CHAPTER 1

The Set Command

Use the **set** command to set the value of a specified attribute of a LightStream 2020 multiservice ATM switch (LS2020 switch), or to set the state of the CLI program. The first argument of the command defines families of **set** commands. The command families are given in the following list, together with the titles of the sections of this chapter in which they are discussed:

set card	Card Attributes
set chassis	Chassis Attributes
set cli	CLI Display and Logging Attributes
set collection	Collections of Statistical Counts
set config	Configuration Lock Attribute
set modem	Modem Attributes
set nettime	Network Timing Attributes
set pid	Process Attributes
set port	Port Attributes (including traffic filters, traffic profiles, and multicast groups)
set snmp	SNMP Attributes
set stb	Spanning-Tree Bridge Attributes
set tcs	Test and Control System Attributes
set trap	Traps

Note The **set** command requires protected mode for the **set modem**, **set tcs**, **set trap**, and **set port** *c.p* **np-deliver** commands only. See the **protected** command in the chapter entitled "CLI Control Commands."

Many of the attributes that you can set with the CLI can also be set using the StreamView configuration tools on your network management workstation. For some tasks you may find StreamView's graphical user interface (GUI) easier to use than the CLI. See the *LightStream 2020 Configuration Guide* for information on using the GUI configuration tools, and for detailed descriptions of attributes that you can set with the GUI configuration tools and with CLI.

Note The **set** command requires that the read/write community name be set first to a name that has been assigned the value `write` in the mma.communities file (unless *parameter1* is **cli**, **modem**, or **snmp**). Because the default community name "public" is read only, the **set** command fails if the read/write community name has not been set first. For information on setting the read/write community, see the description of the command **set snmp community** in this chapter and in the *LightStream 2020 Network Operations Guide*.

Card Attributes

Use the **set card** command family to set the administrative state of the card to active, inactive, or testing. Use it also to set the peak cell rate on a CLC card configured for 4-port T3/E3 trunk or 1-port OC-3c trunk operation.

The **set card** commands require a card number (in the range 1–10) as an argument.

set card card# active

Use the **set card** *card#* **active** command to set the administrative state of the specified card to **active**.

When the card is set active from some other state, card parameters are set to defaults, then overwritten from on-board memory (if temporary changes were made) and from the configuration database, in that order. The result can be a combination of defaults, "temporary" changes, and database settings, depending upon which parameters were set in EEPROM and in the configuration database.

Note After a power reset or reboot of the node, the operational status of a card may be `down` while its administrative status and configuration register values are both up. To bring the card up in these circumstances, set it to **inactive** and then to **active**.

set card card# inactive

Use the **set card** *card#* **inactive** command to set the administrative state of the specified card to **inactive**.

Note Do not use the Verify function of the configurator when a card is set to **inactive.** The Verify function copies attribute values from run-time memory. When a card is inactive (or down for any reason), the Verify function can access only the card's type, number, and administrative status. If you choose to write values to the local database, the Verify function deletes all other configured attribute values stored there. See the *Lightstream 2020 Configuration Guide* for details about the Verify function.

set card card# testing

Use the **set card** *card#* **testing** command to set the administrative state of the specified card to **testing**. This is done during some troubleshooting procedures. This command is of interest primarily to support personnel and developers.

Note The **test** command is the preferred way to run card diagnostics from the CLI. It automatically sets the card state to testing.

set card card# peak-cell-rate

Use the **set card** *card#* **peak-cell-rate** *rate* command to set the peak per-port cell rate (in cells per second) for a 4-port T3/E3 or a 1-port OC-3c trunk card. The value of *rate* must be in the range 0 – 446,000. Use this parameter to ensure that ATM traffic over a virtual path connection (VPC) does not exceed the maximum rate enforced in an ATM hub or network through which the VPC passes. This maximum cell rate applies to all ports on the card.

Chassis Attributes

Use the **set chassis** command family to set values of specified chassis attributes. For constraints among the various IP addresses and masks, refer to the *LightStream 2020 Network Operations Guide* and the *LightStream 2020 Configuration Guide*.

The arguments of the **set chassis** command are given in the following paragraphs.

set chassis activeip

Use the **set chassis activeip** *IPaddress* command to set the IP address that is used to communicate network management traffic between this node and other LS2020 nodes in the network, and between the active NP and the backup NP in a node with redundant NPs. When an NP becomes the active NP in the chassis, it uses this address.

This address is made known to both NPs and to all nodes in the LS2020 network. For one to connect to this address via a host or router outside the LS2020 network, the address must be included in the static routing table on that host or router.

set chassis secondaryip

Use the **set chassis secondaryip** *IPaddress* command to set the IP address that is used to communicate network management traffic between the backup NP and the active NP in a node with redundant NPs. When one NP becomes the active NP in the chassis, the other NP uses this address.

This address is made known to both NPs in a redundant system. Although there is seldom any need to connect to it, it is also made known to all nodes in the LS2020 network. For one to connect to this address via a host or router outside the LS2020 network, the address must be included in the static routing table on that host or router.

set chassis congestion { maxpermitinterval | minpermitinterval | mincainfointerval }

Use the **set chassis congestion** commands to set three time values used to control congestion avoidance operations. Use the **set chassis congestion maxpermitinterval** *microseconds* command to set the maximum interval, in microseconds, during which trunk cards and outgoing edge cards can report permit limits. Use the **set chassis congestion minpermitinterval** *microseconds* command to set the minimum interval, in microseconds, during which trunk cards and outgoing edge cards can report permit limits. Use the **set chassis congestion mincainfointerval** *microseconds* command to set the minimum interval, in microseconds, during which congestion avoidance processes can distribute aggregated congestion avoidance updates to input edge cards.

set chassis consoletraplevel

Use the **set chassis consoletraplevel** *level* command to set the console trap reporting threshold (the level of traps that are reported by this node to the console). The control of traps reported to the console is independent of the control of traps that are reported to the NMS (see **set chassis traplevel** and **set cli traplevel**). The trap levels are as follows:

off	No traps
oper	Operational traps
info	Informational and operational traps
trace	Trace, informational, and operational traps
debug	All traps

Each trap level is progressively more inclusive: the info level includes oper traps, the trace level includes info and oper traps, and the debug level includes all traps. See the *LightStream 2020 Traps Reference Manual* for information about trap levels.

There must be a compelling reason to use any argument other than **off**, **info**, or **oper**. Instead of the **trace** or **debug** argument, use the **set trap** command for individual traps. By doing this, you avoid flooding the node with traps, which could degrade performance.

set chassis defrouter

Use the **set chassis defrouter** *IPaddress* command to set the default router address for network management traffic originating at the local NP. This address is used in the absence of any other routing information for such traffic.

set chassis ethernetaddr

Use the **set chassis ethernetaddr** *OBLANaddress* command to set the Ethernet address for the on-board Ethernet LAN interface of the NP. It is used by whichever NP is active. Not all LS2020 nodes need an Ethernet connection.

set chassis ethernetmask

Use the **set chassis ethernetmask** *mask* command to set the subnet mask for the on-board Ethernet LAN interface of the NP.

set chassis name

Use the **set chassis name** *chassis_name* command to set the chassis name (node name). The name may be any alphanumeric string up to 39 characters long.

set chassis netmask

Use the **set chassis netmask** *mask* command to set the subnet mask for the active and secondary IP addresses. This mask must be the same for every NP in the LS2020 network.

set chassis primaryswitch

Use the **set chassis primaryswitch** {**sa** | **sb**} command to establish the specified switch card (SA or SB) as the primary or active switch. The other switch card becomes the inactive backup switch. (With Release 1 switch cards, this command causes the chassis to reboot.)

set chassis traplevel

Use the **set chassis traplevel** *level* command to set the chassis trap reporting threshold (the level of traps that are reported for this node). This is independent of what is reported to the console (see **set chassis consoletraplevel**) and what is reported to the CLI or NMS (see **set cli traplevel**). The trap levels are as follows:

oper Operational traps

info Informational and operational traps

trace Trace, informational, and operational traps

debug All traps

Each trap level is progressively more inclusive: the info level includes oper traps, the trace level includes info and oper traps, and the debug level includes all traps. See the *LightStream 2020 Traps Reference Manual* for information about trap levels.

There must be a compelling reason to use any argument other than **info** or **oper**. Instead of the **trace** or **debug** argument, use the **set trap** command for individual traps. By doing this, you avoid flooding the node with traps, which could degrade performance.

set chassis traplog

Use the **set chassis traplog** {**on** | **off**} command to control the logging of traps in the file mma.traplog. The default state, when node software is started, is to log traps.

CLI Display and Logging Attributes

Use the **set cli** command family to set values of specified CLI attributes.

set cli debug

Use the **set cli debug** {**on** | **off**} command to set the debug flag. If the debug flag is on, additional information about the course of command execution is displayed, including the names of MIB variables as they are queried or set, and each trap message becomes quite verbose. This command is of interest only to developers and support personnel.

set cli echosource

Use the **set chassis echosource** {**on** | **off**} command to turn the echoing of sourced commands on or off. The default is to display shell commands as they are executed under the **source** command (see the chapter entitled "CLI Control Commands").

set cli lineedit

Use the **set chassis lineedit** {**on** | **off**} command to turn line editing capability on or off. When this function is turned on, CLI command lines can be edited with control keys (see the *LightStream 2020 Network Operations Guide*).

set cli log

Use the **set cli log** {**"***logfile***"** | **off**} command to record a copy of all user input and CLI output that is displayed on the screen in the current CLI session.

Note Always surround the file name or pathname of *logfile* with quotation marks, as in the following example:

```
cli> set cli log "cli.log.9502"
```

If you fail to do so, the CLI reports a syntax error.

This command turns the CLI logging function on and directs its output to the specified file *logfile*. If *logfile* is not in the current working directory (usually the same directory as the user account you are using), you must enter the full pathname of the file. All user input and output of the current CLI session is copied to *logfile* until you either turn the logging function off with the **set cli log off** command or exit the CLI. (The log file cannot be displayed until the logging function has been turned off.) If you re-open the same log file, output from the new session is appended to the previously logged session output.

set cli retries

Use the **set cli retries** *retries* command to specify the number of times the CLI repeats an SNMP request if no response is received to the first attempt. The value of *retries* must be in the range 0 – 10 (the default is 0). CLI's retries value interacts as follows with the timeout value set by the command "**set cli timeout**": (retries + 1) * timeout = maximum interval, in seconds, between the

entry of a command and its result. Thus, for example, if you set retries to 2 and timeout to 10, you may wait up to 30 seconds for the results of a command and a new CLI prompt. If you experience SNMP timeout errors, increasing the retries value may be helpful.

set cli term

Use the **set cli term** *termtype* command to set the terminal type to *termtype*. See the file /etc/termcap for acceptable values.

set cli timeout

Use the **set cli timeout** *seconds* command to specify the time that CLI waits for a response after issuing an SNMP request. The value of *seconds* must be in the range 6 – 200 (the default is 6). After waiting the specified number of seconds, CLI either times out and returns a new CLI prompt, or sends the request again, depending on the retry status. (See the command "**set cli retries**.") If you experience SNMP timeout errors, increasing the timeout value may be helpful.

set cli timer

Use the **set cli timer** command to reinitialize the timer that normally indicates time elapsed since the current CLI session was started.

set cli timestamp

Use the **set cli timestamp** {**on** | **off**} command to control the appearance of a timestamp after each CLI prompt. When this parameter is set **on**, a time stamp appears after each prompt, as an aid to tracking and reporting operational problems.

set cli traplevel

Use the **set traplevel** *level* command to set the CLI trap reporting threshold (the level of traps that are reported to the CLI and to an NMS). This is independent of what is reported to the console (see **set chassis consoletraplevel**) and what is reported by the chassis (see **set chassis traplevel**). The trap levels are as follows:

off	No traps
oper	Operational traps
info	Informational and operational traps
trace	Trace, informational, and operational traps
debug	All traps

Each trap level is progressively more inclusive: the info level includes oper traps, the trace level includes info and oper traps, and the debug level includes all traps. See the *LightStream 2020 Traps Reference Manual* for information about trap levels.

There must be a compelling reason to use any argument other than **off**, **info**, or **oper**. Instead of the **trace** or **debug** argument, use the **set trap** command for individual traps. By doing this, you avoid flooding the node with traps, which could degrade performance.

Collections of Statistical Counts

Use the **set collection** command family to create, configure, or control a specified collection process. Such a process collects statistical counts of specified traffic or events that are recorded in specified MIB objects. See the *LightStream 2020 Network Operations Guide* for information about data collections and how to use them and monitor them.

You must first create a collection with the **set collection** *n* **create** command. If you attempt to use any of the other **set collection** commands before creating collection number *n*, an error message says there is no such collection.

set collection n addvar

Use the **set collection** *n* **addvar** *MIB_object* command to add *MIB_object* to the MIB objects whose values are included in the specified collection. Here, *MIB_object* must be a counter (see the chapter entitled "LightStream 2020 MIB Reference"), and collection number *n* must first have been created with the **set collection** *n* **create** command.

Note A very large collection may degrade system response time.

---

set collection n create

Use the **set collection** *n* **create** command to create collection number *n*. You must execute this command before any other **set collection** commands. Other parameters of the **set collection** command cannot be specified for a given collection until that collection has been created. Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n del

Use the **set collection** *n* **del** command to remove collection number *n* from the system. Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n delvar

Use the **set collection** *n* **delvar** *MIB_object* command to remove *MIB_object* from the set of objects whose values are included in collection number *n*. Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n halt

Use the **set collection** *n* **halt** command to suspend collection process number *n*. It may be started again with the **set collection** *n* **start** command any time before the time specified by the **endtime** argument (or with the **filesize** argument or the **frequency** argument). Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n start

Use the **set collection** *n* **start** command to invoke collection number *n*. It may be halted and started any number of times in the time range specified by the **begintime** and **endtime** arguments (or with the **filesize** argument or the **frequency** argument). Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n begintime

Use the **set collection** *n* **begintime** [[[[*yy***:**]*mm*:]*dd***:**]*hh***:***mm***:***ss*] command to set the time at which collection number *n* is available to be started with the **start** argument. The default beginning time is the current time. Here, *yy* is the year, *mm* is the month, *dd* is the day, and *hh***:***mm***:***ss* is the time of day. (This value can also be set with the **filesize** argument or the **frequency** argument.) Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n endtime

Use the **set collection** *n* **endtime** [[[[*yy***:**]*mm*:]*dd***:**]*hh***:***mm***:***ss*] command to set the time at which collection number *n* is no longer available to be started with the **start** argument. Here, *yy* is the year, *mm* is the month, *dd* is the day, and *hh***:***mm***:***ss* is the time of day. The default ending time is 23:59:59 on December 31, 2037. (This value can also be set with the **filesize** argument or the **frequency** argument.) Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n filesize

Use the **set collection** *n* **filesize** [*KB*] [: *begintime* [: *endtime*]] command to set the maximum size of the collection file in kilobytes, the time at which collection number *n* begins, and the time at which collection number *n* ends. The optional times *begintime* and *endtime* are in [[[*yy*:]*mm*:]*dd*:]*hh*:*mm*:*ss* format. The collection file is a circular file: when the collection data attains the configured file size limit, the collection process begins overwriting the data in the file from the beginning. The default file size is 100 KB. For the other defaults, see **begintime** and **endtime**. Collection number *n* must first have been created with the **set collection** *n* **create** command.

set collection n frequency

Use the **set collection** *n* **frequency** [*ss* [: *begintime* [: *endtime*]]] command to set the frequency (specified as *ss* seconds) at which collection is to be done, the time at which collection number *n* begins, and the time at which collection number *n* ends. The times *begintime* and *endtime*, in [[[*yy*:]*mm*:]*dd*:]*hh*:*mm*:*ss* format, are optional. The default frequency *ss* is 60 seconds. For the other defaults, see **begintime** and **endtime**. Collection number *n* must first have been created with the **set collection** *n* **create** command.

Note Making the value of *n* (the intervals between collections) too small may affect system response time.

Configuration Lock Attribute

Use the **set config** command family to control write access to the MMA configuration database on the node.

Note The **set config** commands require CLI protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.")

---

set config lock

Use the **set config lock** command to lock the configuration database before setting parameters with CLI commands. When you use this command, all changes to configuration parameters are written to the disk, and other concurrent users are prevented from making configuration changes with CLI commands. The CLI issues a periodic reminder that the database is locked. The lock times out automatically 2 minutes after the termination of the CLI session in which the lock was issued.

This command is equivalent to the **setsnmp mmaSetLock.0 3** command.

You can use the command **setsnmp mmaSetLock.0 2** to lock the chassis (that is, its local database) without writing changes to the disk. This is useful for making experimental changes without interference from others. When **setsnmp** is used to set the mmaSetLock object to 2 or 3, the lock automatically times out after 2 minutes of no input from the user. However, with these commands, in contrast to the **set config lock** command, the CLI does not issue a periodic reminder that the chassis is locked.

A user of the CLI who attempts to use CLI set commands while the local configuration database is locked by any of these commands receives the following generic SNMP error message:

```
SNMP error
```

Limitations of SNMP preclude making this message more informative.

Note After you make configuration changes and write them to the disk, as described above, the local database is out of synch with the global database. As soon as possible, use the Verify function in the configuration tool on the network management station to copy configuration changes from the local configuration database on the LS2020 node to the global configuration database on the network management station. The Verify function retrieves the local settings and allows you to write them over the global values.

---

set config unlock

Use the **set config unlock** command to unlock the configuration database for changes made with CLI commands. Multiple users can concurrently make configuration changes with CLI commands, none of which are written to disk. By default, CLI commands affect configuration parameters in run-time memory only.

This command is equivalent to the **setsnmp mmaSetLock.0 1** command.

Note Use the **set config lock** command before changing between **trunk** and any edge protocol with the **set characteristics protocol** command. This step is required because the card resets and the value is read back from the local configuration database during the card restart process.

Modem Attributes

Use the **set modem** command family to set the modem initialization string and modem password for the specified switch card.

Syntax

```
set modem {sa | sb} {initstring "init_string" | password password}
```

set modem switch initstring

Use the **set modem** *switch* **initstring** "*modem_commands*" command to set the modem initialization string to *modem_commands* for the specified switch card. The *switch* argument must be either **sa** or **sb**; it indicates whether the initialization string is to be configured for Switch Card A or Switch Card B. The modem initialization string *modem_commands* must be placed in quotation marks.

The modem initialization string is a sequence of modem commands specifying the state that a modem must assume in order to make a connection. The default string is in Hayes modem command format, as follows:

```
AT&F&D2&C1S0=1S2=128S7=30S36=7S95=44
```

The Hayes-Format commands in the modem initialization string are as follows:

AT	The attention command.
&F	Restore the factory configuration (set register values to Hayes defaults).
&D2	DTR option: Following loss of the data terminal ready (DTR) signal, the modem disconnects, sends the OK result code, and disables auto answer while DTR is off.
&C1	DCD option: The received line signal detected (RLSD) follows the state of the data carrier from the remote modem.
S0=1	The number of rings until auto-answer = 1.
S2=128	The escape process is disabled. (It is disabled because this command assigns the escape character to a value higher than ASCII 127.)
S7=30	The local modem waits 30 seconds for a carrier signal from the remote modem before hanging up.
S36=7	If the attempted error correction link fails, an MNP connection is attempted. If the MNP connection fails, a normal mode connection is established.
S95=44	Extended result code bit map. The binary equivalent of 44 is 101100. A bit set to 1 enables a set of result codes as follows: Bit 2: Enable the carrier result codes. Bit 3: Enable the protocol result codes. Bit 5: Enable the compression result codes.

If the modem initialization string must be set for a modem that requires a different command format, the modem commands in it must put the modem in an equivalent state.

set modem switch password

Use the **set** *switch* **modem password** *password* command to set the modem password to *password* for the specified switch card. The *switch* argument must be either **sa** or **sb**; it indicates whether the password is to be configured for Switch Card A or Switch Card B. When a connection is made to the node's modem port, a password prompt is issued and this password is required.

Note This command affects *only* the node on which the CLI is running when you execute it, regardless of any target that has been set with the command **set snmp hostname** *name*.

The **set modem** command requires CLI protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.")

Network Timing Attributes

Use the **set nettime** command family to configure a preference table of clocking sources and to specify the switch card that distributes clocking to interface modules (line cards) that are capable of receiving it. If a clocking source fails, the software seeks clocking from each source in the table in turn until it finds a viable source. When it reaches the end of the table it defaults to the local oscillator on the switch card; it does not wrap to the top of the table.

set nettime delete

Use the **set nettime delete** *n* command to delete the *n*th entry from the net time table.

set nettime insert

Use the **set nettime insert** *n clocking-source* command to insert *clocking-source* as entry *n* in the clocking-source preference table. Position *n* must be empty in the table, either because it has not been specified with a previous use of **set nettime prefer-table** or **set nettime insert**, or because its value has been deleted with the **set nettime delete** command. The preference level *n* must be in the range 1 – 10, and *clocking-source* may be any of the following:

c.p	A port number
bits	The BITS plug
osc	The local oscillator on the switch card

set nettime prefer-table

Use the **set nettime prefer-table** *clocking-source1*[**,** *clocking-source2* ...] command to create the clocking-source preference table, specifying up to ten sources. The command overwrites any existing table and triggers a change to the clocking source specified at the top of the new table. The

clocking sources are listed in the preference table in the same sequence in which the *clocking-source* arguments are specified; the tenth argument corresponds to preference level 10, the ninth to preference level 9, and so on. The *clocking-source* arguments may be any of the following:

c.p	A port number
bits	The BITS plug
osc	The local oscillator on the switch card

You may specify a given clocking source at more than one place in the table. This is useful if you wish to re-try the most-preferred clocking source after trying each less-preferred source. For example, the following command creates a table specifying that the BITS plug should be re-tried after each of a series of ports on card 3:

```
cli> set nettime prefer-table bits,3.0,bits,3.1,bits,3.2,bits,3.3,bits,3.4
```

This command specifies a preference table with a clocking source at each of the ten preference levels, as follows:

1 BITS
2 3.0
3 BITS
4 3.1
5 BITS
6 3.2
7 BITS
8 3.3
9 BITS
10 3.4

set nettime reset-level

Use the **set nettime reset-level** *n* command to trigger a change to the clocking source which is specified as the *n*th entry in the clocking-preference table, where *n* is in the range 1 – 10. Use the command **set nettime reset-level 1** to resume use of the clocking source specified at the top of the table if you believe it has become available again after being unavailable.

Note This command requires protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.")

---

set nettime switch

Use the **set nettime switch** {**sa** | **sb** | **auto**} command to specify which switch card is to distribute clocking. With the **auto** argument, the node software selects whichever switch card is active. The **sa** or **sb** argument can be used to force selection of a particular switch card for diagnostic or other purposes.

Process Attributes

Use the **set pid** command family to set the trap level or administrative status of a process.

set pid PID adminstatus

Use the **set pid** *PID* **adminstatus** {**active** | **inactive**} command to set to active or inactive the administrative status (that is, the administratively preferred state) of process number *PID*. Whenever the operational status of process number *PID* changes, the system restores it to this preferred state as soon as it can.

set pid PID traplevel

Use the **set pid** *PID* **traplevel** *level* command to set the per-process trap reporting threshold (the level of traps that are reported for process number *PID*). The control of traps for a process is independent of the control of traps reported to the console (see **set chassis consoletraplevel**), and it is independent of the control of traps reported by the chassis (see **set chassis traplevel**).

The four trap levels are as follows:

oper Operational traps

info Informational and operational traps

trace Trace, informational, and operational traps

debug All traps

Each trap level is progressively more inclusive: the info level includes oper traps, the trace level includes info and oper traps, and the debug level includes all traps. See the *LightStream 2020 Traps Reference Manual* for more information about trap levels and for information about the relationships among traps, PIDs, and processes.

There must be a compelling reason to use any argument other than **info** or **oper**. Instead of the **trace** or **debug** argument, use the **set trap** command for individual traps. By doing this, you avoid flooding the node with traps, which could degrade performance.

Port Attributes

Use the **set port** command family to configure a port, to assign a traffic filter or traffic profile to a port, to create a multicast flow through a port, or to configure virtual LAN internetworking (VLI) workgroups.

The **set port** commands are described under the following headings:

- Port States
- Port Characteristics
- ATM UNI Ports
- Spanning Tree Bridge Ports
- Constant Bit Rate PVCs
- FDDI Ports
- Frame Forwarding Ports
- Frame Relay Ports
- Traffic Filters, Profiles, and Multicast Groups
- Virtual LAN Internetworking

Port Identifiers

These commands require a port identifier in dot-separated format *c.p*,where *c* is the number of a card and *p* is the number of a port on that card.

- Use the **show chassis cards** command to see card numbers.
- Use the **show card** *card#* **ports** command to see port numbers on card *card#*.

Restrictions By Port Type

Many port attributes can be set only for a given port type. Table 1-1 lists the different port types. It gives the protocol and the card type of each port type (as displayed by **show card** commands) and the **set port** commands that may be used on it, listed under the titles of the sections of this document in which the commands are described.

Use the **show chassis cards** command to display the card types listed in Table 1-1; use the **show card** *card#* command to display the protocols listed in Table 1-1. See the *LightStream 2020 Configuration Guide* for information about the different configurable attributes of the various card types.

Table 1-1 Commands That Are Restricted to Certain Port and Card Types

Port Type	Protocol	Card Type	Command Description	Note
Frame Relay and Frame Forwarding Ports	Frame Relay, Frame Forwarding	LS Edge SAC edge	Frame Relay Ports set port c.p framerelay set port c.p dlci Frame Forwarding Ports set port c.p frameforwarding Port Characteristics set port c.p characteristics dce-dte-type set port c.p characteristics dce-bitrate-bps set port c.p characteristics dte-bitrate set port c.p characteristics executechange set port c.p characteristics protocol	
Trunk Ports	T1 Trunk	LS Trunk SAC Trunk	Port Characteristics set port c.p characteristics dce-dte-type set port c.p characteristics dce-bitrate-bps set port c.p characteristics dte-bitrate set port c.p characteristics executechange set port c.p characteristics protocol	
	MS Trunk CLC Trunk	MS Trunk T3 Trunk E3 Trunk OC-3c Trunk	Port Characteristics set port c.p characteristics cable len set port c.p characteristics cell-scrambling set port c.p characteristics executechange set port c.p characteristics oc3-type set port c.p characteristics protocol set port c.p characteristics vpi	Not OC-3c OC-3c only Not MS
ATM UNI Ports	ATM-UNI	MS Edge T3 Edge E3 Edge OC-3c Edge	Port Characteristics set port c.p characteristics cable len set port c.p characteristics cell-scrambling set port c.p characteristics executechange set port c.p characteristics oc3-type set port c.p characteristics protocol ATM UNI Ports set port c.p vci	 Not OC-3c OC-3c only Not MS
Inter-networking Ports	FDDI ETHERNET	FDDI Ethernet	FDDI Ports Spanning Tree Bridge Ports Virtual LAN Internetworking Traffic Filters, Profiles, and Multicast Groups	FDDI only
constant bit rate (CBR) Ports	T1 Circuit Emulation E1 Circuit Emulation	CEMAC	Port Characteristics set port c.p characteristics clkmode set port c.p characteristics cable len set port c.p characteristics cable db set port c.p characteristics linecoding set port c.p characteristics circuit-id Constant Bit Rate PVCs set port c.p cbrpvc	

Port States

Use the **set port** *state* command family to configure or modify the state of a port. The arguments are **active**, **inactive**, **testing**, **loop**, and **unloop**. Except as noted for the **loop** argument, these commands apply to every port type.

set port c.p active

Set the administrative state of the specified port to active when it has been in the inactive state or the testing state. When the operational state of a card is active, the card is powered up and able to handle traffic.

The command in the following example makes port 5 on card 8 active:

```
cli> set port 8.5 active
```

set port c.p inactive

Set the administrative state of the specified port to inactive. When the operational state is inactive, the card is powered down. To restore power to the card, use TCS commands or CLI **set tcs** commands.

set port c.p testing

Set the administrative state of the specified port to the testing state. When the operational state of the card is testing, the card is powered up but prevented from handling traffic, in the expectation that it will run diagnostics. The **test** command is the preferred way to set the port to the testing state.

set port c.p loop internal

Loop the specified port internally.

Note Internal looping of a Frame Relay UNI interface provides no useful diagnostic information because the UNI protocol is asymmetric. To loop such a port, first convert it to an NNI interface, and then use the set **port** *c.p* **framerelay netinterfacetype nni** command to set the Frame Relay net interface type to NNI. A successful loop sets the administrative state of the port to testing and the operational state to up. To set the Frame Relay net interface type to UNI again, use the **set port** *c.p* **framerelay netinterfacetype uni** command.

Ethernet and FDDI ports cannot be looped.

---

set port c.p loop remote

Loop the specified port externally.

Note Ethernet and FDDI ports cannot be looped.

---

set port c.p unloop

Unloop the specified port.

Port Characteristics

Use the **set port** *c.p* **characteristics** commands to configure or modify port characteristics. Some characteristics are limited to certain port types, as indicated in the descriptions of the individual commands.

set port c.p characteristics cable len

For constant bit-rate (CBR) circuits and for T3 and E3 ports, use the **set port** ***c.p*** **characteristics cable len** *length* command to set the signal attenuation factor (line buildout) due to the electrical impedance of connective cabling. (For a CBR circuit using a CEMAC card, the command **set port** ***c.p*** **characteristics cable db** is an alternative.)

Several ranges are provided for each card type, as follows:

Card Type	Feet of Cable
T3	0 – 450
	450 – 900
E3	0 – 350
	351 – 800
	801 – 1000
	1001 – 1250
CEMAC	0 – 133
	133 – 266
	266 – 399
	399 – 533
	533 – 655

The value of *length* is mapped to a range that is appropriate for the card type. Thus, there is no effective difference between a value of 10 feet and a value of 110 feet.

For an E3 connection, the ranges of actual cable lengths overlap. A value in the range 351 – 800 is adequate for a cable as short as 300 feet; a value in the range 801 – 1000 is adequate for a cable as short as 650 feet; and a value in the range 1001 – 1250 is adequate for a cable as short as 900 feet. Bear this in mind if you have estimated the E3 cable length, and there is a possibility that the actual cable length is significantly greater than your estimate.

The measurements given in feet above correspond to measurements in meters as follows:

Feet	Meters	Feet	Meters	Feet	Meters
133	41	450	137	900	274
266	81	533	162	1000	305
300	92	650	198	1250	381
350	107	655	200		
399	122	800	244		

The software interprets the numeric *length* argument of this command as a number of feet.

set port c.p characteristics cable db

For constant bit rate (CBR) circuits, you may use the **set port** *c.p* **characteristics cable db** *value* command (as an alternative to the **set port** *c.p* **characteristics cable len** *feet* command) to set the signal attenuation factor (line buildout) due to electrical impedance of connective cabling. The significance of the *value* argument is shown in the following table.

Argument	Attenuation
0	0.0 dB (no attenuation)
1	–7.5 dB
2	–15.0 dB

set port c.p characteristics cell-scrambling

Use the **set port** *c.p* **characteristics cell-scrambling {enable | disable}** command to enable or disable cell payload scrambling on a medium-speed port or a T3/E3 edge or trunk port (on an 8-port card). This attribute must be set the same at both ends of a connection. For OC-3c, it cannot be disabled; for DS-3, it can be in either state.

set port c.p characteristics clkmode

Use the **set port** *c.p* **characteristics clkmode** *type* command to set the clock mode type for CBR circuit emulation. The value of *type* may be **adaptive**, **srts**, or **synchronous**.

set port c.p characteristics clocking

Use the **set port** *c.p* **characteristics clocking** {**internal** | **external**} command to set the clocking source for an OC-3c, T1, or E1 port to the port's receive line (**external**) or to the node-wide network timing source provided by the switch card (**internal**).

set port c.p characteristics circuit-id

For constant bit rate (CBR) circuits, use the **set port** *c.p* **characteristics circuit-id** *string* command to set the transmission vendor's circuit identifier. The string can be up to 64 characters. This command sets the value of the dsx1CircuitIdentifier object in the DS1 standard MIB.

set port c.p characteristics csu

Use the **set port** *c.p* **characteristics csu {none | larse}** command to set the CSU/DSU type of a port on a low-speed card or serial access card to **larse** or to specify that no CSU/DSU is present.

You must use the **set port** *c.p* **characteristics executechange** command in order to make this change operational.

set port c.p characteristics dce-bitrate-bps

Use the **set port** *c.p* **characteristics dce-bitrate-bps** *bps* command to set the DCE bit rate for the specified port on a low-speed or serial interface module. The port must first have been configured as a DCE with the **set port** *c.p* **characteristics dce-dte-type** command. The DCE bit rate is used when a port is being driven through use of internal clocking.

You must use the **set port** *c.p* **characteristics executechange** command in order to make this change operational.

For an 8-port serial interface module, the value of *bps* for the DCE bit rate may be any of the following:

55854	192000	455111	945230	1755428	4096000
56109	256000	512000	1228800	2048000	6144000
64000	384000	768000	1365333	2457600	
128000	438857	877714	1536000	3072000	

For a low-speed interface module (line card), the value of *bps* for the DCE bit rate may be any of the following:

56000	192000	448000	896000	1792000	(4000000)
64000	256000	512000	1344000	2688000	(5376000)
128000	384000	768000	1536000	3584000	

(For the low-speed interface module, the values 4,000,000 and 5,376,000 are available but are not supported; they may work for large packet sizes.)

You must use the **set port** *c.p* **characteristics executechange** command in order to make this change operational.

set port c.p characteristics dte-bitrate

Use the **set port** *c.p* **characteristics dte-bitrate** *bps* command to set the DTE bit rate for the specified port on a low-speed or serial interface module. The card must first have been configured as a DTE with the **set port** *c.p* **characteristics dce-dte-type** command. The value of *bps* for the DTE bit rate is unrestricted in the range of decimal integers 9,000 – 3,840,000. (Values up to 6,000,000 are available but not supported; they may work for large packet sizes.)

You must use the **set port** *c.p* **characteristics executechange** command in order to make this change operational.

The DTE bit rate setting is used when a port is being driven through the use of external clocking on a serial line. If the value is incorrect, and differs from the bit rate actually received from the DCE, the incorrect value either limits the data on the port too much, or it causes the allocation of excess bandwidth that cannot be used. If the bit rate of the DCE varies, the interface module issues traps.

set port c.p characteristics dce-dte-type

Use the **set port** *c.p* **characteristics dce-dte-type {dce | dte | dce-internal}** command to set the specified port on a low-speed or serial interface module to be a DCE, a DTE, or an internal DCE. The **dce** setting connects the receive clock to the TT interface signal. The **dce-internal** setting connects the receive clock to a locally generated clock. A DCE internal port can interface with DTE devices that cannot return the TT signal. This value is interdependent with the values described under the **dce-bitrate-bps** and **dte-bitrate** arguments.

You must use the **set port** *c.p* **characteristics executechange** command in order to make this change operational.

set port c.p characteristics executechange

Use the **set port** *c.p* **characteristics executechange** command to make certain previously set administrative values operational for the specified port. The distinction between administrative and operational values applies only to the following port characteristics: **csu**, **protocol**, and the DCE and DTE attributes.

set port c.p characteristics framing-type

Use the **set port** *c.p* **characteristics framing-type {plcp | t3-hec | g-804}** command to set the framing type of a T3 port to PLCP or T3 HEC, or to set the framing type of an E3 port to PLCP or G.804.

set port c.p characteristics linecoding

For constant bit rate (CBR) circuits, use the **set port** *c.p* **characteristics linecoding {ami | b8zs | hdb3}** command to set the type of line coding (zero code suppression) used on the link. For E1 circuit emulation, the default is HDB3, and for T1 circuit emulation the default is B8ZS. In either case, the line type may be set to AMI. This command sets the value of the dsx1LineCoding object in the DS1 standard MIB. The effects of the different types of line coding are as follows:

- With B8ZS line coding and with HDB3 line coding, a specified pattern of normal bits and bipolar violations replaces a sequence of zero bits of specified length.
- AMI line coding does not use zero code suppression. Instead, the higher layer must provide data which meets or exceeds the pulse density requirements, for example, by inverting HDLC data.

set port c.p characteristics oc3-type

Use the **set port** *c.p* **characteristics oc3-type {sonet | sdh}** command to configure an OC-3c trunk or edge port to support SONET (STS-3c) or SDH (STM-1).

set port c.p characteristics protocol

Use the **set port** *c.p* **characteristics protocol {atm-uni | frameforward | framerelay | trunk}** command to configure an edgeprotocol (ATM-UNI, Frame Forwarding, or Frame Relay) or the trunk protocol on the specified port. The following considerations apply when you interchange the trunk protocol and an edge protocol on a port:

- Use the **set config lock** command before changing between the trunk protocol and an edge protocol. This procedure is necessary because the card resets and the value is read back from the local configuration database.
- Use the **set port** *c.p* **characteristics protocol** command only for port *card#*.**0** (although the lowest configured port number is accepted). This command affects all ports on the interface module because trunk and edge protocols cannot be mixed on a single card.
- Only half of the ports on an 8-port T3/E3 card or a 2-port OC-3c card are available when they are configured as trunk ports.

You must use the **set port** *c.p* **characteristics executechange** command in order to make this change operational.

set port c.p characteristics vpi

Use the **set port** *c.p* **characteristics vpi** *vpi#* command to configure this port as a virtual path connection trunk (VP trunk) port with virtual path identifier (VPI) number *VPI#*. This command can be used only on an 8-port or 4-port T3/E3 interface module or on an OC-3c module. The port must be configured as a trunk port with the **set port** *c.p* **characteristics protocol trunk** command. Use the **show port** *c.p* **vpi** command to display the VPI number.

ATM UNI Ports

This section gives an overview of commands used to configure and control ATM UNI permanent virtual connections (PVCs). Complete descriptions of **set port** commands for ATM UNI ports follow the overview.

ATM UNI PVCs

Use the **set port** *c.p* **vci** *vci#* commands to configure and control an ATM UNI PVC on the specified port. The VCI number must be in the range 1 – 32399. (This range may be further restricted depending upon the type of interface module. The software informs you of such restrictions.)

To create an ATM UNI permanent virtual connection (PVC), use the **set port** *c.p* **vci** commands. A typical command sequence would be as follows:

- **set port** *c.p* **vci** *vci#* **destnode** {*chassisID* | *chassisname*}
- **set port** *c.p* **vci** *vci#* **destport** *c.p*
- **set port** *c.p* **vci** *vci#* **destvci** *destvci#*
- **set port** *c.p* **vci** *vci#* **activate**

You could use the **insured-rate**, **max-rate**, and **transmit-priority** arguments in additional **set port** commands, but most users accept the default values for these three parameters. It is recommended that you accept the defaults for the insured burst and maximum burst parameters. (In any case, the maximum burst size must be at least as great as the insured burst size.)

A PVC must be configured explicitly in both directions—that is, you must configure the circuit for the ports at both ends of the PVC. To configure a bidirectional ATM UNI PVC with VCI number 17 between port 3.1 on node-A and port 7.0 on node-B, use the following commands:

On Node-A	On Node-B
set port 3.1 vci 17 destnode node-B	**set port 7.0 vci 17 destnode node-A**
set port 3.1 vci 17 destport 7.0	**set port 7.0 vci 17 destport 3.1**
set port 3.1 vci 17 destvci 17	**set port 7.0 vci 17 destvci 17**

Using the same VCI number at both ends of the PVC is administratively convenient, but not necessary. Insured rate and max rate may be configured with different values at the two ends of the PVC if an asymmetric PVC is desired. All other PVC parameters should be configured the same at both ends of the PVC.

set port c.p vci vci# activate

Use the **set port** *c.p* **vci***vci#* **activate** command to enable the specified ATM UNI PVC on the specified port after setting its parameters with other **set port** *c.p* **vci** commands. The destination node, destination port, and destination VCI number may not be altered after activating the PVC. Configure both ends of a bidirectional PVC before activating the PVC.

set port c.p vci vci# deactivate

Use the **set port** *c.p* **vci***vci#* **deactivate** command to deactivate the specified PVC without deleting it. This is useful, for example, when you wish to keep an ATM UNI PVC as a backup circuit.

set port c.p vci vci# del

Use the **set port** *c.p* **vci***vci#* **del** command to deactivate and delete the specified ATM UNI PVC from the specified port.

set port c.p vci vci# destnode

Use the **set port** *c.p* **vci** *vci#* **destnode** {*chassisID* | *chassisname*} command to set the destination node for the specified ATM UNI PVC on the specified port. Identify the node by its chassis number, or by its chassis name if the name has previously been set with the **set chassis name** command.

set port c.p vci vci# destport

Use the **set port** *c.p* **vci** *vci#* **destport** *c.p* command to set the destination port to *c.p* for the specified ATM UNI PVC.

set port c.p vci vci# destvci

Use the **set port** *c.p* **vci** *vci#* **destvci** *destvci#* command to set the destination VCI to *destvci#* for the specified ATM UNI PVC. The VCI numbers *vci#* and *destvci#* must both be in the range 1 – 32399.

set port c.p vci vci# insured-burst

Use the **set port** *c.p* **vci** *vci#* **insured-burst** *cells* command to set the insured burst to *cells* for the specified ATM UNI PVC. The insured burst is the upper bound on the non-sharable bandwidth that the connection may use in bursts, that is, the amount by which bursts may exceed the insured rate (see **insured-rate**). The range is 0 – 1023. The default is 128 cells. This value cannot exceed the value of the maximum burst parameter (see the **set port** *c.p* **vci** *vci#* **max-burst** command).

set port c.p vci vci# insured-rate

Use the **set port** *c.p* **vci** *vci#* **insured-rate** *cells/sec* command to set the insured rate to *cells/sec* for the specified ATM UNI PVC. The insured rate is the upper bound on the non-sharable bandwidth that the connection may use in a sustained way. The range is 0 – 353,000 cells per second. The default for ATM UNI circuits is 0 cells per second.

set port c.p vci vci# max-burst

Use the **set port** *c.p* **vci** *vci#* **max-burst** *cells* command to set the maximum burst to *cells* for the specified ATM UNI PVC. The default is 128 cells. This value must be at least as great as the value of the insured burst parameter (see the **set port** *c.p* **vci** *vci#* **insured-burst** command).

set port c.p vci vci# max-rate

Use the **set port** *c.p* **vci** *vci#* **max-rate** *cells/sec* command to set the maximum rate to *cells/sec* for the specified ATM UNI PVC. The maximum rate is the upper bound on the rate of all traffic (insured and noninsured) allowed to enter the LightStream 2020 network, congestion permitting. The default rate is the line rate for all cards.

set port c.p vci vci# principal-service-type { guaranteed | insured }

Use the **set port** *c.p* **vci** *vci#* **principal-service-type {guaranteed | insured}** command to set the bandwidth type (cell-drop priority) on the primary portion of the specified ATM UNI PVC to guaranteed or insured. The default is insured.

set port c.p vci vci# transmit-priority { 0 | 1 }

Use the **set port** *c.p* **vci** *vci#* **transmit-priority {0 | 1}** command to set the transmit priority of the specified ATM UNI PVC. This priority is used at each LS2020 node in the PVC across the network. The default for ATM UNI circuits is 1.

Spanning Tree Bridge Ports

Use the **stb** argument of the **set port** command to set spanning-tree bridge attributes for the specified LAN port (see also the **set stb** command).

Note These attributes are not affected when the card is reset.

---

set port c.p stb priority

Use the **set port** *c.p* **stb priority** # command to set the priority of the specified port for a path that uses STP. The range is 0 – 255, and the default (if it is not explicitly set) is 128.

set port c.p stb enable

Use the **set port** *c.p* **stb enable** command to enable bridge forwarding on the specified port. Ports are enabled when they come up, but the spanning-tree protocol may disable a port to prevent loops if the topology of the bridged networks connected to this port changes.

set port c.p stb disable

Use the **set port** *c.p* **stb disable** command to disable bridge forwarding on the specified port.

set port c.p stb pathcost

Systems using the spanning-tree protocol calculate the relative costs of different paths toward the root bridge. A port's path cost is the contribution that the port makes to this calculation. Use the **set port** *c.p* **stb pathcost** # command to set the port's path cost. The range is 1 – 65535. The default value is calculated as 1000 divided by the speed of the network connection in megabits per second (Mbps). Thus, Ethernet has a default cost of 100, and FDDI has a default cost of 10.

Constant Bit Rate PVCs

Use the command **set port** *c.p* **cbrpvc** *PVC#* commands to configure constant bit rate PVCs.

set port c.p cbrpvc PVC# destination

Use the **set port** *c.p* **cbrpvc** *PVC#* **destination** *chassis*:*c.p*:*PVC2* command to create a constant bit rate PVC with ID *PVC#* on local port *c.p* connecting to remote PVC with ID *PVC2* on remote port *chassis*:*c.p*. Here, *chassis* is either the chassis ID number or the chassis name of an LS2020 node in the network. For the CEMAC card, *PVC#* is always **1**.

set port c.p cbrpvc PVC# {targetdepth | maxdepth}

Use the **set port** *c.p* **cbrpvc** *PVC#* {**targetdepth** | **maxdepth**} *bytes* command to control the reassembly buffer at the point where input cells are converted back into a constant bit rate (CBR) stream. An adaptive control loop maintains data in the buffer close to the level specified by **targetdepth** *bytes*. Data in excess of **maxdepth** *bytes* is discarded.

The default values of the target depth and maximum depth attributes are usually best left unchanged. If the target depth is set too high or if the maximum depth is set too far above the target, end-to-end delay for the entire circuit increases. With voice traffic, such delay can cause annoying echo. If the target depth is set too low or if the maximum depth is set too close to the target depth, random cell delay variation (CDV) may cause the circuit to overflow or underflow sporadically, causing data errors and reframe events for equipment downstream. For certain applications, such as video and phone, where some discarding of overflow data is an acceptable cost of maintaining a constant bit rate, it may be preferable to set these two parameters closer together.

set port c.p cbrpvc PVC# activate

Use the **set port** *c.p* **cbrpvc** *PVC#* **activate** command to activate the specified constant bit rate PVC.

set port c.p cbrpvc PVC# deactivate

Use the **set port** *c.p* **cbrpvc** *PVC#* **deactivate** command to deactivate the specified constant bit rate PVC.

set port c.p cbrpvc PVC# del

Use the **set port** *c.p* **cbrpvc** *PVC#* **del** command to delete the specified constant bit rate PVC.

set port c.p cbrpvc PVC# datarate

Use the **set port** *c.p* **cbrpvc** *PVC#* **datarate** {**bps** *bits/sec* | **cps** *cells/sec* | **slots** *slots*} command to set the data rate used by this fractional CBR circuit. The value of *bits/sec* is expressed in multiples of 64,000. The value of *slots* is either a list or a range of time slots. This parameter applies to ports on FCEMAC cards only.

FDDI Ports

Use the **set port** c.p **fddi** {**aport** | **bport**} commands to set FDDI port and station management (SMT) parameters of FDDI port A or port B.

set port c.p fddi {aport | bport} action enable

Use the **set port** *c.p* **fddi** {**aport** | **bport**} **action enable** command to enable the specified FDDI port.

set port c.p fddi {aport | bport} action disable

Use the **set port** *c.p* **fddi {aport | bport} action disable** command to disable the specified FDDI port.

set port c.p fddi {aport | bport} action start

Use the **set port** *c.p* **fddi {aport | bport} action start** command to start the specified FDDI port.

set port c.p fddi {aport | bport} action stop

Use the **set port** *c.p* **fddi {aport | bport} action stop** command to stop the specified FDDI port.

set port c.p fddi {aport | bport} connectpolicy

Use the **set port** *c.p* **fddi {aport | bport} connectpolicy {none | lct | loop | both}** command to specify the FDDI connection policy for this port. Use the **lct** argument for a MAC link competence test with the remote station (remote loop). Use the **loop** argument for an internal loop at the MAC. Enter **none** for no loop (internal or external), or enter **both** for both.

set port c.p fddi {aport | bport} lercutoff

Use the **set port** *c.p* **fddi {aport | bport} lercutoff** *error-rate* command to set the link error rate estimate. This is an estimate of the rate at which an FDDI link connection on this port is broken. The range is 4 – 15 and the default is 7, meaning 10^{-7} errors per second.

Note In the unlikely event that this rate needs adjustment, it should be changed only by someone who is very knowledgeable about FDDI.

---

set port c.p fddi smt t-notify

Use the **set port** *c.p* **fddi smt t-notify** *sec* command to set the timer used in the Neighbor Notification Protocol. The range is 2 – 30 seconds, and the default is 30 seconds.

Note In the unlikely event that this timer needs adjustment, it should be changed only by someone very knowledgeable about FDDI.

---

set port c.p fddi smt stat-report

Use the **set port** *c.p* **fddi smt stat-report {yes | no}** command to determine whether status reporting frames for FDDI events and conditions are sent to the SMT management software. The value **yes** is the default. Depending on your network management system, SMT may pass some of these messages on to higher levels, where they become visible to the operator as SNMP traps.

set port c.p fddi smt station connect

Use the **set port** *c.p* **fddi smt station connect** command to begin an FDDI connection sequence. The port is controlled as an FDDI station.

set port c.p fddi smt station disconnect

Use the **set port** *c.p* **fddi smt station** {**connect** | **disconnect**} command to break an FDDI connection when the port is controlled as an FDDI station.

set port c.p fddi smt station path-test

The **set port** *c.p* **fddi smt station path-test** command is intended to test the viability of the FLDSUP path when the port is controlled as an FDDI station. However, the FDDI path test is not supported in the current release.

set port c.p fddi smt station {disable-a | disable-b}

Use the **set port** *c.p* **fddi smt station disable-a** command to disable the FDDI circuit on the (FDDI) A port ; use the **set port** *c.p* **fddi smt station disable-b** command to disable the FDDI circuit on the B port. The port is controlled as an FDDI station, and the port mode at the other end of the link must be peer (not master).

Frame Forwarding Ports

Use the **set port** *c.p* **frameforwarding** commands to configure and control a frame forwarding port.

set port c.p frameforwarding activate

Use the **set port** *c.p* **frameforwarding activate** command to enable a Frame Forwarding circuit on the specified port.

set port c.p frameforwarding deactivate

Use the **set port** *c.p* **frameforwarding deactivate** command to disable the Frame Forwarding circuit on the specified port.

set port c.p frameforwarding destnode

Use the **set port** *c.p* **frameforwarding destnode** {*chassisID* | *chassisname*} command to set the destination node for Frame Forwarding on the specified port. The node is identified by its chassis ID, or it may be identified by its chassis name if the name has been set. Use the **set chassis name** command to set the chassis name.

set port c.p frameforwarding destport

Use the **set port** *c.p* **frameforwarding destport** *c2.p2* command to set the destination port to *c2.p2* on the remote node for the Frame Forwarding circuit configured on port *c.p* on the local node.

set port c.p frameforwarding insured-rate

Use the **set port** *c.p* **frameforwarding insured-rate** *bits/sec* command to set the insured rate to the bit rate *bits/sec* for the specified Frame Forwarding port. The insured rate is the upper bound on the nonsharable bandwidth that the connection may use in a sustained way. The range is 0 – 100,000,000 bits per second. The administrative default is 0.

set port c.p frameforwarding insured-burst

Use the **set port** *c.p* **frameforwarding insured-burst** *bytes* command to set the insured burst rate to *bytes* for the specified Frame Forwarding port. The insured burst is the upper bound on the nonsharable bandwidth that the connection may use in bursts. It is, therefore, the amount by which traffic on the connection may exceed the insured rate (see the preceding "set port c.p frameforwarding insured-rate" section). The range is 0 – 64,000. This value cannot exceed the value of the maximum burst parameter (see the **set port** *c.p* **frameforwarding max-burst** command).

set port c.p frameforwarding max-rate

Use the **set port** *c.p* **frameforwarding max-rate** *bits/sec* command to set the maximum rate for the specified Frame Forwarding port to the bit rate *bits/sec*. The maximum rate is the upper bound on the rate of all traffic (insured and non-insured) allowed to enter the LightStream 2020 network, congestion permitting. The range is 64,000 – 100,000,000 bps.

set port c.p frameforwarding max-burst

Use the **set port** *c.p* **frameforwarding max-burst** *bytes* command to set the maximum burst rate for the specified Frame Forwarding port to *bytes*. This value must be at least as great as the value of the insured burst parameter (see the **set port** *c.p* **frameforwarding insured-burst** command).

Frame Relay Ports

Use the **set port** *c.p* **framerelay** commands to configure and control a Frame Relay port, or each DLCI on a Frame Relay port.

set port c.p framerelay lmiconfig

Use the **set port** *c.p* **framerelay lmiconfig {none | frif | ansi_t1_617d | q933a}** command to set the LMI configuration type to FRIF, ANSI T1 617D, or Q933A, or to specify that there is no LMI for the specified port.

set port c.p framerelay netinterfacetype

Use the **set port** *c.p* **framerelay netinterfacetype {uni | nni}** command to set the Frame Relay net interface type to UNI or NNI for the specified port.

set port c.p dlci DLCI# activate

Use the **set port** *c.p* **dlci** *DLCI#* **activate** command to enable the circuit on the specified DLCI. The range of DLCI numbers is 16 – 991.

set port c.p dlci DLCI# deactivate

Use the **set port** *c.p* **dlci** *DLCI#* **deactivate** command to deactivate the circuit on the specified DLCI. The range of DLCI numbers is 16 – 991.

set port c.p dlci DLCI# del

Use the **set port** *c.p* **dlci** *DLCI#* **del** command to remove the specified DLCI from the system. The range of DLCI numbers is 16 – 991.

set port c.p dlci DLCI# destnode

Use the **set port** *c.p* **dlci** *DLCI#* **destnode** {*chassisID* | *chassisname*} command to set the destination node for the specified DLCI. The destination node is identified by its chassis number, or it may be identified by its chassis name if the name has been previously set with the **set chassis name** command. The range of DLCI numbers is 16 – 991.

set port c.p dlci DLCI# destport

Use the **set port** *c.p* **dlci** *DLCI#* **destport** *c2.p2* command to set the destination port for the specified DLCI to port *c2.p2*. The range of DLCI numbers is 16 – 991.

set port c.p dlci DLCI# destdlci

Use the **set port** *c.p* **dlci** *DLCI#* **destdlci** *destDLCI#* command to set the destination DLCI to *destDLCI#* for the DLCI specified as *DLCI#*. The range of DLCI numbers is 16 – 991 for both the *DLCI#* argument and the *destDLCI#* argument.

set port c.p dlci DLCI# insured-rate

Use the **set port** *c.p* **dlci** *DLCI#* **insured-rate** *bits/sec* command to set the insured rate for the specified DLCI to the bit rate *bits/sec*. The range of DLCI numbers is 16 – 991. This is the upper bound on the nonsharable bandwidth that the connection may use in a sustained way. The range is 0 – 100,000,000 bits per second.

set port c.p dlci DLCI# insured-burst

Use the **set port** *c.p* **dlci** *DLCI#* **insured-burst** *bytes* command to set the insured burst rate to *bytes* for the specified DLCI. The range of DLCI numbers is 16 – 991. The insured burst is the upper bound on the non-sharable bandwidth that the connection may use in bursts, that is, the amount by which traffic on the connection may exceed the insured rate (seethe **insured-rate** argument). The range is 0 – 64,000. This value cannot exceed the value of the maximum burst parameter (see the **set port** *c.p* **dlci** *DLCI#* **max-burst** command).

set port c.p dlci DLCI# max-rate

Use the **set port** *c.p* **dlci** *DLCI#* **max-rate** *bits/sec* command to set the maximum rate for the specified DLCI to the bit rate *bits/sec*. The range of DLCI numbers is 16 – 991. The maximum rate is the upper bound on the rate of all traffic (insured and noninsured) allowed to enter the LightStream 2020 network, congestion permitting. The range is 64,000 – 100,000,000 *bits/sec*.

set port c.p dlci DLCI# max-burst

Use the **set port** *c.p* **dlci** *DLCI#* **max-burst** *bytes* command to set the maximum burst rate to *bytes* for the specified DLCI. The range of DLCI numbers is 16 – 991. This value must be at least as great as the value of the insured burst parameter (see the **set port** *c.p* **dlci** *DLCI#* **insured-burst** command).

Traffic Filters, Profiles, and Multicast Groups

The following **set port** commands are used to filter traffic that is received over the specified port.

set port c.p bcast-limit discard-all

Use the **set port** *c.p* **bcast-limit discard-all** command to discard all bridge broadcast packets sent to this port. Broadcast frames that are recognized by filters are handled by the LS2020 hardware. Consequently, the broadcast limit attribute does not apply to broadcast traffic that matches a custom filter set on the port.

set port c.p bcast-limit forward-all

Use the **set port** *c.p* **bcast-limit forward-all** command to forward all bridge broadcast packets sent to this port. This command restores the default broadcast limit. Broadcast frames that are recognized by filters are handled by the LS2020 hardware. Consequently, the broadcast limit attribute does not apply to broadcast traffic that matches a custom filter set on the port.

set port c.p bcast-limit

Use the **set port** *c.p* **bcast-limit** *packets/sec* command to set the maximum rate of bridge broadcast packets to be forwarded through this port. The value is given in packets per second and is in the range 1 – 127. Excess broadcast packets are dropped. Broadcast frames that are recognized by filters are handled by the LS2020 hardware. Consequently, the broadcast limit attribute does not apply to broadcast traffic that matches a custom filter set on the port.

set port c.p bflt filterID block

Use the **set port** *c.p* **bflt** *filterID* **block** *priority* command to assign bridge traffic filter number *filterID* to block traffic received over port *c.p*. Traffic filter *filterID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). Up to 32 bridge filters can be assigned to the same port, the maximum being 1024 filters for all ports on an LS2020 node. A given filter can be associated with more than one port.

Note Resetting the card does not affect filter attributes. Bridge filters are applied to incoming traffic before IP and IPX filters are applied.

When an incoming packet on port *c.p* matches the blocking filter, the packet is discarded.

The *priority* argument is a number that determines the sequence in which multiple filters are considered on this port. Each filter on a given port must have a unique priority number. The lowest number is considered first. It is best to assign priority numbers by 10s (10, 20, 30, ...), leaving gaps for possible future insertions into the sequence. If two filters can match the same packet, give the more specific filter the higher priority, so that it is considered first.

set port c.p bflt filterID forward

Use the **set port** *c.p* **bflt** *filterID* **forward** *priority* [**mcast** *mcastID*] [**tprof** *tprofID*] command to assign bridge filter number *filterID* to forward traffic over a port. Traffic filter *filterID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). Up to 32 bridge filters can be assigned to the same port, the maximum being 1024 filters for all ports on an LS2020 node. A given filter can be associated with more than one port.

Note Resetting the card does not affect filter attributes. Bridge filters are applied to incoming traffic before IP and IPX filters.

When an incoming packet on port *c.p* matches the forwarding filter, a flow is generated (if it is not already established). For a point-to-point flow, the destination port is determined from information in the header of the incoming packet.

priority

The *priority* argument is a number that determines the sequence in which multiple filters are considered on this port. Each filter on a given port must have a unique priority number. The lowest number is considered first. It is best to assign priority numbers by 10s (10, 20, 30, ...), leaving gaps for possible future insertions into the sequence. If two filters can match the same packet, give the more specific filter the higher priority, so that it is considered first.

The optional arguments are discussed in the following paragraphs.

mcast *mcastID*

You can associate the multicast group identified as number *mcastID* with the flow, making it a multicast (point-to-multipoint) flow. The multicast group must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). The action taken by the filter must be forward.

Note For a multicast flow to be bidirectional, the same multicast group must be defined for and assigned to the remote endpoints.

Caution Multicast groups are network-wide constructs. Define them consistently on all nodes of the network. If you fail to do so, it may be difficult to debug problems involving multicast traffic. For administrative convenience, it is also advisable to define traffic profiles and filters consistently across the network or across relevant portions of the network.

tprof *tprofID*

You can associate the traffic profile identified as number *tprofID* with the flow. A traffic profile is a set of type-of-service attributes. Traffic profile number *tprofID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). The action taken by the filter must be forward.

Flows defined by different filters are multiplexed over the same connection under the following conditions:

- If the source ports match (that is, the port numbers *c.p* specified with the **set port** command)
- If the destinations (output port or multicast ID) match
- If the traffic profile IDs are the same (or null)

If you want to prevent multiplexing of a flow, define a second multicast group ID with the same list of ports, or a second traffic profile ID with the same values for traffic profile parameters. Associate the new ID with the filter that specifies the flow that you do not want multiplexed.

set port c.p bflt filterID del

Use the **set port** *c.p* **bflt** *filterID* **del** command to break the association between the specified bridge filter and the specified port. You must do this before you can delete the filter itself, using the **delete** command (see the chapter entitled "The Define and Delete Commands").

set port c.p bflt-def block

Use the **set port** *c.p* **bflt-def block** command to set the default bridge filter action for the specified port to **block**.

Note This attribute is not affected when the card is reset.

---

set port c.p bflt-def forward

Use the **set port** *c.p* **bflt-def forward** command to set the default bridge filter action for the specified port to **forward**.

Note This attribute is not affected when the card is reset.

---

set port c.p ipflt filterID block

Use the **set port** *c.p* **ipflt** *filterID* **block** *priority* command to assign filter number *filterID* to block traffic received over port *c.p*. Traffic filter *filterID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). Up to 32 IP filters can be assigned to the same port, the maximum being 1024 filters for all ports on an LS2020 node. A given filter can be associated with more than one port.

Note Resetting the card does not affect these attributes. IPX filters are applied to incoming traffic after bridge filters.

When an incoming packet on port *c.p* matches the blocking filter, the packet is discarded.

The *priority* argument is a number that determines the sequence in which multiple filters are considered on this port. Each filter on a given port must have a unique priority number. The lowest number is considered first. It is best to assign priority numbers by 10s (10, 20, 30, ...), leaving gaps for possible future insertions into the sequence. If two filters can match the same packet, give the more specific filter the higher priority, so that it is considered first.

set port c.p ipflt ID forward

Use the **set port** *c.p* **ipflt** *filterID* **forward** *priority* [**mcast** *mcastID*] [**tprof** *tprofID*] command to assign IP filter number *filterID* to forward traffic over a port. Traffic filter *filterID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). Up to 32 IP filters can be assigned to the same port, the maximum being 1024 filters for all ports on an LS2020 node. A given filter can be associated with more than one port.

Note Resetting the card does not affect filter attributes. IP filters are applied to incoming traffic after bridge filters.

When an incoming packet on port *c.p* matches the forwarding filter, a flow is generated (if it is not already established). For a point-to-point flow, the destination port is determined from information in the header of the incoming packet.

The *priority* argument is a number that determines the sequence in which multiple filters are considered on this port. Each filter on a given port must have a unique priority number. The lowest number is considered first. It is best to assign priority numbers by 10s (10, 20, 30, ...), leaving gaps for possible future insertions into the sequence. If two filters can match the same packet, give the more specific filter the higher priority, so that it is considered first.

The optional arguments are discussed in the following paragraphs.

mcast *mcastID*

You can associate the multicast group identified as number *mcastID* with the flow, making it a multicast (point-to-multipoint) flow. The multicast group must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). The action taken by the filter must be forward.

Note For a multicast flow to be bidirectional, the same multicast group must be defined for and assigned to the remote endpoints.

Caution Multicast groups are network-wide constructs. Define them consistently on all nodes of the network. If you fail to do so, it may be difficult to debug problems involving multicast traffic. For administrative convenience, it is also advisable to define traffic profiles and filters consistently across the network or across relevant portions of the network.

tprof *tprofID*

You can associate the traffic profile identified as number *tprofID* with the flow. A traffic profile is a set of type-of-service attributes. Traffic profile number *tprofID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). The action taken by the filter must be forward.

Flows defined by different filters are multiplexed over the same connection under the following conditions:

- If the source ports match (that is, the port numbers *c.p* specified with the **set port** command)
- If the destinations (output port or multicast ID) match
- If the traffic profile IDs are the same (or null)

If you want to prevent multiplexing of a flow, define a second multicast group ID with the same list of ports, or a second traffic profile ID with the same values for traffic profile parameters. Associate the new ID with the filter that specifies the flow that you do not want multiplexed.

set port c.p ipflt ID del

Use the **set port** *c.p* **ipflt** *ID* **del** command to break the association between the specified IP filter and the specified port. You must do this before you can delete the filter itself, using the **delete** command (see the chapter entitled "The Define and Delete Commands").

set port c.p ipflt-def block

Use the **set port** *c.p* **ipflt-def block** command to set to **block** the default IP filter action for the specified port.

Note Filter attributes are not affected when the card is reset.

---

set port c.p ipflt-def forward

Use the **set port** *c.p* **ipflt-def forward** command to set the default IP filter action for the specified port to **forward**.

Note Filter attributes are not affected when the card is reset.

---

set port c.p ipxflt filterID block

Use the **set port** *c.p* **ipxflt** *filterID* **block** *priority* command to assign filter number *filterID* to block traffic received over port *c.p*. Traffic filter *filterID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). Up to 32 IPX filters can be assigned to the same port, the maximum being 1024 filters for all ports on an LS2020 node. A given filter can be associated with more than one port.

Note Resetting the card does not affect filter attributes. IPX filters are applied to incoming traffic after bridge filters.

When an incoming packet on port ***c.p*** matches the blocking filter, the packet is discarded.

The *priority* argument is a number that determines the sequence in which multiple filters are considered on this port. Each filter on a given port must have a unique priority number. The lowest number is considered first. It is best to assign priority numbers by 10s (10, 20, 30, ...), leaving gaps for possible future insertions into the sequence. If two filters can match the same packet, give the more specific filter the higher priority, so that it is considered first.

set port c.p ipxflt ID forward

Use the **set port** *c.p* **ipxflt** *filterID* **forward** *priority* [**mcast** *mcastID*] [**tprof** *tprofID*] command to assign IPX filter number *filterID* to forward traffic over a port. Traffic filter *filterID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). Up to 32 IPX filters can be assigned to the same port, the maximum being 1024 filters for all ports on an LS2020 node. A given filter can be associated with more than one port.

Note Resetting the card does not affect filter attributes. IPX filters are applied to incoming traffic after bridge filters.

When an incoming packet on port ***c.p*** matches the forwarding filter, a flow is generated (if it is not already established). For a point-to-point flow, the destination port is determined from information in the header of the incoming packet.

The *priority* argument is a number that determines the sequence in which multiple filters are considered on this port. Each filter on a given port must have a unique priority number. The lowest number is considered first. It is best to assign priority numbers by 10s (10, 20, 30, ...), leaving gaps for possible future insertions into the sequence. If two filters can match the same packet, give the more specific filter the higher priority, so that it is considered first.

The optional arguments are giving in the following paragraphs.

mcast *mcastID*

Optionally associate the multicast group identified as number *mcastID* with the flow, making it a multicast (point-to-multipoint) flow. The multicast group must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). The action taken by the filter must be forward.

Note For a multicast flow to be bidirectional, the same multicast group must be defined for and assigned to the remote endpoints.

Caution Multicast groups are network-wide constructs. Define them consistently on all nodes of the network. If you fail to do so, it may be difficult to debug problems involving multicast traffic. For administrative convenience, it is also advisable to define traffic profiles and filters consistently across the network or across relevant portions of the network.

tprof *tprofID*

Optionally associate the traffic profile identified as number *tprofID* with the flow. A traffic profile is a set of type-of-service attributes. Traffic profile number *tprofID* must previously have been created with the **define** command (see the chapter entitled "The Define and Delete Commands"). The action taken by the filter must be forward.

Flows defined by different filters are multiplexed over the same connection under the following conditions:

- If the source ports match (that is, the port numbers *c.p* specified with the **set port** command)
- If the destinations (output port or multicast ID) match
- If the traffic profile IDs are the same (or null)

If you want to prevent multiplexing of a flow, define a second multicast group ID with the same list of ports, or a second traffic profile ID with the same values for traffic profile parameters. Associate the new ID with the filter that specifies the flow that you do not want multiplexed.

set port c.p ipxflt ID del

Use the **set port** *c.p* **ipxflt** *ID* **del** command to break the association between the specified IPX filter and the specified port. You must do this before you can delete the filter itself, using the **delete** command (see the chapter entitled "The Define and Delete Commands").

set port c.p ipxflt-def block

Use the **set port** *c.p* **ipxflt-def block** command to set to **block** the default IPX filter action for the specified port.

Note This attribute is not affected when the card is reset.

---

set port c.p ipxflt-def forward

Use the **set port** *c.p* **ipxflt-def forward** command to set to **forward** the default IPX filter action for the specified port.

Note This attribute is not affected when the card is reset.

---

set port c.p np-deliver block

Use the **set port** *c.p* **np-deliver block** command to prevent received frames from being delivered to any NP in the network.

Note This command requires protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.")

---

set port c.p np-deliver forward

Use the **set port** *c.p* **np-deliver forward** command to enable delivery of received frames to NPs in the network.

Note This command requires protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.")

Virtual LAN Internetworking

Use the **set port** *c.p* **wgrp** commands to maintain the workgroup list for each port. There is one workgroup list per port. The port is either *included in* or *excluded from* all the listed workgroups (see the **include** and **exclude** arguments, below).

- The default is an include list that contains just Workgroup 1 (the default workgroup).
- An empty include list is treated the same as this default case.
- An empty exclude list permits this port to communicate with ports in every workgroup. This differs from the default if any workgroups have been defined in the network in addition to workgroup 1.

Note Run-time changes to the workgroup list are not affected when the card is reset.

Caution Workgroups are network-wide constructs. Define them consistently on all nodes of the network. If you fail to do so, problems involving the workgroups may be difficult to debug.

set port *c.p* wgrp add

Use the **set port** *c.p* **wgrp add** *ID* [**,** *ID* ...] command to add one or more workgroup IDs to the list for the specified port, separated by commas. There can be up to seven workgroup IDs per port in an include list (up to six in an exclude list). Use the **show port** *c.p* **wgrp** command to display the current list (see the chapter entitled "The Show Command").

Note Adding a workgroup to the default list with the **set port** *c.p* **wgrp add** *ID* command does not delete the default workgroup automatically. The corresponding action with the configuration tool does delete the default workgroup automatically.

---

set port *c.p* wgrp include

Use the **set port** *c.p* **wgrp include** command to allow this port to intercommunicate with ports in the workgroups that are in the list (no communication with workgroups not in the list). An include list may name up to seven workgroups per port.

In practically all cases, the workgroup list for a port should be defined in the **include** sense. The default is an include list that contains just Workgroup 1 (the default workgroup). An empty include list is treated the same as this default case.

set port *c.p* wgrp exclude

Use the **set port** *c.p* **wgrp exclude** command to allow this port to intercommunicate with ports in all workgroups in the range 1 – 65,535 *except* those listed. An exclude list can name up to six workgroups per port.

The most important use of an exclude list is to enable a port to communicate with all workgroups, where workgroups other than the default (workgroup 1) are defined in the network. To use the exclude list in this way, configure an empty list (delete all workgroup IDs, including Workgroup 1) and change the sense to **exclude**.

Note The **set** command does not accept the mnemonic workgroup names (aliases) maintained by the configuration tool. If you use the **set port** *c.p* **wgrp** commands, you should maintain a list showing how the group IDs correspond to mnemonic workgroup names.

---

set port *c.p* wgrp del

Use the **set port** *c.p* **wgrp del** {*ID* | **all**} command to delete the specified workgroup, or all workgroups, from the list for the specified port. *ID* is a workgroup ID number in the range 1 – 65,535. An empty include list is equivalent to the default group (Workgroup 1). An empty exclude list permits communication with every workgroup.

SNMP Attributes

Use the **set snmp** commands to set the value of the read-write community name and of the target host name for the specified port.

Note The **set snmp** commands affect *only* the node on which the CLI is running when you execute them, regardless of any target that has been set with the command **set snmp hostname** *name*.

---

set snmp community

Use the **set snmp community** *name* command to set the read-write community name to *name*. The string *name* must be assigned the value write in the mma.communities file. Three default communities are defined on each LS2020 switch: public (read-only privileges), trap (read-write privileges), and write (read-write privileges). See the *LightStream 2020 Installation Guide* for descriptions of SNMP communities and the mma.communities file.

set snmp hostname

Use the **set snmp hostname** {*name* | *IPaddress*} command to set the target host to *name* or *IPaddress*. When the target is the node on which the CLI is running, *name* is the string **localhost**.

The command in the following example sets the target system to be the node whose alias is **boston5**:

```
cli> set snmp hostname boston5
```

Spanning-Tree Bridge Attributes

Use the **set stb** commands to define the spanning-tree bridge parameters for the node. See also the **set port** *c.p* **stb** command, which is used to set per-port spanning-tree bridge parameters.

Note These attributes are not affected when the card is reset.

---

set stb maxage

Use the **set stb maxage** *age* command to set the maximum age that should be used to time out STP information. This value takes effect only when this node becomes the root bridge. The value is in hundredths of a second, truncated to seconds. For example, 400, 401, and 499 each signify 4 seconds. The range of *age* is 600 – 4000, and the default is 2000. The limits on this value are as follows (in seconds):

2 * (**hellotimer** +1) ≤ *maxage* ≤ **2** * (**forwdelay** -1)

set stb forwdelay

Use the **set stb forwdelay** *time* command to set the interval before changing to another state. This value takes effect only when this node becomes the root bridge. The value is in hundredths of a second, truncated to seconds. For example, 400, 401, and 499 each signify 4 seconds. The range of *time* is 400 – 3000, and the default is 1500 (15 seconds). The limits on this value are as follows (in seconds):

2 * (**hellotimer** +1) ≤ *maxage* ≤ **2** * (**forwdelay** -1)

set stb hellotimer

Use the **set stb hellotimer** *time* command to set the interval between bridge protocol data units (BPDUs) sent out by this port. This value takes effect only when this node becomes the root bridge. The value is in hundredths of a second, truncated to seconds. For example, 400, 401, and 499 each signify 4 seconds. The range of *time* is 100 – 400, and the default is 200 (2 seconds). The limits on this value are as follows (in seconds):

2 * (**hellotimer** +1) ≤ *maxage* ≤ **2** * (**forwdelay** -1)

set stb priority

Use the **set stb priority** *priority* command to set the priority for using this node in a path using the spanning tree protocol, relative to the priority for using other nodes. The range of *priority* is 0 – 65535, and the default is 32768.

set stb static

Use the **set stb static** *MACaddr* **rcv {***c.p* **| any} xmit** *c.p* [*c.p* ...] command to enter a static entry into the bridge forwarding database. Use the **set stb static** *MACaddr* **rcv {***c.p* **| any} status** {**invalid** | **deleteonreset** | **permanent**} command to delete a static entry from the bridge forwarding database or to prevent it from being deleted automatically when the bridge is reset. For each entry

- You must specify the MAC address *MACaddr* to be used for forwarding, in the standard *xx***:***xx***:***xx***:***xx***:***xx***:***xx* format, a sequence of six colon-separated hex octets.
- You must use the **rcv** argument to assign this MAC to a receive port, either port *c.p* or the keyword **any**, a wildcard that matches any port.

- Use the **xmit** argument to create an entry, specifying the transmit port or ports *c.p* [*c.p* ...] to which received frames are to be forwarded. You cannot use the **status** argument in the same command. (The transmit ports can only be ports on the same node. To create a route to a port on another node, use the **define mcast** command.)
- Use the **status** argument to modify a previously specified entry. You cannot use the **xmit** argument in the same command. The possible **status** values are as follows:

invalid	Delete the entry now.
deleteonreset	Delete the entry when the bridge is reset.
permanent	Do not delete the entry when the bridge is reset.

Test and Control System Attributes

Use the **set tcs** command family to access the test and control system (TCS) command interface from the CLI. You can access only a few basic functions of the TCS from the CLI. See the *LightStream 2020 Hardware Reference & Troubleshooting Manual* for additional information about the TCS commands.

Note The **set tcs** commands require CLI protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.")

These commands affect *only* the node on which the CLI is running when you execute them, regardless of any target that has been set with the command **set snmp hostname** *name*.

The **set tcs** commands do not work on a network management workstation. When you start the CLI on an NMS, you see the message "Warning: No TCS available."

---

set tcs card# midplane

Use the **set tcs** `card#` **midplane** *node_address* command to set the midplane address for the specified card to the node address *address*.

Note All cards in a chassis must have the same midplane address. In particular, Switch A and Switch B in a redundant system must have the same midplane address.

---

set tcs card# power

Use the **set tcs** `card#` **power** {**on** | **off**} command to turn power on or off for the specified card. (Not supported on Release 2 switch cards.)

set tcs card# reset

Use the **set tcs**`card#` **reset** command to reset the specified card.

Traps

Use the **set trap** command family to control the display of specified traps. See the *LightStream 2020 Traps Reference Manual* for information about LS020 traps.

The following default status settings should be in effect:

- Oper traps are displayed on the console and on network management systems.
- Info and Oper traps are logged in the mma.traplog file.
- Trace and debug traps are not displayed.

Although we do not recommend it, these default settings can be changed through use of one or more of the following commands:

- **set chassis consoletraplevel**
- **set chassis traplevel**
- **set cli traplevel**
- **set pid** *PID#* **traplevel**

The preceding commands change the ranges of traps affected by the **on**/**off** and **disable**/**enable** arguments. To avoid confusion, we recommend that you not use these commands to change the default effect of the **set trap** commands.

Note The **set trap** commands require CLI protected mode. (See the **protected** command in the chapter entitled "CLI Control Commands.") These commands affect *only* the node on which the CLI is running when you execute them, regardless of any target that has been set with the command **set snmp hostname** *name*.

---

trapspec

In the following command descriptions, *trapspec* stands for a trap name or a trap number. See the *LightStream 2020 Traps Reference Manual* for trap names and numbers. You can also specify a range of trap numbers or a name for a group of traps previously defined in the cli.groups file, but doing so is not recommended, as you could easily disrupt the system by flooding it with traps.

The *trapspec* arguments are used to specify traps to be set. The following list shows ways that the trap or traps can be specified:

trapname	The trap identified by its trap name (see the *LS2020 Traps Reference Manual*)
trapgroup	The traps listed in the definition of the name trapgroup given in the cli.groups file
trap#	The trap identified by *trap#*
trap#-trap#	The set of traps identified by the range of trap numbers *trap# – trap#*

set trap {disable | enable}

Use the **set trap** {**disable** | **enable**} *trapspec* command to disable specific traps that are being displayed on the console (normally, oper traps), or enable them again after they have been disabled. (This does not apply to traps that are being displayed only because they were turned on with the **set trap on** command.) The *trapspec* argument is a trap name or a trap number; see the *LightStream 2020 Traps Reference Manual* for trap names and numbers.

set trap [global] {on | off}

Use the **set trap** [**global**] {**on** | **off**} *trapspec* command to turn on traps that are currently being ignored (normally, trace traps and debug traps), or to turn them back off again after they have been turned on. The *trapspec* argument is a trap name or a trap number as described under the preceding heading “trapspec”.

The **set trap on** *trapspec* command does not affect traps that are being ignored because they were disabled with the **set trap disable** *trapspec* command.

The default is to apply this operation to all processes system-wide, but you may explicitly specify this behavior with the optional **global** argument. (You use the **set trap pid** {*PIDname* | *PID#*} {**on** | **off**} *trapspec* command to control traps on a per-process basis.)

set trap pid

The **set trap pid** commands are for debugging and support use only. They are of no use unless you know which traps are issued by a given process, or which processes issue a given set of traps. In normal operation, you never use the **pid** argument of the **set trap** command.

Use the **set trap pid** {*PIDname* | *PID#*} {**on** | **off**}*trapspec* command to make the **on** or **off** switch apply to the process with alias *PIDname* or number *PID#* (instead of globally to all processes). The *trapspec* argument is a trap name or a trap number as described under the preceding heading “trapspec.”

Trace and debug traps include the PID and alias of the process in which the trap occurred. You can also display a list of process aliases with the **walksnmp lwmaTrapCliAlias** command.

Example

The following command sets the SNMP read/write community attribute to the name “write,” so that you can use the **set trap** command:

```
cli> set snmp community write
```

The community named “write” is defined in the mma.communities file as having write permission.

The following command disables the oper trap LCC_1, which reports a high error rate:

```
cli> set trap disable lcc_16
```

After correcting the problem, re-enable the trap with the following command:

```
cli> set trap enable lcc_16
```