CHAPTER 6

Detecting and Correcting Failures

The LightStream 2020 multiservice ATM switch (LS2020 switch) helps you to detect failures in a node and isolate them to a field-replaceable-unit (FRU) level. Through component redundancy in the LS2020 switch, coupled with the ability to perform power-on servicing, you can correct failures in a node while it continues to operate. This chapter describes these facilities.

LS2020 Failure Reporting Mechanisms

An LS2020 switch detects the following types of failures:

- Failure of a node to participate in the periodic exchange of messages between cards in a chassis or between cards connected to external devices in the network
- Failure of node diagnostic tests
- The existence of a problem detected by a node's test and control system (TCS)
- The loss of carrier signal or the existence of a parity/checksum failure in software
- Sending or receiving illegal messages or poorly timed messages

The LS2020 switch provides several mechanisms for reporting these failure conditions:

- Trap messages
- Network statistics
- LEDs

Using these failure-reporting mechanisms, a network administrator can determine if the network is experiencing a problem and, if so, isolate and correct the failure.

Trap Messages

When an error condition exists or a significant change in node status occurs, software processes generate trap messages, commonly referred to as traps. Traps usually provide the first indication of a real or potential problem in your network. Subsequent troubleshooting procedures can be based on textual information provided by the trap. Some traps require immediate action; others do not, even though they provide important information.

The LS2020 switch generates the following types of traps:

- **SNMP traps**—The Simple Network Management Protocol (SNMP) traps displayed by an LS2020 system consist of "generic" traps defined in the industry-standard SNMP MIB-II specification. SNMP is the network management protocol used by LS2020 systems.
- **Operational traps**—These traps provide operational information about key system components; they help you find and correct problems in the network. Of primary interest to network operators, operational traps indicate that something is wrong in the network or that a significant change has occurred in system status.
- **Informational traps**—These traps provide supplemental details about system problems reported in operational and SNMP traps.
- **Trace traps**—These traps are used to track a sequence of actions through an active software process.
- **Debug trap**—These traps are used to find and resolve serious software problems in an LS2020 switch.

Note Informational, trace, and debug traps are typically used by a customer support representative to perform advanced troubleshooting and software debugging in an LS2020 network.

Two trap formats are defined for use in an LS2020 environment:

- **SNMP-standard traps**—These are the standard, generic SNMP traps defined in the MIB-II specification.
- **Enterprise-specific traps**—These traps are specific to an LS2020 switch.

You can record trap messages in a log file or display them on a terminal. By default, the LS2020 switch records SNMP, operational, and informational traps in a log file on its local network processor (NP) disk and displays SNMP and operational traps on the local console (if one is attached).

The LS2020 switch allows you to customize the trap log and the trap display. In addition, you can select the types of traps to be reported by setting their respective priority levels. Furthermore, you can turn the trap log off, view the trap log from the CLI or the LynxOS shell (in the real-time, UNIX-like operating system), or move the trap log to another system for viewing.

For detailed information about LS2020 traps, see the *LightStream 2020 Traps Reference Manual.*

Network Statistics

You can use the statistics facilities provided by the LS2020 switch for a variety of purposes. For instance, you can use statistics to evaluate network performance and usage or to troubleshoot a particular problem.

The LS2020 network provides a predefined set of statistical categories for every port. These per-port statistics provide such information as the number of packets sent and received and the number of send and receive errors.

You can tailor statistics collection to your own needs by using an LS2020 switch data collection facility called the collector. Using the collector, you can determine which management information base (MIB) variables you want to collect and the collection interval you want to use. You can save the collected information in a file that can be viewed from a local or remote CLI or moved to another workstation or host for viewing.

For detailed information about statistics collection, see the *LightStream 2020 Network Operations Guide.*

Light Emitting Diodes

Light emitting diodes (LEDs) are present on the bulkheads of many cards in an LS2020 switch. The LEDs serve the following purposes:

- Indicate that power is applied to the card
- Alert you to a malfunctioning card or to a card that has failed its diagnostics
- Provide an informal indication that traffic is flowing through the node
- Indicate the status of elements of the test and control system (TCS) that cannot be obtained through the TCS itself. For example, LEDs indicate which TCS hub is primary.

LEDs for switch cards, NPs, and line cards are visible from the front of the LS2020 chassis. The LEDs on the access cards are visible from the rear of the LS2020 chassis.

For a description of the LEDs on each LS2020 card, see the *LightStream 2020 Hardware Reference & Troubleshooting Guide*.

Isolating LS2020 Failures

LS2020 diagnostics help you to isolate hardware failures to the field-replaceable unit (FRU) level. LS2020 diagnostics exist in two forms:

- **Power-on self-tests (POSTs)**—Provide a high-level check of LS2020 hardware when power is applied
- **Diagnostic packages**—Provide in-depth testing of hardware

The POST is initiated automatically whenever the system or a line card is powered up or when a card is reset. Each NP module, switch card module, and interface module runs a POST test. A card that passes the POST demonstrates its functional and operational readiness. This readiness is signaled when the card's green RDY LED is lit. If the card fails the POST, its yellow FLT LED is lit. You can display POST results from the TCS or the CLI using the **show** command. More detailed failure information is available through the TCS help facility. The POST completes in approximately one minute.

Note Other failures may also light the FLT LED. For more details about fault indications, see the *LightStream 2020 Hardware Reference & Troubleshooting Guide.*

The POST performs a high-level check of card functionality, and diagnostic packages stored on the network processor (NP) hard disk perform in-depth testing. Diagnostic software is available for the NP, the switch card, and various interface modules in an LS2020 switch. These diagnostics can be run remotely (through a Telnet or modem connection) or locally (from a console connected to the LS2020 console port).

Most diagnostic testing can be done on line. Note, however, that you cannot perform switch interface tests or NP tests in an LS2020 switch equipped with a single NP without first taking that switch off line. In all other cases, only the card under test is removed from service.

For more detailed information about diagnostic procedures, see the *LightStream 2020 Hardware Reference & Troubleshooting Guide.*

Correcting LS2020 Failures

An LS2020 switch is designed to promote a low mean time to repair (MTTR). FRUs are easy to access and replace. In addition, an LS2020 switch provides hardware redundancy and power-on servicing, allowing portions of the LS2020 switch to be serviced while the unit continues to operate.

Hardware Redundancy

The LS2020 switch has full critical-element redundancy. Any hardware element that is essential to system operation has a backup that can be brought into service automatically. These critical elements include:

- Blowers
- Switch cards
- Network processors and associated disk drives
- Power supplies

Every LS2020 system has redundant blowers. Redundancy for all other elements is optional. When both blowers are functioning properly, they share the cooling load for the LS2020 switch. If one blower fails, the other blower has sufficient capacity to cool the entire unit.

If an LS2020 switch has two switch card modules, one of the switch cards acts as the primary card and handles all switch functions. The second switch card serves as a backup unit. If the primary switch card fails, the backup switch card takes control.

If an LS2020 switch is equipped with two NPs, one NP acts as the primary, handling all NP functions for the switch. The second NP acts as a backup unit, and its configuration is identical to that for the primary NP. However, the backup NP is not part of the active configuration. If the backup NP determines that the primary NP has failed, the backup NP automatically assumes the role of primary. In this case, all interface modules perform a warm reboot, and network edge interface connections are rerouted.

If an LS2020 switch has two power supplies, both power supplies are connected to the same 48-volt rail and share the load between them. However, if one power supply fails, the other power supply automatically takes on the entire load without any disruption of power.

Power-on Servicing

Power-on servicing enables you to remove and install components while the rest of the system remains fully functional. This feature is supported for the following field replaceable units (FRUs) in an LS2020 switch:

- Switch card modules
- NPs
- Interface modules (line cards and access cards)
- Bulk power supplies
- Disk assemblies
- Blowers

LS2020 hardware and software support power-on servicing. The LS2020 chassis midplane and associated cards are designed to prevent pin damage during component insertion and removal.

System processes (such as the TCS, self-configuration, and network management agents) also support power-on servicing. For example, an NP maintains regular communications with each interface module under its control. When the NP determines that an interface module is out of service, the NP updates the topology database to reflect this status and begins rerouting virtual channel connections (VCCs) associated with that interface module.

Dynamic Routing Around Failures

An LS2020 network can reroute VCCs whenever a failure of one or more communications links interrupts existing traffic flows on configured PVCs or explicitly established VCCs.

VCCs are rerouted using the standard call setup mechanisms to establish new connection paths. When a trunk fails, each VCC that runs through the failed trunk is recreated over a new path, if one is available. The LS2020 switches at each end of a VCC must establish the new path. Between the time of failure and the creation of each new circuit, service is temporarily disrupted on each circuit.