CHAPTER 6

Detecting and Correcting Failures

The LightStream 2020 multiservice ATM switch (LS2020 switch) enables 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 an LS2020 switch while it continues to operate. This chapter describes these failure detection and correction facilities.

This chapter is recommended reading for anyone who will control, monitor, or troubleshoot an LS2020 network.

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 an LS2020 chassis or between cards connected to external devices in the network
- Failure of node diagnostic tests
- The existence of a hardware 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
- Light emitting diodes (LEDs) that signal error conditions

With these failure-reporting mechanisms, a network administrator can determine if an LS2020 switch or 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, which are commonly referred to as traps. Traps usually provide the first indication of a real or potential problem in an LS2020 switch or the network. Subsequent troubleshooting procedures can be performed, based on textual information provided by trap messages.

Some traps require immediate action; others traps do not, even though they may provide important operational or problem-related information.

The LS2020 switch generates the following types of traps:

- **SNMP traps**—Display “generic” Simple Network Management Protocol (SNMP) traps generated by an LS2020 system. Such traps are defined in the industry-standard SNMP MIB-II specification, which is the standardized network management protocol used by LS2020 switches and other SNMP-compatible network management devices.
- **Operational traps**— Provide information about key system components that help you to isolate 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 network status.
- **Informational traps**— Provide supplemental details about system problems reported in operational and SNMP traps.
- **Trace traps**— Track a sequence of actions through an active software process.
- **Debug traps**—Find and resolve 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**—The standard, generic SNMP traps defined in the MIB-II specification.
- **Enterprise-specific traps**—The traps that are specific to an LS2020 switch.

You can record trap messages in a log file or display them on a terminal or both. 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. Also, you can turn the trap log off, view the trap log from the CLI or the LynxOS shell, or move the trap log file 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 reporting facilities provided by the LS2020 switch for a variety of purposes. For example, you can use statistics to evaluate network performance and usage characteristics or to troubleshoot a particular problem in the network.

A predefined set of statistical categories is defined for every port in the network. These port statistics provide such information as the number of packets sent and received over the port and the number of send and receive errors experienced.

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

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

Light Emitting Diodes (LEDs)

LEDs are built into the bulkheads of many of the cards in an LS2020 chassis. These LEDs serve the following purposes:

- Indicate that power is applied to the card
- Alert you to a card that has malfunctioned or failed its diagnostic tests
- 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. The LEDs, for example, indicate which TCS hub is primary.

LEDs for switch cards, NPs, and line cards are visible from the front of the LS2020 chassis, while the LEDs on the access cards are likewise visible from the rear of the 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 a field-replaceable unit (FRU) level. LS2020 diagnostics exist in two forms:

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

The POST is initiated automatically whenever the system or a line card is powered up or when a card is reset. The POST takes approximately one minute to complete.

Each NP module, switch card module, and interface module runs a POST. A card that passes the POST demonstrates its functional and operational readiness when the card’s green RDY LED is lit. If the card fails the POST, its yellow FLT LED is lit.

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

You can display POST results from the TCS or the CLI using the **show** command.

The POST performs a high-level check of card functionality, while diagnostic packages stored on the network processor (NP) hard disk perform in-depth testing.

Diagnostic software is available for the NP and the 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 console port of an LS2020 switch card).

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.

For more detailed information about LS2020 fault isolation and diagnostic procedures, see the *LightStream 2020 Hardware Reference & Troubleshooting Guide.*

Correcting LS2020 Failures

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

Hardware Redundancy

The LS2020 switch provides full critical-element redundancy. Any hardware element essential to system operation can be supported with an optional backup unit that can be brought into service automatically. These critical elements include the following chassis components:

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

Every LS2020 system contains redundant blowers. Redundancy for all other critical chassis components is optional.

When both blowers are functioning properly, they share the cooling load for the entire LS2020 chassis. If one blower fails, the other blower has sufficient capacity to cool the entire unit.

If an LS2020 chassis contains two switch cards, one of the cards acts as primary to handle all switch functions. The second card serves as a backup module. If the primary switch card fails, the backup card assumes control automatically.

If an LS2020 chassis contains dual NPs, one NP acts as primary, handling all NP functions for the entire chassis. The second NP acts as backup unit and is configured identically to the primary NP.

The backup NP, however, is not part of the active LS2020 configuration. If the backup NP determines that the primary NP has failed, the backup NP automatically assumes the role of primary.

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

Power-on Servicing

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

- Switch card modules (relevant only to systems with two switch card modules, since the system ceases to operate if you remove the only switch card from the LS2020 chassis)
- NP modules (relevant only to systems with two NPs, since the system ceases to operate if you remove the only NP from the LS2020 chassis)
- Interface modules (line cards and associated access cards)
- Bulk power supplies (relevant only to systems with two power supplies, since the system ceases to operate if you remove the only power supply from the LS2020 chassis)

- Disk assemblies
- Blowers

LS2020 hardware and software both support power-on servicing. In addition, the LS2020 chassis midplane and associated interface modules are designed in a way that helps to prevent pin damage during component insertion and removal.

System-level processes (such as those performed by the TCS 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 for some reason, the NP updates the network topology database to reflect this change of state and begins rerouting the 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 manually configured PVCs or explicitly-established VCCs.

VCCs are rerouted using the standard connection admission control (CAC) mechanisms to establish new paths. When a trunk fails, each VCC that runs through the failed trunk is recreated over a new path, if such a path is available.

The LS2020 switch at each end of the failed VCC (both the source and destination endpoint) must establish a new communication path. Between the time of failure of the existing connection and the creation of each new VCC, service between the two LS2020 switches is temporarily disrupted.