CHAPTER 1

About LightStream 2020 Traps

This chapter provides an overview of trap messages generated by the LightStream 2020 (LS2020) enterprise ATM 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 LightStream 2020 switch sends a trap message, or possibly a series of messages, to one or more user-specified destinations that may include the management station, the switch's local console, a log file on the switch, or a terminal running the CLI. 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 at all. You can initiate further interactions with the LightStream 2020 switch to determine the nature and extent of the event.

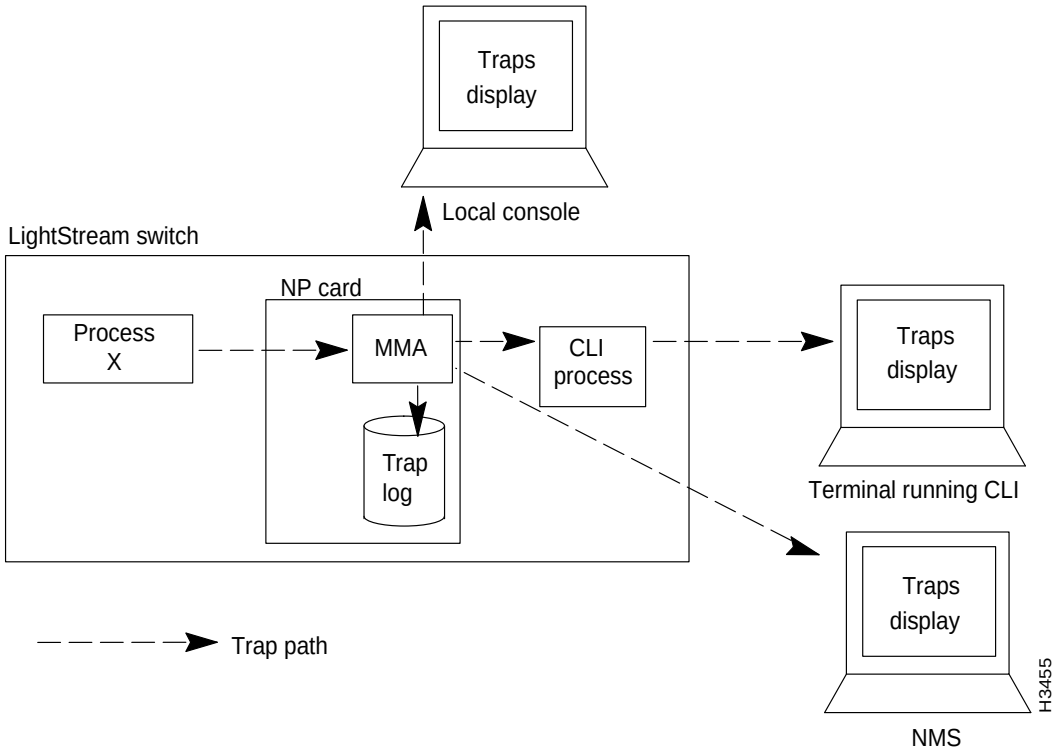
How Traps Are Generated

Figure 1-1 shows the flow of traps through the LightStream 2020 system. Traps are generated by the processes running on a LightStream 2020 switch and are sent to a process called the master management agent (MMA).

By default, the MMA writes the traps to a log on the switch's network processor (NP) and from there they are sent to the local console, if one is present. Traps can also be displayed on one or more network management systems (NMSs) and on a terminal running the command line interface (CLI).

(If you are using an NMS, note that only one instance of the CLI may run there at any given time.)

Figure 1-1 Traps are passed from software processes to the MMA, stored in the trap log, and sent to the local console, the CLI process, or an NMS.



How Traps Are Reported

By default, a switch sends traps only to its trap log and to its local console, if one is present. However, you can configure a switch to send traps to another NP or to an NMS, so you can view them there. This capability can be used to collect the traps for all of the switches in the network in a single place. See the *LightStream 2020 Installation Guide* for information on how to send traps to another device.

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

Trap Types

LightStream 2020 switches generate five types of traps:

- SNMP (or "generic")
- Operational
- Informational
- Trace
- Debug

An overview of each type of trap is provided in this section.

SNMP Traps

The SNMP traps displayed by the LightStream 2020 switch are the standard SNMP traps defined by the SNMP MIB-2 specifications. They are displayed as “generic” traps. SNMP traps are used by LightStream 2020 network operators.

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

Operational Traps

Operational traps provide information on the key system components to help you find and correct problems. Operational traps indicate that something is wrong with the system or that a significant change has occurred in the system status. They can also be used to report the status of hardware 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

  Traps in this category provide information only, such as notification that a line card has come up.

- Traps that require a response

  Traps in this category 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

  Traps in this category indicate that there may be a problem with the LightStream 2020 software. These traps are *very* unlikely to occur. If you receive a trap from this category, it is important that you record it and contact your customer support representative immediately, so he or she can determine what actions should be taken.

Within each software process, operational traps are numbered from 1 to 1999. Traps numbered 1000 to 1999 are not documented because the only response is to call your customer service representative.

Informational Traps

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.

`Trunk emtb7.2.5->emtb8.4.2 DOWN [transitioning to down (from has-vci)]` is an example of an informational trap.

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

Trace Traps

Trace traps are used to track a sequence of actions through a process. Trace traps are used by customer support representatives 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 this manual in detail.

Note Do not turn on trace traps. If you do so, you may reduce your network's performance.

Debug Traps

Debug traps are used to find and solve serious software problems within a LightStream 2020 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 use by customers, they are not discussed in this manual in detail.

Note Do not turn on debug traps. If you do so, you may reduce your network's performance.

Trap Type Priorities

Each type of trap is assigned a priority level that cannot be changed. Table 1-1 illustrates the priorities of the different trap types. SNMP traps have the highest priority, followed by operational, informational, trace, and debug traps.

Table 1-1 Trap Levels

Trap Type	Priority
SNMP	Highest
Operational	v
Informational	v
Trace	v
Debug	Lowest

You can use the priority levels to set a *trap reporting threshold* that controls which trap types are reported. Setting the reporting threshold to a given priority level causes the system to report all traps at or above that level, and to discard traps below that level. For example, if you set the reporting threshold to informational, the system reports informational, operational, and SNMP traps, while discarding trace and debug traps.

By default, the system displays all SNMP and operational traps and logs all SNMP, operational, and informational traps for your network. (Trace and debug traps are discarded.) This arrangement works well for most networks. If you want to change the trap reporting threshold, refer to the chapter "Managing LightStream 2020 Traps."

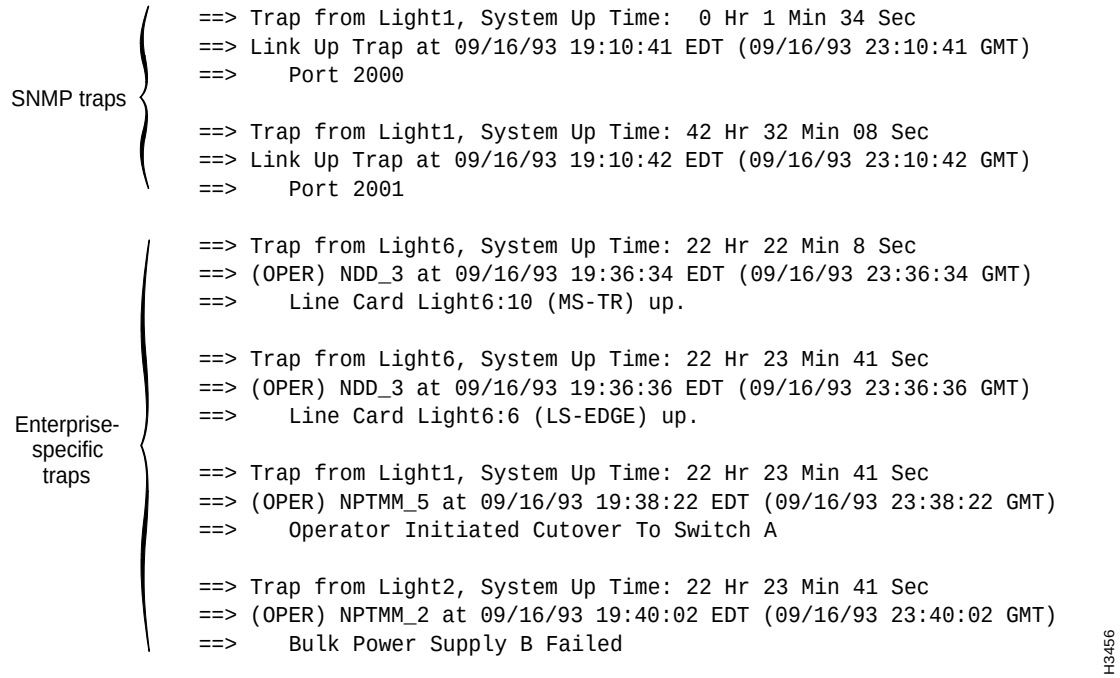
Trap Formats

There are two trap formats:

- SNMP standard traps
- Enterprise-specific traps

SNMP trap format is defined by MIB-II specifications. The enterprise-specific traps are specific to the LightStream 2020 switch. Their format is defined in this section. Figure 1-2 shows a sample trap display, from nodes called Light1 and Light6, containing both SNMP and enterprise-specific traps.

Figure 1-2 Trap examples.



Note If you are using an NMS to display traps, the display may differ, but the content is the same.

SNMP Standard Traps

The standard SNMP traps include the following information:

- LightStream 2020 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. (Note that the node name is omitted from traps displayed on the same node where they were 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 MMA received the trap. In the CLI display, however, the system up time indicates the up time of the originating LightStream 2020 node. (Note that the system up time is omitted from traps displayed on the same node where they were generated.)

- Trap name
- Trap generation time
- Port number associated with the trap (if applicable)

Enterprise-specific Traps

Enterprise-specific traps contain the following information:

- LightStream 2020 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. (Note that the node name is omitted from traps displayed on the same node where they were 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 MMA received the trap. In the CLI display, however, the system up time indicates the up time of the originating LightStream 2020 node. (Note that the system up time is omitted from traps displayed on the same node where they were generated.)

- Trap severity level (oper, info, trace, or debug)

- Symbolic trap name

  This 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

  This is shown in two forms: the time zone you selected during installation and Greenwich Mean Time.

- Trap text

  A description of the event being reported.

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

Figure 1-3 shows each field of a sample enterprise-specific trap.

Figure 1-3 Fields in a trap message.