CHAPTER 1

About LightStream 2020 Traps

This chapter provides an overview of trap messages generated by the LightStream 2020 multiservice ATM switch (LS2020 switch). It describes how traps are generated, the types of traps generated, their formats, and their relative priorities.

Traps inform you of network events. When a network event occurs, the LS2020 switch sends a trap message, or possibly a series of messages, to one or more user-specified destinations, such as the network management station (NMS) or a log file on the switch. A trap may notify you of a serious condition that requires immediate corrective action, or it may give you information that, while important, may not require any action. You can initiate further interaction with an LS2020 switch to determine the nature and extent of the event signaled by the trap.

Another aspect of traps is called *trap filter levels.* By assigning a trap filter level, you can control which trap types are viewed where. This allows you, for instance, to save some traps in the traps log, view other traps on your console, and view still others on your NMS.

How Traps Are Generated and Reported

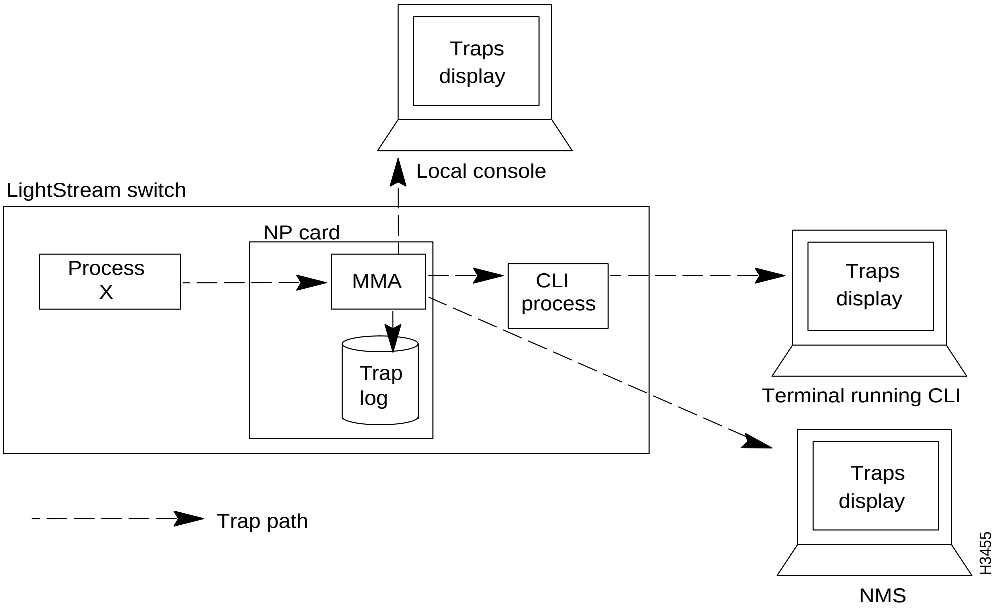
Figure 1-1 shows the flow of traps through the LS2020 system. Traps are passed from software processes to another process called the master management agent (MMA). By default, the MMA writes the traps to a log file on the switch's network processor (NP). From there, traps are sent to the local console, if one is present. Traps can also be displayed on one or more NMSs, as well as on a terminal running the CLI.

Note If you are using an NMS, only one instance of the CLI can run on the NMS at any given time.

By default, a switch sends traps only to its trap log and to its local console. However, you can configure a switch to send traps to another NP or to an NMS for viewing. You can do that if you want to collect traps for all the switches in the network in a single place or to send traps to as many as 25 different destinations in the network. See the *LightStream 2020 Installation Guide* for information about changing trap delivery addresses.

You can also copy a switch's trap log to an NMS or workstation and view it there. See the section entitled "Moving the Trap Log from the NP" in the chapter "Managing LightStream 2020 Traps" for information about copying the trap log to another LS2020 system.

Figure 1-1 The Paths Traps Travel in a LightStream 2020 System



Trap Message

This section describes the types of traps generated by an LS2020 switch and the format of those traps.

Trap Types

LS2020 switches generate five types of traps:

SNMP Traps—Are the standard SNMP traps defined by the SNMP MIB-2 specifications. Such traps are displayed as "generic" traps. SNMP traps are used by LS2020 network operators.

`Link Up` and `Link Down` are examples of SNMP traps.

Operational Traps—Provide information on key system components. Operational traps are of primary interest to network operators.

`Port 3 down` is an example of an operational trap.

Operational traps are divided into three categories:

- Traps that provide information only, such as notification that a line card has come up.
- Traps that require a response. These traps indicate problems that you can usually fix by following the procedures described in this manual.
- Traps that require you to contact your customer support representative. These traps indicate that there may be a problem with LS2020 software. Such traps are *very* unlikely to occur. However, if you receive a trap in this category, it is important that you record it and contact your customer support representative immediately, so that remedial action can be taken.

Within each software process, operational traps are numbered from 1 to 1999. Traps numbered from 1000 to 1999 are generally not documented here, because your only response in such cases is calling your customer service representative.

Informational Traps—Provide supplemental details on problems that are reported by some operational and SNMP traps. Informational traps are used by customer support representatives to do advanced troubleshooting and software debugging.

The following is an example of an informational trap:

```
Trunk emtb7.2.5->emtb8.4.2 DOWN [transitioning to down (from has-vci)]
```

Within each software process, informational traps are numbered from 2000 to 2999.

Trace Traps—Are used to track a sequence of actions through a process. Customer support representatives use trace traps to do advanced troubleshooting and software debugging. Within each software process, trace traps are numbered from 3000 to 3999. Because trace traps are not intended for customer use, they are not discussed in detail in this manual.

Debug Traps—Are used to find and solve serious software problems in an LS2020 switch. Debug traps are used by customer support representatives and developers. Within each software process, debug traps are numbered from 4000 to 4999. Because debug traps are not intended for customer use, they are not discussed in detail in this manual.

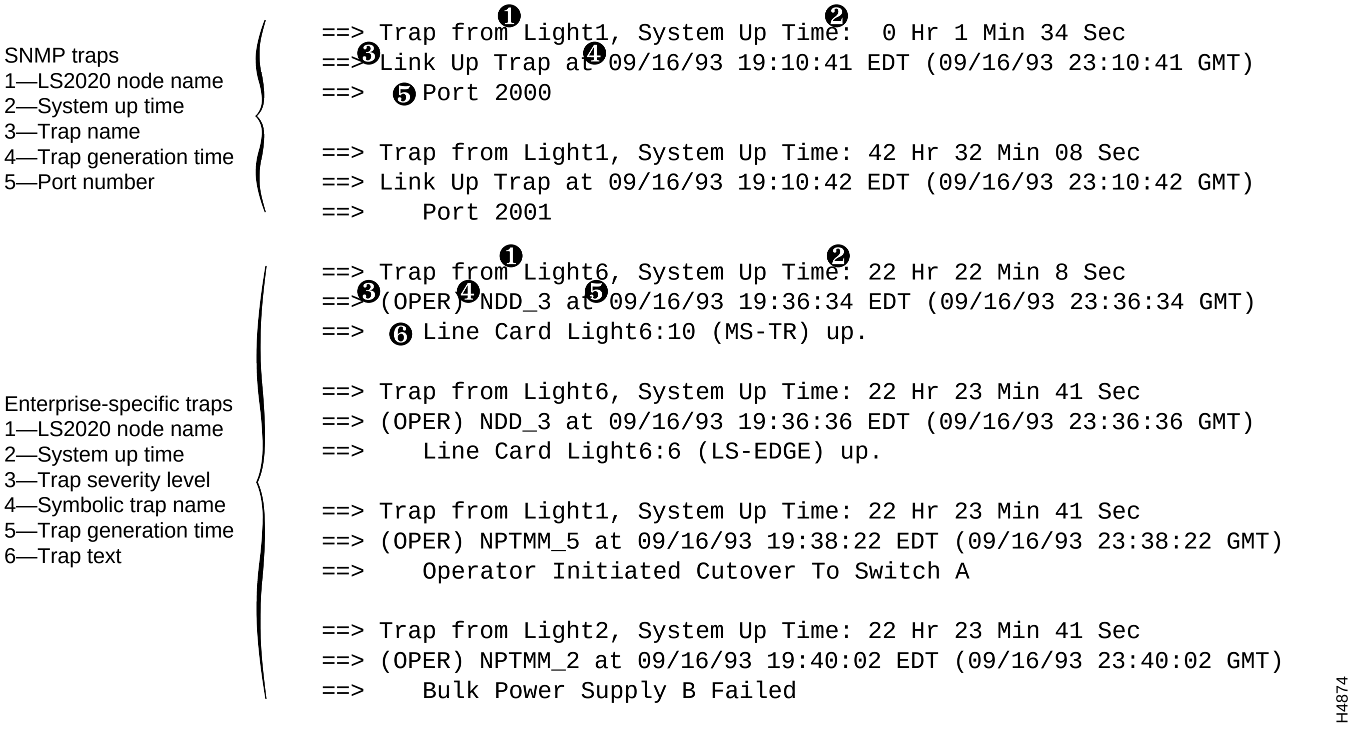
Trap Formats

Two trap formats have been defined for the LS2020 switch, one for SNMP standard traps and one for enterprise-specific traps.

The SNMP trap format is defined by prevailing MIB-2 specifications. Enterprise-specific traps pertain only to the LS2020 switch. Figure 1-2 shows a sample trap display from nodes called *Light1* and *Light6*. The display contains both SNMP standard and enterprise-specific traps.

If you are using an NMS to display traps, the display may differ somewhat in format from that shown in Figure 1-2, but the content will be identical.

Figure 1-2 Examples of SNMP Standard and Enterprise-Specific Traps


❶
❷
❸
❹
❺
❶
❷
❸
❹
❺
❻
H4874

SNMP traps
1—LS2020 node name
2—System up time
3—Trap name
4—Trap generation time
5—Port number

```
==> Trap from Light1, System Up Time:  0 Hr 1 Min 34 Sec
==> Link Up Trap at 09/16/93 19:10:41 EDT (09/16/93 23:10:41 GMT)
==>    Port 2000

==> Trap from Light1, System Up Time: 42 Hr 32 Min 08 Sec
==> Link Up Trap at 09/16/93 19:10:42 EDT (09/16/93 23:10:42 GMT)
==>    Port 2001
```

Enterprise-specific traps
1—LS2020 node name
2—System up time
3—Trap severity level
4—Symbolic trap name
5—Trap generation time
6—Trap text

```
==> Trap from Light6, System Up Time: 22 Hr 22 Min 8 Sec
==> (OPER) NDD_3 at 09/16/93 19:36:34 EDT (09/16/93 23:36:34 GMT)
==>    Line Card Light6:10 (MS-TR) up.

==> Trap from Light6, System Up Time: 22 Hr 23 Min 41 Sec
==> (OPER) NDD_3 at 09/16/93 19:36:36 EDT (09/16/93 23:36:36 GMT)
==>    Line Card Light6:6 (LS-EDGE) up.

==> Trap from Light1, System Up Time: 22 Hr 23 Min 41 Sec
==> (OPER) NPTMM_5 at 09/16/93 19:38:22 EDT (09/16/93 23:38:22 GMT)
==>    Operator Initiated Cutover To Switch A

==> Trap from Light2, System Up Time: 22 Hr 23 Min 41 Sec
==> (OPER) NPTMM_2 at 09/16/93 19:40:02 EDT (09/16/93 23:40:02 GMT)
==>    Bulk Power Supply B Failed
```

Standard SNMP traps include the following information:

- **LS2020 node name**—The system uses the IP address of the packet containing the trap to look up the name of the node in the /etc/hosts file. If the name is not available, the IP address is displayed in its place. The node name is omitted from any trap displayed on the same node where the trap was generated.
- **System up time when the trap occurred**—In the trap log (mma.traplog) or on the console display, the system up time indicates when the MMA received the trap. In the CLI display, however, the system up time indicates the up time of the originating LS2020 node. (The system up time is omitted from any trap displayed on the same node where the trap was generated.)
- **Trap name**—The trap name is the name of the trap.
- **Trap generation time**—The trap generation time is shown in two forms: (1) that for Greenwich Mean Time and (2) the form appropriate for the time zone you selected during installation.
- **Port number**—The port number associated with the trap (if applicable).

Enterprise-specific traps contain the following information:

- **LS2020 node name**—The system uses the IP address of the packet containing the trap to look up the name of the node in the /etc/hosts file. If the name is not available, the IP address is displayed. (The node name is omitted from any trap displayed on the same node where the trap was generated.)
- **System up time**—In the trap log (*mma.traplog*) or on the console display, the system up time indicates when the MMA received the trap. In the CLI display, however, the system up time indicates the up time of the originating LS2020 node. (The system up time is omitted from any trap displayed on the same node where the trap was generated.)
- **Trap severity level**—The trap severity level indicates whether the trap is oper, info, trace, or debug.
- **Symbolic trap name**—The symbolic trap name consists of an abbreviation for the software module that generated the trap, followed by a number that identifies the specific trap and the trap type. For example, if the symbolic trap name is LCC_14, it is an operational trap generated in the line card control (LCC) process.
- **Trap generation time**—The trap generation time is shown in two forms: (1) that for Greenwich Mean Time and (2) the form appropriate for the time zone you selected during installation.
- **Trap text**—The trap text describes the event being reported.

Trace and debug traps also include the process identification (PID) number and process alias name for the process in which the trap occurred.

Trap Filter Levels

Because an LS2020 switch is capable of reporting a vast amount of information, you may want to adjust the number of traps that are logged or displayed.

As shown in Figure 1-1, trap messages travel distinct routes to any of several destinations: the trap log, the console, the terminal running a CLI session, or the NMS. On their journey, traps encounter filters. These filters, shown in Figure 1-3, limit the type of traps that reach the device.

With default settings, the traps journey looks like this:

1. When the traps reach the process filter, it drops trace and debug traps and allows info, oper, and SNMP traps to proceed.

2 The info, oper, and SNMP traps enter the traps log, go to the console filter, and go to the chassis filter.

3 The console filter drops info traps, so that only oper and SNMP traps proceed. These traps are displayed on the local console.

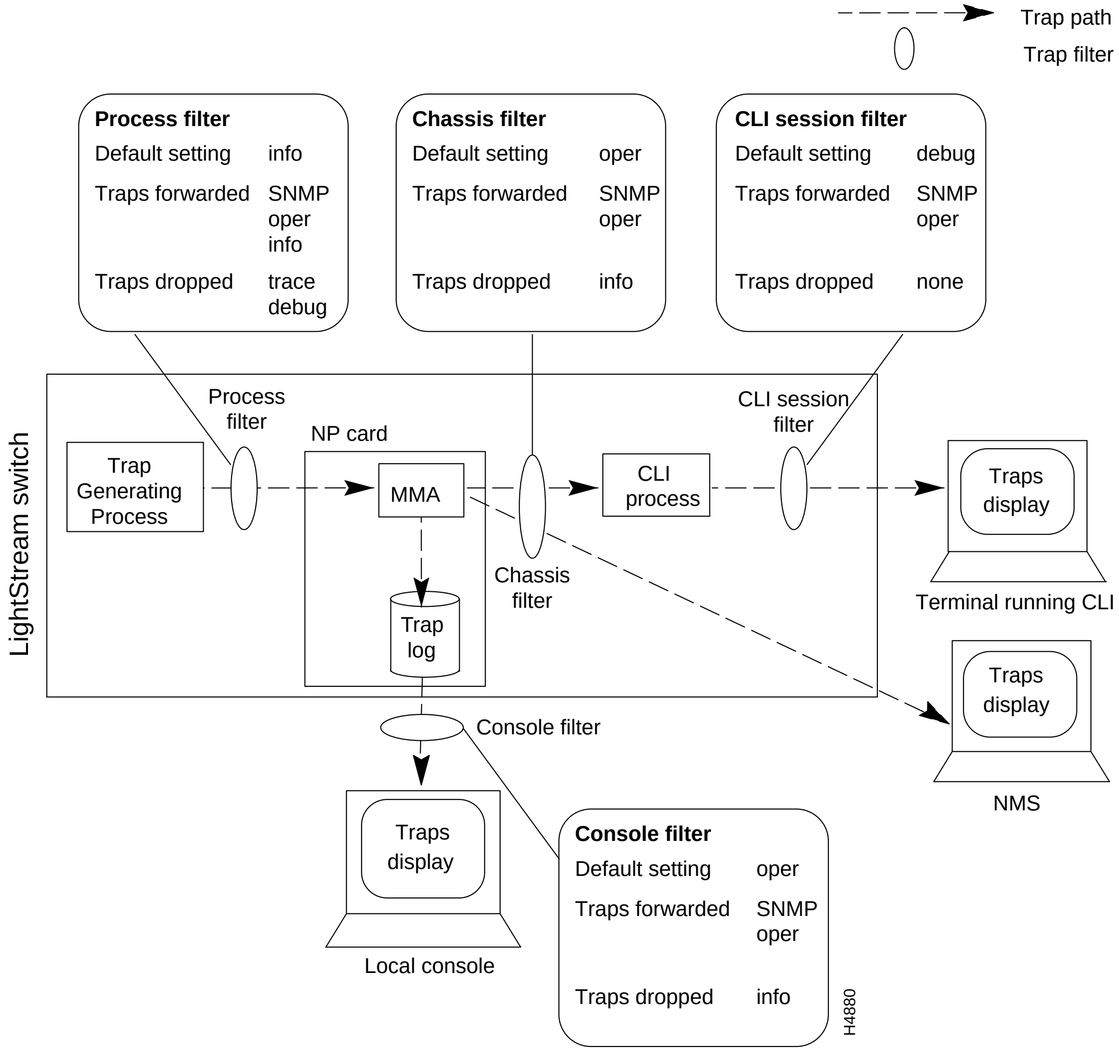
4 Like the console filter, the chassis filter drops info traps, so that only oper and SNMP traps proceed. These traps are displayed on the NMS and also proceed to the CLI session filter.

5 Any traps that make it to the CLI session filter are allowed to proceed; thus, both oper traps and SNMP traps are displayed on the terminal running the CLI session.

You set the filters in the CLI, by assigning a trap filter level to each filter. There are four trap filter levels.

- **Debug**. Let all traps that have not already been filtered proceed.
- **Trace**. Let all traps, other than debug, that have not already been filtered proceed.

Figure 1-3 Traps Filter Levels and Default Settings



- **Info**. Let all traps, other than debug and trace, that have not already been filtered proceed.
- **Oper**. Let all traps, other than debug, trace, and info, that have not already been filtered proceed.

Procedures for managing traps are in the chapter entitled "Managing LightStream 2020 Traps." That chapter explains how to change the trap filter levels or override the settings for individual trap numbers.