decmon** starts the DECnet Statistics Manager **frmon** starts the Frame Relay Statistics Manager **ipmon** starts the IP Statistics Manager **ipxmon** starts the IPX Statistics Manager **lbmon** starts the Learning Bridge Statistics Manager **ospfmon** starts the Open Shortest Path First Statistics Manager **pqmon** starts the Protocol Prioritization Statistics Manager **smdsmon** starts the Switched Multimegabit Data Service Statistics Manager **srmon** starts the Source Routing Statistics Manager **vnsmon** starts the Vines Statistics Manager **xnsmon** starts the Learning Bridge Statistics Manager

You can add options to the startup commands to override Site Manager default settings. Table 1-2 lists the options, the startup commands with which they can be used, their function, the default setting, and an example of how you enter the option.

Table 1-2. Site Manager Startup Command Options

Startup Option	Startup Commands	Function	Default Setting	Sample Use of Option
-c <SNMP Community>	All	Specifies the SNMP community string	public	**wfsm -c Sitemgr**
-a <SNMP Agent IP Address>	All	Specifies the SNMP agent IP address	none	**ipmon -a 192.32.4.2**
-m <SNMP MIB Definitions File>	All	Specifies the MIB definitions file in the path */usr/wf/lib*	WFMIB.defs	**wfcfg -m mymib.defs**
-r <SNMP retry count>	All	Specifies the number of SNMP retries	3	**wfrfs -r 5**
-t <SNMP Timeout>	All	Specifies the number of seconds for the SNMP timeout	5	**wflog -t 10**
-s <SNMP Destination Port>	All	Specifies the UDP port for the SNMP destination. The default setting causes the application to retrieve the SNMP destination port from */etc/services*.	0	**wftraps -s 1161**

Table 1-2. Site Manager Startup Command Options

Startup Option	Startup Commands	Function	Default Setting	Sample Use of Option
-e <SNMP Trap Port>	wfsm wftraps	Specifies the UDP port on which the Trap Monitor should listen for SNMP traps. The default setting causes the application to retrieve the SNMP trap port from */etc/services*.	0	**wftraps -e 1161**
-v <Config Volume>	wfsm wfcfg	Specifies the volume for remote configuration file access	2	**wfsm -v 3**
-f <Config File>	wfcfg	Specifies the configuration filename	2	**wfcfg -f file.cfg**
-o <Config Mode>	wfcfg	Specifies the configuration mode: local, remote, or dynamic	local	**wfcfg -o remote**
-p <Polling Interval>	<xx>mon	Specifies the polling interval in seconds for traffic statistics screens	10	**ipmon -p 5**

Starting Up Management Applications on the PC

Table 1-1 in the previous section shows the Site Manager startup commands you use to start the management applications from the windows application. Table 1-2 in the previous section lists the startup command options. This section describes how to use the Windows application on the PC to enter these commands and options.

To start up management applications, you must first create Program Item icons for these applications. Once you have created the icons, you double-click the PC Site Manager application and double-click the icons associated with the management applications you want to run.

Note: The procedures in this section are optional and are recommended only for experienced Site Manager users. The procedures for starting up the management applications described in the *Starting Up Management Applications* introductory section are the simpler alternative.

You set up the management applications as follows:

1. Ensure Windows is up. To start Windows, enter the following after the DOS (*C:*) prompt:

   win

2. Select the Wellfleet menu.
3. Press and hold the **<ctrl>** key.
4. Click on the PC Site Manager icon with the left mouse button and drag the icon image to a blank location on the screen.
5. Release the left mouse button.

   A duplicate PC Site Manager icon appears.
6. Click on the duplicate PC Site Manager icon with the left mouse button.
7. Press **<Alt>F.**

8. Enter P for Properties.

   The Program Item Properties Window appears.

9. In the Description box, enter the name to appear under the icon. For example, if you are creating an icon for a configuration manager with a connection to SNMP Agent IP Address 192.32.4.2, you might choose to enter the description **Cfg 192.32.4.2.**

10. In the Command Line box, enter **c:\wf** and append to this path one of the commands listed in Table 1-1 and any number of command options you want from Table 1-2 to create the management application you want. For example, you enter the following to create an icon for a configuration manager with a connection to SNMP Agent IP Address 192.32.4.2 and an SNMP timeout of 10 seconds:

    c:\wf\wfcfg -a 192.32.4.2 -t10

11. Leave the Working Directory box blank.

12. Leave the Shortcut Key box set to None.

13. Select OK.

The description you entered is displayed under the icon you selected.

Note: The Site Manager window must be open in order for you to open a management application, regardless of whether you choose to open it by selecting a Site Manager Window option or double-clicking the icon associated with the management application.

When the Site Manager Window is displayed and you double-click an icon associated with the management applications you want to run, the management application window appears. This window displays the IP address and community name of the Wellfleet router it is ready to manage.

Starting Up Management Applications on the SPARC

Table 1-1 shows the Site Manager startup commands you use to start the management applications from the windows application. Table 1-2 lists the startup command options. This section describes how to use the OpenWindows application of the SPARCstation to enter these commands and options.

Note: The procedures in this section are optional and are recommended only for experienced Site Manager users. The procedures for starting up the management applications described in the *Starting Up Management Applications* section of this chapter are the simpler alternative.

You start up the management applications as follows:

1. Ensure OpenWindows is up. To start OpenWindows, enter the following after the UNIX prompt:

   openwin

2. Click in the cmdtool window.
3. Enter one of the commands listed in Table 1-1 and any number of command options you want from Table 1-2 to start the management application you want. Append the command with a space and an ampersand (&) so that you can continue to enter commands in the cmdtool window while the management application is running. For example, you enter the following to start a configuration manager with a connection to SNMP Agent IP Address 192.32.4.2 and an SNMP timeout of 10 seconds:

   wfcfg -a 192.32.4.2 -t10 &

The management application window appears. This window displays the IP address and community name of the Wellfleet router it is ready to manage.

Shutting Down

The sections that follow describe how to shut down the Site Manager and its associated management applications.

Shutting Down the Site Manager

Shut down the Site Manager as follows:

1. Select File/Exit from the Wellfleet Site Manager Window.

   A confirmation window appears.

2. Click Ok.

When you shut down the Site Manager on the PC, all management applications and associated windows also shut down, regardless of how you started them up.

When you shut down the Site Manager on the SPARCstation, only those management applications and associated windows started up from the Site Manager Window shut down. Refer to the next section to shut down management applications started up from the cmdtool window.

Shutting Down Management Applications

Shut down the Site Manager management applications as follows:

1. Select File/Exit from the management application window.

   A confirmation window appears.

2. Click Ok.

All windows associated with the management application close when you shut down the application.

Editing SNMP Option Parameters

When you display the Site Manager, Configuration Manager, Events Manager, File System Manager, or Statistics Manager windows, the address of the Wellfleet router with which you established communication is automatically displayed, indicating you can perform the associated management functions on the Wellfleet router.

The Options menu selection on the Site Manager Window allows you to change the Wellfleet router (IP address) with which you are communicating. When you change the IP address, it becomes the default address. When you open new management windows, the new windows display the default address. However, existing management windows retain the IP address previously displayed in those windows.

Each of the managers has its own Options menu selection so that you can change the Wellfleet router associated with that manager. By opening multiple windows associated with one or more managers and using the Options menu selection associated with each window, you can perform individual management functions on different Wellfleet routers simultaneously.

To open the SNMP Options Window associated with the Site Manager, begin at the Site Manager Window and select Options. The SNMP Options Window appears (see Figure 1-2).

To open the SNMP Options Window associated with the Configuration Manager, Events Manager, File System Manager or Statistics Manager, begin at the Site Manager Window and select the associated menu option. When the associated manager window appears, select Options. The SNMP Options Window appears.

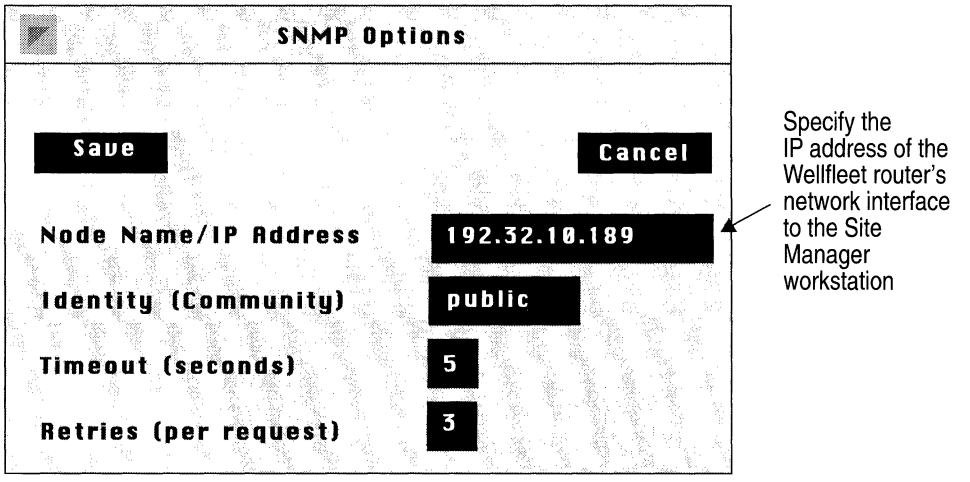


Figure 1-2. SNMP Options Window

Refer to the descriptions that follow to edit the parameters you wish to change. When finished, click the Save button to exit the window and save your changes.

The format for the parameter descriptions is as follows:

- Wellfleet default
- Range of valid settings
- Parameter's function
- Instructions for setting the parameter

Parameter :	**Node Name/IP Address**
Wellfleet Default:	NONE
Options:	Valid host name or valid IP address
Function:	Specifies the host name or IP address of the Wellfleet router with which you wish to establish a management session.
Instructions:	Enter the Wellfleet router's IP address or host name. You may only use the host name to establish a management session if the host name is included in the workstation's host file.

Note: The Configuration Manager's SNMP Options Window does *not* display the Node Name/IP Address parameter. Each instance of the Configuration Manager application allows you to access one Wellfleet router only. To configure two Wellfleet routers simultaneously, you must display the SNMP Options Window from the Wellfleet Site Manager Window, specify the new Wellfleet router, and then run another instance of the Configuration Manager application, which automatically communicates with the Wellfleet router.

Parameter :	**Identity (Community)**
Wellfleet Default:	public
Options:	Any valid SNMP community name.
Function:	Specifies the SNMP community name you wish the Site Manager to use when communicating with the Wellfleet router.
Instructions:	Enter the SNMP community name. The community must have READ/WRITE access to the specified Wellfleet router, if you wish to use the Configuration Manager to reconfigure the Wellfleet router.

Parameter :	**Timeout (seconds)**
Wellfleet Default:	5 seconds
Options:	1 to 300 seconds
Function:	Specifies the number of seconds the Site Manager waits for a response from the Wellfleet router, after it issues an SNMP SET or GET before reissuing the command.
Instructions:	Enter the number of seconds.

Parameter :	**Retries (per request)**
Wellfleet Default:	3
Options:	0 to 30
Function:	Specifies the number of times the Site Manager will reissue a command when the Wellfleet router does not respond.
Instructions:	Enter the number of times.

Pinging a Remote Device

The ping option tests the reachability of a remote device. The Packet Internet Groper (ping) program residing on the Wellfleet router sends an Internet Control Message Protocol (ICMP) echo request to the remote IP address you specify. The remote device responds to the Wellfleet router if it is reachable, and the Wellfleet Site Manager Window displays the response or the result of the request.

Send an ICMP echo request (ping) to a remote device as follows:

1. Select the Admin/Ping option. The Ping Window appears (see Figure 1-5).

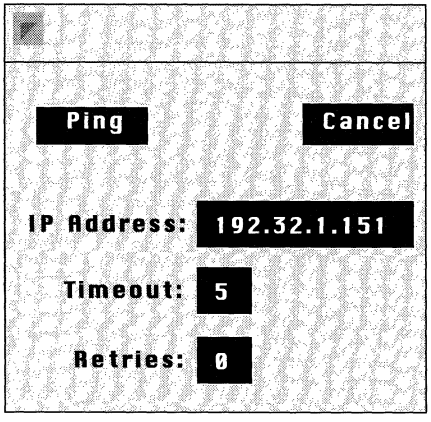


Figure 1-3. Ping Window

Note: Enter the IP address, in dotted decimal notation, of the remote device you want to ping in the IP Address field. (The ICMP echo request [ping] does not support loopback or broadcast addresses.)

You can override the default Timeout and Retries values by entering them in their associated boxes. They are as follows:

The Timeout box displays the number of seconds each ping times out. If the system receives a response to a ping after it

times out, it does not send an "alive" message to the console. The default Timeout is 5.

The Retries box displays the number of successive times to repeat the ping. The system does not wait for the timeout before sending the next ping. The default Retries is 0.

The Administration Window displays one of the following messages when you send a ping: (If you overwrite a value in the Retry box, the system displays one of the following messages for the default ping plus one for each additional ping:)

- An *alive* message: The message appears if the system receives an ICMP echo response from the target device within the timeout allowed. The message also indicates the size of the test packet. A sample message follows:

  ping: 192.32.1.151 is alive (size = 16 bytes)

- A *does not respond* message: The message appears if the MAC address of the target device is resolved, but the system does *not* receive an ICMP echo response from the target device within the timeout allowed. A s3737ample message follows:

  ping: 193.32.1.151 does not respond

- An *ICMP host unreachable from y.y.y.y* message: The message appears if the local Wellfleet router or remote router whose address is *y.y.y.y* cannot forward the ping request any further along the path to the target device. IP updates its IP routing or ARP table accordingly. A sample message follows, where *y.y.y.y* is the address of the ICMP host:

  ping: ICMP host unreachable from 192.32.243.1

- A target address *is unreachable* message: The local Wellfleet router previously issued an *ICMP host unreachable from y.y.y.y* message. Within forty seconds, the local Wellfleet router received a subsequent ICMP echo request addressed to the same target device. The ARP timed out or the address could not be resolved. A sample message follows:

  ping: 192.32.1.151 is unreachable

Chapter 2

Managing Events and Traps

List of Figures

List of Tables

Managing Events and Traps

About this Chapter

This chapter describes how to use the Site Manager to manage events and traps. Managing events and traps involves receiving them from the Wellfleet router, filtering and displaying them, responding to them, and saving them to files on your workstation for later viewing.

A list of the events issued by the Wellfleet router, complete with instructions for responding to them, is provided at the end of this chapter.

Using the Events Manager

You use the Events Manager to retrieve and display the event log generated by a specific Wellfleet router. The event log is a circular (FIFO) buffer containing event messages. By examining a Wellfleet router's event log, you can monitor the Wellfleet router's operating status.

Each time you want to view the most current version of a Wellfleet router's event log, you must command the Events Manager to retrieve the event log. The Events Manager does *not* display event messages in real-time.

Assuming memory is available on the Site Manager workstation, you can run up to eight Events Manager applications simultaneously. Each Events Manager receives events from the Wellfleet router whose IP address you specified in the Wellfleet Site Manager Window. You can also specify the Wellfleet router from which you want to receive events using the Options menu selection in the Events Manager Window. The SNMP options displayed are the same as those for the Wellfleet Site Manager Window. Refer to the *Editing SNMP Option Parameters* section of the chapter *Introduction to the Site Manager* for instructions.

You can use the Events Manager to do the following:

- Display a Wellfleet router's current event log
- Save an event log to a file on the Site Manager workstation
- Display a previously saved event log file stored on the Events Manager workstation
- Clear the events currently displayed on the Events Manager Window

When you specify that you want to display a Wellfleet router's event log, the Events Manager captures the events currently logged in the Wellfleet router's event memory buffer. Then it saves the event log to a binary file, and uses TFTP to transfer the file from the Wellfleet router to the workstation. Finally, the Events Manager translates the log file from binary to ASCII format, saves it to a file, and displays the event log on the screen.

When the remote workstation receives a new event log file, it overwrites the event log file it received previously. You can use the Events Manager to save the event log to another local file before retrieving an updated event log if you want to display the old file later. Refer to *Saving Event Log Files to Your Workstation* for instructions.

You can specify the types of event messages that are displayed on the screen by selecting event filters. That is, although the Events Manager retrieves the entire event log file from the Wellfleet router (or from your Site Manager workstation if you a getting a locally stored file), the Events Manager displays only those types of events that are filtered.

Displaying the Events Manager Window

To display the Events Manager Window, begin at the Wellfleet Site Manager Window and proceed as follows:

1. Select the Events/Log Files option.

   The Events Manager Window appears.

2. Select File/Get Remote Events File.

   The Events Manager transfers the events file to the Wellfleet router and displays them in the Events Manager Window (see Figure 2-1).

Note: Each time you retrieve an event log from a Wellfleet router, the router overwrites the log file in Flash memory with the contents of the new log and transfers (TFTPs) the log to the remote workstation. Frequent remote retrievals of the log increases the Flash card write activity, which in turn rapidly consumes its free contiguous space, requiring frequent compacts of its memory. Prudent use of the events log remote retrieval procedure minimizes the frequency with which you need to compact Flash card memory. Configuring the router to send traps to the remote workstation and then using the Trap Monitor is the recommended procedure for routine viewing of events, and does not increase Flash write activity. Also, viewing the log from the TI does not increase Flash write activity.

Refer to the section Compacting File Space for more information about the **compact** command. Refer to the *Configuring SNMP* chapter of the *Configuring System Software* guide for instructions on how to configure a Wellfleet router to send traps to the Site Manager.

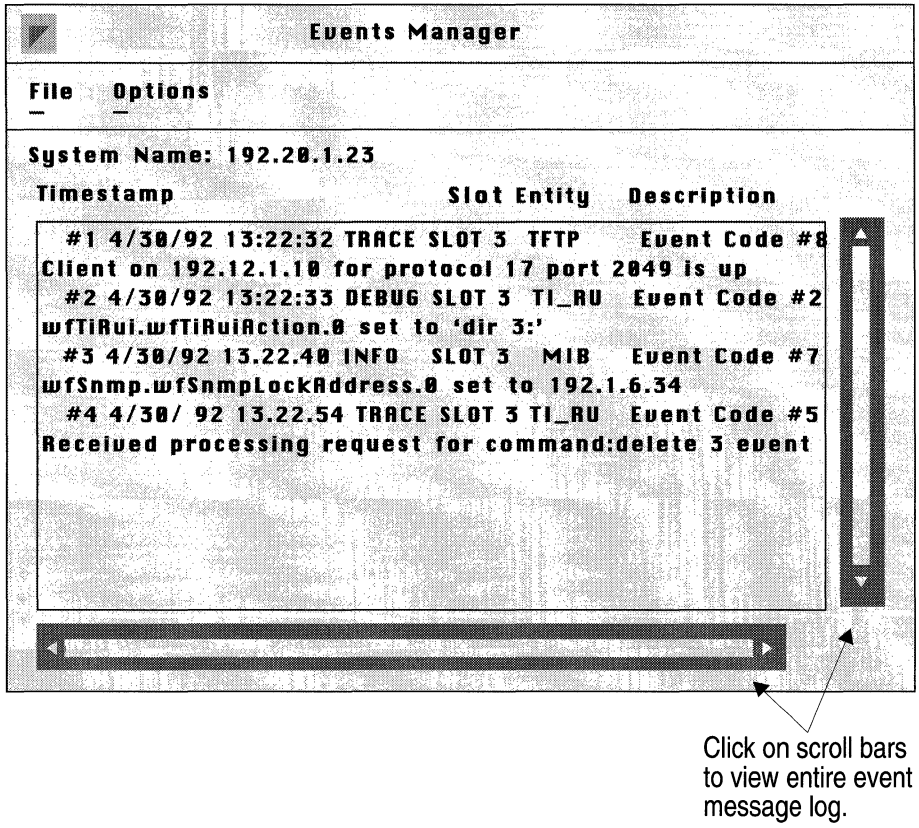


Figure 2-1. Events Manager Window

You can scroll through the event messages using the scroll bars on the bottom and right hand side of the window.

The section *Events* lists the specific events and shows how to read them.

Filtering Events By Type

The Events Manager allows you filter the events displayed on the screen by event type.

You begin from the Events Manager Window and proceed as follows:

1. Select the Options/Display/Select Event Types option.

   The Filter window appears, showing the five event types (see Figure 2-2).

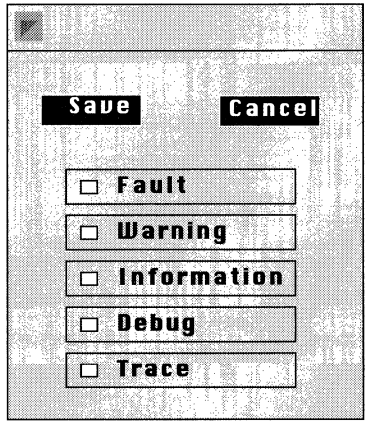


Figure 2-2. Event Type Filter Window

The event types are as follows:

— FAULT indicates a major service disruption. This disruption may be caused by a configuration, network, or hardware problem. The entities (software services) involved attempt to restart and recover until the problem is resolved.

— WARNING indicates a service behaved in an unexpected fashion.

— INFORMATION indicates routine events.

— DEBUG indicates information used by Wellfleet Customer Support only.

— TRACE indicates information about each packet that traversed the network. Wellfleet recommends filtering this event type only when diagnosing network problems.

2. Select the types of events you want the Events Manager to display; then select the Save button.

The next time you get or load an event log, the Events Manager displays only the events that are of the types you selected.

Saving Event Log Files to Your Workstation

The Events Manager allows you to save the event log file currently displayed on the screen to a file on your local system for later retrieval.

You begin from the Events Manager Window as follows:

1. Select the File/Save Events option.

   The Events Manager prompts you to name the event log file that you want to store on your local system.

2. Enter the file name, then select the Save button.

Note: The Events Manager saves the entire event log file. Thus, when displaying an event log file, you can view some or all of the event messages stored in the file by resetting the event filters.

Displaying Event Log Files Stored on Your Workstation

The Events Manager allows you to load event log files stored on the Site Manager workstation and display them on the screen. You begin from the Events Manager Window as follows:

1. Select the File/Load Local Events Log File option.

   The Events Manager prompts you to specify the name of the event log file you want to retrieve.

2. Enter the filename of the event log file you previously saved to your workstation, then select the Save button.

   The Events Manager retrieves and displays the event log file on the screen.

Clearing the Events Manager Window

Select the Options/Display/Clear Window Option to clear the events currently displayed on the Events Manager Window.

The Events Manager Window clears. It remains empty until the next time you get or load an event log file.

Using the Trap Monitor

The Events Manager stores a running history of traps in a file. You use the Trap Monitor to display these traps. Traps are simply event messages that are sent to the Events Manager from all nodes on the network that are configured to do so.

The Trap Monitor displays traps in real time; that is, the Trap Monitor continually updates the screen with new, incoming traps.

The Events Manager also stores all incoming traps in a file called the trap history file. By loading the trap history file, you can examine all of the traps that were sent to the Events Manager since the last time you emptied the trap history file.

You can save traps to an ASCII file on your workstation if you want to examine the file at a later time, or want to edit the file with a text editor.

You can use the Trap Monitor to do the following:

- Display incoming traps
- Display the trap history file
- Empty the trap history file
- Save traps to a file on the Site Manager workstation (a file that can be edited using a text editor)
- Clear the Trap Monitor Window

You can specify which trap messages are displayed on the screen by creating trap filters. That is, although all traps sent to the Events Manager are stored in the trap history file, the Trap Monitor displays only those types of traps that you specify.

You can also filter traps by specifying the source addresses from which they originate. The Events Manager filters out traps originating from nodes whose IP addresses don't match the address requirements you specify.

By default, both trap message type filters and source address filters are set to display all trap messages received by the Events Manager.

Note: Only those nodes on the network that are specifically configured to transmit traps to the Events Manager will do so. For information on configuring the Wellfleet router to generate traps, see *Configuring SNMP* in the *Configuring System Software* guide.

Refer to the section that follows to configure the Site Manager to bind to an alternate trap port if you are using the Site Manager and another SNMP manager on the same workstation. Otherwise, refer to the section *Displaying Incoming Traps*.

Configuring the Site Manager to Bind to an Alternate Trap Port

Only one SNMP application can bind to a UDP port. By default, the Site Manager application binds to UDP port 162, which is dedicated to receiving SNMP traps. If you are using the Site Manager and another SNMP manager (such as HP OpenView or SunNet Manager) bound to UDP port 162 on the same workstation, then you must reconfigure the Site Manager application to bind to another UDP port, as follows:

1. Shut down the Site Manager application.
2. Enter the following command at the command line of the Site Manager workstation to assign a new UDP port to receive traps:

   wfsm -e 163 &

   Where:

   wfsm is the command that invokes the Site Manager application.

   -e is the trap-binding parameter.

   163 is a currently unassigned UDP port that is not in use by another application on the workstation.

   & is an optional parameter that ensures the accompanying command runs in the background.

In order for the Site Manager to receive traps from a Wellfleet router, you must configure the Wellfleet router to send traps to the Site Manager UDP port you specified in step 2 above. Refer to the *Configuring SNMP* chapter of the *Configuring System Software* guide for instructions on how to configure a Wellfleet router to send traps to the Site Manager.

Displaying Incoming Traps

The Trap Monitor dynamically displays all incoming trap messages that are of the types you select and from the source addresses that you specify.

To display the Trap Monitor Window, begin at the Wellfleet Site Manager Window and select the Events/Trap Monitor option. The Events Manager displays the Trap Monitor Window (see Figure 2-3).

You can scroll through the traps using the scroll bars on the bottom and right hand side of the window.

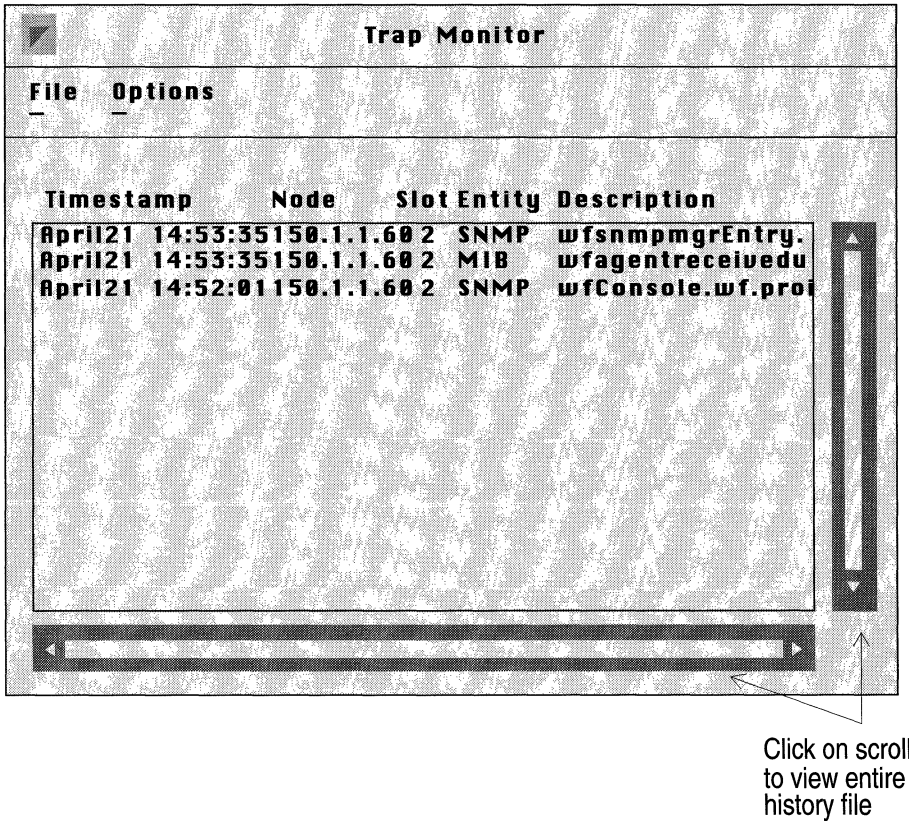


Figure 2-3. Trap Monitor Window

Each trap message consists of the following:

- Timestamp: Date and time the trap (event) was issued by the remote device
- Node: IP address of the node that generated the trap
- Slot: Slot hosting the software entity (service) that generated the event
- Entity: Software service that generated the trap. The entities include software modules dedicated to the operation of a software service, such as TFTP and IP; and the GAME operating system.
- The event text explaining the trap (Description)

Refer to the *Events* section for information about specific trap (event) messages.

Filtering Traps by Type

The Trap Monitor allows you to filter the traps displayed on the screen by trap type. You begin from the Trap Monitor Window and proceed as follows:

1. Select the Display/Options/Select Trap Types option.

   The Filter window appears, showing the five trap types (see Figure 2-4).

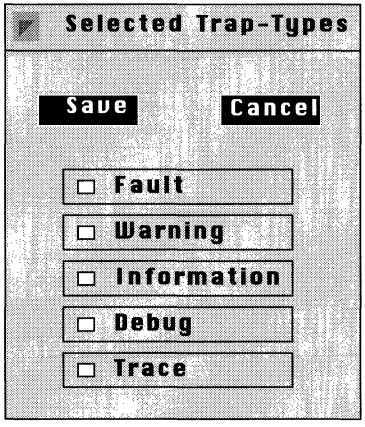


Figure 2-4. Trap Type Filter Window

The trap types are as follows:

— FAULT indicates a major service disruption. This disruption may be caused by a configuration, network, or hardware problem. The entities involved attempts to restart and recover until the problem is resolved.

— WARNING indicates a service behaved in an unexpected fashion.

— INFORMATION indicates routine events.

— DEBUG indicates information used by Wellfleet Customer Support only.

— TRACE indicates information about each packet that traversed the network. Wellfleet recommends filtering this event type only when diagnosing network problems.

2. Click on the types of traps you want the Trap Monitor to display, then select the Save button.

   After you save the trap types, the Events Manager returns to the Trap Monitor Window. In the future, the Trap Monitor only displays traps that are of the types you selected.

Filtering Traps by Source Address

The Trap Monitor allows you to filter the traps displayed on the screen based on the source address of the nodes from which the traps originate. You begin from the Trap Monitor Window and proceed as follows:

1. Select the Options/Set Address Filters option.

   The Address Filters Window appears (see Figure 2-5).

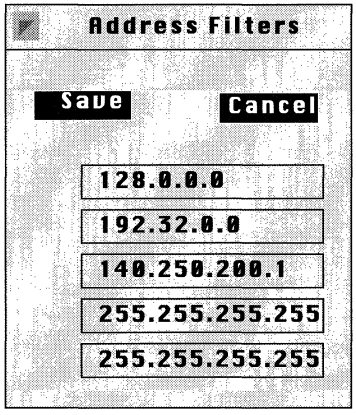


Figure 2-5. Address Filters Window

2. Specify one or more IP address filters for the nodes whose traps you want to filter in, then select the Save button.

   You can specify up to five IP address filters. The default address filter of 0.0.0.0 displays traps from *all* nodes configured to send traps to the Events Manager.

   The examples in Figure 2-5 filter all traps from all systems whose IP addresses start with 128 and 192.32, and from the system whose address is 140.250.200.1. The address filter of 255.255.255.255 is used to refuse traps from *all* other nodes.

   After you save the address filters, the Events Manager returns to the Trap Monitor Window. In the future, the Trap Monitor displays only the traps that originate from nodes whose source address meets the address filter requirements you specified.

Displaying the Trap History File

The Trap Monitor allows you to load and display the trap history file on the screen.

Beginning from the Trap Monitor Window, select the File/Load History File option. The Trap Monitor retrieves all traps received since the last time you cleared the trap history file and displays them on the screen. The Trap Monitor continues to display new, incoming traps as they arrive.

See *Saving Traps to a File on Your Workstation* for instructions on saving traps to a local file that you can edit.

Clearing the Trap History File

The Trap Monitor allows you to clear the trap history file.

Beginning from the Trap Monitor Window, select the File/Clear History File option. The Trap Monitor empties the trap history file. (See *Clearing the Trap Monitor Window* for instructions on clearing the Trap Monitor window.)

As new traps arrive, the Events Manager saves them to its trap history file once again.

Saving Traps to a File on Your Workstation

The Trap Monitor allows you to save the traps currently displayed in the Trap Monitor Window to an ASCII file on your workstation. (To save the *entire* trap history file to an ASCII file, first turn off all trap filters and redisplay the trap history file). By saving traps to a file to your workstation, you can later edit the file using a text editor.

You begin from the Trap Monitor Window and proceed as follows:

1. Select the File/Save Traps option.

   The Trap Monitor prompts you to name the file to store traps on your workstation.

2. Name the file, then select the Save button.

   The Events Manager returns to the Trap Monitor Window.

Clearing the Trap Monitor Window

To clear the Trap Monitor Window, select the Options/Display/Clear Window option. The Trap Monitor clears the screen of all traps displayed on the window.

Note: Clearing the Trap Monitor Window simply clears the traps displayed on the screen; it does not empty the trap history file. You can view the traps again by redisplaying the trap history file.

Events

The sections that follow describe how to read an event log entry, identifies the trap codes used by the Wellfleet router when trapping events, and lists all events. Each event is accompanied by a description and a recommended response if one is required.

How to Read Events

The Site Manager and the TI display events in the same format, as shown in Figure 2-6.

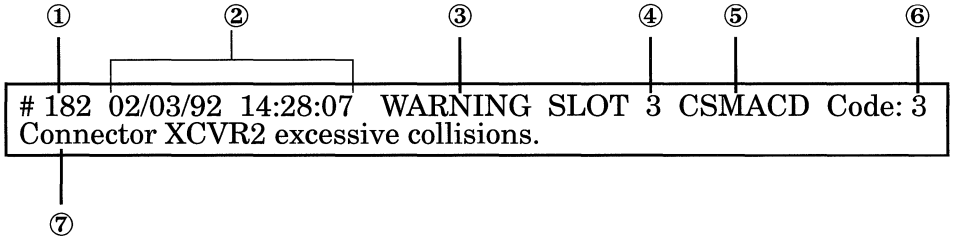


Figure 2-6. Sample Event Message

Each event display provides the following information:

① Log event number. Figure 2-6 shows the 182nd event in the event log.

② Date and time the event was issued.

③ Severity of the event. The following severity types appear in the event log:

— FAULT indicates a major service disruption. This disruption may be caused by a configuration, network, or hardware problem. The entity involved attempts to restart and recover until the problem is resolved.

— WARNING indicates a service behaved in an unexpected fashion. Following sections describe the appropriate action to take in response to each warning message.

— TRACE indicates information about each packet that traversed the network.

Note: The event log overwrites itself frequently when you filter TRACE events. Generally, TRACE event messages are filtered only to assist in the diagnosis of network problems.

— INFO indicates routine events. Usually, no action is required in response to INFO event messages.

④ Slot hosting the entity that generated the event.

⑤ Entity that generated the event. The entities include software modules dedicated to the operation of a software service, such as TFTP and IP; and the Wellfleet router's Gate Access Management Entity (GAME) operating system.

⑥ The event code assigned to the event. You enter the event code to match traps to the operations you want when using third-party software. Refer to the section that follows for instructions.

⑦ The event text describing the event.

The events sections list the events that can appear in the event log. These sections are organized by entity and severity. Events are organized alphabetically within each severity type.

The format of each event description is as follows:

Event text

Event code

Severity of the event

Meaning of the event

Action (if necessary)

SNMP Trap Code Numbers

Some third-party networking software applications, such as OpenView and SunNet, allow you to configure them to trigger a desired operation when a certain trap is received. This section describes the SNMP trap format and lists the code numbers used. Refer to your third party documentation for instructions on matching these code numbers to the operations you want.

The SNMP trap code is a 32-bit number consisting of four 8-bit bytes that represent the following:

- Slot hosting the entity that generated the trap. Slots in the BLN are numbered from 1 to 5 from the base to the top.
- Severity associated with the trap (e.g., FAULT, WARNING, TRACE, or INFO). The previous section defines the severity levels. Table 2-1 lists the codes associated with these levels.

Table 2-1.Trap Severity Codes

Severity	Code
INFO	2
WARNING	4
FAULT	8
TRACE	10

- Entity that generated the trap. Table 2-2 lists the entity codes.
- Trap. Event codes appear below the event text for each event in this chapter. The event log displays these event codes with the event text (see the previous section for an example). Refer to the events in this chapter for the event codes.

Table 2-2. Trap Entity Codes

Entity	Code	Entity	Code
ARP	19	NVFS (Non-Volatile File System	11
AT (AppleTalk)	36	OSPF	12
BOOT	22	SMDS	24
CSMACD	9	SNMP	3
DECNET	4	SPAN (Spanning Tree)	16
DP (Data Path)	6	SR (Source Routing)	29
E1	35	SYNC	20
FDDI	8	T1	34
FR (Frame Relay)	25	TBL	14
GAME	5	TF (Traffic Filters)	15
HSSI	27	TFTP	7
HWF (Hardware Filters)	37	TI (Technician Interface)	0
IP	2	TI_RUI (Site Manager-TI interface	18
IPX	30	TOKEN (Token Ring)	26
LB (Learning Bridge	1	TTY	17
MIB	13	VINES	23
MODULE	21	XNS	31

For example, the following event issued by the CSMACD (Carrier Sense Multiple Access/Carrier Detect) entity may be configured as an SNMP trap:

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The CSMACD driver experienced a fatal error and is restarting automatically. CSMACD will attempt to restart up to five times.

Action: Verify the configuration is correct. Determine if the FAIL LED on each Link Module is off. Call Customer Support if CSMACD fails to restart.

Figure 2-7 is a sample SNMP trap that indicates the following:

- An entity running on slot 3 issued the trap.
- The severity code (8) indicates the trap is a FAULT.
- The entity (9) issuing the trap is CSMACD.
- The event code (1) uniquely identifies the event shown above.

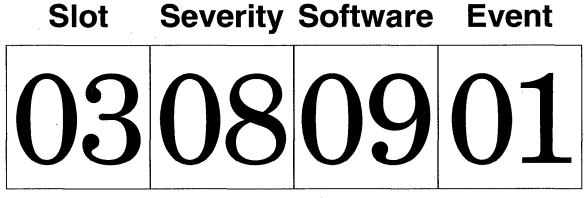


Figure 2-7. Sample SNMP Trap

AppleTalk Events

The following event messages are issued by the AppleTalk router entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

AppleTalk panic: <fatal_error_message>

Event Code: 01

Severity: Fault

Meaning: The AppleTalk router experienced the fatal error <fatal_error_message> and is restarting automatically. The AppleTalk router will attempt to restart up to five times.

Action: Verify that the configuration is correct. Call Customer Support if the AppleTalk router fails to restart.

Warning Events

A zip reply had a net number <Network_ID> not found in rtmp table on circuit <circuit>

Event Code: 37

Severity: Warning

Meaning: The AppleTalk router received a ZIP reply containing network number <Network_ID> which is not present on the router's RTMP table for this interface. This could occur if the network is unstable.

Action: None.

Bad distance <distance> for net <Network_ID> from <Network_ID>.<Node_ID>

Event Code: 33

Severity: Warning

Meaning: The AppleTalk router received an RTMP packet from router <Network_ID>.<Node_ID> specifying an illegal hop count of between 16 and 30. A valid hop count is between 0 and 15.

Action: Check the configuration of the originating router.

Bad net range <network_start_no.> - <network_end_no.> from <Network_ID>.<Node_ID>

Event Code: 31

Severity: Warning

Meaning: The AppleTalk router received an RTMP packet from router <Network ID>.<Node ID> that contained an illegal network range.

Action: Check the configuration of the originating router.

Bad non extended net <Network_ID> from <Network_ID>.<Node_ID>

Event Code: 32

Severity: Warning

Meaning: The AppleTalk router received an RTMP packet from router <Network_ID> .<Node_ID> that contained an illegal network number.

Action: Check the configuration of the originating router.

Bad zip reply

Event Code: 42

Severity: Warning

Meaning: The AppleTalk interface received a malformed ZIP reply packet.

Action: None.

Could not get complete zone list

Event Code: 27

Severity: Warning

Meaning: The AppleTalk router could not get the entire zone list from the seed router to which it sent out a GetnetInfo request. This can only happen if the router fails, or if the router is configured on a highly unstable network.

Action: Reenable the AppleTalk interface.

Couldn't add default zone

Event Code: 25

Severity: Warning

Meaning: The AppleTalk router could not add the default zone specified for this network to its zone list. This could be caused by lack of memory on the slot.

Action: None

Default zone - seed conflict

Event Code: 39

Severity: Warning

Meaning: When the AppleTalk interface initialized, a seed router was configured with a default zone that was different than the default zone configured for other routers.

Action: Check the configuration of the seed routers on the network.

Failed adding local net - no buffers

Event Code: 30

Severity: Warning

Meaning: This slot is running low on buffers, probably due to excessive traffic.

Action: None.

GNI Timeout - No NetInfoReply received

Event Code: 26

Severity: Warning

Meaning: An AppleTalk interface that is configured as a nonseed router sent out GetNetInfo packets but did not receive a valid GetNetInfo reply in the time allowed (6 seconds)

Action: Every network must contain at least one seed router; make certain that a seed router is configured on this network.

GetNetInfo reply: bad multicast length

Event Code: 38

Severity: Warning

Meaning: A GetNetInfo reply received by the AppleTalk router contained an invalid multicast length (the valid length for Token Ring and Ethernet is 6; the valid length for SMDS is 8).

Action: Check the configuration of the originating router.

Getnetinfo reply: zone should have been null

Event Code: 24

Severity: Warning

Meaning: Another AppleTalk router sent an incorrect response to this router's GeNetInfo request.

Action: Check to see if the other router is misconfigured.

Illegal net range <network_start_no.> - <network_end_no.> for circuit < circuit>

Event Code: 15

Severity: Warning

Meaning: The circuit <circuit> has been configured with a network range that is invalid.

Action: Assign a valid network range using the AppleTalk router's Network Start and Network End parameters, then reenable the interface. See the chapter entitled *Configuring AppleTalk* in the *Configuring System Software* guide for instructions.

Illegal network number <Network_ID> for circuit <circuit>

Event Code: 17

Severity: Warning

Meaning: The circuit <circuit> has been assigned an illegal network number <Network_ID>.

Action: Assign a valid network number to the circuit, then reenable the interface. See the chapter entitled *Configuring AppleTalk* in the *Configuring System Software* guide for instructions.

Illegal node id in aarp response <response_no.>

Event Code: 14

Severity: Warning

Meaning: The AppleTalk router received an illegal response (one that specified 0 or FF as the Node ID) in reply to an AARP request.

Action: None. The packet could be corrupted.

Illegal node number <Node_ID> for circuit <circuit>

Event Code: 18

Severity: Warning

Meaning: The circuit <circuit> has been assigned an illegal node number <Node_ID>.

Action: Assign a valid node number to circuit <circuit> then reenable the interface. See the chapter entitled *Configuring AppleTalk* in the *Configuring System Software* guide for instructions.

Invalid zone len <zone_name_length> - zone <first_four_characters_of_zone _name>

Event Code: 36

Severity: Warning

Meaning: The AppleTalk router received an illegal zone name from another router. The zone name length <zone_name_length> is in hexadecimal, as are the first four characters of the zone name <first_four_characters_of_zone name>

Action: Check configuration of all routers on the network.

Local net range conflict

Event Code: 28

Severity: Warning

Meaning: The network range assigned to this router is different than the network range assigned to other routers on the network.

Action: Check the configuration of this router and reconfigure if necessary.

Net or node were zero - dynamically obtaining address for circuit <circuit>

Event Code: 19

Severity: Warning

Meaning: The circuit <circuit> has been statically assigned an illegal address with either the Network ID portion or Node ID portion of the address equal to 0; which is an invalid value for either of these fields.

Action: None. The AppleTalk router will dynamically obtain a valid address for circuit <circuit_no>.

No default zone configured on circuit <circuit>

Event Code: 16

Severity: Warning

Meaning: The circuit <circuit> has not been assigned to a default zone.

Action: Assign the circuit to the default zone specified for this network, then reenable the interface. See the chapter entitled *Configuring AppleTalk* in the *Configuring System Software* guide for instructions.

No free node numbers

Event Code: 23

Severity: Warning

Meaning: No valid node numbers are available for use by circuits connecting to this network.

Action: Reduce the number of AppleTalk nodes on the network, or increase the size of the network range. (For example, if the network range is 2-3, increase it to 2-4).

Number of zones on extended net conflict

Event Code: 40

Severity: Warning

Meaning: When the AppleTalk interface initialized, a seed router was configured with a total zone count for this network that was different than the total zone count configured on other routers.

Action: Check the configuration of the seed routers on the network.

Range overlap <network_start_no.> - <network_end_no.> from <Network_ID> .<Node_ID>

Event Code: 34

Severity: Warning

Meaning: The AppleTalk router received an RTMP packet from router <Network_ID> .<Node_ID> containing a network range <network_start_no.> - <network_end_no.> that overlapped with an existing network range.

Action: Check the configuration of the originating router.

Range type conflict for net <Network_ID> from <Network_ID> .<Node_ID>

Event Code: 35

Severity: Warning

Meaning: The AppleTalk router received an RTMP packet from router <NetworkID>.<Node ID> containing an unexpected range type (either nonextended or extended).

Action: Check the configuration of all routers on the network.

Received invalid BrRq from <Network_ID> .<Node_ID> on circuit <circuit>.

Event Code: 20

Severity: Warning

Meaning: The circuit <circuit> received an invalid broadcast request packet from the node whose AppleTalk address is <Network_ID> .<Node_ID>.

Action: None. The packet could possibly be corrupted.

Received invalid FwdReq from <Network_ID>.<Node_ID> on circuit <circuit>

Event Code: 21

Severity: Warning

Meaning: The circuit <circuit> received an invalid forward request packet from the node whose AppleTalk address is <Network_ID>.<Node_ID>.

Action: None. The packet could possibly be corrupted.

RTMP Timeout - No RTMP DATA recvd

Event Code: 29

Severity: Warning

Meaning: An AppleTalk interface, which is configured as nonseed router, did not receive a response to its RTMP request in the time allowed (6 seconds).

Action: Check the status of other routers on the network, then reenable the AppleTalk interface.

Static configuration conflict - address in use

Event Code: 22

Severity: Warning

Meaning: This circuit has been statically assigned an address that is already in use on the AppleTalk network.

Action: Either assign a new address to this circuit, (checking first to make certain that it is unique on the AppleTalk network) or allow the router to dynamically assign an address to the circuit.

Zone name conflict

Event Code: 41

Severity: Warning

Meaning: When the AppleTalk interface initialized, a seed router found a zone name in a ZIP reply that was not on its local zone list.

Action: Check the configuration of the seed routers on the network.

Trace Events

AARP: node <Network_ID>.<Node_ID> added

Event Code: 06

Severity: Trace

Meaning: The AppleTalk router added the node whose address is <Network_ID>.<Node_ID> to its AARP table.

AARP: node <Network_ID>.<Node_ID> deleted

Event Code: 07

Severity: Trace

Meaning: The AppleTalk router deleted the node whose address is <NetworkID>.<Node ID> from its AARP table.

FWD: entry <Network_ID>.<Node_ID> to <Network_ID>. <Node_ID> came up

Event Code: 10

Severity: Trace

Meaning: The AppleTalk router added the nodes <Network_ID>.<Node_ID> - <Network_ID>.<Node_ID> to its forwarding table.

FWD: entry <Network_ID>.<Node_ID> to <Network_ID>.<Node_ID> went down

Event Code: 11

Severity: Trace

Meaning: The AppleTalk router deleted the nodes <Network_ID>.<Node_ID> -<Network_ID> .<Node_ID> from its forwarding table.

RTMP: net <network_start_no.> - <network_end_no.> came up

Event Code: 08

Severity: Trace

Meaning: The AppleTalk router added the network <network_start_no.> - <network_end_no.> to its RTMP table.

RTMP: net <network_start_no.> - <network_end_no.> went down

Event Code: 09

Severity: Trace

Meaning: The AppleTalk router deleted the network <network_start_no.> - <network_end_no.> from its RTMP table.

ZIP: entry <zone_name> on net <Network_ID> came up

Event Code: 12

Severity: Trace

Meaning: The AppleTalk router added zone <zone_name> on network <Network_ID> to its Zone Information Table.

ZIP: entry <zone_name> on net <Network_ID> went down

Event Code: 13

Severity: Trace

Meaning: The AppleTalk router deleted zone <zone_name> on network<Network_ID> from its Zone Information Table.

Info Events

Interface <Network_ID>.<Node_ID> down on circuit <circuit>

Event Code: 03

Severity: Info

Meaning: The circuit identified by <circuit> has become disabled thus disabling AppleTalk routing service to the interface. The interface's AppleTalk address is <Network_ID>.<Node_ID>.

Interface <Network_ID>.<Node_ID> up on circuit <circuit>

Event Code: 02

Severity: Info

Meaning: The circuit identified by <circuit> has become enabled thus providing AppleTalk routing service to the interface. The interface's AppleTalk address is <Network_ID>.<Node_ID>.

Protocol initializing

Event Code: 04

Severity: Info

Meaning: AppleTalk routing is initializing.

Protocol terminating

Event Code: 05

Severity: Info

Meaning: AppleTalk routing is terminating.

ARP Events

The following event messages are issued by the ARP (Address Resolution Protocol) entity.

Info Events

Service is down on circuit <circuit>

Event Code: 02

Severity: Info

Meaning: ARP is no longer providing service to the specified circuit.

Service is up on circuit <circuit>

Event Code: 01

Severity: Info

Meaning: ARP is providing service to the specified circuit.

BOOT Events

The following event messages are issued by the BOOT entity. Event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The boot server experienced a fatal error and is restarting automatically. It will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the router fails to boot.

Warning Events

Boot client could not acquire a buffer

Event Code: 14

Severity: Warning

Meaning: The boot client could not acquire a buffer due to a buffer shortage.

Action: Reset the slot that received this warning.

Boot image <image_name> is not in executable format

Event Code: 09

Severity: Warning

Meaning: The boot server detects a formatting error in the boot image.

Action: Restore the boot image and try to boot again.

Checksum error encountered in image '<image_name>'

Event Code: 11

Severity: Warning

Meaning: The boot server detected a checksum error in the boot image.

Action: Restore the boot image.

Checksum failure: expected = <checksum_read>, actual = <checksum_calculated>, retrying...

Event Code: 20

Severity: Warning

Meaning: The boot client detected a checksum error and is restarting the boot process with a boot server. The slot that produced this warning will become a boot client, and will boot itself after receiving an image from a boot server on another slot.

Client received unexpected opcode <operation_code>, expected <operation_code>

Event Code: 22

Severity: Warning

Meaning: The boot client received an unexpected response from the boot server during the boot process. The boot client ignores the response and the boot process continues.

Decompressor encountered a bad compressed image checksum

Event Code: 24

Severity: Warning

Meaning: The boot server detected an image checksum error before decompressing a compressed image. The slot that generated this warning will become a boot client and boot itself after receiving an image from a boot server on another slot.

Decompressor encountered a bad uncompressed image checksum

Event Code: 25

Severity: Warning

Meaning: The boot server detected an image checksum error after decompressing a compressed image. The slot that generated this warning will become a boot client and boot itself after receiving an image from a boot server on another slot.

Error encountered during reading of boot image

Event Code: 08

Severity: Warning

Meaning: The boot server cannot read the boot image.

Action: Restore the boot image and try to boot again.

Named boot specified, but not for this volume

Event Code: 05

Severity: Warning

Meaning: A named boot procedure was initiated on a Wellfleet router that has more than one Flash memory card. All slot(s) that have Flash cards, but are not involved in the boot procedure, generate this warning.

Server received unexpected opcode <operation_code>, expected <operation_code>

Event Code: 23

Severity: Warning

Meaning: The boot server received an unexpected request from the boot client during the boot process. The boot server ignores the request and the boot process continues.

Slot <slot_no.> bootstrap has incompatible revision <old_release_ID>, upgrade to <new_release_ID>

Event Code: 02

Severity: Warning

Meaning: The boot server detected that the boot image is not up to date.

Action: Upgrade the bootstrap PROMS on the slot <slot_no.> to the current release.

Bridge Events

The following event messages are issued by the Bridge entity. Event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The Bridge experienced a fatal error and is restarting automatically. The Bridge will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the Bridge fails to restart.

Trace Events

MAC addr <source_address> learned by cct <circuit_1> from cct <circuit_2>.

Event Code: 07

Severity: Trace

Meaning: A packet containing <source address> has been received on <circuit_2>, and the forwarding table for <circuit_1> has been duly modified.

Info Events

Bridge port <circuit> changing state to <state>.

Event Code: 06

Severity: Trace

Meaning: The port on the specified circuit will be transitioned to the identified state.

Interface down on circuit <circuit>.

Event Code: 05

Severity: Info

Meaning: The Bridge has gone down on the specified circuit.

Interface up on circuit <circuit>.

Event Code: 04

Severity: Info

Meaning: The Bridge has come up on the specified circuit.

Service initializing.

Event Code: 02

Severity: Info

Meaning: The Bridge is initializing.

Service terminating.

Event Code: 03

Severity: Info

Meaning: The Bridge is terminating.

Frame Relay Events

This section describes how to read a frame relay event log entry and lists all events. Each event is accompanied by a description and a recommended response if one is required.

Fault Event

System error, service attempting restart.

Event Code:	10
Severity:	Fault
Meaning:	Frame relay experienced a fatal error and is restarting automatically. Frame relay will attempt to restart up to five times.
Action:	Verify the configuration is correct. Call Customer Support if frame relay fails to restart.

Warning Events

cct <circuit_number>: Address length invalid of specified address type.

Event Code:	07
Severity:	Warning
Meaning:	Frame Relay has found a configuration error in the record for the specified circuit. This message generally indicates that extended (two or three byte) addressing has been paired with an address type (for example Q921) that does not support address extension. This error should only be seen if the configuration was done with the TI. The Site Manager guards against such improper association.
Action:	Repair the configuration record.

cct <circuit_number>: DLCMI process receiving non-DLCMI messages.

Event Code: 05

Severity: Warning

Meaning: The DLCMI is receiving data messages.

Action: Call Wellfleet Customer Support as this condition is symptomatic of serious problems in driver processing.

Excessive DLCMI errors on cct <circuit_number>.

Event Code: 06

Severity: Warning

Meaning: Frame Relay has taken down the specified circuit because of excessive errors, as measured by the Error Threshold and Monitored Events configuration parameters.

Action: None may be required as Frame Relay will monitor the line for quality and attempt to restart. If condition persists check the integrity of the physical connection.

cct <circuit_number>: Invalid Address encoding type.

Event Code: 08

Severity: Warning

Meaning: Frame Relay has found a configuration error in the record for the specified circuit, namely an unknown address type. This message generally indicates that the configuration was done via the TI as Site Manager enforces correct typing.

Action: Repair the configuration

Service configured but disabled for circuit <circuit_name>.

Event Code: 04

Severity: Warning

Meaning: Frame Relay is configured on the synchronous interface which supports the specified circuit. However, the Frame Relay DLCMI MIB entry is marked disabled.

Action: Use the TI to enable the Frame Relay DLCMI MIB entry to initiate Frame Relay service.

VC <<dlci_#> configured as <pvc_type> but no cct was specified.

Event Code: 09

Severity: Warning

Meaning: The specified Hybrid or Direct (as identified by <pvc_type> PVC has been configured, but not associated with a circuit. This error should only be seen if the configuration was done with the TI. The Site Manager guards against such improper association.

Action: Repair the configuration.

Trace Events

cct <circuit_number>: adding new over old pvc - <dlci_no.> - <state>.

Event Code: 17

Severity: Trace

Meaning: Frame Relay has received a status message from DLCMI that notes as new an already existing PVC, identified by <dlci_no.>. The PVC state is noted as Active or Inactive.

Action: None required.

cct <circuit_number>: Can't add signalling DLCI <dlci_no.>. Entry is deleted.

Event Code: 20

Severity: Trace

Meaning: The user has attempted to add DLCI 0 or 1023 to the specified Frame Relay interface. These DLSI's are reserved for network signalling. Note that Site Manager does not allow the user designation of either of these dlci's.

Action: None required as Frame Relay does not honor the user request.

cct <circuit_number>: DLCI <dlci_no.> out of range in PVC status IE.

Event Code: 45

Severity: Trace

Meaning: Frame Relay has received a status message containing a PVC in which the information element (IE) was not within valid bounds.

Action: Check the Frame Relay switch.

cct <circuit_number>: DLCI <dlci_no.> out of range - invalidated.

Event Code: 19

Severity: Trace

Meaning: The user has added a PVC which is not within the allowable range specified by the addressing format.

Action: None required as Frame Relay does not honor the user request.

cct <circuit_number>: DLCI extract failed for a <pkt_type>.

Event Code: 39

Severity: Trace

Meaning: Frame Relay received a packet with an improperly formatted dlci address. <pkt_type> indicates the packet type, either a data packet or a dlcmi status message.

Action: None is required as Frame Relay discards the frame.

cct <circuit_number>: DLCI message has invalid type - 0x<type>.

Event Code: 29

Severity: Trace

Meaning: Frame Relay received a DLCMI message other than a status or status enquiry type (or status update if LMI is present). The <type> field contains the received hexadecimal value of the received report. type.

Action: Verify the integrity of the Frame Relay switch.

cct <circuit_number>: DTE not receiving our seq number.

Event Code: 34

Severity: Trace

Meaning: Frame Relay is responding to status enquiries from the switch, but the switch (functioning as DTE) is not responding with the correct sequence number.

Action: Verify the integrity of the Frame Relay switch. This event is quite rare and will probably be seen only in testing and set-up.

cct <circuit_number>: DTE sequence number mismatch.

Event Code: 33

Severity: Trace

Meaning: The switch (functioning as DTE) has transmitted an enquiry with an unexpected sequence number.

Action: Verify the integrity of the Frame Relay switch. This event is quite rare and will probably be seen only in testing and set-up.

cct <circuit_number>: IE 0x<IE_value> is too short. Not used.

Event Code: 46

Severity: Trace

Meaning: Frame Relay encountered a status message which contained an information element (IE) of less than expected length.

Action: None is required as Frame Relay drops the message. If the error repeats, check the integrity of the Frame Relay switch.

cct <circuit_number>: Illegal mode change to <mode> for dlci <dlci_#>. Not performed.

Event Code: 22

Severity: Trace

Meaning: The specified dlci was changed to an unrecognized mode value (not direct, hybrid, or group). This event is only encountered when VC's are configured with the TI, as Site Manager prohibits the assignment of other than the three recognized modes.

Action: Repair the configuration.

cct <circuit_number>: Illegal state change to <state> for dlci <dlci_#>. Not performed.

Event Code: 21

Severity: Trace

Meaning: The specified dlci was changed to an unrecognized state value (not active, inactive, or invalid). This event is only encountered when VC's are configured with the TI, as Site Manager prohibits the assignment of other than the three recognized states.

Action: Repair the configuration.

cct <circuit_number>: Invalid call reference found - 0x<hex_value>.

Event Code: 26

Severity: Trace

Meaning: DLCMI has received a frame with a non-null call reference value on the specified circuit. <hex_value> contains the first, and possibly only, byte of the invalid call reference value.

Action: None is required as Frame Relay discards the frame. If the error persists, verify the integrity of the switch.

cct <circuit_number>: Invalid discriminator found - 0x<hex_value>.

Event Code: 25

Severity: Trace

Meaning: DLCMI has received a packet with an invalid discriminator field on the specified circuit. The contents of the received filed are contained in <hex_value>. Valid discriminator field contents are 0x9 for LMI, and 0x8 for both Annex A and Annex D.

Action: None is required as Frame Relay discards the frame.

cct <circuit_number>: Invalid locking shift found - 0x<hex_value>.

Event Code: 27

Severity: Trace

Meaning: Annex D DLCMI has received a frame with an invalid locking shift indicator on the specified circuit.

Action: None is required as Frame Relay discards the frame.

cct <circuit_number>: No master DLCMI entry for <master_circuit_no.>.

Event Code: 43

Severity: Trace

Meaning: The specified hybrid or direct access PVC is unsupported by a MIB entry for the enabling ("master") Frame Relay interface specified by <master_circuit_no.>.

Action: Repair the configuration. If the error persists, call Wellfleet Customer Support.

cct <circuit_number>: Outgoing pkt dropped; no header space.

Event Code: 42

Severity: Trace

Meaning: A bridged frame was dropped from the specified circuit because of insufficient space to add Frame Relay encapsulation.

cct <circuit_number>: pkt length error - <short/long>.

Event Code: 40

Severity: Trace

Meaning: Frame Relay received a packet on the specified circuit that was either too long or too short.

cct <circuit_number>: PVC IEs out of order.

Event Code: 37

Severity: Trace

Meaning: Frame Relay received a full status message on the specified circuit that failed to list PVCs in ascending order as is required by the standards.

Action: Frame Relay ignores the full status message.

cct <circuit_number>: Status message not received within time out.

Event Code: 36

Severity: Trace

Meaning: The Frame Relay switch failed to respond to a status enquiry transmitted on the specified circuit within the timeout period.

Action: If the error persists, check the connector to the Frame Relay switch; also verify that Frame Relay and the switch agree on the DLCMI type.

cct <circuit_number>: Status msg error; Bad Report Type or Keep Alive IE.

Event Code: 28

Severity: Trace

Meaning: A DLCMI frame was received which contained either an error in the Report type or Keep Alive information element (IE), or in which these two elements were out of order in a status enquiry message.

Action: None is required as Frame Relay discards the frame.

cct <circuit_number>: Switch not receiving our seq number.

Event Code: 31

Severity: Trace

Meaning: The sequence number that the Frame Relay switch returned as the last received sequence number is not what Frame Relay last sent.

Action: Probably none is required as the switch may have erred in its sequence number acceptance processing. The message is dropped and ignored.

cct <circuit_number>: Switch sequence number mismatch.

Event Code: 30

Severity: Trace

Meaning: Frame Relay received an unexpected sequence number from the Frame Relay switch.

Action: Probably none is required as Frame Relay may have missed the switch's last transmission or the switch may be resetting.

cct <circuit_number>: Switch sequence number mismatch during recovery - accepted.

Event Code: 32

Severity: Trace

Meaning: Frame Relay received a status message that contained an unexpected sequence number from the Frame Relay switch.

Action: Probably none is required as Frame Relay may have missed the switch's last transmission or the switch may be resetting.

cct <circuit_number>: Unknown IE found 0x<hex_value>.

Event Code: 38

Severity: Trace

Meaning: DLCMI has received an unknown/unsupported information element (IE) value, contained in <hex_value>, on the specified circuit. Supported IE values are: for LMI and Annex D — 05 (multicast status) and 07 (PVC status); for Annex A — 57 (PVC status).

Action: Investigate a mismatch between DTE/DCE processing.

cct <circuit_number>: Unknown report type 0x<hex_value>.

Event Code: 35

Severity: Trace

Meaning: DLCMI has received a frame, on the specified circuit, which contains an unknown Report type value, contained in <hex_value>. Supported Report type values are: for LMI and Annex A — 00 (full status) and 01 (sequence number exchange); for Annex D — 00 (full status), 01 (link interface), and 02 (single PVC).

cct <circuit_number>: unsupported control 0x<hex_value>.

Event Code: 41

Severity: Trace

Meaning: Frame Relay has received a data packet whose control field is other than Unnumbered Information. <hex_value> contains the first byte of the erroneous control.

Action: Frame Relay discards the packet.

cct <circuit_number>: Unsupported Management Type <type_value>.

Event Code: 24

Severity: Trace

Meaning: Frame Relay has found a configuration error in the record for the specified circuit. This message generally indicates that the configuration was done via the TI as Site Manager enforces correct typing.

Action: Repair the configuration.

cct <circuit_number>: VC <dlci_no.> added - <state>.

Event Code: 13

Severity: Trace

Meaning: The specified DLCI has been added by the user or by DLCMI to the specified Frame Relay interface. <state> specifies the DLCI state, Active, Inactive, or (for LMI only) XOFF.

cct <circuit_number>: VC <dlci_no.> changed to <state>.

Event Code: 15

Severity: Trace

Meaning: The user or DLCMI has changed the state of the specified PVC to either Active, Inactive, or (for LMI only) XOFF.

cct <circuit_number>: VC <dlci_no.> deleted.

Event Code: 12

Severity: Trace

Meaning: The user or DLCMI has deleted the specified PVC.

cct <circuit_number>: VC <dlci_no.> has been initialized - <state>.

Event Code: 23

Severity: Trace

Meaning: The specified PVC has initialized in the specified state. Note that this event will be logged only for those PVCs which are explicitly configured by the user (hybrid and direct PVCs).

cct <circuit_number>: VC <dlci_no.> has been re-added - <state>.

Event Code: 18

Severity: Trace

Meaning: DLCMI has added the specified PVC in the specified state. The PVC had previously been listed in the MIB in the Invalid state.

cct <circuit_number>: VC <dlci_no.> is now used as <address_type>.

Event Code: 14

Severity: Trace

Meaning: DLCMI or the user has changed the addressing type (Unicast or Multicast) of the specified DLCI.

cct <circuit_number>: VC <dlci_no.> mode changed to <mode_type>.

Event Code: 16

Severity: Trace

Meaning: The user has changed the access mode (group, direct, hybrid) of the specified DLCI.

No Frame Relay DLCMI entry found for configured circuit <circuit_number>.

Event Code: 11

Severity: Trace

Meaning: The synchronous line is configured to run Frame Relay but the MIB records lacks DLCMI information for the circuit.

Action: Repair the configuration.

Info Events

Service initialized for circuit <circuit_number>.

Event Code: 01

Severity: Info

Meaning: Frame Relay has completed initialization on the specified circuit.

Service recovery for cct <circuit_number>.

Event Code: 03

Severity: Info

Meaning: DLCMI has recovered from an error condition on the specified circuit. After shutting down, DLCMI has received a sufficient number of valid polls to verify the present integrity of the line.

Service terminating for circuit <circuit_number>.

Event Code: 02

Severity: Info

Meaning: Frame Relay has terminated on the specified circuit.

CSMACD Events

The following event messages are issued by the CSMACD (Carrier Sense Multiple Access/Carrier Detect) entity. Event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The CSMACD driver experienced a fatal error and is restarting automatically. CSMACD will attempt to restart up to five times.

Action: Verify the configuration is correct. Determine if the FAIL LED on each Link Module is off. Call Customer Support if CSMACD fails to restart.

Warning Events

Connector XCVR <no.> carrier lost.

Event Code: 02

Severity: Warning

Meaning: The CSMACD entity detected the loss of the carrier signal on the connector identified by XCVR <no.>.

Action: Verify transceiver and physical medium integrity.

Connector XCVR <no.> diagnostic failed.

Event Code: 05

Severity: Warning

Meaning: The CSMACD connector identified by XCVR <no.> failed power-up diagnostics and has been disabled.

Action: Verify the integrity of the Link Module.

Connector XCVR <no.> excessive collisions.

Event Code: 03

Severity: Warning

Meaning: The CSMACD entity dropped a frame after it detected collisions on 16 successive transmission attempts over the connector identified by XCVR <no.>.

Action: If message occurs frequently, investigate and remedy the cause(s) of LAN congestion.

Connector XCVR <no.> no SQE.

Event Code: 07

Severity: Warning

Meaning: The CSMACD entity detected a loss of the Signal Quality Error (SQE or Heartbeat) signal over connector XCVR <no.>.

Action: Verify transceiver integrity.

Connector XCVR <no.> not verified with diagnostic.

Event Code: 08

Severity: Warning

Meaning: Power-up diagnostics aborted and did not verify the CSMA/CD connector identified by XCVR <no.>.

Action: Rerun power-up diagnostics if you wish to verify XCVR <no.> integrity.

Connector XCVR <no.> out of range.

Event Code: 06

Severity: Warning

Meaning: The CSMA/CD connector XCVR <no.> is invalid and will be ignored.

Action: Modify the configuration record to accurately describe the Link Module installed in the specified slot.

Connector XCVR <no.> transmitter time-out.

Event Code: 04

Severity: Warning

Meaning: The CSMA/CD connector identified by XCVR <no.> timed out on transmission after a user-programmable time.

Info Events

Connector XCVR <no.> configuration deleted.

Event Code: 12

Severity: Info

Meaning: The CSMA/CD connector identified by XCVR <no.> has been removed from the configuration.

Connector XCVR <no.> disabled.

Event Code: 10

Severity: Info

Meaning: The CSMA/CD connector identified by XCVR <no.> is disabled.

Connector XCVR <no.> enabled.

Event Code: 11

Severity: Info

Meaning: The CSMA/CD connector identified by XCVR <no.> is enabled.

Connector XCVR <no.> LLC1 service withdrawn.

Event Code: 14

Severity: Info

Meaning: The CSMA/CD connector identified by XCVR <no.> is *not* providing LLC1 service.

Connector XCVR <no.> providing LLC1 service.

Event Code: 13

Severity: Info

Meaning: The CSMA/CD connector identified by XCVR <no.> is enabled and providing LLC1 (datagram) service.

Service initializing.

Event Code: 09

Severity: Info

Meaning: CSMACD is initializing.

DECnet Events

The following event messages are issued by the DECnet entity. Event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Severity: Fault

Meaning: DECnet experienced a fatal error and is restarting automatically. DECnet will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if DECnet fails to restart.

Warning Events

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Bad Packet

Severity: Warning

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the identified circuit) is declared down because it transmitted an erroneous packet.

Action: Verify integrity of the adjacent DECnet node.

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Checksum error

Severity: Warning

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the identified circuit) is declared down because it transmitted a routing topology packet that contained an erroneous checksum.

Action: Verify integrity of the adjacent DECnet node.

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Out of range

Severity: Warning

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the identified circuit) is declared down because its area and/or node address has become corrupted and now exceeds the maximum values configured for these parameters.

Action: Verify address integrity.

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Router Table Full

Severity: Warning

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the identified circuit) is declared down and deleted from the current adjacent router table. The node is deleted because the router table contains the maximum number of entries, and DECnet has detected the presence of a new router on the adjacent network. In such an instance, DECnet checks the "priority" (node number) of the newly detected router, and, if the priority is greater than that of the lowest priority node in the router table, drops the lower-priority node and adds the new router to the table.

Action: Consider setting the NBRA value to its maximum value (33).

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Version skew

Severity: Warning

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the identified circuit) is determined to be down because of a DECnet version mismatch between the local DECnet router and the adjacency.

Action: Reconcile the version mismatch.

Adjacency Rejected Circuit <circuit>, Adjacency=<area>.<node>, Endnode Table Full

Severity: Warning

Meaning: DECnet has detected a previously unknown node (potentially accessible through the identified circuit), whose area and node address is <area>.<node>. DECnet will not establish an adjacency as its Adjacent Endnode Table is full.

Action: Consider setting the NBEA value to its maximum value (1023).

Adjacency Rejected Circuit <circuit>, Adjacency=<area>.<node>, Out of range

Severity: Warning

Meaning: DECnet has detected a router whose address is <area>.<node> (potentially accessible through the identified circuit). DECnet will not establish an adjacency as the newly detected router's area and/or node address exceeds the maximum values configured for these parameters.

Action: Verify address integrity and/or modify the DECnet configuration record.

Adjacency Rejected Circuit <circuit>, Adjacency=<area>.<node>, Router Table Full

Severity: Warning

Meaning: DECnet has detected a router whose address is <area>.<node> (potentially accessible through the identified circuit). DECnet will not establish an adjacency as its Adjacent Router Table is full and the "priority" (node number) of the newly detected router is less than that of the lowest priority node in the table.

Action: Consider setting the NBRA value to its maximum value (33).

Adjacency Rejected Circuit <circuit>, Adjacency=<area>.<node>, Router Table Full - low node id

Severity: Warning

Meaning: DECnet has detected a router whose address is <area>.<node> (potentially accessible through the identified circuit). DECnet will not establish an adjacency as its Adjacent Router Table is filled with higher priority routers.

Action: Consider setting the NBRA value to its maximum value (33).

Adjacency Rejected Circuit <circuit>, Adjacency=<area>.<node>, Router Table Full - low priority

Severity: Warning

Meaning: DECnet has detected a router whose address is <area>.<node> (potentially accessible through the identified circuit). DECnet will not establish an adjacency as its Adjacent Router Table is filled with higher priority routers.

Action: Consider setting the NBRA value to its maximum value (33).

Adjacency Rejected Circuit <circuit>, Adjacency=<area>.<node>, Using this node address

Severity: Warning

Meaning: DECnet has detected an "adjacent" node (potentially accessible through the identified circuit) whose address, <area>.<node>, is identical to DECnet's address. No adjacency is established.

Action: Establish address integrity and/or look for loops in the network topology.

Initialization Failed Circuit <circuit>, Block size <no._bytes> too small

Severity: Warning

Meaning: An adjacent host (potentially accessible over the indicated circuit) failed to complete initialization because of an insufficient configured block size.

Action: Configure the block size of the adjacent node to match the block size of the Wellfleet router.

Multicast address change not allowed on circuit <circuit>

Severity: Warning

Meaning: The circuit <circuit> is not a Frame Relay circuit; thus, statically configuring a multicast address for this circuit is incorrect.

Action: Reconfigure the DECnet circuit and accept the default values for the End Nodes MAC, End Routes MAC and Area Routes MAC parameters.

Static Adjacency rejected Circuit <circuit>, Adjacency=<area>.<node>

Severity: Warning

Meaning: The DECnet router rejected static adjacency entry circuit <circuit>, Adjacency=<area>.<node>.

Action: None

Static Adjacency rejected Circuit <circuit>, Adjacency=<area>.<node>, Table Full

Severity: Warning

Meaning: The DECnet router rejected a static adjacency entry circuit <circuit>, Adjacency=<area>.<node> because its Static Adjacency table is full.

Action: None.

Trace Events

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Address change

Severity: Trace

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the specified circuit) has been declared down because of a type change (that is, from a non-routing to a routing node, or vice-versa).

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Dropped

Severity: Trace

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the specified circuit) has been dropped because it transmitted a faulty *Hello* packet.

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, System resource failure

Severity: Trace

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the specified circuit) is down because of the failure of local resources.

Action: None required as DECnet will repair this transient condition.

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Sync lost

Severity: Trace

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the specified circuit) is down because of circuit failure.

Action: Investigate and repair cause of circuit failure.

Adjacency Down Circuit <circuit>, Adjacency=<area>.<node>, Timeout

Severity: Trace

Meaning: The adjacent DECnet node whose address is <area>.<node> (previously accessible through the specified circuit) is down because the DECnet router failed to receive three consecutive *Hello* packets from the adjacency.

Adjacency Up Circuit <circuit>, Adjacency=<area>.<node>

Severity: Trace

Meaning: The adjacent DECnet node whose address is <area>.<node> (accessible through the specified circuit) is up.

Area Reach Change, Area <area>, Reachable

Severity: Trace

Meaning: The previously unreachable DECnet area has become reachable.

Area Reach Change, Area <area>, Unreachable

Severity: Trace

Meaning: The previously reachable DECnet area has become unreachable.

DRS Traffic Filter - Rule <rule_no.>, Circuit <circuit> (Drop packet)

Severity: Trace

Meaning: A DECnet packet has been dropped in accordance with the specified filter rule.

DRS Traffic Filter - Rule <rule_no.>, Circuit <circuit> (Log only)

Severity: Trace

Meaning: A DECnet packet has been logged in accordance with the specified filter rule.

Node Reach Change, Node <area>.<node>, Reachable

Severity: Trace

Meaning: The previously unreachable DECnet node, whose address is <area>.<node>, has become reachable.

Node Reach Change, Node <area>.<node>, Unreachable

Severity: Trace

Meaning: The previously reachable DECnet node, whose address is <area>.<node>, has become unreachable.

Static Adjacency Up Circuit <circuit>, Adjacency=<area>.<node>

Severity: Trace

Meaning: The DECnet router accepted static adjacency entry circuit <circuit>, Adjacency=<area>.<node>.

Info Events

Interface <area>.<node> down on circuit <circuit>

Severity: Info

Meaning: The interface whose DECnet address is <area>.<node> has gone down on the specified circuit.

Interface <area>.<node> up on circuit <circuit>

Severity: Info

Meaning: The interface whose DECnet address is <area>.<node> has come up on the specified circuit.

Protocol initializing

Severity: Info

Meaning: DECnet is initializing.

Protocol terminating

Severity: Info

Meaning: DECnet is terminating

DP Events

The following event messages are issued by the DP (Data Path) entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: DP experienced a fatal error and is restarting automatically. DP will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if DP fails to restart.

Warning Events

Failure to initialize protocol prioritization.

Event Code: 70

Severity: Warning

Meaning: Protocol prioritization cannot be initialized because of a lack of memory resources.

Action: Reboot. If this fails, you may have to disable some other entity.

Invalid priority returned for Circuit <circuit>

Event Code: 69

Severity: Warning

Meaning: An invalid priority was returned for the specified circuit, probably due to memory corruption or invalid configuration data.

Action: Check your configuration.

Mixed media types on Circuit <circuit>.

Event Code: 09

Severity: Warning

Meaning: There are mixed media types on the specified circuit. This message is a result of a configuration error.

Action: Make sure only one line is configured for a single circuit.

Multiple lines configured on Circuit <circuit>, subsequent lines ignored.

Event Code: 10

Severity: Warning

Meaning: There are multiple lines configured on the specified circuit, and subsequent lines are being ignored. This message is a result of a configuration error.

Action: Make sure only one line is configured for a single circuit.

Protocol prioritization Length Based Filter disabled, cannot use the LBP filter for IP Circuit <circuit>.

Event Code: 68

Severity: Warning

Meaning: A Length Based Filter has been configured for IP. This is not allowed, and therefore the filter has been disabled.

Action: Remove this IP filter and specify IP-specific prioritizations.

Info Events

Bridge Traffic Filter - Rule <filter_rule_no.>, Circuit <circuit>. (Drop packet)

Event Code: 05

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was dropped as specified by the filter.

Bridge Traffic Filter - Rule <filter_rule_no.>, Circuit <circuit>. (Flood packet)

Event Code: 07

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was flooded as specified by the filter.

Bridge Traffic Filter - Rule <filter_rule_no.>, Circuit <circuit>. (Forward to specific circuits)

Event Code: 08

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was forwarded as specified by the filter.

Bridge Traffic Filter - Rule <filter_rule_no.>, Circuit <circuit>. (Log only)

Event Code: 06

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was logged as specified by the filter.

Circuit <circuit> down.

Event Code: 02

Severity: Info

Meaning: The specified circuit has gone down.

Circuit <circuit> up.

Event Code: 03

Severity: Info

Meaning: The specified circuit has come up.

Service initializing.

Event Code: 04

Severity: Info

Meaning: DP is initializing.

E1 Events

This section describes how to read an E1 event log entry and lists all events. Each event is accompanied by a description and a recommended response if one is required.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The E1 driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the E1 driver fails to restart.

Warning Events

Connector E1_<connector_no.> diagnostic failed.

Event Code: 03

Severity: Warning

Meaning: The specified E1 connector failed power-up diagnostics and has been disabled.

Action: Verify the integrity of the E1 link module.

Connector E1_<connector_no.> not verified with diagnostic.

Event Code: 04

Severity: Warning

Meaning: Power-up diagnostics were aborted/terminated prior to verifying the specified E1 connection.

Action: Rerun diagnostics to verify the integrity of the E1 link module.

Connector E1_<connector_no.> out of range.

Event Code: 02

Severity: Warning

Meaning: The E1 connector identified by <connector_no.> is invalid (a value other than 1 or 2) and will be ignored.

Action: Modify the E1 configuration to reflect a connector number of 1 or 2.

Note: This message should not be seen if E1 has been configured via the Site Manager, as the Site Manager checks guards against invalid connector identification.

Connector E1_<connector_no.> unknown state variable value.

Event Code: 05

Severity: Warning

Meaning: The E1 line driver state MIB object (wfE1state) contained an invalid entry. Valid entries are as follows:
1 for UP; 3 for INITializing; and, 4 for NOTPRESENT.

Action: None may be required as E1 will restart the connection.

Info Events

Connector E1_<connector_no.> clock being recovered from port 1.

Event Code: 18

Severity: Info

Meaning: The E1 connector identified by <connector_no.> is recovering the master clock via Port 1.

Connector E1_<connector_no.> clock being recovered from port 2.

Event Code: 17

Severity: Info

Meaning: The E1 connector identified by <connector_no.> is recovering the master clock via Port 2.

Connector E1_<connector_no.> instance record deleted.

Event Code: 06

Severity: Info

Meaning: The E1 record for the connector identified by <connector_no.> has been deleted from the configuration.

Connector E1_<connector_no.> line disabled.

Event Code: 07

Severity: Info

Meaning: E1 service has been disabled on the connector identified by <connector_no.>.

Connector E1_<connector_no.> line enabled.

Event Code: 08

Severity: Info

Meaning: E1 service has been enabled on the connector identified by <connector_no.>.

Connector E1_<connector_no.> providing framer service.

Event Code: 09

Severity: Info

Meaning: E1 is enabled and providing service on the connector identified by <connector_no.>.

Connector E1_<connector_no.> remote alarm active.

Event Code: 11

Severity: Info

Meaning: E1 has received a message indicating an alarm condition has been declared/generated by the network/CPE equipment.

Connector E1_<connector_no.> remote alarm cleared.

Event Code: 16

Severity: Info

Meaning: The condition which generated a previously transmitted alarm message has been rectified.

Connector E1_<connector_no.> remote alarm clearing.

Event Code: 15

Severity: Info

Meaning: The condition which generated a previously transmitted alarm message is being rectified.

Connector E1_<connector_no.> remote multiframe alarm active.

Event Code: 12

Severity: Info

Meaning: E1 has received a Distant Multiframe Alarm signal (issued when bit 6 of time slot 16 in frame 0 is set for 3 consecutive frames).

Connector E1_<connector_no.> remote multiframe alarm cleared.

Event Code: 21

Severity: Info

Meaning: The condition which generated a previously transmitted multiframe alarm message has been rectified.

Connector E1_<connector_no.> remote multiframe alarm clearing.

Event Code: 20

Severity: Info

Meaning: The condition which generated a previously transmitted multiframe alarm message is being rectified.

Connector E1_<connector_no.> sync loss condition clearing.

Event Code: 13

Severity: Info

Meaning: Signal resync is in progress.

Connector E1_<connector_no.> sync loss condition deactivated.

Event Code: 14

Severity: Info

Meaning: Signal resync has been completed.

Connector E1_<connector_no.> Sync loss detected.

Event Code: 10

Severity: Info

Meaning: Framing sequence has been lost.

Service initializing.

Event Code: 19

Severity: Info

Meaning: E1 is initializing.

FDDI Events

This section describes how to read an FDDI event log entry and lists all events. Each event is accompanied by a description and a recommended response if one is required.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The FDDI driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the FDDI driver fails to restart.

Warning Events

Node <FDDI_connector_no.> claim initiated (TVX or LateCt).

Event Code: 18

Severity: Warning

Meaning: Station Management (SMT) has initiated the token claim process triggered by the expiration of TVX.

Action: This is a normal event when the station has not seen the token in given period of time.

Node <FDDI_connector_no.> diagnostic failed.

Event Code: 03

Severity: Warning

Meaning: The specified FDDI connector failed power-up diagnostics and has been disabled.

Action: Verify the integrity of the FDDI link module.

Node <FDDI_connector_no.> directed beacon received.

Event Code: 16

Severity: Warning

Meaning: Station Management (SMT) received a directed beacon frame.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> duplicate address detected.

Event Code: 19

Severity: Warning

Meaning: Station Management (SMT) detected another ring member using the identical MAC address.

Action: Resolve the duplicate address.

Node <FDDI_connector_no.> generating directed beacons.

Event Code: 14

Severity: Warning

Meaning: Station Management (SMT) fault recovery software is generating/transmitting beacon frames.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> LCT reject <local | remote | both> on PHY <A | B>.

Event Code: 09

Severity: Warning

Meaning: The Link Confidence Test (LCT) has rejected Station Management (SMT) on the specified physical connector

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> LEM reject on PHY <A | B>.

Event Code: 08

Severity: Warning

Meaning: The Link Error Monitor(LEM) has rejected Station Management (SMT) on the specified physical connector

Action: Text the link quality. Clean and reseat the FDDI connector.

Node <FDDI_connector_no.> link fault.

Event Code: 23

Severity: Warning

Meaning: Station Management (SMT) cannot generate directed beacons or jam beacons because SMT is already in the beaconing state.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> link unavailable.

Event Code: 25

Severity: Warning

Meaning: Station Management (SMT) found that the link has become unavailable because of a ring fault.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> MAC beaconing initiated (TRT).

Event Code: 17

Severity: Warning

Meaning: Station Management (SMT) has initiated beaconing triggered by the expiration of the TRT timer.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> not verified with diagnostic.

Event Code: 05

Severity: Warning

Meaning: Power-up diagnostics were aborted/terminated prior to verifying the specified FDDI connection.

Action: Rerun diagnostics to verify the integrity of the FDDI link module.

Node <FDDI_connector_no.> out of range.

Event Code: 04

Severity: Warning

Meaning: The configured FDDI connection is invalid and will be ignored.

Action: Repair the configuration record to provide a valid connection value.

Node <FDDI_connector_no.> PC trace initiated.

Event Code: 11

Severity: Warning

Meaning: The PC (Physical Connection) trace function, which provides a recovery mechanism for stuck Beacon conditions on the ring, has been initiated.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> PC trace path test.

Event Code: 12

Severity: Warning

Meaning: FDDI has initiated a Physical Connection (PC) path test to determine if there is a faulty MAC or datapath on the ring.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> PC trace received.

Event Code: 13

Severity: Warning

Meaning: FDDI has received and is repeating a Physical Connection (PC) trace signal. Reception of a PC trace signal indicates that the other end of the link has initiated PC trace after detecting a stuck Beacon condition.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> PHY <A | B> disconnected.

Event Code: 24

Severity: Warning

Meaning: The specified physical connection has failed. The physical connection is considered disconnected if the Physical Connection Management (PCM) state machine transitions from the Active to the Break state. Consequently, this message is not necessarily an indication of a faulty or disconnected physical connector.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> SMT failed initialization.

Event Code: 06

Severity: Warning

Meaning: Station Management (SMT) cannot be initialized on the specified FDDI connection.

Action: Restart the FDDI slot.

Node <FDDI_connector_no.> SMT failed to enable station.

Event Code: 07

Severity: Warning

Meaning: Station Management cannot enable dual attachment ports.

Action: Restart the FDDI slot.

Node <FDDI_connector_no.> SMT link database initialization failed.

Event Code: 21

Severity: Warning

Meaning: The Station Management (SMT) link database is corrupted.

Action: Restart the FDDI slot.

Node <FDDI_connector_no.> SMT PHY <A | B> database initialization failed.

Event Code: 22

Severity: Warning

Meaning: The specified Station Management (SMT) PHY database is corrupted.

Action: Restart the FDDI slot.

Node <FDDI_connector_no.> SMT station database initialization failed.

Event Code: 20

Severity: Warning

Meaning: The Station Management (SMT) station database is corrupted.

Action: Restart the FDDI slot.

Node <FDDI_connector_no.> SMT unknown response frame.

Event Code: 10

Severity: Warning

Meaning: Station Management (SMT) has received an unexpected response frame.

Action: The station automatically returns to an operational state unless the ring is broken or a fatal error occurs.

Node <FDDI_connector_no.> stopping directed beacons.

Event Code: 15

Severity: Warning

Meaning: FDDI has ceased the transmission of directed beacons (informing the ring of a stuck Beacon condition) over the specified FDDI connector.

Action: Either the ring will repair itself, or Station Management will initiate Physical Connection (PC) Trace to isolate the fault.

Info Events

Node <FDDI_connector_no.> configuration deleted.

Event Code: 29

Severity: Info

Meaning: The specified FDDI record has been deleted from the configuration.

Node <FDDI_connector_no.> disabled.

Event Code: 27

Severity: Info

Meaning: FDDI service has been disabled on the specified connector.

Node <FDDI_connector_no.> enabled.

Event Code: 28

Severity: Info

Meaning: FDDI service has been enabled on the specified connector.

Node <FDDI_connector_no.> hardware filter enabled.

Event Code: 63

Severity: Info

Meaning: Hardware filtering has been enabled on the specified FDDI connection.

Node <FDDI_connector_no.> link available.

Event Code: 36

Severity: Info

Meaning: The specified FDDI connection is now available for transmission (LLC data frames can now be queued).

Node <FDDI_connector_no.> LLC1 service withdrawn.

Event Code: 31

Severity: Info

Meaning: The specified FDDI connection is no longer providing LLC1 service.

Node <FDDI_connector_no.> PHY <A | B> connected.

Event Code: 35

Severity: Info

Meaning: Station Management (SMT) has placed the specified PHY (A or B) into the Active state and inserted the PHY into the ring.

Node <FDDI_connector_no.> providing LLC1 service.

Event Code: 30

Severity: Info

Meaning: The specified FDDI connection is enabled and providing LLC1 service.

Node <FDDI_connector_no.> SMT services available.

Event Code: 32

Severity: Info

Meaning: Station Management (SMT) is enabled on the specified FDDI connection.

Node <FDDI_connector_no.> station deinserted (bypass on).

Event Code: 33

Severity: Info

Meaning: Station Management (SMT) has switched the optical bypass to remove the station from the ring.

Node <FDDI_connector_no.> station inserted (bypass off).

Event Code: 34

Severity: Info

Meaning: Station Management (SMT) has switched the optical bypass to insert the station into the ring.

Service initializing.

Event Code: 26

Severity: Info

Meaning: FDDI is initializing.

GAME Events

The following event messages are issued by the Gate Access Management Entity (GAME) operating system. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Events

Out of memory

Event Code: 03

Severity: Fault

Meaning: GAME ran out of memory. The slot reboots automatically.

Action: Call Customer Support.

System error, all services attempting restart

Event Code: 04

Severity: Fault

Meaning: GAME detected a fatal error due to an inter- or intra-slot communication failure. All configured entities restart automatically when the condition clears.

Action: Hot-swap the board if the restart does not succeed within one minute.

System error, service attempting restart

Event Code: 01

Severity: Fault

Meaning: An entity on a slot experienced a fatal error and is restarting automatically.

Action: Verify the configuration is correct. Examine the log for other events indicating the cause of the error. Call Customer Support if the event is unexpected or if the entity fails to restart.

Service terminated due to excessive failures

Event Code: 02

Severity: Fault

Meaning: An entity experienced an excessive number of fault events within a short period of time. GAME will not restart the entity.

Action: Verify the configuration is correct. Call Customer Support.

Warning Events

BackBone <PPX_rail_no.> became disconnected

Event Code: 07

Severity: Warning

Meaning: The specified PPX (Parallel Packet Express) rail (channel) is no longer in service. This event occurs as follows:

- When a single processor (slot) reports one or more of these events, it may have run out of buffer space. The *BackBone <PPX_rail_no.> became re-connected* Info event indicates the condition is cleared. If the condition does not clear as

indicated by this message within several seconds, the error may have been caused by a hardware failure. Hot-swap the FRE module on the slot indicated.

- When all processors report this event for both backbones 0 and 1, and do *not* report *BackBone <PPX_rail_no.> became re-connected* for both backbones within several seconds, the event indicates an SRM-F has failed or has been removed. Replace the SRM-F.
- When all processors report this event for backbone 0 or 1 (but not both), and do *not* report *BackBone <PPX_rail_no.> became re-connected* within several seconds, the event indicates an SRM-F hardware error has occurred. Hot-swap the SRM-F.
- When all processors report this event for both backbones 2 and 3, and do *not* report *BackBone <PPX_rail_no.> became re-connected* for both backbones within several seconds, the event indicates an SRM-L has failed or has been removed. Replace the SRM-L.
- When all processors report this event for backbone 2 or 3 (but not both), and do *not* report *BackBone <PPX_rail_no.> became re-connected* within several seconds, the event indicates an SRM-L hardware error has occurred. Hot-swap the SRM-L.

Action: Refer to the items that follow the meaning for the correct action to take.

Slot <slot_no.> became disconnected

Event Code: 08

Severity: Warning

Meaning: The specified slot is no longer in service. This event occurs as follows:

- When all surviving processors report this event for the same slot, the event indicates one of the following:
  - -- A user issued the **reset <slot-number>** command.
  - -- A user hot-swapped a FRE module on the slot indicated.
  - -- A total GAME failure occurred on the slot indicated.

  The *Slot <slot_no.> became re-connected* Info event occurs after the FRE processor boots and initiates entities. Hot-swap the FRE module if it fails to re-connect within one minute.
- When all surviving processors report this event for the same slot, and the *Slot <slot_no.> became re-connected* Info event does *not* occur, the event indicates a FRE module has failed or has been removed. Replace the FRE module.

Action: Refer to the items that follow the meaning for the correct action to take.

Info Events

BackBone <PPX_rail_no.> became re-connected

Event Code: 09

Severity: Info

Meaning: The specified PPX (Parallel Packet Express) rail (channel) is in service.

Slot <slot_no.> became re-connected

Event Code: 10

Severity: Info

Meaning: The specified slot is in service.

Starting image <release_ID> <time_stamp>

Event Code: 11

Severity: Info

Meaning: GAME is initializing with the image specified by the Release_ID at the date and time indicated.

HSSI Events

This section describes how to read an HSSI event log entry and lists all events. Each event is accompanied by a description and a recommended response if one is required.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The HSSI driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the HSSI driver fails to restart.

Warning Events

Connector HSSI<connector_no.> Data Comms Equipment (DCE) unavailable (lost CA).

Event Code: 04

Severity: Warning

Meaning: The DCE-generated CA (Communications Equipment Available) signal has been lost.

Action: Verify the cable connection and the cable integrity. Verify the integrity of the associated DTE equipment.

Connector HSSI<connector_no.> diagnostic failed.

Event Code: 05

Severity: Warning

Meaning: The HSSI connector identified by <connector_no.> failed power-up diagnostics and has been disabled.

Action: Verify the integrity of the HSSI link module.

Connector HSSI<connector_no.> not verified with diagnostic.

Event Code: 07

Severity: Warning

Meaning: The HSSI connector identified by <connector_no.>, has been placed in service. However, power-up diagnostics aborted and did not verify the integrity of the connector.

Action: Rerun power-up diagnostics if you wish to ensure the integrity of the HSSI link module.

Connector HSSI<connector_no.> out of range.

Event Code: 06

Severity: Warning

Meaning: The HSSI connector identified by <connector_no.> is invalid (a value other than 1) and will be ignored.

Action: Modify the HSSI configuration to reflect a connector number of 1.

Note: This message should not be seen if HSSI has been configured via the Site Manager, as the Site Manager checks guards against invalid connector identification.

Connector HSSI<connector_no.> receiver timeout.

Event Code: 03

Severity: Warning

Meaning: HSSI has not received a response to a BofL transmission (sent over the connector identified by <connector_no.>) within the time specified by the BofL timeout timer.

Action: None may be required as HSSI will attempt to restart the connection. If the connection cannot be restarted, verify the integrity of the remote peer and that the remote peer is configured for BofL.

Connector HSSI<connector_no.> transmitter timeout.

Event Code: 02

Severity: Warning

Meaning: HSSI has not received a a BofL transmission on the connector identified by <connector_no.> within the time specified by the BofL timeout timer.

Action: None may be required as HSSI will attempt to restart the connection. If the connection cannot be restarted, verify the integrity of the remote peer and that the remote peer is configured for BofL.

Info Events

Connector HSSI<connector_no.> configuration deleted.

Event Code: 11

Severity: Info

Meaning: The HSSI record for the connector identified by <connector_no.> has been deleted.

Connector HSSI<connector_no.> disabled.

Event Code: 09

Severity: Info

Meaning: The HSSI connector identified by <connector_no.> has been disabled.

Connector HSSI<connector_no.> enabled.

Event Code: 10

Severity: Info

Meaning: The HSSI connector identified by <connector_no.> has been enabled.

Connector HSSI<connector_no.> LLC1 service withdrawn.

Event Code: 13

Severity: Info

Meaning: The HSSI connector identified by <connector_no.> has ceased providing LLC1 service.

Connector HSSI<connector_no.> providing LLC1 service.

Event Code: 12

Severity: Info

Meaning: The HSSI connector identified by <connector_no.> is enabled and providing LLC1 service.

Service initializing.

Event Code: 08

Severity: Info

Meaning: HSSI is initializing.

IP Events

The following event messages are issued by the IP (Internet Protocol) entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: IP experienced a fatal error and is restarting automatically. IP will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if IP fails to restart.

Warning Events

Duplicate IP Address Detected <IP_address>

Event Code: 06

Severity: Warning

Meaning: IP has detected a host on the local network with the same IP address as one of the router's interfaces, identified by <IP_address>. IP detected the address duplication when it ARPed for its own address over the interface in question.

Action: Resolve duplicate addresses by changing either the local interface address or that of the host.

Interface <IP_address> Misconfigured -- Disabled

Event Code: 07

Severity: Warning

Meaning: The IP Interface identified by <IP_address> has been determined to have a configuration error. IP designates the interface as "disabled", and waits for a change in the configuration record before attempting to enable the interface.

Action: Repair the configuration record.

Info Events

Interface <IP_address> down on circuit <circuit>

Event Code: 03

Severity: Info

Meaning: The circuit identified by <circuit> has become disabled thus disabling service to the interface identified by <IP_address>.

Interface <IP_address> up on circuit <circuit>

Event Code: 02

Severity: Info

Meaning: The circuit identified by <circuit> has become enabled thus providing service to the interface identified by <IP_address>.

IP Traffic Filter - Rule <filter_rule_no.>, Interface <IP_address>, Circuit <circuit> (Drop packet)

Event Code: 21

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <IP_address>. The packet was dropped as specified by the filter.

IP Traffic Filter - Rule <filter_rule_no.>, Interface <IP_address>, Circuit <circuit> (Forward to next hop: <IP_address>)

Event Code: 22

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <IP_address>. The packet was forwarded to the specified next-hop router.

IP Traffic Filter - Rule <filter_rule_no.>, Interface <IP_address>, Circuit <circuit> (Log only)

Event Code: 23

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <IP_address>. The packet was logged as specified by the filter.

Protocol initializing

Event Code: 04

Severity: Info

Meaning: IP is initializing.

Protocol terminating

Event Code: 05

Severity: Info

Meaning: IP is terminating.

IPX Events

The following event messages are issued by the IPX entity. Event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: IPX experienced a fatal error and is restarting automatically. IPX will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if IPX fails to restart.

Trace Events

Host <host_address> added to Table of Hosts

Event Code: 09

Severity: Trace

Meaning: The host indicated was added to the table of hosts.

Host <host_address> deleted from Table of Hosts

Event Code: 10

Severity: Trace

Meaning: The host indicated was deleted from the table of hosts.

Network <network_address> added to Table of Networks

Event Code: 07

Severity: Trace

Meaning: The network indicated was added to the table of networks.

Network <network_address> removed from Table of Networks

Event Code: 08

Severity: Trace

Meaning: The network indicated was deleted from the table of networks.

rip_recv received operation <1_or_2> from Host <host_address>

Event Code: 15

Severity: Trace

Meaning: An IPX RIP packet was received from the network and host indicated. Operation 1 indicates the packet is a RIP request. Operation 2 indicates the packet is a RIP response.

rip_update sent Network <target_network_address> hops <no._hops> from Network <source_network_address>

Event Code: 16

Severity: Trace

Meaning: An IPX RIP update packet was sent to the target network indicated.

sap_recv received operation <operation> from Host <host_address>

Event Code: 13

Severity: Trace

Meaning: An IPX SAP packet was received from the network and host indicated.

sap_update sent serv <server_name> type <server_type> on Network <network_address>

Event Code: 14

Severity: Trace

Meaning: An IPX SAP update packet was sent to the server and network indicated.

Server <server_name> type <server_type> added to Table of Services

Event Code: 11

Severity: Trace

Meaning: The server indicated was added to the table of services.

Server <server_name> type <server_type> deleted from Table of Services

Event Code: 12

Severity: Trace

Meaning: The server indicated was deleted from the table of services.

Info Events

ADD Nwif Network <network_address> Host <host_address>

Event Code: 47

Severity: Info

Meaning: The router's full IPX address has been added to the table for an interface.

DEL Nwif Network <network_address> Host <host_address>

Event Code: 48

Severity: Info

Meaning: The router's full IPX address has been deleted from the table for an interface.

IPX on Interface <address> up on circuit <circuit>

Event Code: 04

Severity: Info

Meaning: The interface indicated has come up on the circuit indicated.

IPX on Interface <address> down on circuit <circuit>

Event Code: 05

Severity: Info

Meaning: The interface indicated has gone down on the circuit indicated.

Network <network_address> mapped to cct <circuit>

Event Code: 51

Severity: Info

Meaning: The interface for the network indicated is monitoring the status of the associated circuit.

Nwif from MIB Non-active Network <network_address> Host <host_address>

Event Code: 50

Severity: Info

Meaning: The software has detected that a MIB interface record is inactive.

Nwif from MIB Active Network <network_address> Host <host_address>

Event Code: 49

Severity: Info

Meaning: The record for an interface is active and the IPX routing software has read the information.

Protocol initializing

Event Code: 02

Severity: Info

Meaning: IPX is initializing.

Protocol terminating

Event Code: 03

Severity: Info

Meaning: IPX is terminating.

RTM out of BUFFERS

Event Code: 58

Severity: Info

Meaning: The Routing Table Manager process is out of buffers. This condition will hinder propagation of information to other slots.

Traffic Filter - drop: Rule <filter_rule_no.>, circuit <circuit> Network <network_address> Host <host_address>

Event Code: 56

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was dropped as specified by the filter.

Traffic Filter: Rule <filter_rule_no.>, circuit <circuit>

Event Code: 57

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was dropped as specified by the filter.

MIB Events

The following event messages are issued by the Management Information Base (MIB) entity. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: MIB experienced a fatal error and is restarting automatically. MIB will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if MIB fails to restart.

Warning Event

Configuration file is CORRUPTED, ignoring.

Event Code: 02

Severity: Fault

Meaning: MIB detected that the configuration file was corrupt. MIB will boot with no, or a partial, configuration.

Action: Repair configuration file/install backup file.

Info Events

Opaque object <object><attribute><instance> was set.

Event Code: 11

Severity: Info

Meaning: MIB has set the specified opaque (and consequently non-displayable) variable.

Service initializing.

Event Code: 03

Severity: Info

Meaning: MIB is initializing.

Using config file '<filename>', to populate MIB

Event Code: 04

Severity: Info

Meaning: MIB is using the named configuration file to initialize the management information base.

<object><attribute><instance> set to <value>

Event Code: 05, 06, 07, 08, 09, or 10

Severity: Info

Meaning: MIB has set the specified MIB variable to the indicated value.

Module Events

The following event messages are issued by the Module driver. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The Module driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Determine if the FAIL LED on each Link Module is off. Call Customer Support if the driver fails to restart.

Warning Events

I/O module has been removed.

Event Code: 03

Severity: Warning

Meaning: A hardware module has been removed.

I/O module is not present.

Event Code: 02

Severity: Warning

Meaning: A hardware module, previously installed, is no longer present.

Action: Ensure the hardware module is properly seated in the router or modify the configuration to represent the new module type.

I/O module is the wrong type.

Event Code: 05

Severity: Warning

Meaning: The hardware module-slot number association does not match the software configuration. This is probably due to an error made during a hot swap procedure.

Action: Insert the hardware module in its previous slot or modify the configuration to represent the new module type.

I/O module PROM error.

Event Code: 04

Severity: Warning

Meaning: Module has detected an error with the serial number PROM on the I/O module in the specified slot.

Action: Call Customer Support.

Info Events

<module> I/O module is present.

Event Code: 06

Severity: Info

Meaning: The hardware module indicated, previously removed, is present.

Service initializing.

Event Code: 07

Severity: Info

Meaning: The Module driver is initializing.

NVFS Events

The following event messages are issued by the Non-Volatile File System (NVFS) driver. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: NVFS experienced a fatal error and is restarting automatically. NVFS will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if NVFS fails to restart.

Warning Events

File System is in a corrupt state, re-format.

Event Code: 02

Severity: Warning

Meaning: The files on the flash card are corrupted.

Action: Issue the compact command. If message reappears, issue the erase command and restore the files from a backup file system.

Flash compact failed: error status = <error_code>

Event Code: 03

Severity: Warning

Meaning: The file management system driver failed to execute the compact command. The files or the flash card may be corrupted.

Action: Issue the erase command and restore the files from a backup file system. If erase command fails, replace the flash card and restore the files.

Flash format failed: address = <physical_address>, error status = <error_code>

Event Code: 04

Severity: Warning

Meaning: The file management system driver failed to execute the format command. The flash card may be corrupted.

Action: Replace the flash card and restore the files from a backup file system.

Info Events

Beginning flash compaction process.

Event Code: 07

Severity: Info

Meaning: NVFS is executing a request to compact (concatenate) the file system on a flash card and cannot accept further requests until it terminates the request.

Flash compaction completed.

Event Code: 08

Severity: Info

Meaning: NVFS successfully executed the compact request.

Service initializing.

Event Code: 05

Severity: Info

Meaning: NVFS is initializing.

Service terminating.

Event Code: 06

Severity: Info

Meaning: NVFS is terminating.

OSPF Events

The following event messages are issued by the OSPF (Open Shortest Path First) software entity. The event messages are separated by type and organized alphabetically within each type. Also, please note the following conventions.

If message begins with.....	Message falls into this category
T#	Topological change in routing domain
C1	Packet rejected, errors in IP/OSPF header
C2	Hello packet rejected, mismatch between packet and configured parameters
C3	DD, LS_REQ, LS_ACK, LS_UP packet rejected, source neighbor in wrong state
R#	Router restarted, losing track of previous LS sequence number.

Fault Event

System error, service attempting restart.

Event Code: 32

Severity: Fault

Meaning: OSPF experienced a fatal error and is restarting automatically. OSPF will attempt to restart up to five times.

Action: Call Customer Support if OSPF fails to restart.

Warning Events

C1: Packet Rejected: AREA MISMATCH <area_id> src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 49

Severity: Warning

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because the Area ID field of the OSPF header neither matched the Area ID of the receiving interface nor indicated the backbone (area 0.0.0.0).

Action: This message may indicate a network configuration problem. Check the config file to make sure the proper Area IDs are configured.

C1: Packet Rejected: AUTH KEY <rcvd_key> src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 52

Severity: Warning

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because the Authentication field (whose contents are echoed in <rcvd_Key>) of the OSPF header did not match the authentication key configured for this interface.

Action: This error message may indicate a network configuration problem. Check the config file to make sure the correct key is configured for this interface. If the key is correct, check the configuration of <rtr_IP_address>.

C1: Packet Rejected: AUTH TYPE <rcvd_type> src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 51

Severity: Warning

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because the Authtype field (whose contents are echoed in <rcvd_type>) of the OSPF header did not match the configured type. Authtype values are as follows:

- 0 No authentication
- 1 Simple Password

Action: This error message may indicate a network configuration problem. Check the config file to make sure that the Authtype for this area is the same as that of <rtr_IP_address>.

C1: Packet Rejected: BAD OSPF VERSION ver: <version_no.> src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 47

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because the Version field of the OSPF header contained an unknown or unsupported value, <version_no.r>.

Action: This error message may indicate a network configuration problem. Check your configuration.

C1: Packet Rejected: BAD VIRTUAL INFO
src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 50

Severity: Warning

Meaning: Either no virtual link has been configured for this neighbor and transit area, or there is a faulty configuration on the other side.

Action: Check your config file to make sure that this virtual link's <rtr_IP_address> is the correct nbr_id. If it is not, the <rtr_IP_address> router may be incorrectly configured. If the <rtr_IP_address> is correct, check to see that the config names <rtr_IP_address> to be the neighbor. Also, check that the virtual link transit area is the same as the <area_ID> configured for the interface at each end of the link.

If you have not configured a virtual link for this interface, check the configuration on both routers to make sure the areas are properly configured.

C1: Packet Rejected: CHECKSUM FAILURE
src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 48

Severity: Warning

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because the packet has an incorrect checksum.

Action: This error message may indicate a network configuration problem or faulty lines. Check both your configuration and your lines.

C1: Packet Rejected: IP Hdr: BAD IP DEST
src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 45

Severity: Warning

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because of an incorrect or unknown IP destination address.

Action: This error message may indicate a network configuration problem. Check that the router specified by <rtr_IP_address>, and this router have the same interface type (bcast, pp, nbma). Otherwise, the destination address does not match our configured address.

C1: Packet Rejected: IP Hdr: BAD OSPF PKT TYPE: <type_value> src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 44

Severity: Warning

Meaning: OSPF has rejected a packet originated by OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because the Type field of the OSPF header contained a value other than those which follow.

- ❒ 1 *Hello* Packet
- ❒ 2 *Database Description* Packet
- ❒ 3 *Link State Request* Packet
- ❒ 4 *Link State Update* Packet
- ❒ 5 *Link State Acknowledgment* Packet

Action: Check the neighboring router; it is creating bad packets.

C1: Packet Rejected: IP Hdr: PKT SRC = MY IP ADDR src <src_IP_address> dst <dst_IP_address> routerid <rtr_IP_address>

Event Code: 46

Severity: Warning

Meaning: OSPF has rejected a packet originated by an OSPF router <rtr_IP_address> whose IP source and destinations are specified by <src_IP_address> and <dst_IP_address>. The packet was rejected because IP source address matches the router's own address.

Action: This error message may indicate a network configuration problem; check your configuration.

C2: Hello Rejected: DEAD INTERVAL MISMATCH
src <src_IP_address> (x) interface <IP_address>(y)

Event Code: 55

Severity: Warning

Meaning: OSPF has rejected an incoming *Hello* packet originated by router <src_IP_address> and received on interface <IP_address>. The packet was rejected because the DeadInt field of the *Hello* packet (x) did not match the Dead Interval configured for the interface (y).

Action: Reconfigure the Dead Interval for either this interface, or for the router specified by <src_IP_address>.

C2: Hello Rejected: EXTERN OPTION MISMATCH
src <src_IP_address> (x) interface <IP_address> (y)

Event Code: 56

Severity: Warning

Meaning: OSPF has rejected an incoming *Hello* packet originated by router <src_IP_address> and received on interface <IP_address>. The packet was rejected because the Options field E-bit for the originating router (x), did not match the Options field E-bit for the local router (y).

Action: Determine which router has the incorrect Option E and reconfigure it. The E-bit is set to indicate that the attached area is capable of processing AS external advertisements (that is, it is *not* a stub area). In this message, a value of 0 for (x), indicates that the originating router thinks this area is a stub area. All routers in an area must agree on the setting of the E-bit

C2: Hello Rejected: HELLO INTERVAL MISMATCH
src <src_IP_address> (x) interface <IP_address> (y)

Event Code: 54

Severity: Warning

Meaning: OSPF has rejected an incoming *Hello* packet originated by router <src_IP_address> and received on interface <IP_address>. The packet was rejected because the HelloInt field of the *Hello* packet(x), did not match the Hello Interval configured for the interface (y).

Action: Check the router specified by <IP_address> for configuration problems, or modify the Hello Interval portion of the OSPF interface record for this interface.

C2: Hello Rejected: NETMASK MISMATCH
src <src_IP_address>:<netmask> interface <IP_address>: <netmask>

Event Code: 53

Severity: Warning

Meaning: OSPF has rejected an incoming *Hello* packet originated by router <src_IP_address> and received on interface <IP_address>. The packet was rejected because the Network Mask field of the *Hello* packet did not match the network mask configured for the interface.

Action: Check the router specified by <IP_address> for configuration problems, or modify the Network Mask for this IP network in the IP record.

C2: Hello Rejected: UNKNOWN NBMA NBR
src <IP_src_address> interface <IP_address>

Event Code: 58

Severity: Warning

Meaning: OSPF has rejected an incoming *Hello* packet originated by router <src_IP_address> and received on this non-broadcast multi access interface <IP_address>. The packet was rejected because it was received from an unknown neighbor. NBMA neighbors need to be configured.

Action: The router specified by src <IP_address> has this interface, specified by interface <IP_address>, as it's neighbor. Either add a statically defined neighbor for this interface, or reconfigure the interface type to Broadcast or Point-to-Point.

C2: Hello Rejected: UNKNOWN VIRTUAL NBR
src <src_IP_address> interface <IP_address>

Event Code: 57

Severity: Warning

Meaning: OSPF has rejected an incoming *Hello* packet originated by router <src_IP_address> and received on interface <IP_address>. The packet was rejected because it was received from an unknown virtual neighbor. The interface is down; the virtual link will come up when this neighbor is reconfigured as an area border router.

Action: If you get this message continually, check to make sure that the router specified by <src_IP_address> is properly configured.

C3: Packet Rejected: DD: EXTERN OPTION MISMATCH
src <src_IP_address> interface <IP_address>

Event Code: 62

Severity: Warning

Meaning: OSPF has received and rejected a *Database Description* Packet originated by <src_IP_address> and received on interface <IP_address>. The packet was rejected because the local and originating routers disagree on the state of the Options field E-bit.

Action: Determine which router has the incorrect Option field E-bit by checking each router's configuration. The E-bit is set to indicate that the attached area is capable of processing AS external advertisements (that is, it is *not* a stub area). All routers within an area must agree on the setting of the E-bit.

C3: Packet Rejected: LS REQ: BAD PACKET
src <src_IP_address> type <LS_type>

Event Code: 64

Severity: Warning

Meaning: OSPF has received and rejected a *Link State Request* Packet originated by <src_IP_address>. Either the <LS-type> is bad, or the advertisement cannot be found in the Link State database. If <LS_type> number is 1 though 5, then this LSA was not found in the Link State database. If the <LS_type> number was a number other than 1 through 5, then the type field is bad.<LS_type> normally contains one of five possible values as follows:

- 1 Router links advertisement (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisement (LS_ASE)

Action: If the <LS_type> is one through 5, then the routers are not synchronized. The router specified by <IP_address> is requesting an lsa that had been advertised as being in this routers database. The routers should synchronize soon.

If the <LS_type> is not 1 through 5, then the neighboring router is sending bad packets. Check the neighboring router; it's database may be corrupted.

C3: Packet Rejected: LS REQ: EMPTY REQUEST
src <src_IP_address> Link State Request

Event Code: 63

Severity: Warning

Meaning: OSPF has received and rejected a *Link State Request* Packet originated by <src_IP_address>. The packet was rejected because it contained no data beyond the packet header.

Action: This is just a warning message that the neighboring router has constructed a link state request packet with no contents. If this message continues to be received, check the neighboring router.

C3: Packet Rejected: LS UPDATE: BAD LS CHECKSUM area <area_id> ls_id <LS_ID> adv_rtr <rtr_IP_address> type <type> src <src_IP_address> ls_seq: <seq_no.> ls_age <age> ls_chksum: <value> orig_chk: <value>

Event Code: 65

Severity: Warning

Meaning: OSPF has received and rejected a *Link State Request* Packet originated by <src_IP_address>. The packet was rejected because one of the advertisements contained a faulty checksum value. <LS_type> contains one of the five following values, which indicates the type of advertisement that had the incorrect checksum.

- ❒ 1 Router links advertisement (LS_RTR)
- ❒ 2 Network links advertisement (LS_NET)
- ❒ 3 Network summary links advertisement (LS_SUM_NET)
- ❒ 4 AS boundary summary links advertisement (LS_SUM_ASB)
- ❒ 5 External links advertisement (LS_ASE)

Action: The neighboring router has an advertisement with a bad checksum in it's database. Check the neighboring router for problems. No action is required for this router.

C3: Packet Rejected: LS UPDATE: LESS RECENT RX <self orig lsa/ not my lsa>
src <IP_address> type <LS_type> ls_id: <LS_ID> adv_rtr <IP_address>
ls_seq: ls_age:
db_seq: db_age: elapse:
freeme: ackcnt: nbr_retrans: nbrEcnt: Fcnt:

Event Code: 66

Severity: Warning

Meaning: OSPF has received and rejected a *Link State Update* Packet originated by <src_IP_address>. The Link State Update received is less recent than this advertisement in the currently stored database. This is not an abnormal condition; when routers go up and down, their neighboring routers will contain their database. When the exchange process begins, the neighboring router will advertise the router original database. The routers will soon synchronize.

- *self orig LSA* indicates that this LSA is one that this router originated.
- *not my LSA* indicates that this LSA is not one that this router originated.
- *ls_seq* is the sequence of the received LSA.
- *ls_age* is the age of the received LSA.
- *db_seq* is the sequence of the LSA in my database.
- *db_age* is the age of the LSA in my database.
- *elapse* is the number of seconds since the LSA in the database was updated or added.
- *freeme*, if "1", indicates that this entry is marked to be deleted from the database.❒*ackcnt* is the number of acknowledgments that are outstanding.
- *nbr_retrans*, if "1", indicates this LSA is on a neighbor retransmission queue.
- *nbrEcnt* is the number of neighbors in the Exchange state or greater.
- *Fcnt* is the number of neighbors in the Full state.

C3: Packet Rejected: <PACKET TYPE>: UNKNOWN TYPE src <src_IP_address> type <LS_type>

Event Code: 67

Severity: Warning

Meaning: OSPF received and rejected *Database Description*, a *Link State Request*, a *Link State Acknowledgment*, or a *Link State Update* Packet identified by <LS_type> from a neighbor identified by <src_IP_address>. The link state type in the packet was not one of the valid types:

- 1 Router links advertisement (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisements(LS_ASE)

Action: Check the neighboring router for problems; it is sending bad packets.

C3: Packet Rejected: NBR's RTR = MY RTRID
src <src_IP_address> type <pkt_type> rtrid <rtr_IP_address>

Event Code: 61

Severity: Warning

Meaning: OSPF received and rejected a *Database Description*, a *Link State Request*, a *Link State Acknowledgment*, or a *Link State Update* identified by <pkt_type> from a neighbor identified by <src_IP_address> whose router id is the same as this router's id.

Action: Check both router's router id configuration parameter.

C3: Packet Rejected: SOURCE NEIGHBOR IN WRONG STATE
src <src_IP_address> state <state> type <pkt_type>

Event Code: 60

Severity: Warning

Meaning: OSPF received and rejected a *Database Description*, a *Link State Request*, a *Link State Acknowledgment*, or a *Link State Update* Packet identified by <pkt_type> from a neighbor identified by <src_IP_address> who is in the wrong state with this router to generate this packet.

Action: This message generally indicates that the identity of the network's Designated Router has changed, causing transient disagreements between adjacencies. This is temporary; the routers will synchronize soon. No action is required.

C3: Packet Rejected: UNKNOWN NBR
src <src_IP_address> type <pkt_type>

Event Code: 59

Severity: Warning

Meaning: OSPF received and rejected a *Database Description*, a *Link State Request*, a *Link State Acknowledgment*, or a *Link State Update* Packet identified by <pkt_type> from a neighbor, identified by <src_IP_address>, with which it has *not* established an adjacency.

R3: Received more recent self-originated LSA: type <LS_type> ls_id <LS_ID> router <rtr_IP_address> neighbor <IP_address>

Severity: Warning

Event Code: 68

Meaning: OSPF received (from the neighbor identified by <IP_address>) a more recent instance of a self-generated advertisement. <rtr_IP_address>) identifies the advertising router. <LS_type> contains one of five possible values as follows:

- 1 Router links advertisements (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisement (LS_ASE)

Depending upon <LS_type>, <LS_ID> contains an IP address as follows:

LS_type	LS_ID
1	Router ID of the originating router
2	IP interface address of network' s DR
3	IP address of destination network
4	Router ID of the described AS boundary router
5	IP address of destination network

Action: This message generally indicates that the router has restarted and lost track of its previous link state advertisement sequences. No action is required. OSPF increments the received sequence number and generates a new advertisement. Persistent messages of this type may indicate duplicate Router IDs within the network.

R4: Ack received for non-existent LSA: type <LS_type> LSID <LS_ID> neighbor <IP_address>

Event Code: 69

Severity: Warning

Meaning: OSPF has received an acknowledgment from the neighbor identified by <IP_address> for the instance of an advertisement not currently found in the database. <LS_type> contains one of five possible values as follows:

- 1 Router links advertisement (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisement (LS_ASE)

Depending upon <LS_type>, <LS_ID> contains an IP address as follows:

LS_type	LS_ID
1	Router ID of the originating router
2	IP interface address of network' s DR
3	IP address of destination network
4	Router ID of the described AS boundary router
5	IP address of destination network

Action: This message generally indicates that the router has restarted and lost track of its previous link state advertisement sequences. As such no action is required. Persistent messages of this type may indicate duplicate Router IDs within the network.

Trace Events

N3: LSA of MaxAge flushed: type <LS_type> LSID <LS_ID> router <rtr_IP_address>

Event Code: 70

Severity: Trace

Meaning: OSPF has removed an advertisement of MaxAge from its database. <rtr_IP_address> identifies the advertising router. <LS_type> contains one of five possible values as follows:

- 1 Router links advertisement (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisement (LS_ASE)

Depending upon <LS_type>, <LS_ID> contains an IP address150 as follows:

LS_type	LS_ID
1	Router ID of the originating router
2	IP interface address of network' s DR
3	IP address of destination network
4	Router ID of the described AS boundary router
5	IP address of destination network

T1: IP Interface <IP_address> Type: <if_type> Event: <OSPF_event> State change: <state_1> to <state_2>

Event Code: 38

Severity: Trace

Meaning: The OSPF interface, of type <if_type> specified by <IP_address> has transitioned from <state_1> to <state_2>. The state change was precipitated by <OSPF_event>. Interface states (*Backup*Dr, *Down*, *DR*, *DR Other*, *Loopback*, *PtoP*, and *Waiting*) are described in Section 9.1 of RFC 1247; events that cause interface state changes (*Backup Seen*, *Interface Down*, *Interface Up*, *Loop Indication*, *Neighbor Change*, *Unloop Indication*, and *Wait Timer*) are described in Section 9.2 of RFC 1247.

T2: Neighbor <IP_address> Event: <OSPF_event> State change: <state_1> to <state_2>

Event Code: 39

Severity: Trace

Meaning: OSPF has detected a state change in the neighbor identified by <IP_address> from <state_1> to <state_2>. The state change was precipitated by <OSPF_event>. Neighbor states (*Down, Attempt*, *Init*, *2 Way, Exch Start, Exchange*, *Loading*, *Full*, and *SCVirtual*) are described in Section 10.1 of RFC 1247; events that cause neighbor state changes (*Hello Received, Start*, *Two Way Received, Adjacency OK*, *Negotiation Done*, *Seq # Mismatch*, *Bad LS Request*, *Loading Done*, *One way*, *Reset Adjacency, Kill Neighbor*, *Inactivity Timer* and *Lower Level Down*) are described in Section 10.2 of RFC 1247.

T3: <Backup>Designated Router changed on network: <IP_address> <old_rtr_IP_address> to <new_rtr_IP_address>

Event Code: 40

Severity: Trace

Meaning: The Designated Router (or the Backup Designated Router) has changed on the network specified by <IP_address>. <old_rtr_IP_address> identifies the previous DR or BDR, while <new_rtr_IP_address> identifies the new DR or BDR.

T4: Originating new LSA - type <LS_type> LSID <LS_ID> router <rtr_IP_address>

Event Code: 41

Severity: Trace

Meaning: OSPF is originating a new instance of a link state advertisement. <rtr_IP_address> identifies the advertising router. <LS_type> contains one of five possible values as follows:

- 1 Router links advertisement (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisement (LS_ASE)

Depending upon <LS_type>, <LS_ID> contains an IP address as follows:

LS_type	LS_ID
1	Router ID of the originating router
2	IP interface address of network' s DR
3	IP address of destination network
4	Router ID of the described AS boundary router
5	IP address of destination network

T5: Received new LSA- type <LS_type> ls_id <LS_ID> router <rtr_IP_address> neighbor <IP_address>

Event Code: 42

Severity: Trace

Meaning: OSPF has received a *Link State Update* packet (originated by <rtr_IP_address> from the neighbor identified by <IP_address> and has recalculated its routing table. <LS_type> contains one of five possible values as follows:

- ❒ 1 Router links advertisement (LS_RTR)
- ❒ 2 Network links advertisement (LS_NET)
- ❒ 3 Network summary links advertisement (LS_SUM_NET)
- ❒ 4 AS boundary summary links advertisement (LS_SUM_ASB)
- ❒ 5 External links advertisement (LS_ASE)

Depending upon <LS_type>, <LS_ID> contains an IP address as follows:

LS_type	LS_ID
1	Router ID of the originating router
2	IP interface address of network' s DR
3	IP address of destination network
4	Router ID of the described AS boundary router
5	IP address of destination network

T6: Routing Table changed - type <LS_type> dst <dst_IP_address> old <old_next_hop> new <new_next_hop>

Event Code: 43

Severity: Trace

Meaning: OSPF has changed an entry in IP's routing table. <IP_address> identifies the changed entry, while <LS_type> specifies the link state type (LS_RTR, LS_NET, LS_SUM_NET, LS_SUM_ASB or LS_ASE). <old_next_hop> and <new_next_hop> specify the IP addresses of the old and new next hop routers. <LS_type> contains one of five possible values as follows:

- 1 Router links advertisement (LS_RTR)
- 2 Network links advertisement (LS_NET)
- 3 Network summary links advertisement (LS_SUM_NET)
- 4 AS boundary summary links advertisement (LS_SUM_ASB)
- 5 External links advertisement (LS_ASE)

Info Events

Interface <IP_address> down on circuit <circuit>.

Event Code: 36

Severity: Info

Meaning: OSPF has gone down on the specified circuit.

Interface <IP_address> up on circuit <circuit>.

Event Code: 35

Severity: Info

Meaning: OSPF has come up on the specified circuit.

Protocol initializing.

Event Code: 33

Severity: Info

Meaning: OSPF is initializing.

Protocol terminating.

Event Code: 34

Severity: Info

Meaning: OSPF is terminating.

SMDS Events

This section lists the event messages are issued by the SMDS (Switched Multi-Megabit Data Service) entity. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: SMDS experienced a fatal error and is restarting automatically. SMDS will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if SMDS fails to restart.

Warning Events

Can't decode DXI Addr/Ctrl 0x<field_contents> received on circuit <circuit_name>.

Event Code: 12

Severity: Warning

Meaning: The Wellfleet router received from the CSU (on the specified circuit) a DXI frame which contained an unparsable Address and/or Control field. The contents of the fields are displayed in hexadecimal format.

Action: Monitor CSU for integrity.

Circuit record does not exist for circuit <circuit_name>.

Event Code: 02

Severity: Warning

Meaning: SMDS has not been configured on the specified circuit.

Action: Configure SMDS on the circuit.

Circuit record is disabled on circuit <circuit_name>.

Event Code: 03

Severity: Warning

Meaning: SMDS has been disabled on the specified circuit.

Action: Reset the Enable parameter to restore SMDS service.

Circuit <circuit_name> rejecting bridge media type of <media_type>.

Event Code: 07

Severity: Warning

Meaning: The Wellfleet router has received a bridged packet over an unsupported media (not Ethernet or FDDI).

Action: Reconfiguration may be required. SMDS can bridge only those frames that originate on Ethernet or FDDI media.

Circuit <circuit_name> rejecting packet - larger than MTU size.

Event Code: 09

Severity: Warning

Meaning: The Wellfleet router received a packet larger than the MTU supported by the interface.

Action: Adjust the MTU parameter.

Circuit <circuit_name> rejecting too small packet of size <x> bytes.

Event Code: 08

Severity: Warning

Meaning: The Wellfleet router has received a runt L3PDU.

Action: Generally no action is required unless the message occurs with some degree of frequency.

Circuit <circuit_name> SMDS address is of incorrect length.

Event Code: 04

Severity: Warning

Meaning: An SMDS entered via the TI is of improper length.

Action: Correct the address.

Note: This message should not be seen if SMDS has been configured via the Site Manager, as the Site Manager checks SMDS addresses for format and length.

Circuit <circuit_name> SMDS address is of incorrect type.

Event Code: 05

Severity: Warning

Meaning: An SMDS address entered via the TI is of the incorrect type. That is, an individual address has been entered as a group address, or a group address has been entered as an individual address.

Action: Correct the address.

Note: This message should not be seen if SMDS has been configured via the Site Manager, as the Site Manager provides formatting for group and individual addresses.

Circuit <circuit_name> SMDS NANP address is incorrect.

Event Code: 06

Severity: Warning

Meaning: An improper NANP address has been entered.

Action: Correct the address.

DSU alarm condition <value> present on circuit <circuit_name>.

Event Code: 14

Severity: Warning

Meaning: The Wellfleet router received an alarm indication from the DSU on the circuit identified by <circuit_name>.

Alarm conditions are as follows:

Far and alarm2
Alarm indication signal4
Loss of frame8
Loss of signal16
Loopback state32

Action: No action may be required, as the state may be transient. If condition persists, check DSU for integrity.

Heartbeat Poll interval not > 5 seconds on circuit <circuit_name>.

Event Code: 11

Severity: Warning

Meaning: A Heartbeat Poll Interval entered via the TI is unacceptably short.

Action: Configure the interval to be greater than 5 seconds.

Note: This message should not be seen if SMDS has been configured via the Site Manager, as the Site Manager provides boundary checking for this interval.

LMI response from DSU timed out on circuit <circuit_name>.

Event Code: 13

Severity: Warning

Meaning: The Wellfleet router has not received a response to an LMI PDU issued on the circuit identified by <circuit_name> within the timeout period.

Action: Verify the integrity of the DSU.

No response to heartbeat poll on circuit <circuit_name>.

Event Code: 10

Severity: Warning

Meaning: The Heartbeat Poll Downcount has been met; the Wellfleet router has issued an unacceptable number of unacknowledged heartbeat poll messages, and has taken the Wellfleet router/CSU connection down.

Action: Verify that the CSU/DSU supports heartbeat polling; verify the integrity of the Wellfleet router/CSU connection.

Trace Events

OUI <oui_value> not registered in dp_undo_smds_snap_isap.

Event Code: 28

Severity: Trace

Meaning: SMDS received a packet from an unknown OUI.

Action: Verify configuration SMDS configuration record.

Proxy agent couldn't get a buffer on circuit <circuit_name>.

Event Code: 24

Severity: Trace

Meaning: The DXI proxy agent could not obtain a buffer on the circuit identified by <circuit_name>.

Action: Condition is probably transient, and mot likely no action is necessary.

Proxy agent received bad response of type <value> on <circuit_name>.

Event Code: 25

Severity: Trace

The DXI proxy agent received an unexpected response (something other than a get_response> to a get_request transmitted on the circuit identified by <circuit_name>. The type of received response is encoded in <value> as follows:

get_request PDU0
get_next_request PDU1
set_request3
trap4

Action: Verify DSU integrity.

Proxy agent received error <value> in response to status query on <circuit_name>.

Event Code: 26

The DXI proxy agent received an unexpected response (something other than a get_response> to a status request transmitted on the circuit identified by <circuit_name>. The type of received response is encoded in <value> as follows:

get_request PDU0
get_next_request PDU1
set_request3
trap4

Action: Verify DSU integrity.

Info Events

Cold Start trap received from DSU on circuit <circuit_name>.

Event Code: 19

Severity: Info

Meaning: SMDS has received a *coldStart Trap* from the CSU/DSU device. A cold start signifies that the CSU/DSU has restarted and may have altered its configuration.

DSU alarm condition<condition_code> present on circuit <circuit_name>.

Event Code: 21

Severity: Info

Meaning: An LMI GetResponse issued by the CSU/DSU notes one of the following conditions for the specified circuit: (2) Far End Alarm, (4) Alarm Indication Signal, (8) Loss of Frame, (16) Loss of Signal, (32) Loopback State.

Enterprise Specific trap received from DSU on circuit <circuit_name>.

Event Code: 23

Severity: Info

Meaning: SMDS has received an enterprise specific trap from the CSU/DSU device.

Interface down on circuit <circuit_name>.

Event Code: 16

Severity: Info

Meaning: SMDS service has been withdrawn on the specified circuit.

Interface up on circuit <circuit_name>.

Event Code: 15

Severity: Info

Meaning: SMDS service is present on the specified circuit.

Link Down trap received from DSU on circuit <circuit_name>.

Event Code: 21

Severity: Info

Meaning: SMDS has received a link down trap from the CSU/DSU device. A link down signifies that the CSU/DSU SNI (Subscriber Network Interface) has been taken out of service.

Link Up trap received from DSU on circuit <circuit_name>.

Event Code: 22

Severity: Info

Meaning: SMDS has received a *linkUp Trap* from the CSU/DSU device. A link up signifies that the CSU/DSU SNI (Subscriber Network Interface) has been put into service, or has been restored to service.

No alarm condition present on circuit <circuit_name>.

Event Code: 18

Severity: Info

Meaning: An LMI GetResponse issued by the CSU/DSU indicates a No Alarm condition for the specified circuit.

Querying DSU for trunk status on circuit <circuit_name>.

Event Code: 17

Severity: Info

Meaning: The Wellfleet router has queried the CSU/DSU for trunk status information.

Warm Start trap received from DSU on circuit<circuit_name>.

Event Code: 20

Severity: Info

Meaning: SMDS has received a *warmStart Trap* from the CSU/DSU device. A warm start signifies that the CSU/DSU has restarted and has not altered its configuration.

Source Routing Events

The following event messages are issued by the Wellfleet Source Routing Bridge entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The Source Routing Bridge experienced a fatal error and is restarting automatically. The source routing bridge will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the source routing bridge fails to restart.

Warning Events

IP Delivery registration failed.

Event Code: 12

Severity: Warning

Meaning: The source routing bridge attempted to communicate with the IP router and failed.

Action: Verify the IP router's configuration and state.

IP Ring not configured.

Event Code: 13

Severity: Warning

Meaning: IP encapsulation has started but no ring number has been assigned to the IP network.

Action: Assign a valid ring number using the source routing bridge's IP Ring parameter. See *Configuring the Source Routing Bridge* in the *Configuring System Software* guide for instructions.

Ring number not configured for circuit <circuit> .

Event Code: 11

Severity: Warning

Meaning: No ring number is configured for the circuit <circuit>.

Action: Assign a valid ring number to the circuit using the Ring ID parameter. See *Configuring the Source Routing Bridge* in the *Configuring System Software* guide for instructions.

Info Events

Interface down on circuit <circuit>

Event Code: 05

Severity: Info

Meaning: The circuit identified by <circuit> has become disabled thus disabling source routing service to the interface.

Interface up on circuit <circuit>

Event Code: 04

Severity: Info

Meaning: The circuit identified by <circuit> has become enabled thus providing source routing service to the interface.

IP encapsulation active

Event Code: 06

Severity: Info

Meaning: IP encapsulation service has become active.

IP encapsulation not active

Event Code: 07

Severity: Info

Meaning: IP encapsulation service has gone from active to not active

Service initializing

Event Code: 02

Severity: Info

Meaning: Source routing is initializing.

Service terminating

Event Code: 03

Severity: Info

Meaning: Source routing is terminating.

Source Routing Traffic Filter - Rule <filter_rule_no.>, Circuit <circuit> (Direct IP Explorers).

Event Code: 10

Severity: Info

Meaning: A source route packet has been logged in accordance with the specified filter rule.

Source Routing Traffic Filter- Rule <filter_rule_no.>, Circuit <circuit> (Drop packet) .

Event Code: 08

Severity: Info

Meaning: A source route packet has been dropped in accordance with the specified filter rule.

Source Routing Traffic Filter - Rule <filter_rule_no.>, Circuit <circuit> (Log only).

Event Code: 09

Severity: Info

Meaning: A source route packet has been logged in accordance with the specified filter rule.

SNMP Events

The following event messages are issued by the SNMP (Simple Network Management Protocol) entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code:	01
Severity:	Fault
Meaning:	SNMP experienced a fatal error and is restarting automatically. SNMP will attempt to restart up to five times.
Action:	Verify the configuration is correct. Call Customer Support if SNMP fails to restart.

Warning Events

Agent could not find a base record, creating one.

Event Code:	02
Severity:	Warning
Meaning:	An SNMP base record was not configured.
Action:	None required as the SNMP agent completes a base record for each slot using default values.

Agent could not find a community, creating community 'public'.

Event Code: 03

Severity: Warning

Meaning: No management community was configured.

Action: None required as the SNMP agent creates a community called "public" with read/write access to ensure that the system is "manageable".

Agent could not find a manager, adding wildcard to community 'public'.

Event Code: 04

Severity: Warning

Meaning: No manager (community member) was configured for a management community.

Action: None required as the SNMP agent creates a default manager (IP address 0.0.0.0, representing any community member) for the "public" community to ensure that the system is "manageable".

Duplicate community <community>, with index <value> deleted.

Event Code: 05

Severity: Warning

Meaning: A user has created an SNMP community, <community_name>, whose name matches that of an existing community. SNMP deletes the newly created community.

Action: None required as SNMP deletes the duplicate community. To add multiple management communities, assign a unique name to each community.

No corresponding community index <value> for manager <IP_address>, deleting instance.

Event Code: 06

Severity: Warning

Meaning: A user has created a manager <IP_address>, who cannot be associated with an existing management community. SNMP deletes the newly created manager.

Action: None required as SNMP deletes the manager record. To add multiple managers, associate them with existing communities, or add new community records.

Trace Event

Agent received unauthorized request from <IP_address> in community <community>.

Event Code: 08

Severity: Trace

Meaning: The SNMP agent received an SNMP packet from an unknown community and manager.

Action: None is required as SNMP drops the packet without a response. Message may indicate a configuration error or an attempt to breach system security.

Info Event

Protocol initializing.

Event Code: 07

Severity: Info

Meaning: The SNMP Agent is initializing.

Span Events

The following event messages are issued by the SPAN (Spanning Tree) entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The Spanning Tree experienced a fatal error and is restarting automatically. The Spanning Tree will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if Span fails to restart.

Warning Events

Invalid forward delay configured.

Event Code: 06

Severity: Warning

Meaning: The configured Forward Delay timer value is not within the bounds specified by IEEE 802.1D, Section 4.10.2. Allowable values for the Forward Delay timer are expressed by the formula:

2*(fwd_delay - 1.0 second) ≥ max_age

Action: Modify the Bridge configuration record to enter a valid Forward Delay timer value.

Invalid max age configured.

Event Code: 07

Severity: Warning

Meaning: The configured Max Age value is not within the bounds specified by IEEE 802.1D, Section 4.10.2. Allowable values for Max Age are expressed by the formula:

max_age ≥ 2*(hello_timer + 1.0 second)

Action: Modify the Bridge configuration record to enter a valid Max Age value.

Invalid Spanning Tree base record instance ignored.

Event Code: 09

Severity: Warning

Meaning: A user attempted to add a base record with an instance other than "0" to the MIB. SPAN ignores the request.

Action: To alter the Spanning Tree base record, specify the instance "0".

Unknown packet type <type_value>.

Event Code: 08

Severity: Warning

Meaning: SPAN received a Bridge Protocol Data Unit (BPDU) packet which contained an unknown value, <type_value>, in the BPDU type field.

Action: Monitor the network to identify and repair the source of the faulty BPDU.

Trace Event

Bridge <bridge ID> chosen as new root of Spanning Tree

Event Code: 10

Severity: Trace

Meaning: The bridge specified by <bridge ID> is now the root bridge for Spanning Tree.

Info Events

Interface <port_priority>.<interface_no.> down on circuit <circuit>.

Event Code: 05

Severity: Info

Meaning: SPAN is down on the circuit identified by <circuit>.

Interface <port_priority>.<interface_no.> up on circuit <circuit>.

Event Code: 04

Severity: Info

Meaning: SPAN is running on the circuit identified by <circuit>.

Protocol initializing.

Event Code: 02

Severity: Info

Meaning: SPAN is initializing.

Protocol terminating.

Event Code: 03

Severity: Info

Meaning: SPAN is terminating.

SYNC Events

The following event messages are issued by the SYNC driver which serves the DSDE2, DSDE1, QSYNC, and HDLC directories. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the driver fails to restart.

Warning Events

Connector COM <no.> : can't run BOFL with chosen WAN protocol.

Event Code: 35

Severity: Warning

Meaning: The BofL is incorrectly configured while a WAN protocol is configured.

Action: Disable BofL or change the selected WAN protocols to STANDARD.

Connector COM <no.> connect attempts exceeded.

Event Code: 05

Severity: Warning

Meaning: A sequence of retransmission attempts disabled the specified SYNC connection previously providing LLC2 service because the router was unable to obtain positive acknowledgment of an outstanding frame. The number of such attempts is determined by the N2, T1, and Connect Retries parameters.

Action: Verify point-to-point connectivity.

Connector COM <no.> not verified with diagnostic.

Event Code: 06

Severity: Warning

Meaning: Power-up diagnostics aborted were not run on the SYNC connection COM <no.>.

Action: Rerun power-up diagnostics by issuing the TI **diags** command to the slot in question if you wish to verify COM <no.> integrity.

Connector COM <no.> out of range.

Event Code: 02

Severity: Warning

Meaning: The SYNC connector COM <no.> is invalid and will be ignored.

Action: Modify the configuration file to accurately describe the Link Module described in the specified slot.

Connector COM <no.> receiver timeout.

Event Code: 04

Severity: Warning

Meaning: The SYNC connector COM <no.> did not receive a BofL ("breath of life") frame within the BofL interval.

Action: Verify cable integrity. Confirm that the remote end is configured for BofL transmission.

Connector COM <no.> transmitter timeout.

Event Code: 03

Severity: Warning

Meaning: The SYNC connector COM <no.> could not transmit a BofL ("breath of life") frame within the BofL interval.

Action: Check for the presence of a valid external clock from the external equipment or check the configuration.

Info Events

Connector COM <no.> configuration deleted.

Event Code: 10

Severity: Info

Meaning: The record for the specified SYNC connection has been deleted from the configuration.

Connector COM <no.> disabled.

Event Code: 08

Severity: Info

Meaning: The SYNC connection COM <no.> is disabled.

Connector COM <no.> enabled.

Event Code: 09

Severity: Info

Meaning: The SYNC connection COM <no.> is enabled.

Connector COM <no.> LLC1 service withdrawn.

Event Code: 13

Severity: Info

Meaning: The specified SYNC connection is not providing LLC1 service.

Connector COM <no.> LLC2 service withdrawn.

Event Code: 14

Severity: Info

Meaning: The specified SYNC connection is not providing LLC2 service.

Connector COM <no.> providing LLC1 service.

Event Code: 11

Severity: Info

Meaning: The specified SYNC connection is enabled and providing LLC1 service.

Connector COM <no.> providing LLC2 service.

Event Code: 12

Severity: Info

Meaning: The specified SYNC connection is enabled and providing LLC2 service.

Service initializing.

Event Code: 07

Severity: Info

Meaning: The SYNC driver is initializing.

T1 Events

This section describes how to read a T1 event log entry and lists all events. Each event is accompanied by a description and a recommended response if one is required.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The T1 driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the T1 driver fails to restart.

Warning Events

Connector DS_<connector_no.> diagnostic failed.

Event Code: 03

Severity: Warning

Meaning: The T1 connector identified by <connector_no.> failed power-up diagnostics and has been disabled.

Action: Verify the integrity of the T1 link module.

Connector DS_<connector_no.> fix configuration.

Event Code: 06

Severity: Warning

Meaning: T1 has detected an error or inconsistency within the configuration record for the connector identified by <connector_no.>.

Action: Verify the configuration record. Refer to sections *Editing T1 Line Details* and *Editing Synchronous Line Details* in *Configuring Circuits* in the *Configuring System Software* manual.

Connector DS_<connector_no.> not verified with diagnostic.

Event Code: 04

Severity: Warning

Meaning: The T1 connector identified by <connector_no.> has been placed in service. However, power-up diagnostics were aborted/terminated prior to verifying the connection.

Action: Rerun diagnostics to verify the integrity of the T1 link module.

Connector DS_<connector_no.> out of range.

Event Code: 02

Severity: Warning

Meaning: The T1 connector identified by <connector_no.> is invalid (a value other than 1 or 2) and will be ignored.

Action: Modify the T1 configuration to reflect a connector number of 1 or 2.

Note: This message should not be seen if T1 has been configured via the Site Manager, as the Site Manager checks guards against invalid connector identification.

Connector DS_<connector_no.> unknown state variable value.

Event Code: 05

Severity: Warning

Meaning: The T1 line driver state MIB object (wfT1state) contained an invalid entry. Valid entries are as follows:
1 for UP; 3 for INITializing; and, 4 for NOTPRESENT.

Action: None may be required as T1 will restart the connection.

Info Events

Connector DS_<connector_no.> carrier loss.

Event Code: 20

Severity: Info

Meaning: T1 has detected a loss of the signal carrier across the connector identified by <connector_no.>.

Connector DS_<connector_no.> clock being recovered from port 1.

Event Code: 19

Severity: Info

Meaning: The T1 connector identified by <connector_no.> is recovering the master clock via Port 1.

Connector DS_<connector_no.> clock being recovered from port 2.

Event Code: 18

Severity: Info

Meaning: The T1 connector identified by <connector_no.> is recovering the master clock via Port 2.

Connector DS_<connector_no.> instance record deleted.

Event Code: 07

Severity: Info

Meaning: The T1 record for the connector identified by <connector_no.> has been deleted from the configuration.

Connector DS_<connector_no.> line disabled.

Event Code: 08

Severity: Info

Meaning: T1 service has been disabled on the connector identified by <connector_no.>.

Connector DS_<connector_no.> enabled.

Event Code: 09

Severity: Info

Meaning: T1 service has been enabled on the connector identified by <connector_no.>.

Connector DS_<connector_no.> providing framer service.

Event Code: 10

Severity: Info

Meaning: T1 is enabled and providing service on the connector identified by <connector_no.>.

Connector DS_<connector_no.> red alarm received.

Event Code: 11

Severity: Info

Meaning: T1 has received a Red Alarm on the connector identified by <connector_no.>. Receipt of a Red Alarm indicates a remotely-detected failure. A Red Alarm generally indicates that the network/CPE equipment has detected an out-of-frame condition (an error in the framing bits).

Connector DS_<connector_no.> red recovery alarm cleared.

Event Code: 15

Severity: Info

Meaning: The remotely-detected failure that led to the issuance of a Red Alarm has been cleared.

Connector DS_<connector_no.> remote blue alarm cleared.

Event Code: 16

Severity: Info

Meaning: The condition(s) that lead to the issuance of a Blue Alarm (indicating loss of signal) has been cleared.

Connector DS_<connector_no.> remote blue alarm transmitted.

Event Code: 12

Severity: Info

Meaning: T1 has lost the DS-1 signal from the CPE for more than 150 milliseconds, and has issued a Blue Alarm (an "all 1's" signal).

Connector DS_<connector_no.> remote yellow alarm removed.

Event Code: 17

Severity: Info

Meaning: The remote end, after issuing a Yellow Alarm, has regained the incoming signal.

Connector DS_<connector_no.> yellow alarm received.

Event Code: 13

Severity: Info

Meaning: T1 has received a Yellow Alarm across the connector identified by <connector_no.>. Receipt of a Yellow Alarm indicates a remotely detected failure.

Connector DS_<connector_no.> yellow alarm transmitted.

Event Code: 14

Severity: Info

Meaning: T1 has transmitted a Yellow Alarm across the connector identified by <connector_no.>. A Yellow Alarm indicates that T1 has effectively lost the incoming signal across the specified connector.

Service initializing.

Event Code: 21

Severity: Info

Meaning: T1 service is initializing.

TF Events

The following event messages are issued by the TF (Traffic Filter) entity. The event messages are organized alphabetically.

Info Events

Traffic Filter Object <object_ID> Instance <instance> deleted

Event Code: 09

Severity: Info

Meaning: TF has deleted the traffic filter indicated by the SNMP object identifier and instance.

Traffic Filter Object <object_ID> Instance <instance> disabled

Event Code: 07

Severity: Info

Meaning: TF has disabled the traffic filter indicated by the SNMP object identifier and instance.

Traffic Filter Object <object_ID> Instance <instance> enabled

Event Code: 06

Severity: Info

Meaning: TF has enabled the traffic filter indicated by the SNMP object identifier and instance.

Traffic Filter Object <object_ID> Instance <instance> modified

Event Code: 08

Severity: Info

Meaning: TF has modified the traffic filter indicated by the SNMP object identifier and instance.

TFTP Events

The following event messages are issued by the TFTP (Trivial File Transfer Protocol) entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: TFTP experienced a fatal error and is restarting automatically. TFTP will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the TFTP fails to restart.

Trace Events

Request Server received malformed request packet from <IP_address>.

Event Code: 05

Severity: Trace

Meaning: TFTP received a faulty request packet (that is, one not conforming to the RFC 783 specifications) from the host identified by <IP_address>.

Request Server received <read/write> request of an illegal filename.

Event Code: 03

Severity: Trace

Meaning: TFTP received a request which specified a faulty or nonexistent file name.

Request Server received <read/write> request of <filename> from <IP_address>.

Event Code: 06

Severity: Trace

Meaning: TFTP received the indicated <read or write> request of <filename> from the client identified by <IP_address>.

Request Server received <read/write> request specifying an unsupported mode.

Event Code: 04

Severity: Trace

Meaning: TFTP received a request which specified a non-supported transfer mode (that is other than Octet or ASCII).

Transfer of <filename> completed successfully.

Event Code: 08

Severity: Trace

Meaning: TFTP successfully transferred the file indicated.

Transfer of <filename> failed with error = <error_code>, <text>.

Event Code: 07

Severity: Trace

Meaning: The TFTP transfer of <filename> failed with one of the following error codes:

Error Code (hexadecimal)	Text
0	Undefined error. See <text>.
1	File not found
2	Access violation. File is not readable.
3	Disk or Flash is full
6	File exists
17	Transfer timed out

Info Event

Protocol initializing.

Event Code: 02

Severity: Info

Meaning: TFTP is initializing.

TI Events

The following event messages are issued by the TI (Technician Interface) entity. Event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Severity:	Fault
Event Code:	01
Meaning:	TI experienced a fatal error and is restarting automatically. TI will attempt to restart up to five times.
Action:	Verify the configuration is correct. Call Customer Support if the TI fails to restart.

Warning Event

Invalid login attempt by <user>

Severity:	Warning
Event Code:	02
Meaning:	The TI manager reported that an invalid login ID, <user>, was entered at the TI *Login:* prompt.
Action:	None required, although the warning may indicate an attempt to breach system security.

TI_RUI Events

The following event messages are issued by the TI_RUI (Technician Interface/Site Manager) entity. Event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning:

Meaning: TI_RUI experienced a fatal error and is restarting automatically. TI_RUI will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the TI_RUI fails to restart.

Warning Events

Could not find a configuration record, creating one.

Event Code: 02

Severity: Warning

Meaning: TI_RUI could not find a configuration record for the remote TI process.

Action: None is required because TI_RUI creates a base configuration record using defaults.

<no.> events lost on slot <slot_no.> because of log wrap during a log aggregation.

Event Code: 03

Severity: Warning

Meaning: Some number of log events <n> associated with <slot_no.> were missed while aggregating the distributed log during a SAVE LOG operation.

Action: None available. Log aggregation proceeds.

Trace Event

Received processing request for command: <command>.

Event Code: 05

Severity: Trace

Meaning: A remote entity executed the command specified by <command>.

Action: None required. TI_RUI executes the specified command.

Info Event

Service initializing.

Event Code: 04

Severity: Info

Meaning: TI_RUI is initializing on the single specified slot.

Token Ring Events

This section describes how to read a Token Ring event log entry and lists all events. Each event is accompanied by a description and a recommended response if one is required.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The Token Ring driver experienced a fatal error and is restarting automatically. The driver will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if the Token Ring driver fails to restart.

Warning Events

Connector MAU<connector_number> cable connection fault.

Event Code: 02

Severity: Warning

Meaning: The Token Ring Driver has detected a faulty connection at the specified connector.

Action: Check for a loose or disconnected cable; verify hardware integrity.

Connector MAU<connector_number> diagnostic failed.

Event Code: 04

Severity: Warning

Meaning: The specified Token Ring connector failed power-up diagnostics and has been disabled.

Action: Verify the integrity of the Token Ring link module.

Connector MAU<connector_number> incorrect Bud/Mac prom rev.

Event Code: 07

Severity: Warning

Meaning: The Token Ring Link Module is out of revision and is not supported by the current software revision.

Action: Upgrade the Token Ring Link Module.

Connector MAU<connector_number> not verified with diagnostic.

Event Code: 06

Severity: Warning

Meaning: Power-up diagnostics were aborted/terminated prior to verifying the specified Token Ring connection.

Action: Rerun diagnostics to verify the integrity of the Token Ring link module.

Connector MAU<connector_number> out of range.

Event Code: 05

Severity: Warning

Meaning: The configured Token Ring connection is invalid and will be ignored.

Action: Repair the configuration record to provide a valid connection value.

Connector MAU<connector_number> Ring beaconing on insertion (Ring speed incorrect?).

Event Code: 03

Severity: Warning

Meaning: The Token Ring adaptor received a beacon MAC frame after attempting insertion into the Token Ring.

Action: Ensure that the Token Ring interface is configured to match the speed of the ring.

Info Events

Connector MAU<connector_number> configuration deleted.

Event Code: 12

Severity: Info

Meaning: The specified Token Ring record has been deleted from the configuration.

Connector MAU<connector_number> disabled.

Event Code: 10

Severity: Info

Meaning: Token Ring service has been disabled on the specified connector.

Connector MAU<connector_number> enabled.

Event Code: 11

Severity: Info

Meaning: Token Ring service has been enabled on the specified connector.

Connector MAU<connector_number> LLC1 service withdrawn.

Event Code: 14

Severity: Info

Meaning: The specified Token Ring connection is no longer providing LLC1 service.

Connector MAU<connector_number> loaded FASTMAC <revision_no.>

Event Code: 09

Severity: Info

Meaning: The accelerator microcode has been downloaded to the Token Ring Link Module.

Connector MAU<connector_number> providing LLC1 service.

Event Code: 13

Severity: Info

Meaning: The specified Token Ring connection is enabled and providing LLC1 service.

Connector MAU<connector_number> Ring Beaconing.

Event Code: 15

Severity: Info

Meaning: The Token Ring adaptor has observed beacon frames on the ring, indicating the presence of a hard error which renders the ring inoperable.

Connector MAU<connector_number> Ring Recovered.

Event Code: 17

Severity: Info

Meaning: The Token Ring adaptor has observed claim token MAC frames on the ring accessed by the specified circuit. Claim token MAC frames indicate that the ring is recovering from an error condition.

Connector MAU<connector_number> This node Beaconing the ring.

Event Code: 16

Severity: Info

Meaning: The Token Ring adapter has observed a hard ring error on the Token Ring accessed by the specified circuit and has initiated the transmittal of beacon frames.

Service initializing.

Event Code: 08

Severity: Info

Meaning: Token Ring service is initializing.

TTY Events

The following event messages are issued by the TTY (teletype) entity, which sets the CRT interface. The event messages are separated by severity and organized alphabetically within each severity type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: The TTY driver experienced a fatal error and is restarting automatically. TTY will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if TTY fails to restart.

Warning Events

DUART detected Framing error. Total: <total>

Event Code: 02

Severity: Warning

Meaning: Transmission error.

DUART detected Overrun error. Total: <total>

Event Code: 03

Severity: Warning

Meaning: Transmission error.

DUART detected Parity error. Total: <total>

Event Code: 04

Severity: Warning

Meaning: Transmission error.

Info Events

DUART Modem connection established.

Event Code: 05

Severity: Info

Meaning: A remote TI connection has been established.

DUART Modem disconnected - hang-up.

Event Code: 06

Severity: Info

Meaning: A remote TI connection has been terminated.

Input FIFO Overflow error - data lost. Total: <total>

Event Code: 07

Severity: Info

Meaning: The system did not respond to the input within the time allotted and the input overflowed in the FIFO buffer, causing a loss of data.

VINES Events

The following event messages are issued by the VINES entity. The event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: VINES experienced a fatal error and is restarting automatically. VINES will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if VINES fails to restart.

Warning Events

Illegal serial number <serial_number> used as Network ID.

Event Code: 47

Severity: Warning

Meaning: An illegal serial number is being used as the router's Network ID.

Action: Call Wellfleet Customer Support at 1-800-2LANWAN.

Trace Events

ARP Assignment issued with subnet <Network_ID>

Event Code: 15

Severity: Trace

Meaning: The router has assigned a VINES network number to the client PC.

Network <Network_ID> is added to Table of Networks

Event Code: 13

Severity: Trace

Meaning: A network has been added to the table of networks. The router has learned of a new network.

Network <Network_ID> is removed from the to Table of Networks

Event Code: 14

Severity: Trace

Meaning: A network has been removed from the table of networks. The network is no longer reachable.

Node <Network_ID>.<Subnetwork_ID> added to table of Neighbors

Event Code: 11

Severity: Trace

Meaning: The adjacent VINES node whose address is <Network_ID>.<Subnetwork_ID> is now a reachable address.

Node <Network_ID>.<Subnetwork_ID> removed from table of Neighbors

Event Code: 12

Severity: Trace

Meaning: The adjacent VINES node whose address is <Network_ID>.<Subnetwork_ID> is no longer a reachable address.

VINES TF - Rule <filter_rule_no.>, Circuit <circuit> (Drop packet) - pkt dst to <Network_ID>.<Subnetwork_ID>.

Event Code: 07

Severity: Trace

Meaning: A VINES packet has been dropped in accordance with the specified filter rule.

VINES TF- Rule <filter_rule_no.>, Circuit <circuit> (Log only) - pkt dst to <Network_ID>.<Subnetwork_ID>.

Event Code: 08

Severity: Trace

Meaning: A VINES packet has been logged in accordance with the specified filter rule.

Info Events

Interface down on circuit <circuit>

Event Code: 05

Severity: Info

Meaning: The circuit identified by <circuit> has become disabled thus disabling VINES service to the interface.

Interface up on circuit <circuit>

Event Code: 04

Severity: Info

Meaning: The circuit identified by <circuit> has become enabled thus providing VINES service to the interface.

Protocol initializing

Event Code: 02

Severity: Info

Meaning: VINES is initializing.

Protocol terminating

Event Code: 03

Severity: Info

Meaning: VINES is terminating.

XNS Events

The following event messages are issued by the XNS entity. Event messages are separated by type and organized alphabetically within each type.

Fault Event

System error, service attempting restart.

Event Code: 01

Severity: Fault

Meaning: XNS experienced a fatal error and is restarting automatically. XNS will attempt to restart up to five times.

Action: Verify the configuration is correct. Call Customer Support if XNS fails to restart.

Trace Events

Host <host_address> added to Table of Hosts

Event Code: 09

Severity: Trace

Meaning: The host indicated was added to the table of hosts.

Host <host_address> deleted from Table of Hosts

Event Code: 10

Severity: Trace

Meaning: The host indicated was deleted from the table of hosts.

Network <network_address> added to Table of Networks

Event Code: 07

Severity: Trace

Meaning: The network indicated was added to the table of networks.

Network <network_address> removed from Table of Networks

Event Code: 08

Severity: Trace

Meaning: The network indicated was deleted from the table of networks.

rip_recv received operation <1_or_2> from Host <host_address>

Event Code: 11

Severity: Trace

Meaning: An XNS RIP packet was received from the network and host indicated. Operation 1 indicates the packet is a RIP request. Operation 2 indicates the packet is a RIP response.

rip_update sent network <target_network_address> hops <no._hops> from Network <source_network_address>

Event Code: 12

Severity: Trace

Meaning: An XNS RIP update packet was sent to the target network indicated.

Info Events

ADD Nwif Network <network_address> Host <host_address>

Event Code: 37

Severity: Info

Meaning: The router's full XNS address has been added to the table for an interface.

DEL Nwif Network <network_address> Host <host_address>

Event Code: 38

Severity: Info

Meaning: The router's full XNS address has been deleted from the table for an interface.

Network <network_address> mapped to cct <circuit>

Event Code: 41

Severity: Info

Meaning: The interface for the network indicated is monitoring the status of the associated circuit.

Nwif from MIB Active Network <network_address> Host <host_address>

Event Code: 39

Severity: Info

Meaning: The record for an interface is active and the XNS routing software has read the information.

Nwif from MIB Non-active Network <network_address> Host <host_address>

Event Code: 40

Severity: Info

Meaning: The software has detected that a MIB interface record is inactive.

Protocol initializing

Event Code: 02

Severity: Info

Meaning: XNS is initializing.

Protocol terminating

Event Code: 03

Severity: Info

Meaning: XNS is terminating.

RTM out of BUFFERS

Event Code: 48

Severity: Info

Meaning: The Routing Table Manager process is out of buffers. This condition will hinder propagation of information to other slots.

Traffic Filter - drop: Rule <filter_rule_no.>, circuit <circuit> Network <network_address> Host <host_address>

Event Code: 46

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was dropped as specified by the filter.

Traffic Filter: Rule <filter_rule_no.>, circuit <circuit>

Event Code: 47

Severity: Info

Meaning: A packet matching filter rule <filter_rule_no.> was received on <circuit>. The packet was dropped as specified by the filter.

XNS on Interface <address> down on circuit <circuit>

Event Code: 05

Severity: Info

Meaning: The interface indicated has gone down on the circuit indicated.

XNS on Interface <address> up on circuit <circuit>

Event Code: 04

Severity: Info

Meaning: The interface indicated has come up on the circuit indicated.

Chapter 3

Managing the File System

List of Figures

Managing the File System

About this Chapter

This chapter describes how to use the Site Manager to manage files on the Wellfleet router.

Each FRE module in the BN can host one volume (Flash memory card). This volume provides the router with nonvolatile file storage (NVFS).

Each volume number is the same number as the slot that hosts the volume: that is, volume 2 resides on slot 2. Additional volumes in the router are optional; they can provide redundancy, additional storage, or both.

Note: If you are providing redundancy, be sure to copy files to the redundant volumes when you modify them.

This chapter describes how to do the following:

- Display the filenames in each volume
- Copy a file from one volume to another, or to the same volume
- Delete a file
- Transfer a file between any Wellfleet router and the Site Manager workstation
- Compact file space
- Format a volume

Displaying the Contents of a Volume

To display all files on a volume, begin at the Wellfleet Site Manager Window and select the Files option. The File System Manager Window displays the filenames in the active volume (see Figure 3-1).

To change the volume directory display to another, click on the Volume box. All slot numbers containing a volume are displayed; select the one you want. The File System Manager Window lists the files in the volume you selected.

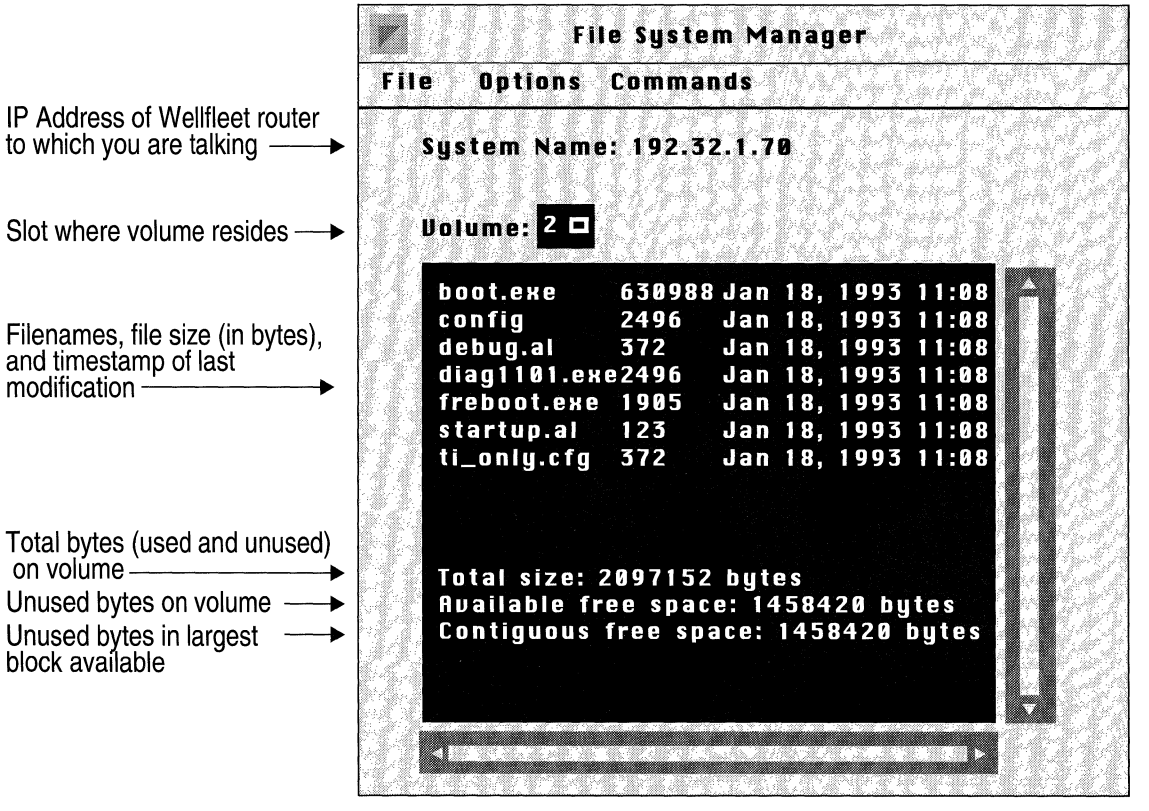


Figure 3-1. File System Manager Window with Sample Directory

The factory-default filenames are as follows:

- *boot.exe* is the bootable image. The system automatically references this binary file for booting instructions unless you specify another bootable image. You *cannot* read or change this file. This file must have the *boot.exe* filename for the system to boot automatically after a cold-start, or after you press the Reset button, select the boot option, or issue the reset command to the entire system.
- *config* is the default configuration file. The system refers to this binary file for configuration data when booting. (However, you can specify another configuration file with the Boot option.) You can change the configuration by copying an alternate configuration file to *config*. Also, you can store alternate or future configurations.

  This file must have the *config* filename for the system to configure automatically after booting. Wellfleet recommends that you copy the *config* file to a new backup filename before overwriting the *config* file.
- *debug.al* is an ASCII file containing aliases (TI commands that abbreviate long or multiple commands) that you can use to debug common network problems. (Refer to the *Managing Aliases* chapter of the *Operations Guide: Technician Interface* to use the aliases in this file.)
- *diag1101.exe* is a backup copy of the diagnostics image resident on the Diagnostics PROM. You *cannot* read or change this file.
- *freboot.exe* is a backup copy of the bootstrap image resident on the Bootstrap PROM. You *cannot* read or change this file.
- *startup.al* is an ASCII file containing aliases that you use during the initial startup.
- *ti_only.cfg* is the configuration file containing only the MIB variables associated with the TI console and modem operating parameters. This file is stored in binary format.

The fields at the bottom of the scroll box are as follows:

- *Total size* is the total number of bytes (used and unused) on the volume.
- *Available free space* is the number of unused bytes on the volume.
- *Contiguous free space* is the number of unused bytes in the largest block available on the volume.

Naming Files: Rules and Conventions

Before you proceed to the next section, you need to know the rules for naming files; they are as follows:

- You must specify the volume location (slot number) of any file you reference and of any file you create.
- Filenames must start with an alphabetical character. The remaining characters must be alphanumeric, and may also include the underscore (_) character.
- Filenames can consist of 1 to 15 characters.
- File extensions are optional, and must be preceded by a filename and a dot. The total limit of the filename and file extension is 15 characters (including the dot).

Also, Wellfleet recommends you use the following conventions when naming files so that you can distinguish files by type.

- Use the *.exe* file extension for software images. (The default software image is *boot.exe*.)
- Use the *.cfg* file extension for alternate configuration files. (The default configuration file is *config*.)
- Use the *.al* file extension for alias files.
- Use the *.log* file extension for log files.

Copying a File

You can use the File System Manager to copy a file on the Wellfleet router; you may copy the file either to a different volume in another slot, or to the same volume.

Warning: The system automatically overwrites any file already on the volume that has the same filename as the file you are creating. To avoid overwriting an existing file, display a list of the volume's contents (see *Displaying the Contents of a Volume*) and determine the filenames that are already in use.

If you are unfamiliar with the file naming rules and conventions, refer to the previous section entitled *Naming Files: Rules and Conventions* before you proceed with this section.

Copy a file as follows:

1. Click on the file to be copied in the list displayed in the File System window.
2. Select the Command/Copy option.

   The Copy Source File Window appears.

   In Figure 3-2, the *March.cfg* file on the volume in slot 2 will be copied.

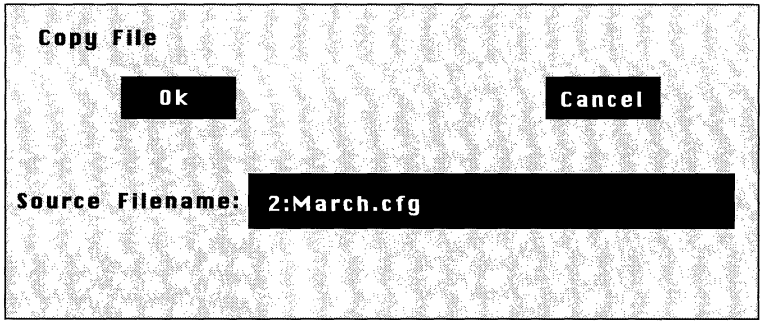


Figure 3-2. Copy Source File Window

3. Click the Ok button.

   The Copy Destination File Window appears (see Figure 3-3).

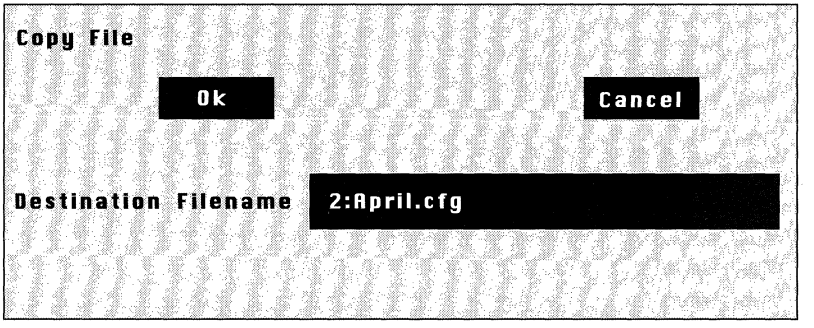


Figure 3-3. Copy Destination File Window

4. Using the following format, overtype the destination volume (slot to which you want to copy the file) and the filename you want to give this file.

   volume:filename

   For example, in Figure 3-3, the original file *March.cfg*, will be copied to the volume in slot 3, and be named *April.cfg*.

5. Click the Ok button.

   A confirmation window appears.

6. Click the Ok button.

   The source file is copied to the filename and volume you specified.

Deleting a File

You can delete any file that you specify from a volume.

Warning: You cannot recover a file after it is deleted.

Delete a file from a volume as follows:

1. Click on the file to be deleted in the list displayed in the File System window.
2. Select the Commands/Delete option.

   The Delete File Window displays the specified filename in the Filename box (see Figure 3-4). The filename appears in the *volume:filename* format.

Figure 3-4. Delete File Window

3. Click the Ok Button.

   A confirmation window appears.
4. Click the Ok button.

The file that you specified is deleted from the volume.

Transferring a File

The File System Manager allows you to transfer files between any Wellfleet router and the Site Manager workstation using the TFTP option. This option invokes the TFTP (Trivial File Transfer Protocol) software to execute file transfers.

The Node Name/IP Address displayed in the File System/Options/ SNMP/SNMP Options Window determines the Wellfleet router with which you transfer files.

Note: Wellfleet recommends that you ping the Wellfleet router before you transfer a file if you are running IP in Host Only mode and you have configured the router with the same IP address on multiple physical interfaces. Refer to the *Introduction to the Site Manager* chapter for instructions.

The following sections describe how to initiate the TFTP get and put functions to transfer files.

Getting a File

The Get option allows you to transfer a file from the Wellfleet router to the Site Manager workstation.

Note: When you get a *config* file, the hardware configuration is *not* included. Refer to the *Configuration Manager Overview* chapter of the *Configuring System Software* guide for instructions on getting the hardware configuration.

To transfer a file from the Wellfleet router to the Site Manager workstation, begin at the File System Manager Window and proceed as follows:

1. Click on the volume box and select the (slot) number of the volume you want to transfer from in the popup menu.

   The File System Manager lists the files stored in the volume you selected.

2. Select the file to be transferred to the Site Manager workstation.

3. Select the File/Tftp/Get File option.

   The TFTP Get File Window appears (see Figure 3-5). The filename you selected in step 2 appears in the Remote Filename box.

Figure 3-5. TFTP Get File Window

In this example, the file *April.cfg* is being transferred from the Wellfleet router to the Site Manager workstation.

4. Click the Ok button.

   The TFTP Get Local File Window appears (see Figure 3-6).

Figure 3-6. TFTP Get Local File Window

5. Overtype a unique filename for the new file to be stored on the Site Manager workstation.

   Refer to *Naming Files: Rules and Conventions* earlier in this chapter if necessary.

6. Click the Ok button.

   A confirmation window appears.

7. Click the Ok button.

   The file is now transferred from the Wellfleet router to the Site Manager workstation.

Putting a File

The Put option allows you to transfer a file from the Site Manager workstation to the Wellfleet router.

Note: Wellfleet recommends that you ping the Wellfleet router before you transfer a file if you are running IP in Host Only mode and you have configured the Wellfleet router with the same IP address on multiple physical interfaces. Refer to the *Introduction to the Site Manager* chapter for instructions.

To transfer a file from the Site Manager workstation to the Wellfleet router, begin at the File System Manager Window and proceed as follows:

1. Click on the volume box and select the (slot) number of the volume you want to transfer to in the popup menu.

   The File System Manager lists the files stored in the volume you selected.

2. Select the File/Tftp/Put File option.

   The TFTP Put Local File Window appears (see Figure 3-7).

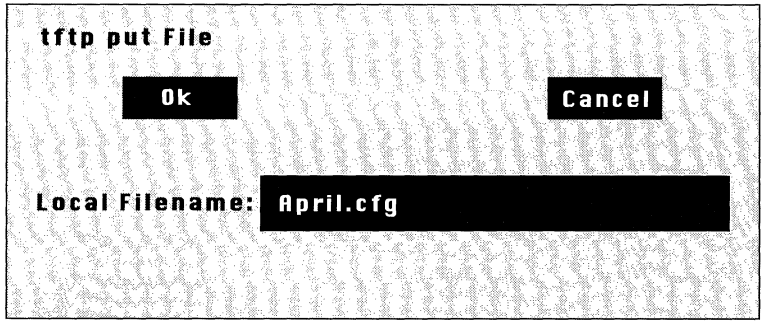


Figure 3-7. TFTP Put Local File Window

3. Specify the name of the file you want to transfer to the Wellfleet router in the Local Filename box.
4. Click the Ok button.

   The TFTP Put Remote File Window appears (see Figure 3-8).

Figure 3-8. TFTP Put Remote File Window

5. Using the following format, specify a volume and filename for the file to be stored on the Wellfleet router.

   volume:filename

   Refer to the volume's list of files to ensure that you are assigning a unique filename. Also, refer to *Naming Files: Rules and Conventions* earlier in this chapter if necessary.
6. Click the Ok button.

   A confirmation window appears.
7. Click the Ok button.

   The file is now transferred from the Site Manager workstation to the appropriate volume on the Wellfleet router.

The file you transferred to the Wellfleet router now appears in the list of files in the specified volume.

Compacting File Space

When you delete a file from a Flash card, the file becomes inaccessible, but the data remains on the Flash card. Eventually, all space is used. The Compact option copies the active files to memory, erases the Flash card, and copies the files back to the Flash card. This procedure gives you more file space, provided that you have more available free space than contiguous free space (refer to the *Displaying the Contents of a Volume* section for definitions of available and contiguous free space).

Warning: Wellfleet recommends that you back up the files by copying them to a second Flash card before using the Compact option.

To compact the files on a Flash card, begin at the File System Manager Window and proceed as follows:

1. Click on the volume box and select the (slot) number of the volume you want to compact from the popup menu.
2. Select the Commands/Compact option.

   A confirmation window appears.
3. Click the Ok button.

Wait at least three minutes before issuing another file system request. The active files are copied to memory, the volume is erased, and the files are rewritten to the volume. The *transaction is completing asynchronously* message displays during this procedure, indicating that the Wellfleet router is unavailable for further file system requests until the compact process is complete. If you issue a file system request before the compact process is complete, a *last command failed* message appears.

Display a list of the volume's contents after three minutes pass. The compact process is complete if the list of files appears empty.

Formatting a Volume

The Format option allows you to format and initialize a volume. Use the Format option to format new volumes if you do not obtain them from Wellfleet.

Warning: You cannot recover files from a volume after using the Format option. Wellfleet recommends that you copy them to a second volume before using the format option.

To format a volume, begin at the File System Manager Window and proceed as follows:

1. Click on the volume box and select the (slot) number of the volume you want to format from the popup menu.
2. Select the Commands/Format option.

   A confirmation window appears.
3. Click the Ok button.

   The system formats and initializes the volume. The File System Manager automatically displays the list of files stored in the volume after it is formatted.

Chapter 4

Displaying Statistics

List of Figures

List of Tables

Displaying Statistics

About this Chapter

This chapter describes how to use the Site Manager to display and interpret the circuit and protocol statistics gathered by the Wellfleet router.

The Site Manager provides Wellfleet router administrators or support personnel with a full battery of real-time data link layer and network layer protocol data. The Site Manager uses an SNMP-based, user-configurable polling mechanism to request circuit and/or protocol data from the Wellfleet router. Upon receipt of data, the Site Manager aggregates, formats, and displays data in a statistics window. Statistics windows refresh automatically to show the most recent data received from the Wellfleet router.

Statistics Overview

The Statistics Manager Window provides access to all circuit-specific and protocol-specific windows.

You access the Statistics Manager from the Wellfleet Site Manager Window. Select the Stats option to display the Statistics Manager Window (see Figure 4-1).

The Protocols and Circuits menu options provide access to the statistics. Refer to the sections that follow for instructions.

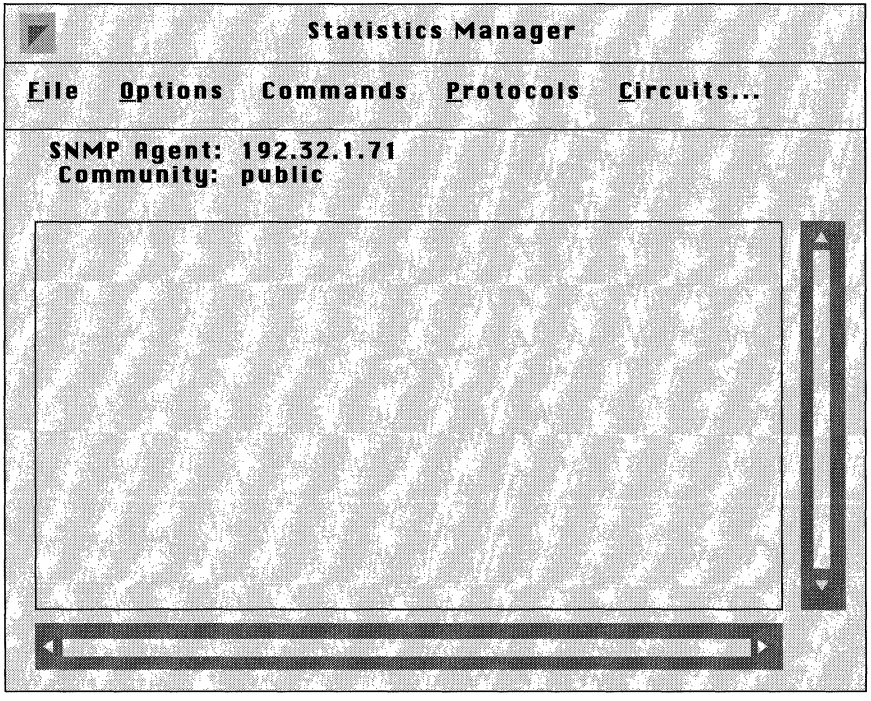


Figure 4-1. Statistics Manager Window

Data Link Layer Statistics

You access data link layer statistics by displaying the Circuit Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Circuits option. The Circuit Statistics Window is displayed.

The Circuit Statistics Window lists all configured circuits on the Wellfleet router, the associated slot and connector, the circuit state, and the MAC (physical layer) address of the circuit. This window also provides access to traffic statistics, error statistics, table statistics, and status statistics.

The sections that follow describe the statistics you access by selecting the options in this window.

CSMACD Statistics

The Wellfleet router gathers the following types of CSMACD statistics for each circuit:

- CSMACD frame reception data
- CSMACD frame transmission data
- CSMACD reception error data
- CSMACD transmission error data
- Miscellaneous CSMACD errors

The sections that follow describe how to display and interpret this data.

CSMACD Traffic

You access a summary listing of CSMACD traffic by displaying the CSMACD Traffic Statistics Window. Begin at the Circuit Statistics Window and select the Traffic/CSMACD Traffic option. The CSMACD Traffic Statistics Window is displayed.

The CSMACD Traffic Statistics Window provides a summary description of the reception and transmission of CSMACD frames across each circuit.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- In Octets contains the total number of octets received on the circuit.
- Out Octets contains the total number of octets transmitted on the circuit.

Frames Received

The Frames Received portion of the CSMACD Traffic Statistics Window displays the following statistics:

- Total contains the number of frames received on the circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.
- Current/s (current frames per second) contains an approximation of the number of frames received on the circuit during the last second.

- Average/s (average frames per second) contains an approximation of the average number of frames received on the circuit.
- Peak/s (peak frames per second) contains an approximation of the greatest number of frames received on the interface.

Frames Transmitted

The Frames Transmitted portion of the CSMACD Traffic Statistics Window displays the following statistics:

- Total contains the number of frames transmitted on the circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.
- Current/s (current frames per second) contains an approximation of the number of frames transmitted on the circuit during the last second.
- Average/s (average frames per second) contains an approximation of the average number of frames transmitted on the circuit.
- Peak/s (peak frames per second) contains an approximation of the greatest number of frames transmitted on the circuit.

CSMACD Errors

The sections that follow describe how to display and interpret the CSMACD reception error, transmission error, and miscellaneous error statistics.

Reception Errors

You access the CSMACD reception error statistics by displaying the CSMACD Receive Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/CSMACD/Rx Errors option. The CSMACD Receive Error Statistics Window is displayed.

The CSMACD Receive Error Statistics Window provides a summary description of the reception errors across each CSMACD circuit.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- Checksum Errors contains the number of frames dropped because they contained an erroneous checksum.
- Alignment Errors contains the number of frames dropped because they did not end on a byte boundary.
- Lack of Resources contains the number of otherwise correct frames that were dropped because of a shortage of available receive buffers.
- Frames Too Big contains the number of frames that were dropped because they exceeded 1518 bytes in length; this byte count does not include the 64-bit preamble and synchronization bits.
- Overflow Errors contains the number of overflow errors. An overflow error occurs when the CSMACD hardware cannot keep pace with the flow of incoming frames and loses all or part of a frame.

Transmission Errors

You access the CSMACD transmission error statistics by displaying the CSMACD Transmit Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/CSMACD/Tx Errors option. The CSMACD Transmit Error Statistics Window is displayed.

The CSMACD Transmit Error Statistics Window provides a summary description of the transmission errors across each CSMACD circuit.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- Deferred Transmittals contains the number of times the CSMACD hardware delayed transmission of a waiting frame because the physical media was busy. In such an instance, the hardware waits for the media to become idle, pauses for an interframe spacing interval, and then attempts to retransmit the frame.
- Collisions Late contains the number of "late collisions". A late collision occurs when the CSMACD hardware detects the collision after the transmission of 64 or more bytes. Following detection of a late collision CSMACD does not retransmit the frame; rather it increments this counter and then transmits the next frame in the transmission queue.
- Collisions Excessive contains the number of times CSMACD detected collisions on 16 consecutive attempts to transmit the same frame. At that point, CSMACD drops the frame, increments this counter, and then transmits the next frame in the transmission queue.
- Frames Too Big contains the number of otherwise correct frames that were dropped because they exceeded 1518 bytes in length; this byte count does not include the 64-bit preamble and synchronization bits.

- Internal Buffer Errors contains the number of otherwise correct frames that were dropped because of a shortage of available transmit buffers.
- Loss of Carrier contains the number of times CSMA detected the loss of the carrier signal.
- Underflow Errors contains the number of underflow errors; an underflow occurs when CSMACD truncates transmission because of the late receipt of data from memory.

Miscellaneous Errors

You access the CSMACD miscellaneous error statistics by displaying the CSMACD Miscellaneous Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/CSMACD/Misc Errors option. The CSMACD Miscellaneous Error Statistics Window is displayed.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- Internal Memory Errors contains the number of times the driver was unable to access memory over the internal data/address bus.
- Collision Errors contains the number of times the driver detected the loss of the Signal Quality Error (SQE) signal.

Sync Statistics

The Wellfleet router gathers the following types of synchronous (SYNC) statistics for each circuit:

- SYNC frame reception data
- SYNC frame transmission data
- SYNC reception error data
- SYNC transmission error data
- Miscellaneous SYNC errors

The sections that follow describe how to display and interpret this data.

SYNC Traffic

You access a summary listing of SYNC traffic by displaying the SYNC Traffic Statistics Window. Begin at the Circuit Statistics Window and select the Traffic/SYNC Traffic option. The SYNC Traffic Statistics Window is displayed.

The SYNC Traffic Statistics Window provides a summary description of the reception and transmission of synchronous frames across each circuit.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- In Octets contains the total number of octets received on the circuit.

- Out Octets contains the total number of octets transmitted on the circuit.

Frames Received

The Frames Received portion of the SYNC Traffic Statistics Window displays the following statistics:

- Total contains the number of frames received on the circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.
- Current/s (current frames per second) contains an approximation of the number of frames received on the circuit during the last second.
- Average/s (average frames per second) contains an approximation of the average number of frames received on the circuit.
- Peak/s (peak frames per second) contains an approximation of the greatest number of frames received on the interface.

Frames Transmitted

The Frames Transmitted portion of the SYNC Traffic Statistics Window displays the following statistics:

- Total contains the number of frames transmitted on the circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.
- Current/s (current frames per second) contains an approximation of the number of frames transmitted on the circuit during the last second.
- Average/s (average frames per second) contains an approximation of the average number of frames transmitted on the circuit.
- Peak/s (peak frames per second) contains an approximation of the greatest number of frames transmitted on the circuit.

SYNC Errors

The sections that follow describe how to display and interpret the SYNC reception error, transmission error, and miscellaneous error statistics.

Reception Errors

You access the SYNC reception error statistics by displaying the SYNC Receive Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/SYNC/Rx Errors option. The SYNC Receive Error Statistics Window is displayed.

The SYNC Receive Error Statistics Window provides a summary description of the reception errors across each synchronous circuit.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- Total contains the total count of receive errors transmitted on the circuit since it was created, the Wellfleet router rebooted, or the slot reset.
- Lack of Buffers contains the number of otherwise correct frames that were dropped because of a shortage of available receive buffers.
- Rejects Rx'ed contains the number of supervisory REJ (Reject) frames received on the interface. A REJ frame is a negative acknowledgment and request retransmittal of specified I (Information) frames.
- Overflows contains the number of overflow errors. An overflow error occurs when the synchronous hardware cannot keep pace with the flow of incoming frames and loses all or part of a frame.
- Incomplete Frames contains the number of incomplete frames (indicated by failure to find the end-of-frame-bit) received on the interface.

- Bad Frames contains the aggregate count of erroneous frames received on the interface.
- Frame Rejects contains the number of unnumbered FRMR (Frame Reject) frames received on the interface. The remote end of the circuit uses an FRMR to report an error condition, such as the request for an unavailable service.
- Runt Frames contains the number of frames of insufficient length received on the interface.

Transmission Errors

You access the SYNC transmission error statistics by displaying the SYNC Transmit Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/SYNC/Tx Errors option. The SYNC Transmit Error Statistics Window is displayed.

The SYNC Transmit Error Statistics Window provides a summary description of the transmission errors across each synchronous circuit.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- Total contains the total count of transmission errors since the circuit was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.
- Lack of Buffers contains the number of otherwise correct frames that were dropped because of a shortage of available transmit buffers.
- Underflow Errors contains the number of underflow errors; an underflow occurs when the synchronous driver truncates transmission because of the late receipt of data from memory.
- Rejects Tx'ed contains the number of unnumbered FRMR (Frame Reject) frames transmitted on the interface. An FRMR reports an error condition, such as the request for an unavailable service, to the remote end of the circuit.

Miscellaneous Errors

You access the SYNC miscellaneous error statistics by displaying the SYNC Miscellaneous Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/SYNC/Misc Errors option. The SYNC Miscellaneous Error Statistics Window is displayed.

The SYNC Miscellaneous Error Statistics Window provides a summary description of the miscellaneous errors across each synchronous circuit.

This window displays the following data:

- Circuit Name contains the user-assigned circuit name.
- Slot and Connector map Circuit Name to a specific slot and connector.
- T1 Timeouts contains the number of T1 timeouts. The T1 timer measures the interval between command transmission and the receipt of a response. If a response is not received within the T1 interval the synchronous driver increments this counter and then retransmits the unacknowledged command.
- Internal Memory Errors contains the number of times the driver was unable to access memory over the internal data/address bus.

E1 Error Statistics

You access E1 error statistics by displaying the E1 Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/E1 Errors option. The E1 Error Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the E1 circuit.

Slot and Conn.

The physical location of the E1 module within the Wellfleet router.

Errors: Frame

The number of instance of received frame errors, a count of frame alignment, Channel Associated Signalling (CAS), and CRC errors.

Errors: CAS Resync

The number of instances of Channel Associated Signalling (CAS) resynchronizations.

Alarms: Remote

The number of received Yellow Alarms. A Yellow Alarm indicates a "remotely-detected" failure that is sent back to the failure source. Receipt of a Yellow Alarm indicates a local E1 problem.

Alarms: Multiframe

The number of instances in which multiframe alignment has been lost. Multiframe alignment is considered lost when for a period of 1 or 2 multiframes all bits in time slot 16 are 0's.

Bipolar Violations

The number of received bipolar violations.

Sync Loss

The number of instances where synchronization was lost.

FDDI Statistics

The Wellfleet router gathers the following types of FDDI statistics for each circuit:

- FDDI frame reception data
- FDDI frame transmission data
- FDDI reception error data
- FDDI transmission error data
- Miscellaneous FDDI errors
- FDDI SMT table statistics
- FDDI MAC table statistics
- FDDI Port table statistics
- FDDI Timer table statistics

The sections that follow describe how to display and interpret this data.

FDDI Traffic

You access a summary listing of FDDI traffic by displaying the FDDI Traffic Statistics Window. Begin at the Circuit Statistics Window and select the Traffic/FDDI Traffic option. The FDDI Traffic Statistics Window is displayed.

The FDDI Traffic Statistics Window provides a summary description of the reception and transmission of FDDI frames across each circuit.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

In Octets

The number of octets received by the FDDI circuit since it was last reset.

Out Octets

The number of octets transmitted by the FDDI circuit since it was last reset.

Frames Received

The Frames Received portion of the FDDI Traffic Statistics Window displays the following statistics:

Total

The number of frames received by the FDDI circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

An approximation of the number of frames received by the FDDI circuit during the last second.

Average/s

An approximation of the number of frames received per second by the FDDI circuit since it was last reset.

Peak/s

An approximation of the greatest number of frames received per second by the FDDI circuit since it was last reset.

Frames Transmitted

The Frames Transmitted portion of the FDDI Traffic Statistics Window displays the following statistics:

Total

The number of frames transmitted by the FDDI circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

An approximation of the number of frames transmitted by the FDDI circuit during the last second.

Average/s

An approximation of the number of frames transmitted per second by the FDDI circuit since it was last reset.

Peak/s

An approximation of the greatest number of frames transmitted per second by the FDDI circuit since it was last reset.

FDDI Errors

The sections that follow describe how to display and interpret the FDDI reception error, transmission error, and miscellaneous error statistics.

Transmission Errors

You access the FDDI reception error statistics by displaying the FDDI Transmission Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/FDDI/Tx Errors option. The FDDI Transmission Error Statistics Window is displayed.

The FDDI Transmission Error Statistics Window provides a summary description of the transmission errors across each FDDI circuit.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Internal Errors

The number of internal operation error events.

Underrun Errors

The number of underruns of the FDDI circuit. An underrun occurs when FDDI truncates a frame because of the late receipt of data from memory. This is an indication of congestion and can be expected in modest numbers on high bandwidth application.

Parity Errors

The number of transmit frames aborted with parity errors.

Ring Errors

The number of LLC/SMT transmit ring error events.

Reception Errors

You access the FDDI reception error statistics by displaying the FDDI Receive Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/FDDI/Rx Errors option. The FDDI Receive Error Statistics Window is displayed.

The FDDI Receive Error Statistics Window provides a summary description of the reception errors across each FDDI circuit.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Checksum Errors

The number of received frames with checksum errors.

Overrun Errors

The number of frames received with internal overrun errors.

Parity Errors

The number of frames received with parity errors.

MAC Errors

The number of frames received with MAC errors.

Ring Errors

The number of receive ring error events.

Ring Overruns

The number of LLC receive ring overrun events.

Miscellaneous Errors

You access the FDDI miscellaneous error statistics by displaying the FDDI Miscellaneous Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/FDDI/Misc Errors option. The FDDI Miscellaneous Error Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Port Op. Errors

The number of port operation error events.

Internal Op. Errors

The number of internal operation error events.

Host Errors

The number of host error events.

FDDI Table Statistics

The sections that follow describe how to display and interpret the statistics in the FDDI SMT, MAC, Port, and Timer tables.

SMT Table

You access the FDDI SMT table statistics by displaying the FDDI SMT Table Statistics Window. Begin at the Circuit Statistics Window and select the Tables/FDDI/SMT option. The FDDI SMT Table Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Station ID

The unique station id.

ECM State

The current state of the ECM (entity coordination management) state machine. Possible states and associated values are as follows:

OUT	1
IN	2
TRACE	3
LEAVE	4
PATHTEST	5
INSERT	6
CHECK	7
DEINSERT	8

CF State

The attachment configuration. Possible values are as follows:

ISOLATED	1
WRAPS	2
WRAPA	3
WRAPB	4
WRAPAB	5
THRU	6

MAC Table

You access the FDDI MAC table statistics by displaying the FDDI MAC Table Statistics Window. Begin at the Circuit Statistics Window and select the Tables/FDDI/MAC option. The FDDI MAC Table Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Upstream Neighbor

The long individual MAC address of the upstream neighbor as determined by the Neighbor Information Frame protocol. A value of 00 00 00 00 00 00 indicates that the address is unknown.

Downstream Neighbor

The long individual MAC address of the downstream neighbor as determined by the Neighbor Information Frame protocol. A value of 00 00 00 00 00 00 indicates that the address is unknown.

SMT Frames Address

The 48-bit individual address of the MAC used for SMT frames.

Ring Management State

The current state of the ring management state machine. Possible states and associated values are as follows:

ISOLATED	1
NONOP	2
RINGOP	4
DETECT	8
NONOPDUP	16
RINGOPDUP	32
DIRECTED	64
TRACE	128

Negotiated TTRT (ms)

The negotiated TTRT (target token rotation time) negotiated during the claim process.

PORT Table

You access the FDDI Port table statistics by displaying the FDDI Port Table Statistics Window. Begin at the Circuit Statistics Window and select the Tables/FDDI/PORT option. The FDDI Port Table Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Port Type

The port type as follows:

TYPE_A	1
TYPE_B	2
TYPE_S	3
TYPE_M	4

Neighbor Port Type

The neighbor port type as follows:

TYPE_A	1
TYPE_B	2
TYPE_S	3
TYPE_M	4
UNKNOWN	5

State

The current state of the physical state machine. Possible states and associated values are as follows:

OFF	1
BREAK	2
TRACE	3
CONNECT	4
NEXT	5
SIGNAL	6
JOIN	7
VERIFY	8
ACTIVE	9
MAINT	10

Timer Table

You access the FDDI Timer table statistics by displaying the FDDI Timer Table Statistics Window. Begin at the Circuit Statistics Window and select the Tables/FDDI/TIMER option. The FDDI Timer Table Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the FDDI circuit.

Slot and Conn.

The physical location of the FDDI module within the Wellfleet router.

Maximum TTRT (ms)

The requested maximum TTRT (token target rotation time) to be supported.

Tvx Time (ms)

The requested Tvx (valid transmission timer) value.

Minimum TTRT (ms)

The requested minimum TTRT (token target rotation time) to be supported.

HSSI Statistics

The Wellfleet router gathers the following types of HSSI statistics for each circuit:

- HSSI frame reception data
- HSSI frame transmission data
- HSSI reception error data
- HSSI transmission error data
- Miscellaneous HSSI errors

The sections that follow describe how to display and interpret this data.

HSSI Traffic

You access a summary listing of HSSI traffic by displaying the HSSI Traffic Statistics Window. Begin at the Circuit Statistics Window and select the Traffic/HSSI Traffic option. The HSSI Traffic Statistics Window is displayed.

The HSSI Traffic Statistics Window provides a summary description of the reception and transmission of HSSI frames across each circuit.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

Circuit Name

The name of the HSSI circuit.

Slot and Conn.

The physical location of the HSSI module within the Wellfleet router.

In Octets

The number of octets received by the HSSI circuit since it was last reset.

Out Octets

The number of octets transmitted by the HSSI circuit since it was last reset.

Frames Received

The Frames Received portion of the HSSI Traffic Statistics Window displays the following statistics:

Total

The number of frames received by the HSSI circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

An approximation of the number of frames received by the HSSI circuit during the last second.

Average/s

An approximation of the number of frames received per second by the HSSI circuit since it was last reset.

Peak/s

An approximation of the greatest number of frames received per second by the HSSI circuit since it was last reset.

Frames Transmitted

The Frames Transmitted portion of the HSSI Traffic Statistics Window displays the following statistics:

Total

The number of frames transmitted by the HSSI circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

An approximation of the number of frames transmitted by the HSSI circuit during the last second.

Average/s

An approximation of the number of frames transmitted per second by the HSSI circuit since it was last reset.

Peak/s

An approximation of the greatest number of frames transmitted per second by the HSSI circuit since it was last reset.

HSSI Errors

The sections that follow describe how to display and interpret the HSSI reception error, transmission error, and miscellaneous error statistics.

Transmission Errors

You access the HSSI transmission error statistics by displaying the HSSI Transmission Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/HSSI/Tx Errors option. The HSSI Transmission Error Statistics Window is displayed.

The HSSI Transmission Error Statistics Window provides a summary description of the transmission errors across each HSSI circuit.

This window displays the following data:

Circuit Name

The name of the HSSI circuit.

Slot and Conn.

The physical location of the HSSI module within the Wellfleet router.

Transmit Aborts

The number of frames queued for transmit on the HSSI circuit that were aborted because of internal abort errors.

Fifo Underruns

The number of underruns on the HSSI circuit. An underrun occurs when HSSI truncates a frame because of the late receipt of data from memory. This is an indication of congestion and can be expected in modest numbers on high bandwidth applications.

Descriptor Ring Errors

The number of transmit ring error events.

Reception Errors

You access the HSSI reception error statistics by displaying the HSSI Receive Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/HSSI/Rx Errors option. The HSSI Receive Error Statistics Window is displayed.

The HSSI Receive Error Statistics Window provides a summary description of the reception errors across each HSSI circuit.

This window displays the following data:

Circuit Name

The name of the HSSI circuit.

Slot and Conn.

The physical location of the HSSI module within the Wellfleet router.

Oversize Frames

The number of frames dropped upon receipt because of the frame's excessive length.

CRC Errors

The number of received frames that contained CRC errors.

Fifo Overruns

The number of overruns on the HSSI circuit. An overrun occurs when HSSI cannot keep pace with the flow of incoming data and loses all or part of a frame. This is an indication of congestion and can be expected in modest numbers on high bandwidth applications.

HDLC Aborts

The number of frames received with abort status.

Desc. Ring Errors

The number of receive ring error events.

Lack of Buffers

The number of frames dropped from reception because of lack of buffer space. This is an indication of congestion and can be expected in modest numbers on high bandwidth applications.

Miscellaneous Errors

You access the HSSI miscellaneous error statistics by displaying the HSSI Miscellaneous Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/HSSI/Misc Errors option. The HSSI Miscellaneous Error Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the HSSI circuit.

Slot and Conn.

The physical location of the HSSI module within the Wellfleet router.

Tx Clip Frames

The number of frames queued for transmission that were discarded because of transmit congestion.

Pkt Buffer Misses

The number of failures to obtain a packet buffer while attempting to replenish the Rx ring.

Port Errors

The number of port operation error events.

Internal Errors

The number of internal operation error events.

Host Parity Errors

The number of parity errors that occurred during accesses to internal registers.

T1 Statistics

You access T1 error statistics by displaying the T1 Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/T1 Errors option. The T1 Error Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the T1 circuit.

Slot and Conn.

The physical location of the T1 module within the Wellfleet router.

Errors: Frame Bit

The number of frame bit errors (the reception of framing bits that do not conform to the expected framing format, D4 or ESF).

Errors: Out of Frame

The number of out-of-frame conditions, indicating a loss of synchronization in the incoming data.

Errors: Superframe

The number of errored ESF superframes.

Alarms: Yellow

The number of received Yellow Alarms (or RAI, Remote Alarm Indications). A Yellow Alarm indicates a "remotely-detected" failure that is sent back to the failure source. Receipt of a Yellow Alarm indicates a local T1 problem.

Alarms: Red

The number of received Red Alarms. A Red Alarm indicates a "locally-detected" failure, such as loss of synchronization, incoming signal loss, or hardware failures. Receipt of a Red Alarm indicates a remote T1 problem.

Bipolar Violations

The number of excessive bipolar violation conditions (defined as the receipt of 1544 bipolar violations within 1000 consecutive seconds).

Lost Carriers

The number of instances of carrier loss. Carrier loss is defined as the reception of 32 consecutive 0's.

Token Ring Statistics

The Wellfleet router gathers the following types of Token Ring statistics for each circuit:

- Token Ring frame reception data
- Token Ring frame transmission data
- Token Ring ring error data
- Miscellaneous Token Ring errors
- Token Ring ring status statistics
- Token Ring ring open status statistics
- Token Ring end station support statistics

The sections that follow describe how to display and interpret this data.

Token Ring Traffic

You access a summary listing of Token Ring traffic by displaying the Token Ring Traffic Statistics Window. Begin at the Circuit Statistics Window and select the Traffic/TOKEN Traffic option. The Token Ring Traffic Statistics Window is displayed.

The Token Ring Traffic Statistics Window provides a summary description of the reception and transmission activity across each Token Ring circuit.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

The Token Ring Traffic Statistics Window displays the following data:

Circuit Name

The name of the Token Ring circuit.

Slot and Conn.

The physical location of the Token Ring module within the Wellfleet router.

In Octets

The number of octets received by the Token Ring circuit since it was last reset.

Out Octets

The number of octets transmitted by the Token Ring circuit since it was last reset.

Frames Received

The Frames Received portion of the Token Ring Traffic Statistics Window displays the following statistics:

Total

The number of frames received by the Token Ring circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

An approximation of the number of frames received by the Token Ring circuit during the last second.

Average/s

An approximation of the number of frames received per second by the Token Ring circuit since it was last reset.

Peak/s

An approximation of the greatest number of frames received per second by the Token Ring circuit since it was last reset.

Frames Transmitted

The Frames Transmitted portion of the Token Ring Traffic Statistics Window displays the following statistics:

Total

The number of frames transmitted by the Token Ring circuit since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

An approximation of the number of frames transmitted by the Token Ring circuit during the last second.

Average/s

An approximation of the number of frames transmitted per second by the Token Ring circuit since it was last reset.

Peak/s

An approximation of the greatest number of frames transmitted per second by the Token Ring circuit since it was last reset.

Token Ring Errors

The sections that follow describe how to display and interpret the Token Ring ring error and miscellaneous error statistics.

Ring Errors

You access the Token Ring ring error statistics by displaying the TokenRing Ring Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/TOKEN/Ring Errors option. The TokenRing Ring Error Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the Token Ring circuit.

Slot and Conn.

The physical location of the Token Ring module within the Wellfleet router.

Line Errors

The number of frames copied or repeated which were badly formatted or contained a faulty FCS. Generally, a line error indicates a code violation between the starting and ending frame delimiter, a code violation within a token, or an FCS error.

Burst Errors

The number of burst errors detected by the Token Ring chip set. A burst error indicates that the chip set failed to detect any signal transitions for 5 1/2 bit times between the starting and ending frame delimiter.

Ari Fci Errors

The number of ARI (address recognized indicator)/FCI (frame copied indicator) set errors detected by the Token Ring chip set An ARI/FCI error generally indicates that the upstream neighbor is unable to sets its ARI/FCI bits in a frame that it has copied.

Frame Errors

The number of Lost Frame Errors detected by the Token Ring chip set. A Lost Frame Error occurs when Token Ring (while in stripping mode) fails to receive back the entire frame which it had transmitted.

Congestion Errors

The number of receive congestion errors, indicating that Token Ring was unable to process a frame addressed to it because of a lack of buffer space.

Frame Copy Errors

The number of Frame Copied Errors detected by the Token Ring chip set. A Frame Copied Error indicates that Token Ring received a frame addressed to it, but found the frame's ARI bits set to a value other than zero. Frame Copied Errors may indicate duplicate addresses on the ring.

Token Errors

The number of Token Errors detected by the Token Ring chip set. This statistic is incremented only when this Token Ring is the Active Monitor, and indicates that the Token Ring has detected a violation within the token.

DMA Bus Errors

The number of bus errors that occurred during read/write operations between the Token Ring chip set and the Wellfleet router.

DMA Parity Errors

The number of parity errors that occurred during read/write operations between the Token Ring chip set and the Wellfleet router.

Miscellaneous Errors

You access the Token Ring miscellaneous error statistics by displaying the Token Ring Miscellaneous Error Statistics Window. Begin at the Circuit Statistics Window and select the Error/TOKEN/Misc Errors option. The Token Ring Miscellaneous Error Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the Token Ring circuit.

Slot and Conn.

The physical location of the Token Ring module within the Wellfleet router.

Upstream MAC Address

The MAC address of the upstream neighbor.

Tx. Clip Frames

The number of frames queued for transmission that were discarded because of transmit congestion.

Pkt Buf Misses

The number of Rx ring packet buffer requests that were denied because there were no free buffers. This is an indication of congestion, but does not necessarily indicate that packets have been lost as a result of this congested condition.

Fatal Adapter Errors

The number of unrecoverable hardware or software errors in the Token Ring adapter on the link module. This is a serious condition although the adapter will restart, and will be disabled only if the condition(s) persist.

Cmd Timeouts

The number or re-initializations caused by command timeouts.

Ring Status Statistics

You access the Token Ring ring status statistics by displaying the TokenRing Ring Status Statistics Window. Begin at the Circuit Statistics Window and select the Status/TOKEN/Ring Status option. The TokenRing Ring Status Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the Token Ring circuit.

Slot and Conn.

The physical location of the Token Ring module within the Wellfleet router.

Signal Losses

The number of ring signal losses detected.

Hard Errors

The number of events that caused the Token Ring chip set to transmit or receive beacons.

Soft Errors

The number of soft errors that the Token Ring chip set reported to the Ring Error Monitor (REM).

Transmit Beacons

The number of events that caused the Token Ring chip set to transmit beacons.

Lobe Wire Faults

The number of cable faults between the Token Ring chip set and the Media Attachment Unit (MAU).

Removal Errors

The number of lobe wrap test failures during the beacon auto-removal process.

Request Moves

The number of "Remove Ring Station" MAC frames received by the Token Ring chip set. This frame is issued the network manager to request the removal of a station from the ring.

Counter Overflows

The number of adapter error counter overflows.

Single Stations

The number of ring status change interrupts while the Wellfleet router was the sole node on the ring.

Ring Recovery

The number of Claim Token MAC frames (ring recoveries) observed on the ring.

Open Status Statistics

You access the Token Ring open status statistics by displaying the TokenRing Open Status Statistics Window. Begin at the Circuit Statistics Window and select the Status/TOKEN/Open Status option. The TokenRing Open Status Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the Token Ring circuit.

Slot and Conn.

The physical location of the Token Ring module within the Wellfleet router.

Open State

The current interface state with regard to entering or leaving the ring. Valid states and associated values are as follows:

OPENED	1
OPENING	2
CLOSING	3
OPENFAILURE	4
RINGFAILURE	5
CLOSED	6

Open Status

Indicates the success, or the reason for failure, of the station's most recent attempt to enter the ring. Valid statuses and associated values are as follows:

OPEN	1
BADPARAM	2
LOBEFAILED	3
SIGNALLOSS	4
INSERTIONTIMEOUT	5
RINGFAILED	6
BEACONING	7
DUPLICATEMAC	8
REQUESTFAILED	9
REMOVERECEIVED	10
UNKERROR	11
NOOPEN	12

End Station Support Statistics

You access the Token Ring end station support statistics by displaying the TokenRing End Station Statistics Window. Begin at the Circuit Statistics Window and select the Tables/Token Ring/ESS option. The TokenRing End Station Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the Token Ring circuit.

Protocol/SAPs

The protocol type using the Routing Information Field (RIF).

MAC Address

The MAC address of the destination node.

Routing Info Field

The Routing Information Field (RIF) that describes the path to the destination node.

Network Layer Statistics

You access network layer statistics by displaying the Protocols popup menu. Begin at the Wellfleet Statistics Manager Window, then select the Protocols option. The Protocols popup menu is displayed.

The Protocols popup menu provides access to all network layer protocol statistics.

The sections that follow describe the statistics you access by selecting the options in this window.

AppleTalk Statistics

You access AppleTalk statistics by displaying the AppleTalk Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk option. The AppleTalk Statistics Window is displayed.

The AppleTalk Statistics Window displays all configured AppleTalk interfaces and provides menu access to detailed AppleTalk statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The AppleTalk Statistics Window displays the following data:

Network.Node

The AppleTalk address of every configured AppleTalk interface.

Circuit Name

Contains the user-assigned name that identifies the source routing interface.

State

The current state (Good, Suspect, Going Bad, or Bad) of the interface.

Network Range

The network range assigned to every configured AppleTalk interface.

Default Zone Name

The user-specified default zone name for the AppleTalk network.

AppleTalk AARP Table

You access the Wellfleet router's AARP table by displaying the AppleTalk AARP Table Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/Tables/AARP Table option. The AppleTalk AARP Table Window is displayed.

The AppleTalk AARP Table Window displays the following data:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Physical address

The equivalent media-dependent physical level/machine address.

AppleTalk RTMP Table

You access the Wellfleet router's AppleTalk RTMP table by displaying the AppleTalk Routing RTMP Table Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/ Tables/RTMP Table option. The AppleTalk Routing RTMP Table Window is displayed.

The AppleTalk Routing RTMP Table Window displays the following data:

Network Range

Network range specified for the destination network.

State

The current state (Good, Suspect, Going Bad, or Bad) of the interface.

Port

The circuit or port on which the AppleTalk network is learned.

Hops

The number of hops that are required to reach the destination network.

Next Hop Network.Node

The AppleTalk address of the next hop used to reach the destination network.

AppleTalk ZIP Table

You access the Wellfleet router's ZIP table by displaying the AppleTalk ZIP Table Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/Tables/ZIP Table option. The AppleTalk ZIP Table Window is displayed.

The AppleTalk ZIP Table Window displays the following information:

The displays the following data:

Network Range

Network range specified for the destination network.

Zone Name

The zone name specified for the destination network.

AppleTalk AARP Traffic

You access the Wellfleet router's AARP traffic statistics by displaying the AppleTalk AARP Traffic Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/Traffic /AARP Stats option. The AppleTalk AARP Traffic Stats Window is displayed.

The AppleTalk AARP Traffic Stats Window displays statistics showing the reception and transmission of AppleTalk datagrams across each AppleTalk interface on the Wellfleet router as follows:

The displays the following data:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Circuit

Contains the user-assigned name that identifies the source routing interface.

AARP Probe Packets

The AARP Probe Packets portion of the AppleTalk AARP Table Window displays the following statistics:

Received

Number of AARP Probe packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Transmitted

Number of AARP Probe packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

AARP Request Packets

The AARP Request Packets portion of the AppleTalk AARP Table Window displays the following statistics:

Received

Number of AARP Request packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Transmitted

Number of AARP Request packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

AARP Response Packets

The AARP Response Packets portion of the AppleTalk AARP Table Window displays the following statistics:

Received

Number of AARP Response packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Transmitted

Number of AARP Response packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

AppleTalk DDP Traffic

You access the Wellfleet router's DDP traffic statistics by displaying the AppleTalk DDP Traffic Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/ Traffic/DDP option. The AppleTalk DDP Traffic Stats Window is displayed.

The AppleTalk DDP Traffic Stats Window displays statistics showing the reception and transmission of AppleTalk datagrams across each AppleTalk interface on the Wellfleet router as follows:

The displays the following data:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Circuit

Contains the user-assigned name that identifies the source routing interface.

Output Requests

The total number of DDP packets that were supplied to the DDP entity on this circuit by local DDP clients in request for transmission. (This does not include those DDP packets counted in the Forward Requests column).

Output No Routes

The total number of DDP packets that were dropped by this circuit because a route could not be found to their final destination.

Input Receives

The total number of DDP packets received by the DDP entity on this circuit, including those received in error.

Local Datagrams

The total number of DDP packets received on this circuit for which this circuit was their final destination.

Forward Requests

The total number of DDP packets received on this circuit for which this circuit was not their final destination. The router then attempted to find a route to use to forward these packets toward their final destination.

AppleTalk Echo Traffic

You access the Wellfleet router's Echo traffic statistics by displaying the AppleTalk Echo Traffic Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/ Traffic/Echo option. The AppleTalk Echo Traffic Stats Window is displayed.

The AppleTalk Echo Traffic Stats Window displays statistics showing the reception and transmission of AppleTalk datagrams across each AppleTalk interface on the Wellfleet router as follows:

The displays the following data:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Circuit

Contains the user-assigned name that identifies the source routing interface.

Echo Requests

Number of Echo Request packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Echo Replies

Number of Echo Reply packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

AppleTalk NBP Traffic

You access the Wellfleet router's NBP traffic statistics by displaying the AppleTalk NBP Traffic Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/ Traffic/NBP option. The AppleTalk NBP Traffic Stats Window is displayed.

The AppleTalk NBP Traffic Stats Window displays statistics showing the reception and transmission of AppleTalk datagrams across each AppleTalk interface on the Wellfleet router as follows:

The displays the following data:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Circuit

Contains the user-assigned name that identifies the source routing interface.

The sections that follow describe the reception and transmission statistics displayed in the AppleTalk NBP Traffic Stats Window.

NBP LookUp Requests

The NBP LookUp Requests portion of the AppleTalk NBP Traffic Stats Window displays the following statistics:

In

Number of NBP LookUp Request packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of NBP LookUp Request packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

NBP LookUp Replies

The NBP LookUp Replies portion of the AppleTalk NBP Traffic Stats Window displays the following statistics:

In

Number of NBP LookUp Reply packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of NBP LookUp Reply packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

NBP Broadcast Requests

The NBP Broadcast Requests portion of the AppleTalk NBP Traffic Stats Window displays the following statistics:

In

Number of NBP Broadcast Request packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of NBP Broadcast Request packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

NBP Forward Requests

The NBP Forward Requests portion of the AppleTalk NBP Traffic Stats Window displays the following statistics:

In

Number of NBP Forward Request packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of NBP Forward Request packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

AppleTalk RTMP Traffic

You access the Wellfleet router's RTMP traffic statistics by displaying the AppleTalk RTMP Traffic Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/ Traffic/RTMP option. The AppleTalk RTMP Traffic Stats Window is displayed.

The AppleTalk RTMP Traffic Stats Window displays statistics showing the reception and transmission of AppleTalk datagrams across each AppleTalk interface on the Wellfleet router as follows:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Circuit

Contains the user-assigned name that identifies the source routing interface.

In Data Pkts

Number of valid RTMP data packets received on this interface since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out Data Pkts

Number of RTMP data packets transmitted by this interface since the interface was created, the Wellfleet router rebooted, or the slot reset.

In Req Pkts

Number of valid RTMP request packets received on this interface since the interface was created, the Wellfleet router rebooted, or the slot reset.

Route Deletes

Number of times the RTMP entity deleted a route because it was aged out of the RTMP table. These statistics help to detect routing problems.

Table Overflows

Number of times the RTMP entity tried to add a route to the RTMP table but failed because their was not enough memory available.

Next IR

The Next IR portion of the AppleTalk RTMP Traffic Stats Window displays the following statistics:

Equal Changes

The total number of times the RTMP entity changes the Next Internet Router listed in a routing entry because the hop count advertised in a routing tuple was equal to the current hop count for a particular network.

Less Changes

The total number of times the RTMP entity changes the Next Internet Router listed in a routing entry because the hop count advertised in a routing tuple was less than the current hop count for a particular network.

AppleTalk ZIP Traffic

You access the Wellfleet router's ZIP traffic statistics by displaying the AppleTalk ZIP Traffic Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/Traffic/ZIP option. The AppleTalk ZIP Traffic Stats Window is displayed.

The AppleTalk ZIP Traffic Stats Window displays statistics showing the reception and transmission of AppleTalk datagrams across each AppleTalk interface on the Wellfleet router as follows:

Network. Node

The AppleTalk address of the configured AppleTalk interface.

Circuit

Contains the user-assigned name that identifies the source routing interface.

ZIP Queries

The ZIP Queries portion of the AppleTalk ZIP Traffic Stats Window displays the following statistics:

In

Number of ZIP Query packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of ZIP Query packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

ZIP Replies

The Net Replies portion of the AppleTalk ZIP Traffic Stats Window displays the following statistics:

In

Number of ZIP Reply packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of ZIP Reply packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Extended Replies

The Extended Replies portion of the AppleTalk ZIP Traffic Stats Window displays the following statistics:

In

Number of ZIP Extended Reply packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of ZIP Extended Reply packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Net Info Replies

The Net Info Replies portion of the AppleTalk ZIP Traffic Stats Window displays the following statistics:

In

Number of ZIP GetNetInfo Reply packets received on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

Out

Number of ZIP GetNetInfo packets transmitted on each AppleTalk interface on the Wellfleet router since the interface was created, the Wellfleet router rebooted, or the slot reset.

AppleTalk Errors

You access AppleTalk error statistics by displaying the AppleTalk Error Stats Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/AppleTalk/Error Stats option. The AppleTalk Error Statistics Window is displayed.

The AppleTalk Error Statistics Window displays statistics showing the error conditions for each AppleTalk interface on the Wellfleet router as follows:

Network.Node

The AppleTalk address of the configured AppleTalk interface.

DDP Too Long

The total number of DDP packets received by this interface that were dropped because the data length portion of the packet received was larger than the data length specified in the DDP header, or because the packet exceeded the maximum DDP packet size.

DDP Too Short

The total number of DDP packets received by this interface that were dropped because the data length portion of the packet received was smaller than the data length specified in the DDP header, or because the packet exceeded the maximum DDP packet size.

DDP Broadcast

The total number of DDP packets received by this interface that were dropped because this interface was not their final destination and they were addressed to the link level broadcast (the link layer made the packet available to AppleTalk).

DDP Hop Count

The total number of DDP packets received by this interface that were dropped because this interface was not their final destination and their hop count would exceed the 15 hop count maximum if they were forwarded.

Zip Zone Conflicts

The total number of times a conflict was detected between this interface's zone information and another interface's zone information.

Zip In Errors

The total number of ZIP packets received by this interface that were dropped because of any type of error.

NBP In Errors

The total number of NBP packets received by this interface that were dropped because of any type of error.

RTMP Network Mismatch Errors

The total number of times the RTMP entity receives a data packet from a router that claims to be on a different network than the network specified for this interface. These error statistics help to detect configuration errors.

Bridge Statistics

You access Bridge traffic data by displaying the Bridge Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Bridge option. The Bridge Statistics Window is displayed.

The Bridge Statistics Window displays statistics information about each Bridge interface on the Wellfleet router.

The Bridge Statistics Window displays data for each Bridge interface on the Wellfleet router as follows:

Circuit Name

The Wellfleet router-assigned number which provides an internal identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

Bridge State

The current state (Up, Down, Initializing, or Not Present), of the interface.

Spanning Tree State

The current state (Up, Down, Initializing, or Not Present), of the Spanning Tree.

Bridge Forwarding Table

You access the Wellfleet router's Bridge's forwarding table(s) by displaying the Bridge Forwarding Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/Bridge option. The Bridge Statistics Window appears. Next, select the Bridge/Forwarding Table option; the Bridge Forwarding Table Window is displayed.

The Bridge Forwarding Table Window displays the following data:

MAC Address

A unicast address for which the bridge has forwarding or filtering information.

Port

The port on which the unicast address was learned.

Status

Indicates that the address has been learned, value is equal to 3.

Bridge Traffic

You access Bridge traffic data by displaying the Bridge Traffic Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Bridge option. The Bridge Statistics Window appears. Next, select the Bridge/Traffic Stats option; the Bridge Traffic Statistics Window is displayed.

The Bridge Traffic Statistics Window displays statistics showing the reception and transmission of IP datagrams across each Bridge interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

The Bridge Traffic Statistics Window displays data for each Bridge interface on the Wellfleet router as follows:

Circuit Name

The Wellfleet router-assigned number which provides an "internal" identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

State

The current state (Up, Down, Inactive, or Not Present), of the interface.

Datagrams Discarded

The number of datagrams that were discarded on this interface since it was last reset.

Datagrams Received

Total

The number of datagrams received on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current datagrams per second (an approximation of the number of datagrams received on the interface during the last second).

Average/s

Average datagrams per second (an approximation of the average number of datagrams received per second on the interface).

Peak/s

Peak datagrams per second (an approximation of the greatest number of IP datagrams received per second on the interface).

Datagrams Transmitted

Total

The number of datagrams transmitted on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current datagrams per second (an approximation of the number of datagrams transmitted on the interface during the last second).

Average/s

Average datagrams per second (an approximation of the average number of datagrams transmitted per second on the interface).

Peak/s

Peak datagrams per second (an approximation of the greatest number of IP datagrams transmitted per second on the interface).

Spanning Tree Global Topology

You access the Spanning Tree Algorithm topology statistics by displaying the Spanning Tree Global Topology Information Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/Bridge option to display the Bridge Statistics Window. Then, select the Spanning Tree/Global Topology option; the Spanning Tree Global Topology Information Window appears.

The Spanning Tree Global Topology Information Window displays data for pertaining to Spanning Tree on the entire Wellfleet router as follows:

Bridge ID

The 8-octet Spanning Tree Bridge ID assigned to the Wellfleet router. The first two octets specify the bridge priority while the last six octets specify the bridge MAC address (generally the MAC address of the first port).

State

The current state (Up, Down, Inactive, or Not Present), of the Spanning Tree.

Protocol Specification

The version of the Spanning Tree as follows: IEEE 802.1d.

Time Since Topology Change

The time (in one-hundredths of a second) since the Bridge last detected a topology change.

Number of Topology Changes

The number of topology changes detected by the Bridge since it was last reset or initialized.

Designated Root Bridge ID

The 8-octet ID of the Spanning Tree root bridge. The first two octets specify the bridge priority while the last six octets specify the bridge MAC address (generally the MAC address of the first port).

Root Cost

The cost to the root as seen from this Bridge.

Root Port

The port identifier of the Bridge port which affords the least-cost path to the root.

Current Maximum Age

The local (user-assigned) value assigned to the Max Age Spanning Tree parameter.

Current Hello Time

The local (user-assigned) value assigned to the Hello Time Spanning Tree parameter.

Current Forward Delay

The local (user-assigned) value assigned to the Forward Delay Spanning Tree parameter.

Configured Maximum Age

The global (root-assigned) Max Age value used throughout the Spanning Tree topology.

Configured Hello Time

The global (root-assigned) Hello Time value used throughout the Spanning Tree topology.

Configured Forward Delay

The global (root-assigned) Forward Delay value used throughout the Spanning Tree topology.

Spanning Tree Interface Topology

You access Spanning Tree interface topology statistics by displaying the Spanning Tree Interface Topology Information Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/ Bridge option to display the Bridge Statistics Window. Then, select the Spanning Tree/Interfaces Topology option; the Spanning Tree Interface Topology Information Window appears.

The Spanning Tree Interface Topology Information Window displays data for Spanning Tree interfaces on the Wellfleet router as follows:

Circuit Name

The Wellfleet router-assigned number which provides an internal identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

State

The current state (Disabled, Blocking, Listening, Learning, Forwarding, or Broken), of Spanning Tree on the interface.

Multicast Address

The MAC multicast address used as a destination for all Bridge Protocol Data Units (BPDUs) generated from this interface.

Path Cost

The contribution of this interface to the total root path cost.

Designated Root

Bridge ID

The Bridge Identifier of the bridge recorded as the root in Configuration Bridge Protocol Data Units (BPDUs) transmitted by the local designated bridge (that is, the designated bridge for the segment to which this interface connects).

Cost

The path cost of the designated port on the segment connected to this interface.

Designated Bridge

Bridge ID

The Bridge Identifier of the bridge which this interface considers to be the designated bridge for this interface's segment.

Port

The port identifier of the port on the designated bridge for this interface's segment.

Forward Transitions

The number of times this interface has transitioned from the Learning to the Forwarding state.

Spanning Tree Traffic

You access Spanning Tree traffic data by displaying the Spanning Tree Traffic Statistics Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/Bridge option. The Bridge Statistics Window appears. Next, select the Spanning Tree/Traffic Stats option; the Spanning Tree Traffic Statistics Window is displayed.

The Spanning Tree Traffic Statistics Window displays statistics showing the reception and transmission of Spanning Tree Bridge Protocol Data Units (BPDUs) across each Spanning Tree interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

The Spanning Tree Traffic Statistics Window displays data for each Spanning Tree interface on the Wellfleet router as follows:

Circuit Name

The user-assigned name which identifies the Spanning Tree/ Bridge interface.

State

The current state (Disabled, Blocking, Listening, Learning, Forwarding, or Broken), of Spanning Tree on the interface.

Spanning Tree PDUs Received

Total

The number of Spanning Tree Protocol Data Units (PDUs) received on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current datagrams per second (an approximation of the number of Spanning Tree Protocol Data Units (PDUs) received on the interface during the last second).

Average/s

The average datagrams per second (an approximation of the average number of Spanning Tree Protocol Data Units (PDUs) received per second on the interface).

Peak/s

The peak datagrams per second (an approximation of the greatest number of Spanning Tree Protocol Data Units (PDUs) received per second on the interface).

Spanning Tree PDUs Transmitted

Total

The number of Spanning Tree Protocol Data Units (PDUs) transmitted on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current datagrams per second (an approximation of the number of Spanning Tree Protocol Data Units (PDUs) transmitted on the interface during the last second).

Average/s

The average datagrams per second (an approximation of the average number of Spanning Tree Protocol Data Units (PDUs) transmitted per second on the interface).

Peak/s

The peak datagrams per second (an approximation of the greatest number of Spanning Tree Protocol Data Units (PDUs) transmitted per second on the interface).

DECnet Statistics

You access DECnet statistics by displaying the DECnet Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/DECnet option. The DECnet Statistics Window is displayed.

The DECnet Statistics Window displays all configured DECnet interfaces and provides menu access to detailed DECnet statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The DECnet Statistics Window displays the following data:

Node Type

Specifies the routing function performed by the node; 3 identifies a DECnet Level 2 router, 4 a DECnet Level 1 router, and 5 a non-routing node.

Circuit Name

Contains the user-assigned name which identifies the DECnet interface.

State

Contains the operational state of the DECnet interface as follows: 1 is UP; 2 is DOWN; 3 is INITIALIZING; and 4 is NOT PRESENT.

Area

Contains the DECnet Phase IV area number for this interface.

Node

Contains the DECnet Phase IV node number for this interface.

Adjacent Node

Contains the DECnet Phase IV address of the adjacent node.

Cost

Contains the routing cost assigned to the interface.

Hello Interval

Contains the frequency (in seconds) of *Hello* (T3) messages sent to the adjacent node on the interface.

Designated Router

Contains the DECnet Phase IV address of the designated router.

Maximum Routers

Contains the maximum number of routers (including the Wellfleet router) which may be present on the interface.

Priority

Contains the priority assigned to the Wellfleet router in the election of the designated router.

DECnet Level 1 Routing Table

You access the Wellfleet router's DECnet Level 1 Routing table by displaying the DECnet Routes Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/DECnet/Routes option. The DECnet Routes Window is displayed.

The DECnet Routes Window displays the following data:

Local Address

Contains the DECnet Phase IV address of the node.

Remote Address

Contains the DECnet Phase IV address of a destination node.

Circuit Name

Contains the DECnet interface over which the destination node is reached.

Cost

Contains the total cost to the destination node.

Hops

Contains the total hop count to the destination node.

Next Hop

Contains the DECnet Phase IV address of the next hop to the destination node.

DECnet Level 2 Routing Table

You access the Wellfleet router's DECnet Level 2 Routing table by displaying the DECnet Areas Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/DECnet/Areas option. The DECnet Areas Window is displayed.

The DECnet Areas Window displays the following data:

Area

Contains the DECnet Phase IV area number for the destination area.

State

Contains the area state: REACHABLE (4) or UNREACHABLE (5).

Cost

Contains the total cost to the destination area.

Hops

Contains the total hop count to the destination area.

Circuit Name

Contains the DECnet interface over which the destination area is reached.

Next Hop

Contains the DECnet Phase IV address of the next hop to the destination area.

DECnet Adjacencies Table

You access the Wellfleet router's DECnet Adjacencies table by displaying the DECnet Adjacencies Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/DECnet/ Adjacencies option. The DECnet Adjacencies Window is displayed.

The DECnet Adjacencies Window displays the following data:

Node

Contains the DECnet Phase IV address of the adjacent node.

Block Size

Contains the interface-specific block size negotiated by the adjacent nodes during routing initialization. The block size value includes the routing header, but does not include the data-link header.

Listen Timer

Contains the maximum time in seconds allowed to elapse before the Wellfleet router's DECnet routing layer receives a messages (either a *Hello* message or routed traffic) from the adjacent node.

Circuit Name

Contains the DECnet interface over which the adjacency is reached.

Type

Contains the type value of the adjacent node as follows: LEVEL 2 ROUTING DECnet PHASE IV (3); LEVEL 1 ROUTING DECnet PHASE IV (4); NON-ROUTING DECnet PHASE IV (5).

State

Contains the data-link layer-specific state of the adjacency as follows: INITIALIZING (1); UP (2); RUN (3); CIRCUIT REJECTED (4): DATA LINK START (5); ROUTING LAYER INITIALIZE (6); ROUTING LAYER VERIFY (7); ROUTING LAYER COMPLETE (8); OFF (9); HALT (10).

Priority

Contains the priority assigned to the adjacent node.

DECnet Traffic

You access the Wellfleet router's DECnet traffic statistics by displaying the DECnet Traffic Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/DECnet/Traffic Stats option. The DECnet Traffic Statistics Window is displayed.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

The DECnet Traffic Statistics Window displays the following data:

Circuit Name

Contains the user-assigned name which identifies the DECnet interface.

State

Contains the current state of the interface (Up, Down, Inactive, or Not Present).

Transit Packets Received

The Transit Packets Received portion of the IP Traffic Statistics Window displays the following reception statistics:

Total

Contains the number of DECnet packets received on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

Contains an approximation of the number of DECnet packets received on the interface during the last second.

Average/s

Contains an approximation of the average number of DECnet packets received per second on the interface.

Peak/s

Contains an approximation of the greatest number of DECnet packets received per second on the interface.

Transit Packets Transmitted

The Transit Packets Transmitted portion of the IP Traffic Statistics Window displays the following transmission statistics:

Total

Contains the number of DECnet packets transmitted on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

Contains an approximation of the number of DECnet packets transmitted on the interface during the last second

Average/s

'Contains an approximation of the average number of DECnet packets transmitted per second on the interface.

Peak/s

Contains an approximation of the greatest number of DECnet packets transmitted per second on the interface.

DECnet Traffic Errors

You access the Wellfleet router's DECnet traffic error statistics by displaying the DECnet Error Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/DECnet/Error Stats option. The DECnet Error Statistics Window is displayed.

The DECnet Error Statistics Window displays the following data:

Circuit Name

Contains the user-assigned name which identifies the DECnet interface.

Total Discard

Contains the total number of DECnet packets dropped on the interface for any reason.

Aged Loss

Contains the number of aged packets that were dropped on the interface.

Node Unreachable

Contains the number of DECnet packets that were dropped because they were addressed to an unknown or unreachable node.

Node Out of Range

Contains the number of DECnet packets that were dropped because the address of the destination node exceeded the value of the Max Node parameter.

Packet Too Big

Contains the number of DECnet packets that were dropped because they exceeded the maximum length.

Bad Packet Format

Contains the number of DECnet packets that were dropped because they contained a syntactically incorrect header.

Partial Rte Update

Contains a count of partial routing update losses.

Frame Relay Statistics

You access Frame Relay statistics by displaying the Frame Relay Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Frame Relay option. The Frame Relay Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the Frame Relay interface.

State

The Frame Relay state variable. Valid states and associated values are as follows:

UP	1
DOWN	2
INIT	3
NOTPRESENT	4

Status

The current status of the Frame Relay interface. Statuses and associated values are as follows:

START	1
RUNNING	2
FAULT	3
RECOVERED	4

START is the state during rebooting or initial start of the circuit; RUNNING is the state after the circuit has come up; FAULT is a transient condition indicating that errors have caused the circuit to be disabled until DLCMI recovery; RECOVERED indicates that the Wellfleet router has recovered from a previous FAULT condition.

Error Type

The type of the last monitored error as follows:

unknown error	1
packet too short	2
packet too long	3
illegal DLCI	4
unknown DLCI	5
DLCMI protocol error	6
DLCMI unknown IE	7
DLCMI sequence error	8
DLCMI unknown RPT	9
no error since reset	10
DLCMI unsupported control	11

Error Discards

The number of inbound frames dropped because of format or because the VC was not known.

Error Drops

The number of outbound frames dropped generally because the specified DLCI was unknown or because a broadcast packet is too large.

Frame Relay Protocol

You access Frame Relay protocol statistics by displaying the Frame Relay Protocol Statistics Window. Begin at the Frame Relay Statistics Window, then select the Protocol Stats option. The Frame Relay Protocol Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the SMDS interface.

State

The state of the Frame Relay V/Cas follows:

invalid	1
active	2
inactive	3
XOFF	4
control	5

V/C

The VC circuit number.

Frame Congestion: Rec FECNs

The number of received FECNs (forward explicit congestion notifications). FECNs notify the data destination that congestion is occurring.

Frame Congestion: Rec BECNs

The number of received BECNs (backward explicit congestion notifications). FECNs notify the data source that congestion is occurring.

Transmitted from V/C: Sent Frames

The number of frames sent from the Frame Relay virtual circuit.

Transmitted from V/C: Sent Octets

The number of octets sent from the Frame Relay virtual circuit.

Received from V/C: Sent Frames

The number of frames received from the Frame Relay virtual circuit.

Received from V/C: Sent Octets

The number of octets received from the Frame Relay virtual circuit.

Frames in Error: Discards

The number of inbound frames that were discarded because of format errors, because the VC was inactive, or because of unregistered protocols.

Frames in Error: Drops

The number of outbound frames that were dropped generally because the VC was not active.

IP Statistics

You access IP statistics by displaying the IP Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/ IP option. The IP Statistics Window is displayed.

The IP Statistics Window displays all configured IP interfaces and provides menu access to detailed IP statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The IP Statistics Window displays the following data:

IP Address

The IP address of every configured IP interface.

State

The current state (Up, Down, Inactive, or Not Present), of the interface.

Mac Address

The Media Access Control (physical layer), address of the interface.

Circuit

The Wellfleet router-assigned number that provides an internal identifier used by the system software.

Address Mask

The address mask of the interface.

IP Routing Table

You access the Wellfleet router's IP routing table by displaying the IP Routes Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/IP option. The IP Statistics Window is displayed. Next, select the Routes option; the IP Routes Window appears.

The IP Routes Window displays the following data:

Destination

The dotted decimal IP address of the destination network.

Metric

The cost to the destination network. Depending upon the protocol which learned the route, this may be a simple hop count or a user-assigned cost value.

Next Hop

The dotted decimal IP address of the next hop.

T/P

The route type (direct/local, invalid, or remote) and the protocol which supplied the routing information (e.g., EGP, OSPF, RIP, static configuration).

Age

The number of seconds since this route was last updated.

Index

The Wellfleet router-assigned number which identifies the interface (circuit) over which the next hop is reached.

IP ARP Table

You access the Wellfleet router's ARP table by displaying the IP Address Translation Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/IP option. The IP Statistics Window is displayed. Next, select the Arp Table Option; the IP Address Translation Table Window is displayed.

The IP Address Translation Table Window displays the following data:

IP Address

The dotted decimal IP address of the directly connected destination network.

Physical address

The equivalent media-dependent physical level/machine address.

Interface

The Wellfleet router-assigned number which identifies the interface (circuit) over which the destination is reached.

Type

The table entry type (1 for other, 2 for invalid, 3 for dynamic, or 4 for static).

IP Traffic

You access IP traffic data by displaying the IP Traffic Statistics Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/IP option. The IP Statistics Window appears. Next, select the Traffic Stats option; the IP Traffic Statistics Window is displayed.

The IP Traffic Statistics Window displays statistics showing the reception and transmission of IP datagrams across each IP interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

The IP Traffic Statistics Window displays data for each IP interface on the Wellfleet router as follows:

IP Address

The dotted decimal address of the IP interface on the Wellfleet router.

Circuit Name

The Wellfleet router-assigned number which provides an "internal" identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Datagrams Received

The Datagrams Received portion of the IP Traffic Statistics Window displays the following statistics:

Total

Number of IP datagrams received on each IP interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current IP datagrams per second (an approximation of the number of IP datagrams received on the interface during the last second).

Average/s

Average IP datagrams per second (an approximation of the average number of IP datagrams received per second on the interface).

Peak/s

Peak IP datagrams per second (an approximation of the greatest number of IP datagrams received per second on the interface).

Datagrams Transmitted

The Datagrams Transmitted portion of the IP Traffic Statistics Window displays the following statistics:

Total

Number of IP datagrams transmitted on each IP interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current IP datagrams per second (an approximation of the number of IP datagrams transmitted on the interface during the last second).

Average/s

Average IP datagrams per second (an approximation of the average number of IP datagrams transmitted per second on the interface).

Peak/s

Peak IP datagrams per second (an approximation of the greatest number of IP datagrams transmitted per second on the interface).

IP Errors

You access IP error statistics by displaying the IP Error Statistics Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/IP option. The IP Statistics Window appears. Next, select the Error Stats option; the IP Error Statistics Window is displayed.

The IP Error Statistics Window displays statistics showing the error conditions for each IP interface on the Wellfleet router as follows:

IP Address

The dotted decimal address of the IP interface on the Wellfleet router.

Circuit Name

The Wellfleet router-assigned number which provides an internal identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

Reassembly Failures

The number of times the Wellfleet router failed to reassemble an IP datagram. This count may be triggered by expiration of the Reassembly Timer, lack of buffer space, or errors in the reassembly process.

Fragment Failures

The number of times the Wellfleet router failed to fragment an IP datagram. This count may be triggered by a failure in the fragmentation process or by the discard of an IP datagram which required fragmentation but had the Do Not Fragment Bit set.

The sections that follow describe the error statistics for the input and output datagrams across each of the IP interfaces on the Wellfleet router.

Discarded Input Datagrams

The Discarded Input Datagrams portion of the IP Error Statistics Window displays the following statistics:

Bad Hdr

The number of IP datagrams received on the interface and discarded because of errors in the IP header. Such errors include faulty checksums, version number mismatches, formatting errors, time-to-live exceeded, bad IP options, etc.

Bad Addr

The number of IP datagrams received on the interface and discarded because of errors in the destination address field of the IP header. Such errors include invalid addresses (e.g. 0.0.0.0) and addresses of unsupported classes (e.g. Class E).

Bad Proto

The number of IP datagrams received on the interface and discarded because of an unknown or unsupported protocol.

No Buffers

The number of IP datagrams received on the interface and discarded because of a lack of system resources. This count does not include any IP datagrams which were discarded while awaiting reassembly.

Discarded Output Datagrams

The Discarded Output Datagrams portion of the IP Error Statistics Window displays the following statistics:

No Buffers

The number of outward bound IP datagrams that were successfully processed but were discarded because of a shortage of available buffer space.

No Routes

The number of outward bound IP datagrams that were discarded because no route could be found to their destination.

IPX Statistics

You access IPX statistics by displaying the IPX Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/IPX option. The IPX Statistics Window is displayed.

The IPX Statistics Window displays all configured IPX interfaces and provides menu access to detailed IPX statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The IPX Statistics Window displays the following data:

Circuit Name

The circuit associated with each IPX interface.

IPX State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Encapsulation Method

The encapsulation method associated with the interface: Ethernet, LSAP, Novell, or SNAP.

MAC Address

The Media Access Control (physical layer) address of the interface.

SMDS Address

The SMDS group address of the interface. In IPX, this address is read from the MAC Address.

IPX Address

The IPX address of the interface.

Cost

The cost associated with the interface.

IPX Base Routing Table

You access the IPX base routing table by selecting the Tables/Base Route Table option from the IPX Statistics Window. The IPX Base Routes Window is displayed. This window shows all current routes from all IPX routing tables as follows:

Destination

The IPX address of the destination network.

Interface

The local interface through which the next hop of this route is reached.

Next Hop

The IPX address of the next hop.

Next Hop Host

The IPX address of the next hop network. If a route is bound to an interface realized via a broadcast media, the IPX address of that interface is used.

Type

The type of route. Routes may be one of the following types:

1 Other
2 Invalid
3 Direct
4 Indirect
5 Static

Metric

The number of hops to the network destination.

Age

The number of seconds the route has been active since the last update.

IPX Base SAP Table

You access the IPX base SAP table by selecting the Tables/Base SAP Table option from the IPX Statistics Window. The IPX Base SAP Table Window is displayed. This window shows the SAP filters configured for IPX as follows:

Name

The name of the server.

Type

The type of service that is being advertised. Refer to Table 4-1 for a current list of the well-known server types.

Network Address

The network address of the service.

Host Address

The host address of the service.

Socket

The socket address of the service.

Age

The number of seconds the SAP entry has been active since the last update.

Hops

The number of hops to the service.

Interface

The network interface to the service.

Table 4-1. Well-Known Server Types

Server Type	Hexadecimal Identifier
Wild	FFFF
Unknown	0000
Print Server	0003
File Server	0004
Job Server	0005
Archive Server	0009
Remote Bridge Server	0024
Advertising Print Server	0047
Reserved Up To	8000

IPX RIP Interface Table

You access the IPX RIP interface table by selecting the Tables/RIP Interface Table option from the IPX Statistics Window. The IPX RIP Interface Table Window is displayed. This window shows the RIP packet activity over each IPX interface as follows:

Interface

The IPX interface for which entries into the RIP table currently exist.

State

The current state (Up, Down, Initializing, or Not Present) of RIP on the interface.

IPX Adjacent Host Table

You access the IPX adjacent host table by selecting the Tables/Adjacent Host Table option from the IPX Statistics Window. The IPX Adjacent Host Table Window is displayed. This window shows the configured adjacent hosts as follows:

Enabled

The state (enabled or disabled) of the adjacent host.

Network Address (Static Host)

The network address of the static adjacent host configured on this interface.

Network Address (This Host)

The host address of the static adjacent host configured on this interface.

IPX Static Route Table

You access the IPX static route table by selecting the Tables/Static Route Table option from the IPX Statistics Window. The IPX Static Route Table Window is displayed. This window shows the configured static routes as follows:

Enable

The state (enabled or disabled) of the static route.

Network Address (This Route)

The address of the destination network to which the static route is configured.

Next Hop Address

The network address of the next hop.

Next Hop Host

The address of the next hop host.

IPX NetBIOS Static Route Table

You access the IPX NetBIOS static route table by selecting the Tables/ NetBIOS Static Route Table option from the IPX Statistics Window. The IPX NetBIOS Static Route Table Window is displayed. This window displays the configured NetBIOS static routes as follows:

Enable

The state (enabled or disabled) of the NetBIOS static route.

Address (This Route)

The address of the destination network to which the NetBIOS static route is configured.

Target Server

The name of the NetBIOS target server to which the static route is configured.

IPX Network Level SAP Filters Table

You access the IPX network level SAP filters table by selecting the Tables/SAP Filter Table option from the IPX Statistics Window. The IPX Network Level SAP Filters Window is displayed. This window displays the configured Network Level SAP filters as follows:

Enable

The state (enabled or disabled) of the SAP filter.

Target Net Address

The address of the destination network for which the SAP filter is configured.

Filter Index

The filter number assigned to the filter.

IPX Server Level SAP Filters Table

You access the IPX server level SAP filters table by selecting the Tables/SAP Server Filters option from the IPX Statistics Window. The IPX Server Level SAP Filters Window is displayed. This window displays the configured Server Level SAP filters as follows:

Enable

The state (enabled or disabled) of the SAP filter.

Server Name

The name of the server associated with the filter.

Type

The type of service associated with the filter. Refer to Table 4-1 in the *IPX Base SAP Table* section for a current list of the well-known server types.

Action

The filtering behavior: Advertise to route SAP advertisements matching the network number and type, or Suppress to drop such SAP advertisements.

Interface

The interface associated with the filter.

Filter Index

The filter number assigned to the filter.

IPX Traffic Filters Table

You access the IPX traffic filters table by selecting the Tables/Traffic Filters option from the IPX Statistics Window. The IPX Traffic Filters Window is displayed. This window displays the traffic filters configured on each IPX interface as follows:

Enable

The state (enabled or disabled) of the traffic filter.

Interface

The interface associated with the filter.

Status

The current status (Active, Inactive, or Error) of the traffic filter. Error indicates the application detected an error in the rule.

Circuit

The circuit to which the filter is applied.

IPX Traffic

You access the IPX traffic statistics by selecting the Traffic Stats option from the IPX Statistics Window. The IPX Traffic Statistics Window is displayed. This window displays statistics showing the current IPX datagram traffic rates across each IPX interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

Circuit Name

The circuit associated with each IPX interface.

State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Datagrams Received

The Datagrams Received portion of the IPX Traffic Statistics Window displays the following statistics:

Total

Number of IPX datagrams received on each IPX interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current IPX datagrams per second (an approximation of the number of IPX datagrams received on the interface during the last second).

Average/s

Average IPX datagrams per second (an approximation of the average number of IPX datagrams received per second on the interface).

Peak/s

Peak IPX datagrams per second (an approximation of the greatest number of IPX datagrams received per second on the interface).

Datagrams Forwarded

The Datagrams Forwarded portion of the IPX Traffic Statistics Window displays the following statistics:

Total

Number of IPX datagrams forwarded from each IPX interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current IPX datagrams per second (an approximation of the number of IPX datagrams forwarded from the interface during the last second).

Average/s

Average IPX datagrams per second (an approximation of the average number of IPX datagrams forwarded from the interface per second).

Peak/s

Peak IPX datagrams per second (an approximation of the greatest number of IPX datagrams forwarded from the interface per second).

Datagrams Delivered

The Datagrams Delivered portion of the IPX Traffic Statistics Window displays the following statistics:

Total

Number of IPX datagrams delivered to each IPX interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current IPX datagrams per second (an approximation of the number of IPX datagrams delivered to the interface during the last second).

Average/s

Average IPX datagrams per second (an approximation of the average number of IPX datagrams delivered to the interface per second).

Peak/s

Peak IPX datagrams per second (an approximation of the greatest number of IPX datagrams delivered to the interface per second).

Datagrams Transmitted

The Datagrams Transmitted portion of the IPX Traffic Statistics Window displays the following statistics:

Total

Number of IPX datagrams transmitted on each IPX interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current IPX datagrams per second (an approximation of the number of IPX datagrams transmitted on the interface during the last second).

Average/s

Average IPX datagrams per second (an approximation of the average number of IPX datagrams transmitted per second on the interface).

Peak/s

Peak IPX datagrams per second (an approximation of the greatest number of IPX datagrams transmitted per second on the interface).

IPX Traffic Errors

You access the IPX traffic error statistics by selecting the Error Stats option from the IPX Statistics Window. The IPX Traffic Error Statistics Window is displayed. This window displays statistics showing the error conditions for each IPX interface on the Wellfleet router as follows:

Circuit

The circuit associated with each IPX interface.

Datagrams Discarded – Bad IPX Hdr

The number of IPX datagrams received on the interface and discarded because of errors in the IPX header. Such errors include faulty checksums, version number mismatches, formatting errors, time-to-live exceeded, bad IPX options, etc.

Datagrams Discarded – Inv Dest Field

The number of IPX datagrams received on the interface and discarded because of an invalid destination in the destination field.

No Route

The number of IPX datagrams received on the interface and discarded because no route could be found to transmit them to their destination.

OSPF Statistics

You access OSPF statistics by displaying the OSPF Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/OSPF option. The OSPF Statistics Window is displayed.

The OSPF Statistics Window displays all configured OSPF interfaces and provides menu access to detailed OSPF statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The OSPF Statistics Window displays the following data:

IP Address

The IP address of every configured OSPF interface.

Area ID

The area to which this interface belongs

State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Cost

The cost metric assigned to this interface.

Priority

The priority value assigned to this interface.

Designated Router

The router that this interface knows to be the designated router for this network.

Backup Designated Router

The router that this interface knows to be the backup designated router for this network.

OSPF Global Topology Statistics

You access OSPF global topology statistics by displaying the OSPF Global Topology Statistics Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Globals option; the OSPF Global Topology Statistics Window appears.

The OSPF Global Topology Statistics Window displays OSPF information pertaining to the entire Wellfleet router. The OSPF Global Topology Statistics Window displays the following data:

Global State

The state of OSPF on the entire Wellfleet router, either enabled or disabled.

Router ID

The IP address Router ID that uniquely identifies this router.

Version Number

The version of OSPF that this router is running.

Area Border Router

Indicates whether or not this router is an area border router.

Autonomous System Boundary Router

Indicates whether or not this router is an AS boundary router.

Type of Service

Indicates whether or not this router supports optional type-of-service routing

OSPF Area Statistics

You access OSPF area statistics by displaying the OSPF Areas Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Areas option; the OSPF Areas Window appears.

The OSPF Areas Window displays OSPF information pertaining to each OSPF area in the OSPF autonomous system. The OSPF Areas Window displays the following data:

Area ID

The four octet dotted decimal number that uniquely identifies this area with the OSPF autonomous system.

State

The state of the area, either enabled or disabled.

Authentication Type

Indicates whether or not authentication exists for this area; either Simplepassword (authentication exists), or None (no authentication exists).

Import AS Extern

Indicates whether or not this area will import AS external advertisements. If NO, this area is a stub area.

Stub Metric

The cost of the default route advertised into the stub area if this area is indeed a stub area.

OSPF Area Range Statistics

You access OSPF area statistics by displaying the OSPF Areas Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Area Range option; the OSPF Areas Table Window appears.

The OSPF Areas Table Window displays OSPF information pertaining to each OSPF area range in the OSPF autonomous system. The OSPF Areas Table Window displays the following data:

Area ID

The four octet dotted decimal number that uniquely identifies the area to which this range belongs.

State

The state of the area range, either enabled or disabled.

Net

Identifies an IP network resident within this OSPF area.

Mask

The network or Wellfleet router mask value.

OSPF Link State Database Statistics

You access link state database statistics by displaying the OSPF LSDB Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Link State DB option; the OSPF LSDB Table Window appears.

The OSPF LSDB Table Window displays OSPF information pertaining to each router's link state database. The OSPF LSDB Table Window displays the following data:

Area ID

The four octet dotted decimal number that uniquely identifies the area to which this router belongs.

Type

Type of link state advertisement (router links, network links, network summary links, AS boundary summary links, or external links).

Link State ID

The link state ID: LS_RTR (originating router's ID), LS_NET (IP interface address of network's designated router), LS_SUM_NET (destination network's IP address), LS_SUM_ASB (router ID of described ASB router), LS_ASE (destination network's IP address).

Router ID

The advertising router of this advertisement.

Sequence

The sequence number of this advertisement.

Age

The age of the advertisement.

Checksum

The checksum of this advertisement.

Adv Len

The length of advertisement.

OSPF Interface Configuration Statistics

You access interface configuration statistics by displaying the OSPF Interface Configuration Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the IF Details/IF Configuration option; the OSPF Interface Configuration Window appears.

The OSPF Interface Configuration Window displays OSPF information pertaining to each OSPF interface, as follows:

IP Address

The IP address of each configured OSPF interface.

Type of Interface

Type of this interface: bcast, point-to-point, or nbma

State of Interface

The state of the interface: Dr, Backup Dr, Dr Other, Loopback, Point-to-Point, or Waiting.

Transit Delay

The estimated number of seconds it takes to transmit a link-state update over this interface,

Retrans. Interval

The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface.

Hello Interval

The number of seconds between Hello Packets that the router sends over this interface.

Router Dead Interval

The number of seconds that a router's Hello Packets have not been seen before it's neighbors declare the router down.

Poll Interval

The largest number of seconds, allowed by this interface, between Hello Packets sent to an inactive non-broadcast multi-access neighbor.

OSPF Interface Activity Statistics

You access interface activity statistics by displaying the OSPF Interface Activity Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the IF Details/IF Activity option; the OSPF Interface Activity Window appears.

The OSPF Interface Activity Window displays OSPF information pertaining to the activity of each OSPF interface, as described in the following sections.

Messages Received

IP Address

The IP address of each configured OSPF interface.

Hello

The total number of Hello Packets received on this interface.

DB Description

The number of Database Description packets received on this interface.

Link St Request

The total number of Link State Requests received on this interface.

Link St Update

The total number of Link State Updates received on this interface.

Link St Ack

The total number of Link State Acknowledgments received on this interface.

Drops

The total number of packets that have been dropped by this interface.

State

The state of this interface, either enabled or disabled.

Messages Transmitted

IP Address

The IP address of each configured OSPF interface.

Hello

The total number of Hello Packets transmitted on this interface.

DB Description

The number of Database Description packets received on this interface.

Link St Request

The total number of Link State Requests transmitted on this interface.

Link St Update

The total number of Link State Updates transmitted on this interface.

Link St Ack

The total number of Link State Acknowledgments transmitted on this interface.

OSPF Virtual Interface Configuration Statistics

You access virtual interface configuration statistics by displaying the OSPF Virtual Interface Configuration Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the IF Details/V IF Configuration option; the OSPF Virtual Interface Configuration Window appears.

The OSPF Virtual Interface Configuration Window displays OSPF information pertaining to each OSPF virtual interface, as follows:

Area ID

The four octet dotted decimal number that identifies the transit area for this virtual interface.

State

State of the interface, either Down or Point-toPoint.

Neighbor

Router ID of virtual neighbor.

Transit Delay

The estimated number of seconds it takes to transmit a link-state update over this interface,

Retrans. Interval

The number of seconds between link state advertisement retransmissions for adjacencies belonging to this interface.

Hello Interval

The number of seconds between Hello Packets that the router sends over this interface.

Router Dead Interval

The number of seconds that a router's Hello Packets have not been seen before it's neighbor declares the router down.

OSPF Neighbor Statistics

You access neighbor statistics by displaying the OSPF Neighbors Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Neighbors/Neighbors Table option; the OSPF Neighbors Table Window appears.

The OSPF Neighbors Table Window displays information pertaining to each the router's neighbors, as follows:

Neighbor IP Address

The IP address router ID that identifies the neighbor.

State of Relationship

The relationship between the router and this neighbor (Down, Attempt, Init, 2 Way, Exch Start, Exchange, Loading, or Full).

Neighbor IF IP Address

The IP address of the interface that connects this router to this neighbor.

Neighbor Router ID

The Neighbor's Router ID.

Options

The neighbor option field. If bit 0 is set, this area accepts external information. If it is not set, this area is a stub area.

Priority

The priority of this neighbor in the designated router election algorithm.

Events

The number of times this neighbor relationship has changed states.

Retransmit Queue len

The current length of the retransmission queue.

OSPF Virtual Neighbor Statistics

You access virtual neighbor statistics by displaying the OSPF Virtual Neighbors Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Neighbors/Virtual Neighbors Table option; the OSPF Virtual Neighbors Table Window appears.

The OSPF Virtual Neighbors Table Window displays information pertaining to each the router's virtual neighbors, as follows:

Transit Area ID

The transit area of the virtual link that connects this router to the virtual neighbor.

State of Relationship

The relationship between the router and this virtual neighbor (Down, Attempt, Init, 2 Way, Exch Start, Exchange, Loading, or Full).

Neighbor IP Address

The IP address router ID that identifies the virtual neighbor.

Neighbor Router ID

The Neighbor's Router ID.

Options

The neighbor option field. If bit 0 is set, this area accepts external information. If it is not set, this area is a stub area.

Priority

The priority of this neighbor in the designated router election algorithm.

Events

The number of times this neighbor relationship has changed states.

Retransmit Queue len

The current length of the retransmission queue.

OSPF Dynamic Neighbor Statistics

You access dynamic neighbor statistics by displaying the OSPF Dynamic Neighbor Table Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/OSPF option. The OSPF Statistics Window is displayed. Then, select the Neighbors/Dynamic Neighbors Table option; the OSPF Dynamic Neighbors Table Window appears.

The OSPF Dynamic Neighbors Table Window displays information pertaining to each the router's virtual neighbors, as follows:

Neighbor IP Address

The IP address router ID that identifies the neighbor.

State of Relationship

The relationship between the router and this virtual neighbor (Down, Attempt, Init, 2 Way, Exch Start, Exchange, Loading, or Full).

Neighbor IF IP Address

The IP address of the interface that connects this router to this neighbor.

Neighbor Router ID

The Neighbor's Router ID.

Options

The neighbor option field. If bit 0 is set, this area accepts external information. If it is not set, this area is a stub area.

Priority

The priority of this neighbor in the designated router election algorithm.

Events

The number of times this neighbor relationship has changed states.

Retransmit Queue len

The current length of the retransmission queue.

Protocol Prioritization Statistics

You access Protocol Prioritization traffic data by displaying the Protocol Prioritization Statistics Windows. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Protocol Prioritization option. The initial Protocol Prioritization Statistics Window is displayed.

The initial Protocol Prioritization Statistics Window displays statistics information about each Protocol Prioritization interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

Circuit Name

The Wellfleet router-assigned number which provides an internal identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

State

The current state (Up, Down, Initializing, or Not Present), of the interface.

High

The queue depth (in packets), of the high priority queue on this interface.

Normal

The queue depth (in packets), of the normal priority queue on this interface.

Low

The queue depth (in packets), of the low priority queue on this interface.

Max Interrupt Latency

The latency value (in milliseconds), of the interrupt queue on this interface. This is non-configurable.

Max High Priority Latency

The latency value (in milliseconds), of the high priority queue on this interface.

Protocol Prioritization Traffic

You access Protocol Prioritization traffic data by displaying the second Protocol Prioritization Statistics Window. Begin at the Wellfleet Statistics Manager Window, and select the Protocols/Protocol Prioritization option. The initial Protocol Prioritization Statistics Window appears. Next, select the Protocol Prioritization Stats option; the second Protocol Prioritization Statistics Window is displayed.

The second Protocol Prioritization Statistics Window displays statistics showing the reception and transmission of packets across each Protocol Prioritization interface on the Wellfleet router, as follows:

Circuit Name

The Wellfleet router-assigned number which provides an "internal" identifier used by the system software. You can use the Circuit Name in the Circuit Statistics Window to map this numeric identifier to a specific slot and connector.

State

The current state (Up, Down, Inactive, or Not Present), of the interface.

Transmitted

High

The total number of packets transmitted from the high priority queue on this interface.

Normal

The total number of packets transmitted from the normal priority queue on this interface.

Low

The total number of packets transmitted from the low priority queue on this interface.

Clipped Packets

High

The total number of packets clipped (discarded), from the high priority queue on this interface.

Normal

The total number of packets clipped (discarded), from the normal priority queue on this interface.

Low

The total number of packets transmitted from the low priority queue on this interface.

High Water Packets

Interrupt Queue

The greatest number of packets that have been in this interface's transmit queue at any one time since last reset.

High Q

The greatest number of packets that have been in this interface's high priority queue *at any one time* since last reset.

Normal Q

The total number of packets that have been in this interface's normal priority queue *at any one time* since last reset.

Low

The total number of packets that have been in this interface's low priority queue *at any one time* since last reset.

Clear

The last time that the High Water Packet counters were reset.

Miscellaneous

Drop Packet

The number of packets that were filtered in Protocol Prioritization.

Large Packet

The number of packets that became exceptions to the latency rules.

Rx Packet

The number of packets received on this interface since last reset.

SMDS Statistics

You access Switched Multi-Megabit Data Service (SMDS) statistics by displaying the SMDS Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/SMDS option. The SMDS Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the SMDS interface.

SMDS State

The SMDS state variable. Valid states and associated values are as follows:

UP	1
DOWN	2
INIT	3
NOTPRESENT	4

LMI NM

The state of LMI network management.

ENABLED	1
DISABLED	2

Indiv Addr

The SMDS E.164 individual address for this interface.

Group Addr

The SMDS E.164 group address for this interface.

ARP Addr

The SMDS E.164 ARP address for this interface.

SMDS Traffic

You access SMDS traffic statistics by displaying the SMDS Traffic Statistics Window. Begin at the SMDS Statistics Window, then select the Traffic Stats option. The SMDS Traffic Statistics Window is displayed.

This window displays the following data:

Circuit Name

The name of the SMDS interface.

SIP L3 PDUs Received: Indiv Addr

The total number of individually addressed, error-free SMDS Interface Protocol (SIP) Level 3 protocol data units received from the remote system across the subscriber network interface (SNI).

SIP L3 PDUs Received: Group Addr

The total number of group addressed, error-free SMDS Interface Protocol (SIP) Level 3 protocol data units received from the remote system across the subscriber network interface (SNI).

SIP L3 PDUs Transmitted: Indiv Addr

The total number of individually addressed SMDS Interface Protocol (SIP) Level 3 protocol data units that have been sent across this interface to the subscriber network interface (SNI).

SIP L3 PDUs Transmitted: Group Addr

The total number of group addressed SMDS Interface Protocol (SIP) Level 3 protocol data units that have been sent across this interface to the subscriber network interface (SNI).

SMDS DXI

You access SMDS Data Exchange Interface (DXI) information through the SMDS DXI Heartbeat Table. Begin at the SMDS Statistics Window, then select the DXI Heartbeats option. The SMDS DXI Heartbeat Table Window is displayed.

This window displays the following data:

Circuit Name

The name of the SMDS interface.

State

The SMDS state variable. Valid states and associated values are as follows:

UP	1
DOWN	2
INIT	3
NOTPRESENT	4

HB Poll Enable

The state of Heartbeat Polling.

ENABLED	1
DISABLED	2

Polling Interval

The number of seconds between the transmissions of Heartbeat Poll messages.

HB Polling Messages Count Down #

The number of unacknowledged Heartbeat Poll messages that cause the interface to be taken down.

SMDS DS1 and DS3 MIB Configuration

You access DS1 MIB configuration information (corresponding to IETF RFC 1232) and DS3 MIB configuration information (corresponding to IETF RFC 1233) by displaying the DS1 or DS3 Configuration Screen. Begin at the SMDS Statistics Window, then select the LMI/DS1/Config option to display the DS1 Configuration Screen; select the LMI/DS3/Config option to display the DS3 Configuration Screen.

Both the DS1 Configuration Screen and the DS3 Configuration Screen display the following data:

Index

The Wellfleet circuit number which may range from 1 to 1024.

Time Elapsed

The number of seconds into the current fifteen minute time interval which may range from 1 to 900.

Valid Ints

The number of fifteen minute intervals over the last 24 hours in which valid data was collected. This value should equal 96 unless the CSU device was brought on line within the last 24 hours.

Line Type

The type of DS1 or DS3 implementing this interface. Possible values are as follows:

DS1

ANSI-ESF	4

DS3

OTHER	1
CBITPARITY	4
CLEARCHANNEL	5

Zero Code

The type of Zero Code Suppression used on the Wellfleet router/CSU interface. Possible values are as follows:

DS1

B8ZS	2
ZBTSI	5

DS3

B3ZS	2

Code Type

The type of code being sent across the interface by the CSU; should always read 2.

Circ ID

The CSU vendor's circuit identifier.

Loopback State

The loopback state of the CSU. Possible values are as follows:

NOLOOP	1
MGRPAYLOADLOOP	2
MGRLINELOOP	3
NETREQPAYLOADLOOP	4
NETREQLINELOOP	5
OTHERLOOP	6

Line Status

The state of the line. Possible values are as follows:

NOALARM	1
FARENDALARM	2

SMDS DS1 and DS3 Current Report

You access DS1 current fifteen minute report information and DS3 fifteen minute report information by displaying the DS1 or DS3 Current Entry Screen. Begin at the SMDS Statistics Window, then select the LMI/DS1/Current Entry option to display the DS1 Current Entry Screen; select the LMI/DS3/Current Entry option to display the DS3 Current Entry Screen.

Both the DS1 Current Entry Screen and the DS3 Current Entry Screen display the following data:

Index

The Wellfleet circuit number which may range from 1 to 1024.

ES

The number of errored seconds within the current interval: an errored second is defined as a second during which one or more CRC errors occurred, or a second during which one or more framing errors occurred.

SES

The number of severely errored seconds within the current interval: a severely errored second is defined as a second during which 320 or more CRC errors occurred, or a second during which one or more framing errors occurred.

SEFS

The number of severely errored framing seconds within the current interval: a severely errored framing second is defined as a second during which one or more framing errors occurred.

UAS

The number of unavailable seconds within the current interval: an unavailable second is defined as a second during which the CSU was in the Unavailable Signal State.

BPV

The number of bipolar violations in the current interval.

CV

The number of CRC errors in the current interval.

SMDS DS1 and DS3 Interval Logs

You access the DS1 interval log and the DS3 interval log by displaying the DS1 or DS3 Interval Table. At the SMDS Statistics Window select the LMI/DS1/Interval Table option to display the DS1 Interval Table; select the LMI/DS3/Interval Table option to display the DS3 Interval Table.

Both the DS1 Interval Table and the DS3 Interval Table display the following data:

Intervals

The fifteen minute reporting interval.

Index

The Wellfleet circuit number which may range from 1 to 1024.

Int #

The interval number, where 1 is the most recent fifteen minute interval and 96 is the least recent fifteen minute interval.

ES

The number of errored seconds within the specified interval: an errored second is defined as a second during which one or more CRC errors occurred, or a second during which one or more framing errors occurred.

SES

The number of severely errored seconds within the specified interval: a severely errored second is defined as a second during which 320 or more CRC errors occurred, or a second during which one or more framing errors occurred.

SEFS

The number of severely errored framing seconds within the specified interval: a severely errored framing second is defined as a second during which one or more framing errors occurred.

UAS

The number of unavailable seconds within the specified interval: an unavailable second is defined as a second during which the CSU was in the Unavailable Signal State.

BPV

The number of bipolar violations in the specified interval.

CV

The number of CRC errors in the specified interval.

SMDS DS1 And DS3 Cumulative Interval Reporting

You access cumulative DS1 interval reporting information and cumulative DS3 interval reporting information by displaying the DS1 or DS3 Total Table. Begin at the SMDS Statistics Window, then select the LMI/DS1/Total Table option to display the DS1 Total Table; select the LMI/DS3/Total Table option to display the DS3 Total Table.

Both the DS1 Total Table and the DS3 Total Table display the following data:

Index

The Wellfleet circuit number which may range from 1 to 1024.

ES

The total number of errored seconds: an errored second is defined as a second during which one or more CRC errors occurred, or a second during which one or more framing errors occurred.

SES

The total number of severely errored seconds: a severely errored second is defined as a second during which 320 or more CRC errors occurred, or a second during which one or more framing errors occurred.

SEFS

The total number of severely errored framing seconds: a severely errored framing second is defined as a second during which one or more framing errors occurred.

UAS

The total number of unavailable seconds: an unavailable second is defined as a second during which the CSU was in the Unavailable Signal State.

BPV

The total number of bipolar violations.

CV

The total number of CRC errors.

SMDS Interface Protocol Tables

You access SMDS Interface Protocol (SIP) tables (corresponding to IETF RFC 1304) by displaying the SIP/L2 Table. Begin at the SMDS Statistics Window, then select the LMI/SIP/L2 Table option. The SIP/L2 Table Window is displayed.

This window displays the following data:

Index

The Wellfleet circuit number which may range from 1 to 1024.

L2 PDUs Received

The total number of error-free SMDS Interface Protocol (SIP) Level 2 protocol data units received from the remote system across the subscriber network interface (SNI).

L2 PDUs Sent

The total number of error-free SMDS Interface Protocol (SIP) Level 2 protocol data units sent to the remote system across the subscriber network interface (SNI).

HCS/CRC

The total number of SMDS Interface Protocol (SIP) Level 2 protocol data units received from the remote system across the subscriber network interface (SNI) that were found to contain Header Check Sequence or CRC errors.

PDU Errors Received due to Len Errs

The total number of SMDS Interface Protocol (SIP) Level 2 protocol data units received from the remote system across the subscriber network interface (SNI) whose payloads were found to be of invalid length.

PDU Errors Received due to Seq # Errs

The total number of SMDS Interface Protocol (SIP) Level 2 protocol data units received from the remote system across the subscriber network interface (SNI) whose sequence number was not the number expected by the SMDS receive process.

PDU Errors Received due to BOMs

The total number of received BOM (beginning of message) Level 2 PDUs which point to an already active receive process.

BOMs/SSMs

The total number of (1) received SMDS Interface Protocol (SIP) Level 2 protocol data units with a segment type 10 (BOM, beginning of message) and a zero message id (MID), and (2) received Interface Protocol (SIP) Level 2 protocol data units with a segment type 11 (SSM, single segment message) and a non-zero message id (MID).

EOMs

The total number of received EOM (end of message) Level 2 PDUs for which no corresponding BOM (beginning of message was found).

SMDS Physical Layer Convergence Procedure Tables

You access the SMDS Physical Layer Convergence Procedure (PLCP) Tables (corresponding to IETF RFC 1304) by displaying the DS1 PLCP and the DS3 PLCP Tables. Begin at the SMDS Statistics Window, then select the LMI/SIP/DS1 PLCP Table option to display the DSI PLCP Table; select the LMI/SIP/DS3 PLCP Table option to display the DS3 PLCP Table.

Both the DS1 PLCP Table and the DS3 PLCP Table display the following data:

Index

The Wellfleet circuit number which may range from 1 to 1024.

SEFS Int

The number of severely errored framing seconds within the current interval: a severely errored framing second is defined as a second during which one or more framing errors occurred.

Alarm State

The alarm state. Possible values are as follows:

NOALARM	1
RECEIVED FAREND ALARM	2
INCOMINGLOF	3

UAS Int

The number of unavailable seconds within the current interval: an unavailable second is defined as a second during which the CSU was in the Unavailable Signal State.

Source Routing Bridge Statistics

You access Source Routing Bridge statistics by displaying the Source Routing Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Source Routing option. The Source Routing Statistics Window is displayed.

The Source Routing Statistics Window displays all configured Source Routing interfaces and provides menu access to detailed Source Routing statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The Source Routing Statistics Window displays the following data:

Circuit Name

Contains the user-assigned name that identifies the source routing interface.

SR Bridge State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Max Route Desc

Contains the maximum number of route descriptors that this interface will accept in explorer frames.

Ring Number

The user-assigned number that identifies the token ring network to which the interface connects.

Source Routing Bridge ID Table

You access the Wellfleet router's Bridge ID table by displaying the Bridge ID Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Source Routing/Bridge Tables/Bridge ID Table option. The Bridge ID Window is displayed.

The Bridge ID Window displays the following statistic:

Bridge IDs Defined

The Bridge IDs that are specified for the Wellfleet Bridges on the network.

Source Routing Bridge IP Explorer Entry Table

You access the Wellfleet router's IP Explorer Entry table by displaying the Explorer Entry Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Source Routing/Explorer Entry Table option. The Explorer Entry Window is displayed.

The Explorer Entry Window displays the following statistic:

IP Explorers Defined

The IP addresses that the Wellfleet router should forward IP explorer packets toward.

Source Routing Bridge IP Encapsulation Table

You access the Wellfleet router's Source Routing IP Encapsulation table by displaying the IP Encapsulation Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Source Routing/ IP Encaps Stats option. The Source Routing IP Encapsulation Window is displayed.

The Source Routing IP Encapsulation Window displays the following data:

Remote Ring Number

The number of the remote destination ring connected to the Wellfleet IP encapsulating router.

IP Addr

The dotted decimal address of the destination IP interface on the Wellfleet router.

Status

Indicates that the ring number was learned.

Source Routing Bridge Traffic

You access Source Routing Bridge traffic data by displaying the Source Routing Bridge Traffic Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Source Routing/ Traffic Stats option. The Source Routing Bridge Traffic Statistics Window appears.

The Source Routing Bridge Traffic Statistics Window displays statistics showing the reception and transmission of source routed frames across each source routing interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

Circuit Name

Contains the user-assigned name that identifies the source routing interface

State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Frames Received

The Frames Received portion of the Source Routing Bridge Traffic Statistics Window displays the following statistics:

Total

Number of source routed frames received on each source routing interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current source routed frames per second (an approximation of the number of frames received on the interface during the last second).

Average/s

Average source routed frames per second (an approximation of the average number of source routed frames received per second on the interface).

Peak/s

Peak source routed frames per second (an approximation of the greatest number of source routed frames received per second on the interface).

Frames Transmitted

The Frames Transmitted portion of the Source Routing Bridge Traffic Statistics Window displays the following statistics:

Total

Number of source routed frames transmitted on each source routing interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current source routed frames per second (an approximation of the number of source routed frames transmitted on the interface during the last second).

Average/s

Average source routed frames per second (an approximation of the average number of source routed frames transmitted per second on the interface).

Peak/s

Peak source routed frames per second (an approximation of the greatest number of source routed frames transmitted per second on the interface).

Source Routing Bridge Traffic Errors

You access Source Routing Bridge traffic error statistics by displaying the Source Routing Traffic Error Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/Source Routing/Error Stats option. The Source Routing Traffic Error Statistics Window is displayed.

The Source Routing Traffic Error Statistics Window displays statistics showing the error conditions for each IP interface on the Wellfleet router as follows:

Circuit Name

Contains the user-assigned name that identifies the source routing interface.

The sections that follow describe the error statistics for the input and output frames across each of the source routing interfaces on the Wellfleet router.

IP Frames Discarded

The IP Frames Discarded portion of the Source Routing Traffic Error Statistics Window displays the following statistics:

Total

The total number of source routing frames received on the interface and discarded since it was created, the Wellfleet router rebooted, or the slot reset.

Current/s

The current source routed frames per second (an approximation of the number of source routed frames discarded on the interface during the last second).

Average/s

Average source routed frames per second (an approximation of the average number of source routed frames discarded per second on the interface).

Peak/s

Peak source routed frames per second (an approximation of the greatest number of source routed frames discarded per second on the interface).

Total Frames Discarded Due to Other Factors

The Total Frames Discarded Due to Other Factors portion of the Source Routing Traffic Error Statistics Window displays the following statistics:

Bad Control Field

The number of source routing frames that were discarded due to an error in the control field portion of the frame.

Inv Incoming Ring

The number of source routing frames that were discarded due to an unexpected value for the incoming ring route descriptor.

No Next Circuit

The number of source routing frames that were discarded due to either an inactive "next" ring or to traffic filters.

VINES Statistics

You access VINES statistics by displaying the VINES Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES option. The VINES Statistics Window is displayed.

The VINES Statistics Window displays all configured VINES interfaces and provides menu access to detailed VINES statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The VINES Statistics Window displays the following data:

Circuit

Contains the user-assigned name that identifies the source routing interface.

State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Interface Type

The type of interface (Ethernet, FDDI, Synchronous, Token Ring).

MAC Address

The equivalent media-dependent physical level/machine address.

Arp

Specifies if the VINES Address Resolution Protocol is enabled on the interface.

Source Routing End Station

Specifies if Source Routing End Station support is enabled on the interface.

VINES Table of Networks

You access the Wellfleet router's VINES Table of Networks by displaying the VINES Table of Networks Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES/Address Tables/Networks option. The VINES Table of Networks Window is displayed.

The VINES Table of Networks Window displays the following data:

Destination Network

Contains the VINES address of the destination network.

Routing Metric

Contains the "cost" to the destination network.

Gateway

Contains the network number of the next hop used for reaching the destination network.

VINES Table of Neighbors

You access the Wellfleet router's VINES Table of Neighbors by displaying the VINES Table of Neighbors Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES/Address Tables/Neighbors option. The VINES Table of Neighbors Window is displayed.

The VINES Table of Neighbors Window displays the following data:

Network ID

Contains the network number of the directly connected destination network.

Subnetwork ID

Contains the subnetwork number of the directly connected destination subnetwork.

Type

Contains the neighbor type (client or server).

IF Type

Contains the type of interface on which this neighbor was learned.

Local Slot

Contains the slot on which this neighbor was learned.

Local Line

Contains the circuit number on which this neighbor was learned.

Remote MAC

Contains the MAC address of this neighbor.

Local MAC

Contains the MAC address of the Wellfleet router's interface on which this neighbor was learned.

Cost

Contains the cost to reach this neighbor. It corresponds to the interface type.

VINES Traffic

You access the Wellfleet router's VINES traffic statistics by displaying the VINES Traffic Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES/Traffic Stats option. The VINES Traffic Statistics Window is displayed.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

The VINES Traffic Statistics Window displays the following data:

Circuit Name

Contains the user-assigned name that identifies the source routing interface

State

Contains the current state of the interface (Up, Down, Inactive, or Not Present).

Messages Received

Contains the number of IPC messages received that were destined for this Wellfleet router.

Packets Received

Total

Contains the number of VINES packets received on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

Contains an approximation of the number of VINES packets received on the interface during the last second

Average/s

Contains an approximation of the average number of VINES packets received per second on the interface.

Peak/s

Contains an approximation of the greatest number of VINES packets received per second on the interface.

Packets Transmitted

Total

Contains the number of VINES packets transmitted on the interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

Contains an approximation of the number of VINES packets transmitted on the interface during the last second

Average/s

Contains an approximation of the average number of VINES packets transmitted on the interface.

Peak/s

Contains an approximation of the greatest number of VINES packets transmitted on the interface.

VINES Traffic Errors

You access the Wellfleet router's VINES traffic error statistics by displaying the VINES Error Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES/Errors Stats option. The VINES Error Statistics Window is displayed.

The VINES Error Statistics Window provides a summary description of error conditions on each VINES interface as follows:

Circuit Name

Contains the user-assigned name that identifies the source routing interface

Packets Received Errors

Contains the number of times the Wellfleet router received packets that had bad checksums or unknown protocol types.

Reassembly Failures

Contains the number of times the Wellfleet router could not successfully reassemble a VINES packet. This count may be triggered by expiration of the Reassembly Timer, lack of buffer space, or errors in the reassembly process.

The sections that follow describe the error statistics for the input and output frames across each of the VINES interfaces on the Wellfleet router.

ICP Errors

The ICP Errors portion of the VINES Error Statistics Window displays the following statistics:

Bad Packets Received

Contains the number or ICP packets received with unknown notification types or unknown error codes.

Error Notifications Received

Contains the number of ICP error notification packets received that were destined for this router. This value shows how many times this router originated packets to an unknown destination.

Error Notifications Sent

Contains the number of times the Wellfleet router could not forward a packet because a destination was unreachable and the error notification bit was set in the packet.

Discards

The Discards portion of the VINES Error Statistics Window displays the following statistics:

No Forwarding Information

Contains the number of VINES packets received on the interface and discarded because no route could be found to their destination.

Zero Hop Counts

Contains the number of VINES packets received on this interface and discarded because the hop count field was set to 0.

VINES IP Global Information Table

You access the Wellfleet router's VINES IP Global Information table by displaying the VINES IP Global Information Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES/ Protocols/Vines IP option. The VINES IP Global Information Window displays the following statistics:

Packets Received

Contains the number of VINES IP packets the Wellfleet router received.

Packets Sent

Contains the number of VINES IP packets the Wellfleet router originated.

Received with Bad Checksum

Contains the number of VINES IP packets received that were corrupted.

Routed Packets

Contains the number of VINES IP packets routed by the Wellfleet router toward other networks.

Broadcast Packets Sent

Contains the number of VINES IP broadcast packets originated by the Wellfleet router.

Packets Reassembled

Contains the number of fragmented VINES IP packets reassembled by the Wellfleet router.

Packets Fragmented

Contains the number of packets fragmented by the Wellfleet router.

VINES ARP Global Information Table

You access the Wellfleet router's ARP Global Information table by displaying the VINES ARP Global Information Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/VINES/ Protocols/Vines ARP option. The VINES ARP Information Window is displayed.

The VINES ARP Information Window displays the following statistics:

State

Contains the current state of the interface (Up, Down, Inactive, or Not Present).

Next Subnetwork ID

Contains the next subnetwork number that the Wellfleet router will assign to a client.

ARP Assignment Denied

Contains the number of VINES ARP assignment packets for which a subnetwork number was not available at the time a request was received.

XNS Statistics

You access XNS statistics by displaying the XNS Statistics Window. Begin at the Wellfleet Statistics Manager Window, then select the Protocols/XNS option. The XNS Statistics Window is displayed.

The XNS Statistics Window displays all configured XNS interfaces and provides menu access to detailed XNS statistics. This section describes the data displayed in this window. The sections that follow describe the statistics you access by selecting the options in this window.

The XNS Statistics Window displays the following data:

Circuit Name

The circuit associated with each XNS interface.

XNS State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Encapsulation Method

The encapsulation method associated with the interface: Ethernet, LSAP, or SNAP.

MAC Address

The Media Access Control (physical layer) address of the interface.

SMDS Address

The SMDS group address configured for the interface.

XNS Address

The IDP address of the interface.

Cost

The cost associated with the interface.

XNS Base Routing Table

You access the XNS base routing table by selecting the Tables/Base Route Table option from the XNS Statistics Window. The XNS Base Routes Window is displayed. This window shows all current routes from all XNS routing tables as follows:

Destination

The IDP address of the destination network.

Interface

The local interface through which the next hop of this route is reached.

Next Hop

The IDP address of the next hop.

Next Hop Host

The IDP address of the next hop network. If a route is bound to an interface realized via a broadcast media, the IDP address of that interface is used.

Type

The type of route. Routes may be one of the following types:

1 Other
2 Invalid
3 Direct
4 Indirect
5 Static

Metric

The number of hops to the network destination.

Age

The number of seconds the route has been active since the last update.

XNS RIP Interface Table

You access the XNS RIP interface table by selecting the Tables/RIP Interface Table option from the XNS Statistics Window. The XNS RIP Interface Table Window is displayed. This window shows the RIP packet activity over each XNS interface as follows:

Interface

The XNS interface for which entries into the RIP table currently exist.

State

The current state (Up, Down, Initializing, or Not Present) of RIP on the interface.

XNS Adjacent Host Table

You access the XNS adjacent host table by selecting the Tables/ Adjacent Host Table option from the XNS Statistics Window. The XNS Adjacent Host Table Window is displayed. This window shows the configured adjacent hosts as follows:

Enabled

The state (enabled or disabled) of the adjacent host.

Network Address (Static Host)

The network address of the static adjacent host configured on this interface.

Network Address (This Host)

The host address of the static adjacent host configured on this interface.

XNS Static Route Table

You access the XNS static route table by selecting the Tables/Static Route Table option from the XNS Statistics Window. The XNS Static Route Table Window is displayed. This window shows the configured static routes as follows:

Enable

The state (enabled or disabled) of the static route.

Network Address (This Route)

The address of the destination network to which the static route is configured.

Next Hop Address

The network address of the next hop.

Next Hop Host

The address of the next hop host.

XNS Traffic Filters Table

You access the XNS traffic filters table by selecting the Tables/Traffic Filters option from the XNS Statistics Window. The XNS Traffic Filters Window is displayed. This window displays the traffic filters configured on each XNS interface as follows:

Enable

The state (enabled or disabled) of the traffic filter.

Interface

The interface associated with the filter.

Status

The current status (Active, Inactive, or Error) of the traffic filter. Error indicates the application detected an error in the rule.

Circuit

The circuit to which the filter is applied.

XNS Traffic

You access the XNS traffic statistics by selecting the Traffic Stats option from the XNS Statistics Window. The XNS Traffic Statistics Window is displayed. This window displays statistics showing the current XNS datagram traffic rates across each XNS interface on the Wellfleet router.

Note: This window is equipped with a Zero Totals option. When you select this option, all statistics displayed in these windows are reset to 0.

This window displays the following data:

Circuit Name

The circuit associated with each XNS interface.

State

The current state (Up, Down, Inactive, or Not Present) of the interface.

Datagrams Received

The Datagrams Received portion of the XNS Traffic Statistics Window displays the following statistics:

Total

Number of XNS datagrams received on each XNS interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current XNS datagrams per second (an approximation of the number of XNS datagrams received on the interface during the last second).

Average/s

Average XNS datagrams per second (an approximation of the average number of XNS datagrams received per second on the interface).

Peak/s

Peak XNS datagrams per second (an approximation of the greatest number of XNS datagrams received per second on the interface).

Datagrams Forwarded

The Datagrams Forwarded portion of the XNS Traffic Statistics Window displays the following statistics:

Total

Number of XNS datagrams forwarded from each XNS interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current XNS datagrams per second (an approximation of the number of XNS datagrams forwarded from the interface during the last second).

Average/s

Average XNS datagrams per second (an approximation of the average number of XNS datagrams forwarded from the interface per second).

Peak/s

Peak XNS datagrams per second (an approximation of the greatest number of XNS datagrams forwarded from the interface per second).

Datagrams Delivered

The Datagrams Delivered portion of the XNS Traffic Statistics Window displays the following statistics:

Total

Number of XNS datagrams delivered to each XNS interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current XNS datagrams per second (an approximation of the number of XNS datagrams delivered to the interface during the last second).

Average/s

Average XNS datagrams per second (an approximation of the average number of XNS datagrams delivered to the interface per second).

Peak/s

Peak XNS datagrams per second (an approximation of the greatest number of XNS datagrams delivered to the interface per second).

Datagrams Transmitted

The Datagrams Transmitted portion of the XNS Traffic Statistics Window displays the following statistics:

Total

Number of XNS datagrams transmitted on each XNS interface since it was created, the Wellfleet router rebooted, the slot reset, or the Zero Totals option was selected.

Current/s

The current XNS datagrams per second (an approximation of the number of XNS datagrams transmitted on the interface during the last second).

Average/s

Average XNS datagrams per second (an approximation of the average number of XNS datagrams transmitted per second on the interface).

Peak/s

Peak XNS datagrams per second (an approximation of the greatest number of XNS datagrams transmitted per second on the interface).

XNS Traffic Errors

You access the XNS traffic error statistics by selecting the Error Stats option from the XNS Statistics Window. The XNS Traffic Error Statistics Window is displayed. This window displays statistics showing the error conditions for each XNS interface on the Wellfleet router as follows:

Circuit

The circuit associated with each XNS interface.

Datagrams Discarded – Bad XNS Hdr

The number of XNS datagrams received on the interface and discarded because of errors in the XNS header. Such errors include faulty checksums, version number mismatches, formatting errors, time-to-live exceeded, bad XNS options, etc.

Datagrams Discarded – Inv Dest Field

The number of XNS datagrams received on the interface and discarded because of an invalid destination in the destination field.

No Route

The number of XNS datagrams received on the interface and discarded because no route could be found to transmit them to their destination.

Chapter 5

System Administration

List of Figures

System Administration

About this Chapter

This chapter describes how to use the Site Manager to display its software version and to display the version of the Wellfleet router software. This chapter also describes how to boot a Wellfleet router, and reset a slot in the Wellfleet router.

Displaying the Site Manager and Wellfleet Router Software Versions

To display the Site Manager version number, begin at the Wellfleet Site Manager Window, then select File/Site Manager Version. The current version of the Site Manager is displayed. Also, the Wellfleet router software version that is compatible with the Site Manager is displayed.

The Description box in the Wellfleet Site Manager Window shows the software version of the Wellfleet router you are currently managing.

Compare the compatible Wellfleet router software version in the Site Manager Version Window to the Description box in the Wellfleet Site Manager Window.

Refer to the Release Notes to ensure the version of the Site Manager is compatible with the Wellfleet router software if the compatible software version does not match the router software version.

Booting the Wellfleet Router

The Site Manager provides you with the following menu options for booting the Wellfleet router:

- The boot option warm-starts the entire Wellfleet router. Pressing the Reset button on the front panel of the Wellfleet router initiates the same procedure.

  When you select the boot option, the Boot window displays the default boot image and configuration filenames. You can enter alternative files in this window.

- The reset option warm-starts a single FRE module or the entire system with the boot image and configuration currently in use on other slots. Resetting the entire system is equivalent to booting it.

  When you select the reset option, the Reset window displays the default slot. You can select another slot to reset in this window.

Refer to the following sections to boot the Wellfleet router or reset a slot. Refer to the *System Administration* chapter in *Operations: Technician Interface* to get more detailed information about how the boot image and configuration file is loaded onto each FRE module.

Booting

You select the boot option to boot the entire system. You begin from the Wellfleet Site Manager Window and proceed as follows:

1. Select the Admin/boot option.

   The Boot Window appears (see Figure 5-1.) The Boot Image and Configuration boxes display the default volume locations and default filenames of the software image (*boot.exe*) and configuration (*config*).

2. Overtype the volume locations and filenames of the image file and configuration file in the designated fields if you want to boot with alternative files.

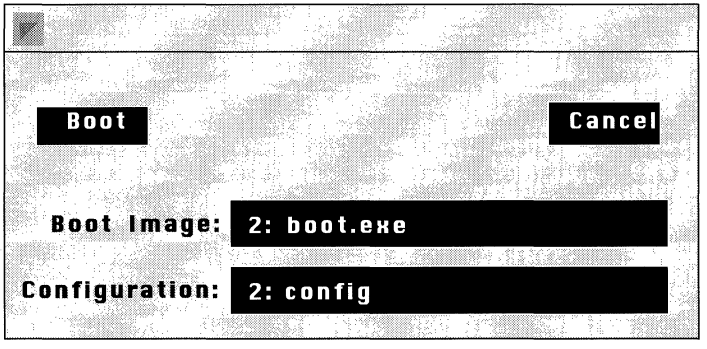


Figure 5-1. Boot Window

3. Click on Ok to boot with the default software image (*boot.exe*).

   A confirmation window appears.

4. Click on Ok.

Note: The software image and configuration file revert to their respective default file names (*boot.exe* and *config*) after every boot. To change the default boot or configuration file, back up the old default file using the copy option; then overwrite the old default file with the new default file using the copy option.

Resetting a Slot

The reset option allows you to reboot a single slot with the boot image currently in use. You begin from the Wellfleet Site Manager Window and proceed as follows:

1. Select the Admin/Reset option.

   The Reset Window appears (see Figure 5-2.)

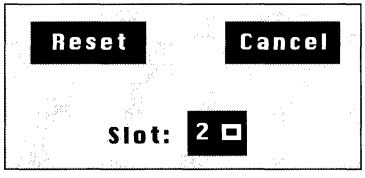


Figure 5-2. Reset Window

2. Click on the box next to the default slot number and select the slot you want to reset from the popup menu.
3. Click on Reset.

   A confirmation window appears.
4. Click the Ok button.

The following occurs when you reset a FRE module:

1. The Gate Access Management Entity (GAME) operating system software running on the FRE module forwards a boot request to the other FRE modules.
2. The first FRE module to respond to the boot request forwards the boot image resident in its memory.
3. The resetting FRE module receives and executes the boot image. At this instant, connectivity to the associated slot and the services provided in the slot are disrupted. The other FRE modules resynchronize their routing tables after the slot fails to receive packets.
4. The resetting FRE module completes the boot process and requests a configuration. The first available FRE module forwards the configuration resident in its memory.
5. The resetting FRE module loads the configuration image and initiates the services provided by the slot; connectivity is thus reestablished. The resetting FRE module alerts the other FRE modules that it can receive packets.
6. The other FRE modules resynchronize their routing tables accordingly.

Appendix A

Utilities

Utilities

About this Appendix

This appendix describes how to use the wf2asc utility. This utility reads configuration files on the Site Manager workstation and outputs them to the screen or to a file in ASCII.

Converting Configuration Files to ASCII

You may want to view a configuration file in order to see a configuration in a condensed format. However, the Wellfleet router and Site Manager software maintain configuration files in binary only.

The wf2asc utility reads binary configuration files on the Site Manager workstation and outputs them to the screen or to a file in ASCII. You can then view the output on the screen or open the new ASCII file using any text editor.

The Site Manager installation software installs the wf2asc utility in a file named *wf2asc.exe* in the *\wf\lib* path on the PC and the */usr/wf/lib* path on the SPARCstation. However, you do not have to access the path to use the wf2asc utility.

You can output the ASCII to the screen or, or to the screen and to a new file.

Enter the following after the MS-DOS *c:* prompt or in the UNIX cmdtool window to display a configuration on the screen, where <config> is the name of the configuration file to be read:

wf2asc <config>

Or, enter the following after the MS-DOS *c:* prompt or in the UNIX cmdtool window to display a configuration on the screen and write it to an ASCII file, where <config> is the name of the configuration file to be read, and <cnfgasci> is the ASCII configuration file to be created:

wf2asc <config> > <cnfgasci>

Refer to the following sample commands.

Examples

If you enter:	The following occurs:
wf2asc config2.cfg	The wf2asc utility reads the *config2.cfg* file and outputs it to the screen in ASCII.
wf2asc config3.cfg > cfg3.asc	The wf2asc utility reads the *config3.cfg* file, outputs it to the screen in ASCII, and creates an ASCII configuration file named *cfg3.asc*.