StorageTek SL8500 Modular Library System

Simple Network Management Protocol

Part Number: 316194703
Novenber 2010
Revision: C

Submit comments about this document by clicking the Feedback [+] link at: http://docs.sun.com

StorageTek SL8500 Modular Library System - Simple Network Management Protocol (SNMP)

316194703 Revision: C

Summary of Changes

Date	Revision	Description
April 2008	A	Initial release
September 2009	B	Refer to this version for a list of updates. Added object identifiers.
November 2010	C	Updates to this revision include: ■ Oracle branding. ■ Engineering updates. ■ New Command Line Interface layout.

Note – Change bars are *not* included in this revision.

Contents

Preface

This reference guide provides information about the Simple Network Management Protocol (SNMP) and the implementation on **Oracle's StorageTek SL8500 Modular Library System.**

Documentation, Support, and Training

Function	URL	Description
Web Site	http://www.oracle.com/index.html	General information and links.
Documentation ■ Customer: ■ Employee: ■ Partner:	http://docs.sun.com/ http://docs.sfbay.sun.com/ https://spe.sun.com/spx/control/Login	Search for technical documentation. Download PDF/HTML documents. Order printed documents.
Downloads ■ Customer: ■ Employee:	http://www.sun.com/download/index.jsp http://dlrequest.sfbay.sun.com:88/usr/login	Download firmware and graphical user interfaces, patches, and features.
Support	http://www.oracle.com/us/support/index.htm	Obtain and escalate support.
Training	http://www.oracle.com/education/training_formats.html	Access training resources. Learn about Oracle courses.
Online Account	https://reg.sun.com/register	Register for an Online Account.

Oracle Welcomes Your Comments

Oracle is interested in improving its documentation and welcomes your comments and suggestions. Submit your comments by clicking the Feedback [+] link at:

http://docs.sun.com

Please include the title and part number of your document with your feedback:

SL8500 Modular Library System: Simple Network Management Protocol,
Part Number: 316194703, Revision C

CHAPTER 1

Introduction

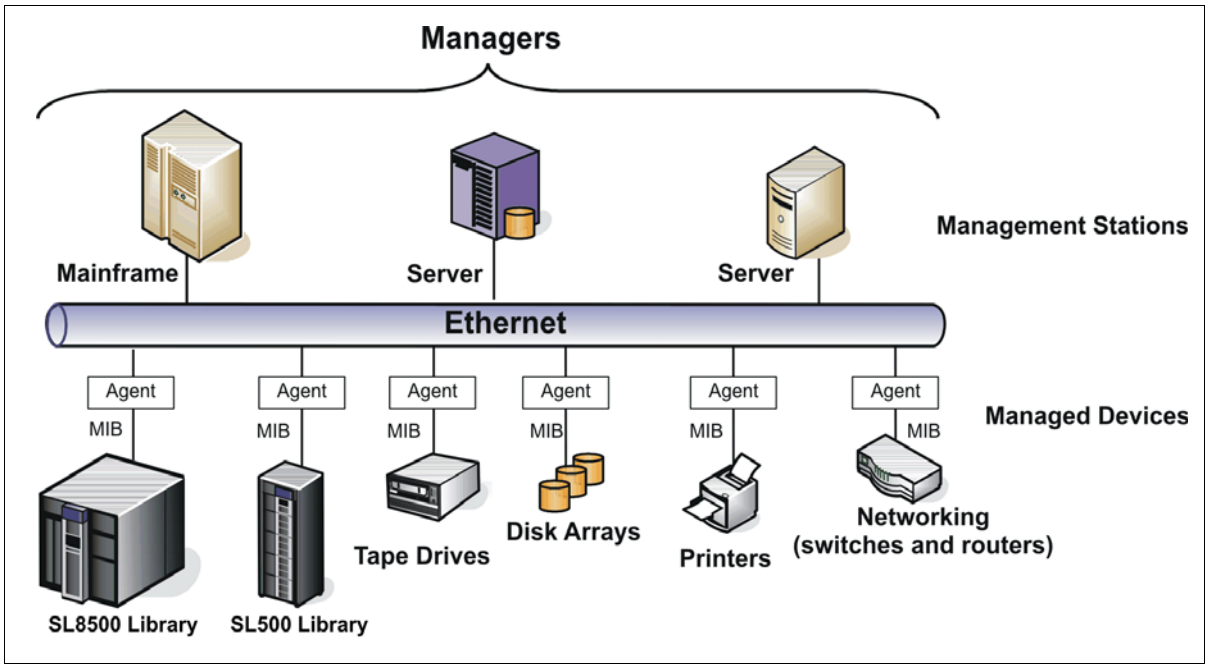
Short for Simple Network Management Protocol, SNMP is a network protocol designed to monitor and manage network-attached devices.

This chapter describes the architecture, versions, protocols, and commands for the Simple Network Management Protocol.

Architecture

The framework for SNMP consists of managed devices, agents, an information base, managers and management station software.

FIGURE 1-1 SNMP Architecture



- A *managed device*—such as the SL8500 library—is a network node that contains an SNMP *agent*, which is an SNMP-capable software module.
- The *manager* or *management station* provides the managing, monitoring, and receiving roles of an SNMP-capable network.

- The *management information base*—called a MIB—is an ASCII text file, organized hierarchically, that describes the elements of a managed device. When a manager requests information, or a managed device generates a trap, the MIB translates the numerical strings into readable text that identifies each data object within the message.

SNMP Terms

SNMP uses a manager/agent structure, a database, and a small set of commands to exchange information. SNMP terms include:

- Advanced Encryption Standard (AES)—An NIST-standard cryptographic cipher that uses a block length of 128 bits and key lengths of 128, 192, or 256 bits.
- Agent—A module that resides in a managed device. The agent is responsible for responding to requests from the manager and for sending traps to a recipient that inform the systems administrator of potential problems.
- Community String—Applications use community strings for access control. The manager includes the community string in its SNMP messages to an agent. This can be a maximum of 31 alpha-numeric characters.
- Data Encryption Standard (DES)—An NIST-standard cryptographic cipher that uses a 56-bit key.
- EngineID—An administratively unique identifier of an SNMP v3 engine used for identification, not for addressing.
- Managed device—A device that hosts the services of an SNMP agent that provides monitored information and controlled operations using SNMP. Sun StorageTek libraries are managed devices.
- Management Information Base (MIB)—A collection of information stored in a database that contains configuration and statistical information for a managed device. For Sun StorageTek libraries, a copy of the MIB is loaded with microcode and stored on the library control card.
- Manager—Provides the communication link between the systems administrator and the managed devices on the network. A management station or server allows the systems administrator to get information about the device through the MIB and to receive traps from an agent.
- Message Digest 5 (MD5)— A popular one-hash function that creates a message digest for digital signatures. MD5 is faster than SHA, but is less secure.
- National Institute of Standards and Technology (NIST)—An agency of the Commerce Department's Technology Administration.
- Recipient—A location on a manager where the SNMP agent sends traps. This location is defined by the combination of either the IP address or DNS name and the port number. The default recipient port number is 162.
- Secure Hash Algorithm—A popular one-hash algorithm that creates a digital signature; it is more secure than MD5.
- Trap/Notification—A message that reports a problem, error, or significant event that occurred within the device.
- Trap Level String—The list of trap levels. The maximum length is 31 alpha-numeric characters.

Versions

Within the group of computer network engineers, *Request for Comments* (RFCs) are a series of documents that members use to define research, innovations, and methodologies applicable to the Internet, such as SNMP.

The Internet Engineering Task Force (IETF) adopts and applies this information creating Internet standards.

There are currently three versions of SNMP; TABLE 1-1 lists these versions and the RFCs that define them.

TABLE 1-1 Versions of SNMP

Version	Comments	Defining RFCs
SNMPv1 is the initial release.		
	The first version of SNMP is described in RFC 1157 This version is a widely used and accepted standard Version 1 has been criticized for its poor security	RFC 1065: Structure RFC 1066: MIB RFC 1067: Protocol
SNMPv2 is a revised protocol, not just a new MIB (RFCs 1592 and 1907).		
– SNMPv2p	**P**arty-based (now obsolete) Includes improvements in performance, security, and communications	RFC 1441 through RFC 1452
– SNMPv2c	**C**ommunity-based Includes SNMPv2p *without* the controversial security Widely considered the "*de facto*" SNMPv2 standard	RFC 1901 through RFC 1908
– SNMPv2u	**U**ser-based Includes USM (user-based security model) Offers greater security, but without the complexity	RFC 1909 and RFC 1910
SNMPv3 is the latest version.		
	Described in RFC 1906, RFC 2572, 2573, and 2574 IETF recognizes this as the current standard version	RFC 3411 through RFC 3418

In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3. Refer to RFC 3584, the *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework,* for more information.

For more listings and information about SNMP and Requests for Comments, go to the: Internet Engineering Task Force (IETF) Web site at: http://www.ietf.org/

For more information about SNMP, go to: http://www.snmp.com/

Protocol

The SNMP specification is based on the User Datagram Protocol (UDP)[1].

Similar to TCP[2], UDP runs on top of IP[3] networks (called UDP/IP) using familiar client-server models, such as the OSI[4] model, for data transmissions.

Note – OSI standards and the IP protocol suite do not conflict with each other because the two protocol stacks were developed concurrently. However, some differences do exist; *for example,* the OSI model contains seven layers where the IP suite only has four layers.

That said, any other differences between the two are only minor.

TABLE 1-2 shows a comparison between the IP Suite and the OSI Model
.

TABLE 1-2 Protocol Comparisons

IP Suite	OSI Model
4. Application layer Applications and end-user processes, such as **SNMP**, DNS, FTP, HTTP, SMTP, and others.	7. Application layer Applications and end-user processes, such as **SNMP**, DNS, FTP, HTTP, SMTP, and others.
	6. Presentation layer Transforms data into a format that the application layer can accept.
	5. Session layer; Connection coordination.
3. Transport layer: TCP and **UDP** Transfers data between system components.	4. Transport layer: TCP and **UDP** Transfers data between system components
2. Internet layer: **IP** (IPv4)	3. Network layer: **IP**
1. Link layers: Makes use of existing standards rather than defining its own, such as: 10/100 BaseT and IEEE 802.x There are two different layers: Data link layer; Physical link layer	2. Data Link layer: Physical addressing, media access control (MAC)
	1. Physical layer: Physical aspects for sending and receiving data

SNMP only uses UDP ports for the transfer of information:

- Port 161 for the *agent*
- Port 162 for the *manager*

1. UDP = User Datagram Protocol, a *connection-less* communications protocol that offers limited service for exchanging messages between networked devices.
2. TCP = Transmission Control Protocol, a *connection-based* protocol that offers reliable, ordered communications between networked devices.
3. IP = Internet Protocol, the connection method over which data is sent from one device to another on a network. UDP like TCP uses the Internet Protocol to actually get a data unit (datagram or packet) from one computer to another.
4. OSI = Open System Interconnection, a model that defines the concept and describes how information flows from one application through the network into another.

Each managed host runs a process called an agent. The agent is a server process that maintains the MIB database for the host.

Hosts that are involved in network management run a process called a manager. A manager is a client application that generates requests for MIB information and processes responses.

The protocol for communications between manager and agent is:

- The manager can send requests from any available port to the agent at port 161. The agent then responds to that source port, to the requesting manager.
- The agent generates traps or notifications and sends them from any available port to the manager at port 162.

Management Information Base

The management information base (MIB) is a collection of *objects* in a database that SNMP uses to manage devices in a network.

This database is hierarchical in structure—tree-like—with entries called *object identifiers* (OIDs).

This structure permits management across all layers of the OSI model, extending into applications, databases, and area-specific information.

As with SNMP, the MIB has defining standards in the Request for Comment (RFC) format shown in TABLE 1-3.

TABLE 1-3 MIB Request for Comment Standards

RFCs	Description
RFC 1155	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1156	Management Information Base for Network Management of TCP/IP-based Internets
RFC 1157	A Simple Network Management Protocol (SNMP)
RFC 1213	Management Information Base for Network Management of TCP/IP-based Internets: MIB-II
RFC 1441	Introduction to Version 2 of the Internet-standard Network Management Framework
RFC 3418	Management Information Base for the Simple Network Management Protocol

See Chapter 2, Management Information Base for more information.

Agents

The SNMP agent:

- Responds to requests from an SNMP manager
- Sends SNMP traps to managers

The objects that an SNMP agent can manipulate are defined in the MIB.

Management Stations

Management stations are systems or servers that have an SNMP application installed. Examples of these applications include:

- Sun Microsystems SunNet Manager
- HP OpenView
- IBM NetView
- CA Unicenter Network and System Management
- Plus several others

Commands

SNMP offers a limited number of commands (protocol data units or PDUs) that follow a simple request and response exchange to communicate between the manager and the agent.

The manager issues requests such as:

- **Get**: A request for information of a specific variable.
- **GetNext**: A request for information of the next specific variable.
- **Set**: A request to change the value of a specific variable.

The agent responds with:

- **Get-Response**: A response to the manager's Get commands.

Another communication element between the agent and the manager is the **trap**—also called a notification. These are asynchronous messages to a manager or other recipient about an error or event.

What is a Trap or Notification?

A trap or notification is a message that reports a problem, error, or significant event that occurred within the device. These messages are sent by the agent to a manager.

CHAPTER 2

Management Information Base

This chapter describes the management information base (MIB) for the StorageTek SL8500 modular library to support the SNMP feature.

Important: SNMP configuration requirements:

- SL8500 library firmware must be version **FRS_3.12** or higher.
- StorageTek Library Console version **FRS_2.95** or higher.
- By default, the SNMP agent is disabled and must be enabled.

Initially, configuring SNMP requires the use of the command line interface (CLI). A service representative working together with the customer's system administrators and network managers can properly configure SNMP for their account (as described in Chapter 3, Configuration).

Note – StorageTek Libraries support the following versions of SNMP:

- **SNMPv2c:** Read-only support, primarily for machine status queries. Any information transmitted *will not* be secure.
- **SNMPv3:** Both read *and* write support, transmitted information *is* secure.

Access Control

Community strings are capable of providing a form of access control in SNMP. Because of this, the StorageTek embedded agent will not allow community strings to make changes to the library's configuration.

The MIB can be retrieved with either SNMPv2c or SNMPv3, however, because SNMPv3 provides encryption capabilities and a stronger user identification, library properties can be changed only with the SNMPv3 `set` command.

Using an administrative password also provides access control and authorization for `set command` operations.

Traps, however, can be sent to recipients using either SNMPv2c and SNMPv3 by adding entries to the Trap Recipient List.

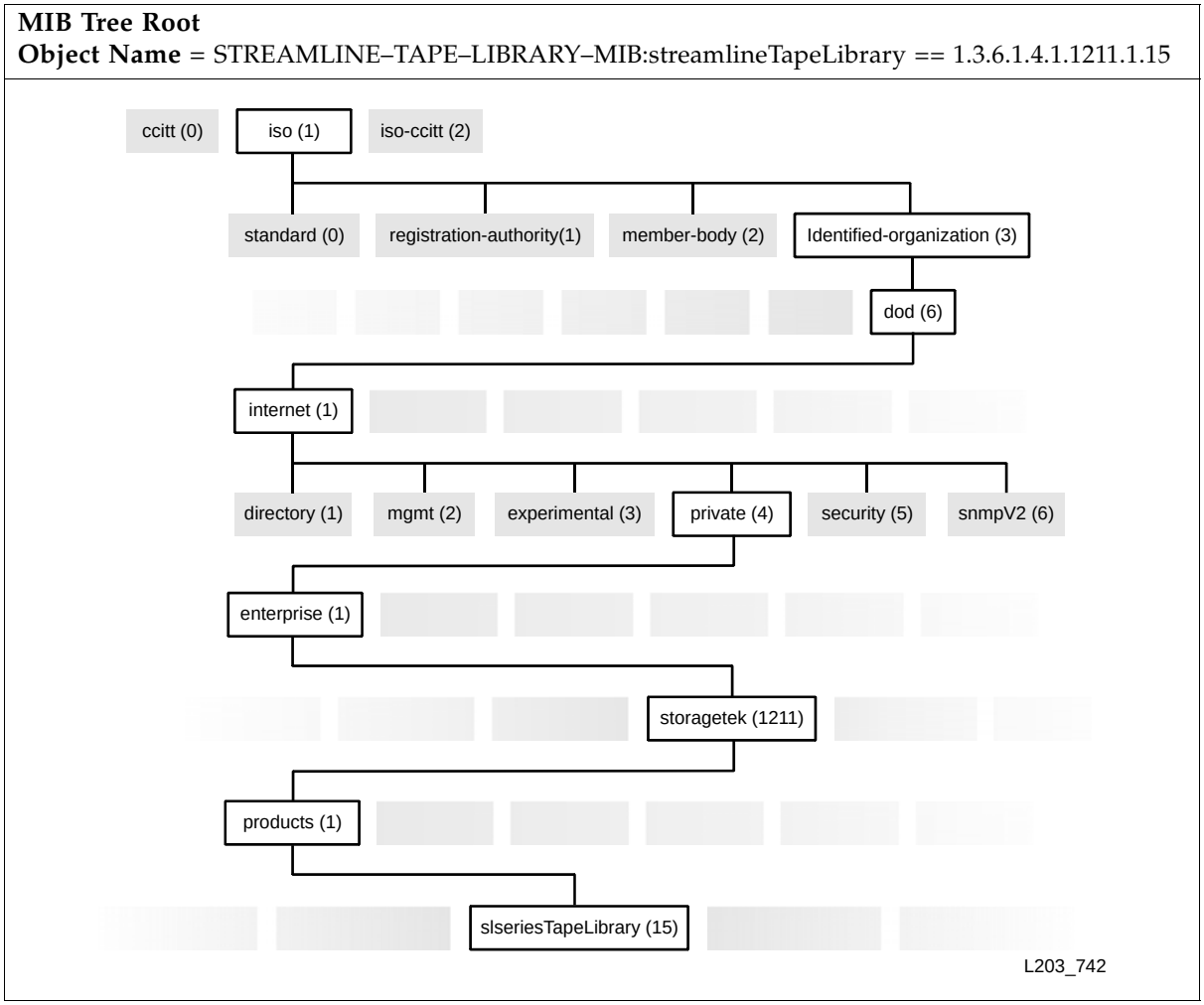
Note – Customers can download the MIB through the StorageTek Library Console, but it cannot be directly viewed from the console itself. However, because the MIB is a plain ASCII text file it can be viewed from any readily available text editor.

Management Information Base

The management information base (MIB) is a viewable document that contains descriptions about the characteristics for a managed device. These characteristics are the functional elements for that device which can be monitored using SNMP software.

FIGURE 2-1 shows the MIB structure for the StorageTek modular libraries. STREAMLINE–TAPE–LIBRARY–MIB

FIGURE 2-1 StreamLine MIB Hierarchy



The following pages describe the MIB variables (or objects), which are a continuation of the MIB hierarchy—tree—and are queried by Get or GetNext commands.

Basic MIB Variables

Basic variables provide minimum functionality for all StorageTek libraries.

Library Type

slLibrary provides information about the library, such as type, serial number, and overall operating condition.

TABLE 2-1 Library Type

Content	Description
slLibStkBaseModel	StorageTek Library model number See vendor specific model data
slLibSerialNumber	Library frame serial number
slLibWWNNumber	Library World Wide Name (WWN). A 64-digit hexadecimal number
slLibraryTopLevelCondition	Library overall condition (for example: normal, degraded, or not-operational)

Library Location

slLibLocation provides information about the location of the library.

TABLE 2-2 Library Location

Content	Description
slLibLocatContact	Primary contact for administration
slLibLocatStreet	Location/site – Street address
slLibLocatState	Location/site – State/province
slLibLocatZip	Location/site – ZIP code or other data
slLibLocatCountry	Location/site – Country
slLibLocatDescr	Location/site – Description or other data
slLibLocatCity	Location/site – City

Library Date

slLibDate provides information about the date and time-of-day.

TABLE 2-3 Library Date and Time of Day

Content	Description
slLibDateString	Date and time in the following format: `YYYY:MM:DD HH:MM:SS.xxxx`

Additional MIB Variables

Similar to the basic variables, additional variables provide a complete set of variables for full functionality of StorageTek libraries and support of SNMP, these include:

- Cartridge Access Ports
- Power Supply
- Robot
- Tape Drives
- Versions

Note – This information is from the standard MIB for StorageTek Libraries; however, the SL8500 library currently does not support all of the variables listed in the MIB, only the variables mentioned above are supported.

The following pages provide the details of the supported variables.

Cartridge Access Ports

slCAP provides information about the cartridge access ports (CAPs).

TABLE 2-4 Cartridge Access Port Data

Content	Description
slCapCount	Number of the CAPs in the CAP table
slCapTable	Table of cartridge access ports (CAPs)
slCapEntry	Cartridge access port
slCapIndex	Integer index into the CAP table
slCapAddress	CAP device address
slCapAccessibility	Accessibility of a CAP (for example: open, allow/prevent)
slCapAccessStateEnum	Access state of the CAP presented as an enumeration
slCapState	Physical state of the CAP
slCapStatusEnum	Operational status of the CAP presented as an enumeration
slCapName	CAP name
slCapRotations	CAP rotation count
slCapRotationRetries	Number of rotation retries performed by the CAP
slCapRotationFails	Number of rotation failures performed by the CAP
slCapIPLs	Number of IPL's performed by the CAP

Power Supply

The **slPowerSupply** variable provides information about the power supplies in the library.

TABLE 2-5 Power Supply Count and Data

Content	Description
slPowerSupplyCount	Number of power supplies installed in the library
slPowerSupplyTable	Table of the library's power supplies
slPowerSupplyEntry	A power supply
slPowerSupplyIndex	Integer index into the power supply table
slPowerSupplyName	Name of the power supply
slPowerSupplyInstalled	Indicates if the supply is: Not installed (1), installed (2)
slPowerSupplyOperational	Indicates if the supply is OK (2), Meaningless if not-installed: Failed (1), Normal (2)

Robot

slRobot provides information about the robotics in the library, such as: quantity, firmware versions, serial numbers, and number of robotic retries.

TABLE 2-6 Robot Data

Content	Description
slRobotCount	Number of robot mechanisms
slRobotTable	A table of robots (HandBots)
slRobotEntry	A robot entry
slRobotIndex	A robot index
slRobotElementID	Element ID / Address or address of the robot
slRobotPosition	Physical position of the robot in counts
slRobotHandCartStatus	Robot hand state (cartridge =1, no cartridge = 0)
slRobotSerialNum	Robot card serial number
slRobotState	Robot state (such as: empty, loaded, or moving)
slRobotFaultLED	Robot card serial number
slRobotStatusEnum	Robot operational status in enumerated form
slRobotCodeVer	Robot code version
slRobotVersion	Robot version
slRobotFirmwareVer	Robot firmware version
slRobotGetRetries	Number of mount retries performed by the robot
slRobotPutRetries	Number of dismount retries performed by the robot

Tape Drives

slDrive provides information about the tape drives.

TABLE 2-7 Tape Drive Data

Content	Description
slDriveCount	Count of the drives in the drive table
slDriveTable	Table of drives
slDriveEntry	Tape drive entry
slDriveIndex	Integer index into the drive table
slDriveElementID	Element ID/Address of the drive
slDriveType	Drive type (for example: STK10000, LTO5, DLT-S4)
slDriveVendor	Drive vendor (for example: STK, HP, and IBM)
slDriveSerialNum	Drive electronic serial number
slDriveInterfaceType	Drive physical data transport type
slDriveID	Drive SCSI ID or Fibre Port assignment
slDriveState	Drive state (such as: empty, loaded, needs cleaning)
slDriveLED	Drive Tray LED sate (0=off and 1=on)
slDriveStatusEnum	Drive operational status in enumerated form
slDriveCodeVer	Drive code version
slDriveVersion	Drive version
slDriveFirmwareVer	Drive firmware version
slDriveGetRetries	Number of mount retries performed to the drive
slDrivePutRetries	Number of dismount retries performed to the drive
slDriveCommandClean	Signal to clean or cancel cleaning of the drive
slDriveCellStatusEnum	Drive cell presented as an enumeration
slDriveCellStatusText	Drive cell status
slDriveCellContentLabel	Label of the cartridge in the drive (zero length string if empty, '??????' if unreadable)
slDriveCellContentType	Type of cartridge in the drive (zero length string if empty)
slDriveIdleSeconds	Number of seconds that the drive has been idle (un-mounted)
slDriveNumMounts	Number of mounts to the drive
slDriveFibreNodeName	Drive Fibre node name

TABLE 2-7 Tape Drive Data

Content	Description
slDriveFibrePortCount	Number of active ports in the drive
slDriveFibrePortAWWN	Port A – World Wide Name (WWN)
slDriveFibrePortAAddressingMode	Port A – Addressing mode
slDriveFibrePortAPortEnabled	Port A – Port enabled
slDriveFibrePortALoopId	Port A – Loop ID
slDriveFibrePortAPortSpeed	Port A – Port speed
slDriveFibrePortBWWN	Port B – World Wide Name
slDriveFibrePortBAddressingMode	Port B – Addressing mode
slDriveFibrePortBPortEnabled	Port B – Port enabled
slDriveFibrePortBLoopId	Port B – Loop ID
slDriveFibrePortBPortSpeed	Port B – Port speed
slDriveWWNEnabled	Drive World Wide Name option. This option can only be set using the command line interface (CLI). Contact a Service Representative.

Versions

slLibraryVersion provides information about the firmware, code, and versions for the library.

TABLE 2-8 Library Firmware Version

Content	Description
slLibVersionFirmRev	Library embedded firmware version per engineering change (EC) field releases
slLibVersionFirmDate	Library embedded firmware build date
slLibVersionBootRev	Library boot software/OS version
slLibVersionHardware	Library controller hardware version

CHAPTER 3

Management Information Base

Important:
Because SNMP can only be enabled through the command line interface (CLI), a service representative must work with the customer's system administrator to obtain the information they require, make the necessary entries, and then enable SNMP.

This chapter lists the default settings, describes how to configure trap notifications, and references the command line interface commands.

SNMP Default Settings

TABLE 3-1 lists the default settings for a StorageTek Library.

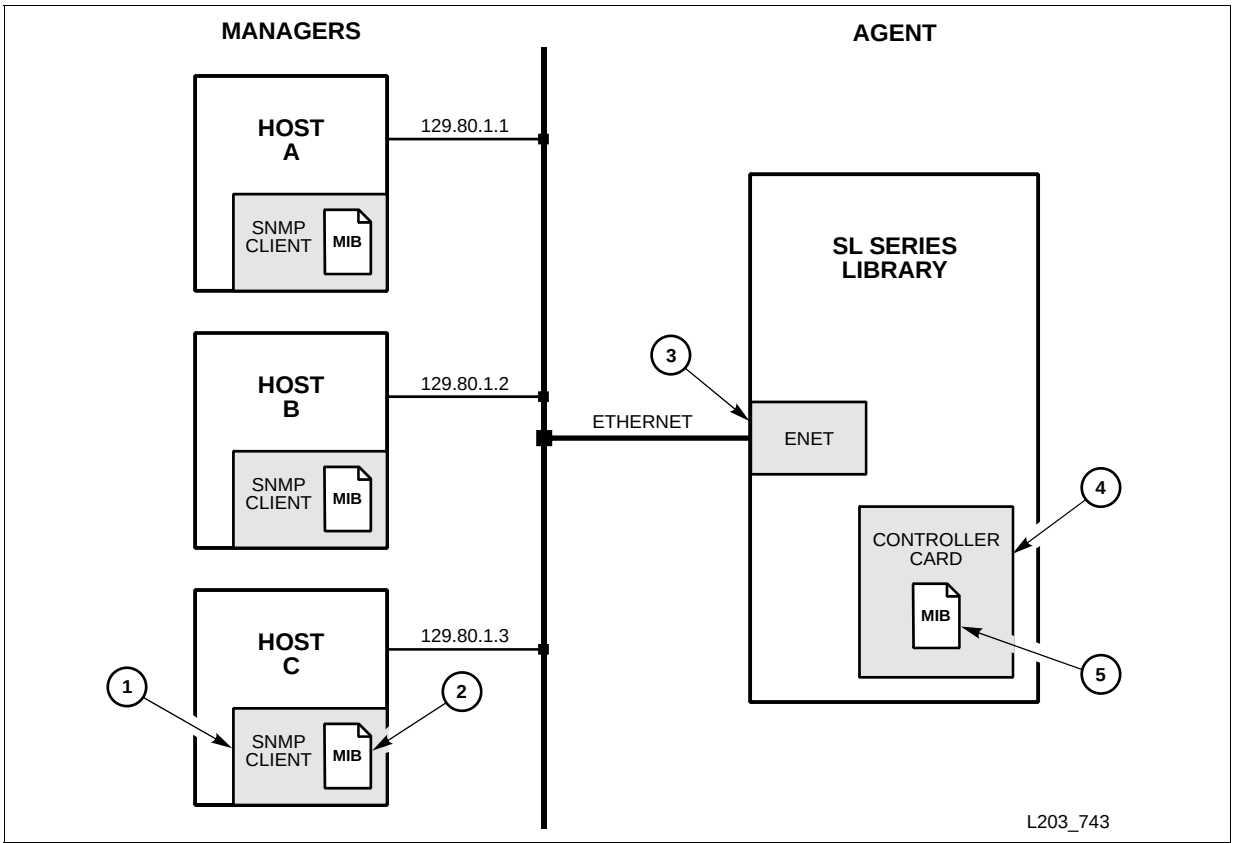
TABLE 3-1 SNMP Default Settings

Setting	Default	Description
Port ID	Disabled	Agent trap requests are sent and received over the HBC card port: ■ 2B = standard, public port ■ 2A = optional, redundant port
Socket number [1]	161	Agent requests are sent and received on the enabled port.
Socket number [1]	162	Traps are sent to this socket on the host port.
SNMPv2c users string[2]	Public	Community String Public Agent Community. Use this field (setting) to *read-only* MIB data.
SNMPv3 users string[2]	Empty	Community String Public Agent Community. Use this field (setting) to both *read* and *write* MIB data.
Trap Recipients	Empty	This list supports up to 20 recipients with no duplicate entries. Users must add themselves to the recipients list for traps to be sent to them. See page 22 for information.
SNMP (agent)	Disabled	Enabled or disabled through CLI command *only.*
1. Socket numbers, or ports, must be enabled to pass through a firewall. 2. User Strings. There can be a maximum of 20 SNMP users total. This field can be changed or deleted.		

Retrieve the Management Information Base

Have a system administrator retrieve the MIB from the library controller card.

FIGURE 3-1 MIB Location



1. Software application
2. Client copy of the MIB
3. Ethernet connection
4. Library SNMP agent (controller)
5. Library MIB

Using the StorageTek Library Console (SLC) and the Transfer File function.

1. Log on to the library using the Library Console.
2. Select Tools ➪ Diagnostics.
3. Click the TransferFile tab.
4. Click the Transfer button next to STREAMLINE_TAPE_LIBRARY_MIB_TEXT.text.
5. In the Save dialog, select a Save in folder, and enter a file name.
6. Click Save Network Auto-Discovery and Mapping.

Note – For auto-discovery to include the library, the SNMP agent provides the "Basic MIB Variables" on page 9.

SNMP Configuration Sequence

To configure SNMP:

1. Have an administrator Retrieve the Management Information Base from the library.
2. Obtain the trap/notification destinations from the administrator:

   ❏ IP address of the hosts receiving the traps

   ❏ `EngineId` of the hosts receiving the traps if using SNMPv3

   ❏ Authentication protocol/authPassPhrase
   (MD5 or SHA /authPassPhrase string)
   for users and hosts receiving traps if using SNMPv3.

   ❏ Authentication privacy protocol/Privacy PassPhrase
   (DES or AES / PrivPassPhrase string)
   for users and hosts receiving the traps if using SNMPv3

   ❏ User names and hosts receiving the traps if using SNMPv3.

3. Have a service representative login and use the "Command Line Interface" to:

   a. Add users:
   SL8500> `addUser`

   b. Configure trap recipients:
   SL8500> `addTrapRecipient`

   c. Double check that the information was entered correctly, using:
   SL8500> `listTrapRecipients` and
   SL8500> `listUsers`

   d. Enable the agent:
   SL8500> `enable port<portID>`

   e. SNMP traps should now be enabled and the agent should respond to **gets** from the clients.

   f. "Configuring the SNMP Service Information" on page 30:
   SL8500> `config serviceInfo set`

Command Line Interface

Important:
Only service representatives can use the command line interface (CLI) to enable and configure the SNMP feature.

Examples of SNMP Entries

An embedded SNMP agent can distinguish and filter trap recipients based on the trap numbers for which they are registered.

Entries must be made *exactly* as displayed in the SNMP help screens—**text is case sensitive**. For example, an entry of "auth**p**ass" instead of "auth**P**ass" will result in a parsing error.

Examples of SNMP entries that you might enter through the CLI are provided in the following sections.

Note – The prompt (*SL8500>*) indicates the library login.

Help

Using the Help command provides supporting information about the command syntax

```
SL8500> help snmp
snmp addTrapRecipient
                        trapLevel <trapLevelString>
                        host <hostName | hostAddr>
                        version [ v2c  community <communityString>] |
                                  [ v3 name 'trapUserName'
                                       auth <MD5 | SHA>
                                       authPass 'authPassPhrase'
                                       [priv <DES | AES>
                                        privPass 'privPassPhrase']
                                       engineId <engineIdString> ]
      where <trapLevelString> is a single number or a comma separated
      list of numbers. Example: 1,2,11,63 or *
      Reference this library's STREAMLINE-TAPE-LIBRARY-MIB for valid
      trap levels and trap level explanations.
      The <hostAddress|hostName> need to be fully qualified.
      The engine ID shall be a string of at most 31 hex characters,
      preceded with 0x.
snmp addUser
              version [ v2c  community <communityString> ] |
                       [ v3 name 'userName'
                            auth <MD5 | SHA>
                            authPass 'authPassPhrase'
                            [priv <DES | AES>
                             privPass 'privPassPhrase']]
snmp deleteTrapRecipient
                           [ id <index> ] |
                           [ host <hostName | hostAddr>
                             version [ v2c community <communityString> ] |
                                       [ v3 name 'trapUserName' ] ]
snmp deleteUser
                  [ id <index> ] |
                  [ version [ v2c community <communityString> ] |
                              [ v3 name 'userName' ] ]
 NOTE: 'community' is a reserved word and can not be used for input
        strings.
 NOTE: All 'UserName' arguments can use upper and lower case letters
        plus the following special characters !@#$%^*()-+=~.
 NOTE: All 'PassPhrase' arguments can use 'UserName' characters and
        letters plus the & character.
 NOTE: All passPhrases must be a minimum of 8 characters.
snmp disable port<portID>: disable SNMP for <portID>
snmp enable port<portID>: enable SNMP for <portID>
  NOTE: <portID> is 1A | 1B | 2A | 2B
         Ports <1A> and <1B> are the private interfaces
         Ports <2A> and <2B> are the public interfaces
snmp listTrapRecipients
snmp listUsers

COMPLETED

SL8500>
```

Adding Trap Recipients

SL8500> snmp **addTrapRecipient**

trapLevel <trapLevelString>
host <hostName | hostAddr>
version < v2c community communityString>
|
v3 name <trapUserName>
auth <MD5 | SHA>
authPass <authPassPhrase>
[priv <DES | AES>
privPass <privPassPhrase>]
[engineId <engineIdString>]>

Where:
<trapLevelString> is a single digit or a comma separated list of digits 1,2,3,4,...
<hostAddr | hostName> need to be fully qualified.
Note: Currently hostName is disabled, the user must use hostAddr.
The engine ID is a string of at most 31 hexadecimal characters, preceded with 0x.

As an example, a CLI entry for SNMP**v2c** to monitor four trap levels—error, warning, informational, and agent start—for an SL8500 library would be:

```
SL8500> snmp addTrapRecipient trapLevel 1,2,3,11 host 128.45.1.162
version v2c community public

    requestId
    requestId     2
    Device         1,0,0,0
    Success        true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

As another example, here is this CLI entry monitoring the same trap levels, but using SNMP**v3** protocol with additional "secure" parameters:

IP address of 128.45.1.162
MD5 authentication,
DES encryption
and an SNMP engine ID of 0x12345678910:

```
SL8500> snmp addTrapRecipient trapLevel 1,2,3,11 host 128.45.1.162
version v3 name snmp auth MD5 authPass snmpsnmp priv DES privPass
snmp engineId 0x12345678910

   requestId
   requestId     2
   Device         1,0,0,0
   Success       true
   Done

   Failure Count 0

   Success Count 1
COMPLETED
OK
SL8500>
```

Note – The "engineId" parameter is required on SNMPv3 traps.
The Engine ID is a string of, at most, 31 hexadecimal characters, preceded with 0x.

In general, the authoritative engineId is from the SNMP agent that sends the traps (such as the library). This can easily be collected by performing a query (snmpget) on the following OID:

SNMP-FRAMEWORK-MIB::snmpEngineID.0

An example using Net-SNMP from any remote host connected to the enabled SNMP port:

$ snmpget -v2c -cpublic monitoredLibrary SNMP-FRAMEWORK-MIB::snmpEngineID.0

SNMP-FRAMEWORK-MIB::snmpEngineID.0 = Hex-STRING: 80 00 1F 88 80 02 53 7D 07 4A 2D 94 6D

This engineId string would then be entered as:

"0x80001F888002537D074A2d946D".

The above now reveals the engineId of the monitored library (the library sending the traps within the addTrapRecipient Cli context).

Adding Users

```
SL8500> snmp addUser
                version <v2c community <communityString>
                |
                v3 name set <UserName>
                  auth <MD5 | SHA>
                  authPass <authPassPhrase>
                  [priv <DES |AES>
                  privPass <privPassPhrase>]
```

Adding an SNMP**v2c** user to a public community string would be:

```
SL8500> snmp addUser version v2c community public

    requestId
    requestId     6
    Device         1,0,0,0
    Success       true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Another example of adding an SNMP**v3** user with a security name of "stkAgentV3," a mixed level of security, MD5 authentication, and DES encryption, would be:

```
SL8500> snmp addUser version v3 name stkAgentV3
auth MD5 authPass snmpsnmp priv DES privPass DESPassPhrase

    requestId
    requestId     10
    Device         1,0,0,0
    Success       true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Deleting Trap Recipients

SL8500> snmp **deleteTrapRecipient**

<id <index>
 |
host <hostName | hostAddr>
version <v2c community <communityString>
 |
v3 name <trapUserName>>>

Where: The <hostAddr | hostName> must be fully qualified. **Currently hostName is disabled.**

Deleting an **SNMPv2c** user (uniquely identified by the recipient's host) from a public community string would be:

```
SL8500> snmp deleteTrapRecipient host 128.45.1.162
version v2c community public

    requestId
    requestId     46
    Device         1,0,0,0
    Success        true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Deleting an **SNMPv3** trap recipient of the same type, but using a trap user name (stkAgentV3), enter:

```
SL8500> snmp deleteTrapRecipient host 128.45.1.162
version v3 name stkAgentV3

    requestId
    requestId    51
    Device       1,0,0,0
    Success      true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Deleting Users

```
SL8500> snmp deleteUser
                <id <index>
                 |
                version <
                     v2c community <communityString>
                     |
                     v3 name <userName>>>
```

Deleting an **SNMPv2c** user by the user ID (1) would be:

```
SL8500> snmp deleteUser id 1

    requestId
    requestId     4
    Device         1,0,0,0
    Success       true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Deleting an **SNMPv3** user by the user name (stkUserV3), the entry would be:

```
SL8500> snmp deleteUser version v3 name stkUserV3

    requestId
    requestId     36
    Device         1,0,0,0
    Success       true
    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Disabling portID

SL8500> snmp **disable port<portID>** disables SNMP for <portID>
Where: <portID> is 2A or 2B
SL8500 ports: Port 2B provides the standard host connection to the library. Port 2A provides a dual-port connection to the library. Not supported by SNMP.

An example to disable Port 2B on an SL8500 would be:

```
SL8500> snmp disable port2B

    requestId
    requestId     53
    Device         1,0,0,0
    Success       true
    Done
Failure Count 0
Success Count 1
COMPLETED
OK
SL8500>
```

Note: There is no space between the word 'port' and the value for the 'portID'. For example: `snmp disable port2B` is the correct syntax for this command. The same applies for the snmp enable command.

Enabling portID

SL8500> snmp **enable port<portID>** enables SNMP for <portID>
Where: <portID> is 2A or 2B
SL8500 ports: Port 2B provides the standard host connection to the library. Port 2A provides a dual-port connection to the library. Not supported by SNMP.

An example to enable Port 2B on an SL8500 would be:

```
SL8500> snmp enable port2B

    requestId
    requestId     53
    Device         1,0,0,0
    Success       true
    Done
Failure Count 0
Success Count 1
COMPLETED
OK
SL8500>
```

Listing Trap Recipients

SL8500> snmp **listTrapRecipients**

To list information about the trap recipients, enter:

```
SL8500> snmp listTrapRecipients

    requestId
    requestId     39

    Attributes   Community   public
                   Host         128.45.1.162
                   Index        1
                   Port         162
                   Trap Level   1,2,3,11
                   Version      v2c
    Object        Snmp         snmp

    Attributes   Auth         MD5
                   AuthPass     *****
                   Engine Id    0x12345678910
                   Host         128.45.1.162
                   Index        2
                   Name         snmp
                   Port         162
                   Priv         DES
                   Priv Pass    *****
                   Trap Level   1,2,3,11
                   Version      v3
    Object        Snmp         snmp

    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Listing Users

SL8500> snmp **listUsers**

To list information about the users, enter:

```
SL8500> snmp listUsers

    requestId
    requestId     21
    Attributes   Community   public
                   Index       1
                   Version     v2c
    Object        Snmp         snmp

    Attributes   Auth         MD5
                   AuthPass    *****
                   Index       2
                   Name         snmp
                   Priv         DES
                   Priv Pass   *****
                   Version     v3
    Object        Snmp         snmp

    Done

    Failure Count 0

    Success Count 1
COMPLETED
OK
SL8500>
```

Configuring the SNMP Service Information

Like configuring for users and traps/notifications, you must also configure the MIB variables that relate to service information.

Service information is also entered through the CLI port. Command syntax for these entries, an example of entering one field (the slLibLocatCountry variable/description), and verifying this entry are supplied below.

Important notes for these entries are:

- The `config serviceInfo set` entries must be entered as a string.
- Each string will be truncated at 80 characters
- Each string must be delimited by single quotation marks (‘ ’)

SL8500> snmp **config print** display configuration of library
(config options are displayed, then the following syntax for the config serviceInfo set command is displayed) **config serviceInfo set** contact ‘<contactString>’ streetAddr ‘<streetAddrString>’ city ‘<cityString>’ state ‘<stateString>’ country ‘<countryString>’ zip ‘<zipString>’ description ‘<descriptionString>’ phone ‘<phoneString>’ Sets the service information NOTE: Users can enter any or all options when performing a serviceInfo set operation.

When configuring the service information, you can set one field or multiple fields with the `config serviceInfo set` command.

An example of setting multiple fields with one entry, would be:

```
SL8500> snmp config serviceInfo set city ‘Denver’ contact ‘Joe’
country ‘USA’ description ‘Manager’ phone ‘303-555-1234’
state ‘CO’ streetAddr ‘One Tape Drive’ zip ‘80028’
```

CHAPTER 4

Traps, Events, and Notifications

This chapter lists the supported SNMP traps—also known as events or notifications—and the supporting data for the SL8500 modular library.

SNMP Traps and Notifications

To obtain the information provided by a trap or notification, users must be added to the recipients list. Currently, this can be only be done by a service representative, through the CLI port, and using a “service” or “advanced service” log in.

See Chapter 3, Configuration for more information.

Organization

SNMP traps provide data that are organized using numeric formats or levels:

- 1 through 10 = Generic traps

Trap numbers 11 and higher are specific; that is, they contain distinct Object IDs (OIDs) within their messages. As such, they are generated from events within the library rather than the log entries.

- 11 through 20 = Agent specific related traps
- 21 through 100 = Device specific related traps
  - 21 through 27 = Library status
  - 41 through 45 = Drive status
  - 61 through 65 = Cartridge access port (CAP) status
  - 81 through 85 = Pass-thru port (PTP) status
- 101 and above = Media specific related traps

Levels

TABLE 4-1 lists the traps or notification levels available. These levels are generally filtered to include only those traps that a user wishes to monitor.

TABLE 4-1 Trap Levels

Traps	Level	Sent When...
slTrapError	1	Errors are posted in the log
slTrapWarning	2	Warnings are posted in the log
slTrapInformation	3	Information is posted in the log
slTrapConfiguration	4	Changes are made in a system property or configuration (such as an IP address)
slTrapAgentStart	11	An SNMP agent has started
slTrapLibStatusGood	21	Library has changed to normal mode
slTrapLibStatusCheck	25	Library has changed from normal mode
slTrapEnvHdwCheck	27	A device in the library has had an environmental check
slTrapDrvStatusGood	41	Drive has changed to a normal mode
slTrapDrvStatusCheck	45	Drive has changed from normal mode
slTrapCapStatusGood	61	CAP has changed to a normal mode
slTrapCapStatusOpen	63	CAP state has changed to open
slTrapCapStatusCheck	65	CAP has changed from normal mode
slTrapPtpStatusGood	81	PTP has changed to a normal mode
slTrapPtpStatusCheck	85	PTP has changed from normal mode

Generic Traps

Generic traps 1 – 4 are **log-based** and contain:

- Severity codes, for indications such as an error or a warning
- Result codes, such as “0000 = success,” or “5010 = robotic position error”
- Activity string, such as “HLI move” or “CLI version print”
- A descriptive text string
- Date and time
- Other information, such as:
  - Date and Time
  - Device address associated with the event
  - User name associated with the activity
  - Interface-specific request identifier

The examples in TABLE 4-2 reflect traps available with each library.

Note – Always consult the MIB for available traps.

TABLE 4-2 Generic Traps

Level	MIB Name	Sent When...	Object ID Content
1	slTrapError	A device condition that is critical to machine operation occurred. *Device inoperable*: Refers to the entire system. Failure of a sub-unit or redundant component is not a Category 1.	TABLE 4-3
2	slTrapWarning	A device condition which may need attention has been encountered. *Device degraded:* Refers to recoverable failures that may allow the system to remain in use, but only in a degraded mode.	TABLE 4-4
3	slTrapInformation	Information is presented for activity monitoring. *Device activity*: A device has reported activity. This information is used to monitor normal activity and messages.	TABLE 4-5
4	slTrapConfiguration	Configuration information is presented. *Device configuratiion*: A device has reported configuration activity.	TABLE 4-6

Error Trap

An error trap indicates a device condition, *which is critical to library operation*, has been encountered.

TABLE 4-3 Error Trap

MIB Name	slTrapError
Level	1
Objects	slTrapLibrarySerialNumber slTrapDeviceId slTrapDeviceTime slTrapDeviceAddress slTrapDeviceUserName slTrapDeviceInterfaceName slTrapDeviceActivity slTrapDeviceRequestId slTrapDeviceSeverity slTrapDeviceResultCode slTrapDeviceFreeFormText

Warning Trap

A warning trap indicates a device condition, *which may need attention*, has been encountered. .

TABLE 4-4 Warning Trap

MIB Name	slTrapWarning
Level	2
Objects	slTrapLibrarySerialNumber slTrapDeviceId slTrapDeviceTime slTrapDeviceAddress slTrapDeviceUserName slTrapDeviceInterfaceName slTrapDeviceActivity slTrapDeviceRequestId slTrapDeviceSeverity slTrapDeviceResultCode slTrapDeviceFreeFormText

Information Trap

An information trap presents information for activity monitoring.

TABLE 4-5 Information Trap

MIB Name	slTrapInformation
Level	3
Objects	slTrapLibrarySerialNumber slTrapDeviceId slTrapDeviceTime slTrapDeviceAddress slTrapDeviceUserName slTrapDeviceInterfaceName slTrapDeviceActivity slTrapDeviceRequestId slTrapDeviceSeverity slTrapDeviceResultCode slTrapDeviceFreeFormText

Configuration Trap

A configuration trap reports configuration activity.

TABLE 4-6 Configuration Trap

MIB Name	slTrapConfiguration
Level	4
Objects	slTrapLibrarySerialNumber slTrapDeviceId slTrapDeviceTime slTrapDeviceAddress slTrapDeviceUserName slTrapDeviceInterfaceName slTrapDeviceActivity slTrapDeviceRequestId slTrapDeviceSeverity slTrapDeviceResultCode slTrapConfigPropertyName, slTrapConfigNewPropertyValue, slTrapConfigNewPropertyEffective

Specific Traps

Specific traps 11 – 85 are **event-based** and have distinct information within their trap messages depending on the trap level. Consult each trap within the STREAMLINE-TAPE-LIBRARY-MIB for the specific data objects returned.

The examples in TABLE 4-7 reflect traps available with library.
Note – Always consult the MIB for available traps.

TABLE 4-7 Specific Traps

Level	MIB Name	Sent When The...	Object ID Content
11	slAgentBootDate	SNMP agent starts	TABLE 4-8
21	slTrapLibStatusGood	Library status changes to Good.	TABLE 4-9
25	slTrapLibStatusCheck	Library status changes to a check condition (degraded, non-operational).	TABLE 4-10
27	slTrapEnvHdwCheck	Library environmental or hardware condition changes.	TABLE 4-11
41	slTrapDrvStatusGood	Drive status changes to Good.	TABLE 4-12
45	slTrapDrvStatusCheck	Drive status changes to a check condition (error, warning, unknown).	TABLE 4-13
61	slTrapCapStatusGood	CAP status changes to Good.	TABLE 4-14
63	slTrapCapStatusOpen	CAP status changes to Open.	TABLE 4-15
65	slTrapCapStatusCheck	CAP status changes to a check condition (error, warning, unknown).	TABLE 4-16
81	slTrapPtpStatusGood	PTP status changes to Good.	
85	slTrapPtpStatusCheck	PTP status changes to a check condition (error, warning, unknown)	

Agent Boot Date

An SNMP agent starts.

TABLE 4-8 Agent Boot (Start) Date

MIB Name	slAgentBootDate
Level	11
Objects	slAgentBootDate

Library Status Good

This trap is sent when the library status changes to Good.

TABLE 4-9 Library Status Good

MIB Name	slTrapLibStatusGood
Level	21
Objects	slLibraryTopLevelCondition slLibStkBaseModel slLibSerialNumber

Library Status Check

This trap is sent when the library condition changes to a check condition, such as degraded or not-operative.

TABLE 4-10 Library Status Check

MIB Name	slTrapLibStatusCheck
Level	25
Objects	slLibraryTopLevelCondition slLibStkBaseModel slLibSerialNumber

Environmental Hardware Check

This trap is sent when the library environment or hardware condition changes.

TABLE 4-11 Environmental Hardware Check

MIB Name	slTrapEnvHdwCheck
Level	27
Objects	slTrapLibrarySerialNumber slTrapDeviceId slTrapDeviceTime slTrapDeviceAddress slTrapDeviceUserName slTrapDeviceInterfaceName slTrapDeviceActivity slTrapDeviceRequestId slTrapDeviceSeverity slTrapDeviceResultCode slTrapDeviceFreeFormText

Drive Status Good

This trap sent when a drive status changes to Good.

TABLE 4-12 Drive Status Good

MIB Name	slTrapDrvStatusGood
Level	41
Objects	slLibSerialNumber slDriveState slDriveAddress slDriveType slDriveVendor slDriveSerialNum

Drive Status Check

This trap sent when a drive status changes to a check condition, such as an error, warning, or unknown.

TABLE 4-13 Drive Status Check

MIB Name	slTrapDrvStatusCheck
Level	45
Objects	slLibSerialNumber slDriveState slDriveAddress slDriveType slDriveVendor slDriveSerialNum

CAP Status Good

This trap sent when the cartridge access port (CAP) status changes to Good.

TABLE 4-14 CAP Status Good

MIB Name	slTrapCapStatusGood
Level	61
Objects	slLibSerialNumber slCapState slCapAddress

CAP Status Open

This trap sent when a CAP status changes to Open.

TABLE 4-15 CAP Status Open

MIB Name	slTrapCapStatusOpen
Level	63
Objects	slLibSerialNumber slCapState slCapAddress

CAP Status Check

This trap sent when a CAP status changes to a check condition, such as an error, warning, or unknown.

TABLE 4-16 CAP Status Check

MIB Name	slTrapCapStatusCheck
Level	65
Objects	slLibSerialNumber slCapState slCapAddress

PTP Status Good

This trap sent when a PTP status changes to Good.

TABLE 4-17 CAP Status Open

MIB Name	slTrapPtpStatusGood
Level	81
Objects	slLibSerialNumber slPtpState slPtpAddress

PTP Status Check

This trap is sent when a PTP status changes to a check condition, such as an error, warning, or unknown.

TABLE 4-18 CAP Status Open

MIB Name	slTrapPtpStatusCheck
Level	85
Objects	slLibSerialNumber slPtpState slPtpAddress

APPENDIX **A**

Hewlett-Packard OpenView

This appendix provides steps to use the SNMP feature with: "Hewlett-Packard OpenView"

SNMP Configuration

Important:
Because SNMP can only be enabled through the command line interface (CLI) by a service representative, they must work with the customer's system administrator to obtain the information they require to make the necessary entries and enable SNMP.

See Chapter 3 and the SNMP Configuration Sequence to configure the SNMP feature.

1. Have an administrator Retrieve the Management Information Base.
2. Obtain the trap/notification destinations from the administrator:

   ❏ IP address of the hosts receiving the traps.
   There can be a maximum of 20 SNMP users (trap recipients) total.

   _____

   _____

   _____

   If using SNMPv3:

   ❏ `EngineId` of the hosts receiving the traps

   ❏ Authentication protocol/authPassPhrase (MD5 or SHA)

   ❏ Authentication privacy protocol/Privacy PassPhrase (DES or AES)

   ❏ User names and hosts receiving the traps

3. Have the service representative log in and use the:

- Command Line Interface and
- Configuring the SNMP Service Information to configure the SNMP application.

Hewlett-Packard OpenView

The following command sequence configures Hewlett-Packard (HP) OpenView Network Node Manager (NNM) on a Solaris operating system. Configuration examples and categories are also provided.

Loading the MIB

To load the SL8500 MIB on an OpenView server:

1. Set up the environment using the `./opt/OV/bin/ov.envvars.sh` script:
   ```
   %> ./opt/OV/bin/ov.envvars.sh
   ```
2. Create a directory for StorageTek MIBs:
   ```
   %> cd $OV_SNMP_MIBS/Vendor
   %> mkdir StorageTek
   ```
3. Copy the SL8500 MIB from your workstation to the new directory,
   ```
   %>cp /var/opt/OV/share/snmp_mibs/Vendor/StorageTek .
   ```
4. Launch OpenView.
5. Select Options ➪ Load/Unload MIBs: SNMP.
6. Press the Load button.
7. Browse to the STREAMLINE MIB file.
8. Press OK to load the trap definitions.
9. If desired, you may use the Tools ➪ SNMP MIB Browser operation to view the new MIB objects.

Configuring SNMP Events

When you load a MIB in to the HP OpenView NNM application's database, OpenView automatically adds the SNMP traps that are defined in the MIB to the Event Configuration application. The Event Configuration defines the rules for sending traps to the OpenView NNM alarm browser.

By default, the Event Configuration application creates the SL8500 traps with:

- Category set to Log and
- Severity set to Normal

To change these values:

1. Select Options ➪ Event Configuration
2. In the Enterprise Identification list, select streamlineTapeLibrary.

3. In the Event Identification list, double-click on an event name (for example: slTrapError).
4. Configure the desired event categories, severities, and event log messages, following the instructions in:

   Managing Your Network with HP OpenView Network Node Manager: Windows, HP-UX, Solaris, and Linux Operating Systems.

The following listing shows some sample trap configurations; the variable $* includes all variables associated with the event in the log message.

Critical, Error Alarms (Red)

- You could classify all *errors* as SNMP critical (**red**) alarms.
- You could format the message with the alarm severity at the start of each message and all other variables displayed in their native order.

For example:

Event name: slTrapError
Category: error alarms
Severity:
critical (red)
Message: An error trap was received. Severity: $9 Serial Number: $1 Device ID: $2 Time: $3 Device address: $4 User name: $5 Interface name: $6 Device activity: $7 Request ID: $8 Result code: $10 Description: $11

- Or you could create a more readable, natural-language message with a leading serial number:

Event name: slTrapError
Category: error alarms
Severity:
critical (red)
Message: SN$1: trapped a $9 error at $3 on device ID $2 at device address $4: result code $10. Error occurred while user $5 on interface $6 was requesting $7 activity (request ID: $8). $11

Major Events (Orange)

You might want to classify *check conditions* as SNMP major (**orange**) events.

For example:

Event name: slTrapLibStatusCheck
Category: status alarms
Severity:
major (orange)
Message: Library status changed to a check condition. Variables: $*

Event name: slTrapDrvStatusCheck
Category: status alarms
Severity:
major (orange)
Message: Drive status changed to a check condition. Variables: $*

Event name: slTrapCapStatusCheck
Category: status alarms
Severity:
major (orange)
Message: CAP status changed to a check condition. Variables: $*

Warning Events (Cyan)

It makes sense that *warnings* be classified as SNMP warning (**cyan**) events.

For example:

Event name: slTrapWarning
Category: Threshold Alarms
Severity:
warning (cyan)
Message: A warning trap was received. Variables: $*

Normal, Informational Events (Green)

The remainder of the trap types are mostly *informational messages* that can be classified as SNMP normal (**green**) events.

For example:

Event name: slTrapInformation
Category: status alarms
Severity:
normal (green)
Message: Trapped an informational message. Variables: $*

Event name: slTrapConfiguration
Category: configuration alarms
Severity:
normal (green)
Message: Trapped a configuration message. Variables: $*

Event name: slTrapAgentStart
Category: status alarms
Severity:
normal (green)
Message: The SNMP agent started. Variables: $*

Event name: slTrapLibStatusGood

Category: status alarms

Severity:

normal (green)

Event name: slTrapEnvHdwCheck

Category: status alarms

Severity:

normal (green)

Message: Library environmental or hardware condition has changed. Variables: $*

Event name: slTrapDrvStatusGood

Category: status alarms

Severity:

normal (green)

Event name: slTrapCapStatusGood

Category: status alarms

Severity:

normal (green)

Message: CAP status changed to good. Variables: $*

APPENDIX **B**

CA Unicenter

This appendix provides steps to use the SNMP feature with CA Unicenter Network and System Management application.

SNMP Configuration

Important:
Because SNMP can only be enabled through the command line interface (CLI) by a service representative, they must work with the customer's system administrator to obtain the information they require to make the necessary entries and enable SNMP.

See Chapter 3 and the SNMP Configuration Sequence to configure the SNMP feature.

1. Have an administrator Retrieve the Management Information Base.
2. Obtain the trap/notification destinations from the administrator:

   ❏ IP address of the hosts receiving the traps.
   There can be a maximum of 20 SNMP users (trap recipients) total.

   _____

   _____

   _____

   If using SNMPv3:

   ❏ `EngineId` of the hosts receiving the traps

   ❏ Authentication protocol/authPassPhrase (MD5 or SHA)

   ❏ Authentication privacy protocol/Privacy PassPhrase (DES or AES)

   ❏ User names and hosts receiving the traps

3. Have the service representative log in and use the:

- Command Line Interface and
- Configuring the SNMP Service Information to configure the SNMP application.

CA Unicenter

The following procedure configures CA Unicenter Network and System Management (NSM) application to collect traps on Windows operating systems.

Make sure that the SNMP agents are installed on the system:

1. Right click on My Computer.
2. Select Manage.
3. Under Services and Applications, click on Services.
4. Check for: SNMP Services and SNMP Trap Services

- If they are **not** there follow the instruction bellow to install the agents.
- If they are there continue with Installing NSM.

To install SNMP services on Windows 2000 and 2003 platforms:

Notes:

- You must be logged on as an administrator or a member of the Administrators group to complete this procedure.
- If your computer is connected to a network, network policy settings may also prevent you from completing this procedure.

a. Click on Start.

b. Go to and click on Control Panel.

c. Double-click on Add or Remove Programs.

d. Click on Add/Remove Windows Components.

e. In Components, click Management and Monitoring Tools—but do not select or clear the check box—then click Details.

f. Select the Simple Network Management Protocol check box, and click OK.

g. Click Next.

h. Insert the application CD or specify the complete path for the location where the files are stored.

The SNMP application starts automatically after installation.

Caution – If Unicenter NSM is installed before the Windows SNMP agents, some of the commands on NSM will not work properly and a re-installation of NSM will be required.

Installing NSM

Components of Unicenter NSM include:

- Enterprise Manager – monitors and displays traps
- Trap Manager – loads the MIBs on the Management system

To install the CA Unicenter Network and System Management application on Windows operating systems follow the provided instructions or:

1. Place the Unicenter NSM Installation DVD/CD in the drive.
   The Unicenter product explorer will start automatically.
2. Under Unicenter for Windows; select Installation Wizard for Unicenter NSM and click Install.
3. Select install any or all Unicenter NSM components and click Next.
4. Accept the License Agreement and click Next.
5. Complete the required information and click Next.
   This launches the component selection window.
6. Under Unicenter NSM components select: Ingres, WorldView, Agent Technologies, and Enterprise Management the click Next.
7. Provide an *nsmadmin password* and click next.
   The installation process starts.
8. After the installation is complete; reboot the system.

Starting the NSM Enterprise Manager

To start the NSM Enterprise Manager (EM) console:

Note – Enterprise Manager console is the window where all the traps (alerts) from devices are displayed.

1. Go to Start ➪ Programs ➪ Computer Associates ➪ Unicenter ➪ NSM ➪ Enterprise Management ➪ EM classics.
   The Enterprise Manager for windows starts.
2. Double click on Windows.
3. Double click on Events.
4. Double click on Console Logs.
   The Enterprise Manager launches the console.

Installing the NSM Trap Manger

1. Place the Unicenter NSM Installation DVD/CD in the drive.

   The Unicenter product explorer will start automatically.

2. Under Unicenter For Windows: Post Installation Utilities, select Trap Manager and click Install.

3. Follow the prompts and directions to complete the installation.

Loading the NSM Trap Manager

To load the Trap Manager with a MIB and traps:

1. Go to Start ➪ Programs ➪ CA ➪ Unicenter.

2. Sign on to the Trap Database.

   The Trap Manager connects to the Trap Database and the Unicenter NSM TrapManager window appears.

3. Select MIBs then All MIBs from the View drop-down menu.

   The view changes to show All MIBs in the left pane.

Note – To add a vendor, MIB, or trap, you must be in the All MIBs view.

4. To add a new trap under a new vendor:

   a. Select Add, Vendor from the File drop-down menu.

   b. Right-click the Root node in the Traps tree in the left pane and select Add Vendor.

   c. A node with the name New Vendor is added to the end of the Traps tree in the left pane.

   d. Enter a name for your new vendor, and press Enter.

      The Vendor name is changed.

Note – The new vendor is not saved in the database until you add at least one MIB and one trap under the new vendor.

5. To add your new trap under a new MIB:

   a. Click the Vendor node under which you want to add a new MIB in the Traps tree in the left pane.

   b. Select Add, MIB File from the File drop-down menu.

   c. A node with the name New Mibname (New Mibfile) is added to the end of the Traps tree for the Vendor node you selected in the left pane.

   d. Enter a name for your new MIB, and press Enter.
      The MIB name is changed.

   e. The new MIB is not saved in the database until you add at least one trap under the new MIB.

6. Do one of the following:

- Click the MIB node under which you want to add a new trap in the Traps tree in the left pane. Select Add, Trap from the File drop-down menu.
- Right-click the MIB node under which you want to add a new trap in the Traps tree in the left pane, and then select Add Trap.

  The Add Trap window appears in the right view pane.

Note – The Vendor, MIB File, and MIB Name fields are automatically updated.

7. Complete the fields on the Add Trap window, and then click Save.

   The new trap is saved and appears under the MIB you selected in the Traps tree in the left pane. The new trap is color-coded to show the trap severity as follows:

   - Green icon - trap severity is informational.
   - Yellow icon - trap severity is warning.
   - Red icon - trap severity is critical.

Glossary

This glossary defines terms and abbreviations used in this publication.

A

Advanced Encryption Standard (AES) An NIST-standard cryptographic cipher that uses a block length of 128 bits and multiple key lengths of 128, 192, or 256 bits to encrypt data.

agent A module that resides in a managed device. The agent is responsible for responding to requests from the manager and for sending *traps* to a recipient that inform the systems administrator of potential problems.

C

community string Applications use community strings for access control. The manager includes the community string in its SNMP messages to an agent.

D

Data Encryption Standard (DES) An NIST cryptographic cipher that uses a 56-bit key.

Dynamic Host Configuration Protocol (DHCP) A set of rules to allow a network attached device to request and obtain an IP address from a server which has a list of addresses available for assignment.

Domain Name System (DNS) A system that translates IP addresses into human readable computer names. Similar to a phone book matching names and numbers.

E

EngineID An administratively unique identifier of an SNMPv3 engine used for identification, not for addressing.

F

firewall In computing, a firewall is a piece of hardware and/or software which controls connectivity between different zones of trust.

File Transfer Protocol (FTP) An internet protocol for transferring files between two hosts over a TCP/IP network.

G

gateway A device on a network that serves as an entrance to another network.

H

host keyword Currently, the host keyword is limited to the machine's IP address. The maximum keyword length is 31 alphanumeric characters.

HyperText Transfer Protocol (HTTP) The protocol most often used to transfer information from World Wide Web servers to browsers.

I

Internet Engineering Task Force (IETF) Develops and promotes internet standards.

Internet Protocol (IP) A data-oriented protocol used for communicating data across a network.

IP is a network layer protocol in the internet protocol suite and is encapsulated in a data link layer protocol such as Ethernet.

M

managed device A device that hosts the services of an SNMP agent that provides monitored information and controlled operations using SNMP.

StoragTek libraries are managed devices.

management information base (MIB) A collection of information stored in a database that contains configuration and statistical information for a managed device.

For StreamLine libraries, a copy of the MIB is loaded with firmware and stored on the processor card.

manager Provides the communication link between the systems administrator and the managed devices on the network. A manager station or server allows the systems administrator to get information about the device through the MIB and to receive traps from an agent.

Message Digest 5 (MD5) A popular one-hash function that is used to create a message digest for digital signatures. MD5 is faster than SHA, but is considered less secure.

N

National Institute of Standards and Technology (NIST) An agency of the Commerce Department's Technology Administration.

notification A message that reports a problem, error, or significant event that occurred within a device—a trap.

netmask A hierarchical partitioning of the network address space.

O

Open Source Initiative (OSI) An organization dedicated to promoting open-source software. The OSI model divides the functions of a protocol into a series of layers

R

recipient A location on a manager where the SNMP agent sends traps. This location is defined by the combination of either the IP address or DNS name and the port number. The default recipient port number is 162.

Request for Comments (RFC) A series of memoranda encompassing new research, innovations, and methodologies applicable to Internet technologies. The Internet Engineering Task Force (IETF) adopts some of the applied information theory published in RFCs as Internet standards.

S

Secure Hash Algorithm (SHA-1/SHA) A popular one-hash algorithm used to create digital signatures; it is more secure, but slightly slower than MD5.

Simple Mail Transfer Protocol (SMTP) A protocol for sending e-mail messages between servers.

T

Transmission Control Protocol (TCP) One of the core protocols of the Internet protocol suite. Using TCP, applications on networked hosts can create connections to one another, over which they can exchange data. The protocol guarantees reliable and in-order delivery of sender to receiver data (see also User Datagram Protocol).

trap A message that reports a problem, error, or significant event that occurred within a device—a notification.

U

User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages sometimes known as datagrams to one another.

UDP does not provide the reliability and ordering guarantees that TCP does. Datagrams may arrive out of order or go missing without notice. Without the overhead of checking if every packet actually arrived, UDP is faster and more efficient for many lightweight or time-sensitive purposes.

W

World Wide Name (WWN) A unique identifier in a Fibre Channel or Serial Attached SCSI storage network. Each WWN is an 8-byte number derived from IEEE and vendor-supplied information.

Index

N

O

P

R

S

T

U

V

Z

Oracle Corporation
Worldwide Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A