CHAPTER 3

SNMP Traps

This chapter lists SNMP traps. These traps display as type "GENERIC." For more detailed information about SNMP traps, refer to IETF RFC 1157, *A Simple Network Management Protocol*, by J. Case et. al.

If you need help interpreting these traps, contact your customer support representative.

Trap Name	Authentication Failure
Trap Text	`Authentication Failure Trap from <node name>, System Up Time <XX Hr XX Min XX Sec>`
Description	This trap indicates that the source of an SNMP request received by the specified switch has been sent a protocol message that is not properly authenticated.
Action	You may wish to verify that the sources of SNMP requests received by the switch are using an SNMP community name string that matches one of those configured on the switch, and that the IP address of the source is among those configured as acceptable on the switch. (See the *LightStream 2020 Configuration Guide* for information on configuring IP addresses for authentication.)

Trap Name	Cold Start
Trap Text	`Cold Start Trap from <node name>, System Up Time <XX Hr XX Min XX Sec>`
Description	This trap indicates that the specified node's power has just come on.
Action	No action is required.

Trap Name	Link Down
Trap Text	`Link down trap from <node name>, System Up Time <XX Hr XX Min XX Sec> Port <port#>`
Description	This trap indicates that a node has missed an established number of trunk up/down messages.
Action	If the trunk is not returned to service within 10 minutes, refer to the *LightStream 2020 Network Operations Guide* for troubleshooting procedures.

Trap Name	Link Up
Trap Text	`Link up trap from <node name>, System Up Time <XX Hr XX Min XX Sec> Port <port#>`
Description	This trap indicates that a node has returned to service.
Action	No action is required.