

# StorageTek SL500 Modular Library System

---

## Simple Network Management Protocol



Part Number: 316194602  
November 2010  
Revision: B

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

StorageTek SL500 Modular Library System - Simple Network Management Protocol (SNMP)

316194602 Revision: B

Copyright © 2007, 2010, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related software documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd.

This software or hardware and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

# Summary of Changes

---

Date	Revision	Description
September 2007	A	Initial release
November 2010	B	Updates to this revision include: <ul style="list-style-type: none"><li>■ Oracle branding.</li><li>■ Engineering updates.</li><li>■ New Command Line Interface layout.</li></ul>

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



# Contents

---

## **1. Introduction 1**

- Architecture 1
- SNMP Terms 2
- Versions 3
- Protocol 4
  - Management Information Base 5
  - Agents 6
  - Management Stations 6
- Commands 6
  - What is a Trap or Notification? 6

## **2. Management Information Base 7**

- Access Control 7
- Management Information Base 8
- Basic MIB Variables 9
  - Library Type 9
  - Library Location 9
  - Library Date 9
- Additional MIB Variables 10
  - Agent 11
  - Agent Trap Recipients 11
  - Agent Trap Recipient for Version 2 11
  - Agent Trap Recipient for Version 3 12
  - Cartridge Access Ports 13
  - Cleaning 14
  - Controller 15

Elevator	16
Physical Hardware	17
Inventory	19
Library State	19
Library Configurations	20
Media Events	21
Network	22
Pass-thru Ports	23
Power Supply	24
Robot	25
Safety Door	25
Statistics	26
Storage	27
Tape Drives	28
Versions	29

### **3. Management Information Base 31**

SNMP Default Settings	31
Retrieve the Management Information Base	32
SNMP Configuration Sequence	33
Command Line Interface	34
Examples of SNMP Entries	34
Help	35
Adding Trap Recipients	36
Adding Users	38
Deleting Trap Recipients	39
Deleting Users	40
Disabling portID	41
Enabling portID	41
Listing Trap Recipients	42
Listing Users	43
Configuring the SNMP Service Information	44

### **4. Traps, Events, and Notifications 45**

SNMP Traps and Notifications	45
Organization	45
Levels	46
Generic Traps	47
Error Trap	48
Warning Trap	48
Information Trap	49
Configuration Trap	49
Specific Traps	50
Agent Boot Date	51
Library Status Good	51
Library Status Check	51
Environmental Hardware Check	52
Drive Status Good	53
Drive Status Check	53
CAP Status Good	54
CAP Status Open	54
CAP Status Check	54
<b>A. Hewlett-Packard OpenView</b>	<b>55</b>
SNMP Configuration	55
Hewlett-Packard OpenView	56
Loading the MIB	56
Configuring SNMP Events	56
Critical, Error Alarms (Red)	57
Major Events (Orange)	58
Warning Events (Cyan)	59
Normal, Informational Events (Green)	59
<b>B. CA Unicenter</b>	<b>61</b>
SNMP Configuration	61
CA Unicenter	62
Installing NSM	63
Starting the NSM Enterprise Manager	63

Installing the NSM Trap Manger	64
Loading the NSM Trap Manager	64



# Preface

---

This reference guide provides information about the Simple Network Management Protocol (SNMP) and the implementation with **Oracle's StorageTek SL500 Modular Library System**.

---

## Documentation, Support, and Training

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

*SL500 Modular Library System: Simple Network Management Protocol*, PN 316194602



# Introduction

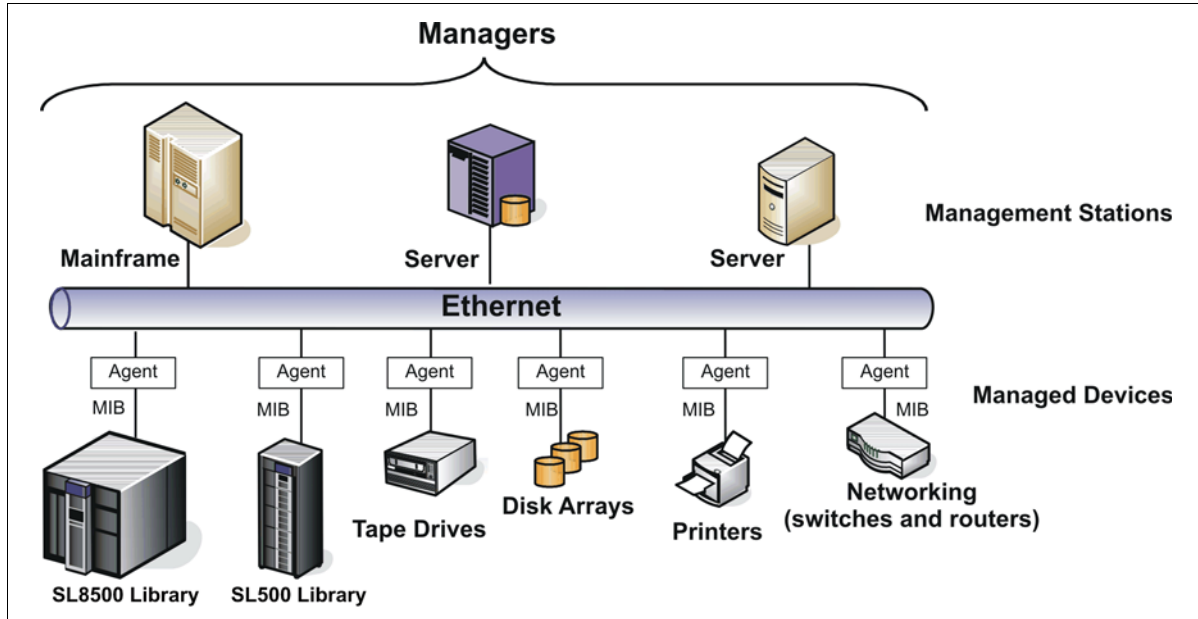
Short for Simple Network Management Protocol, SNMP is a network protocol designed to monitor and manage network-attached devices.

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. SNMP Architecture**



- A *managed device*—such as the SL500 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
<b>SNMPv1</b> 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
<b>SNMPv2</b> is a revised protocol, not just a new MIB (RFCs 1592 and 1907).		
– SNMPv2p	Party-based (now obsolete) Includes improvements in performance, security, and communications	RFC 1441 through RFC 1452
– SNMPv2c	Community-based Includes SNMPv2p <i>without</i> the controversial security Widely considered the “ <i>de facto</i> ” SNMPv2 standard	RFC 1901 through RFC 1908
– SNMPv2u	User-based Includes USM (user-based security model) Offers greater security, but without the complexity	RFC 1909 and RFC 1910
<b>SNMPv3</b> 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
<p>In practice, SNMP implementations often support multiple versions: typically SNMPv1, SNMPv2c, and SNMPv3. Refer to RFC 3584, the <i>Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework</i>, for more information.</p> <p>For more listings and information about SNMP and Requests for Comments, go to the Internet Engineering Task Force (IETF) Web site at: <a href="http://www.ietf.org/">http://www.ietf.org/</a></p> <p>For more information about SNMP, go to: <a href="http://www.snmp.com/">http://www.snmp.com/</a></p>		

# Protocol

The SNMP specification is based on the User Datagram Protocol (UDP)<sup>1</sup>.

Similar to TCP<sup>2</sup>, UDP runs on top of IP<sup>3</sup> networks (called UDP/IP) using familiar client-server models, such as the OSI<sup>4</sup> 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 <b>SNMP</b> , DNS, FTP, HTTP, SMTP, and others.	7. Application layer Applications and end-user processes, such as <b>SNMP</b> , 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 <b>UDP</b> Transfers data between system components.	4. Transport layer: TCP and <b>UDP</b> Transfers data between system components
2. Internet layer: <b>IP</b> (IPv4)	3. Network layer: <b>IP</b>
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.



# Management Information Base

---

This chapter describes the management information base (MIB) for the StorageTek SL500 modular library to support the SNMP feature.

**Important:** SNMP configuration requirements:

- SL500 library firmware must be version **1067** or higher.
- StorageTek Library Console version FRS\_2.95 or higher.
- By default, the SNMP agent is disabled and must be enabled through the Command Line Interface (CLI) for customers wanting to use this feature.

Initially, SNMP can be configured only through the command line interface (CLI)—which requires a service representative working together with system administrators and network managers to properly configure SNMP for their account (as described in [Chapter 3, Configuration](#)).

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.

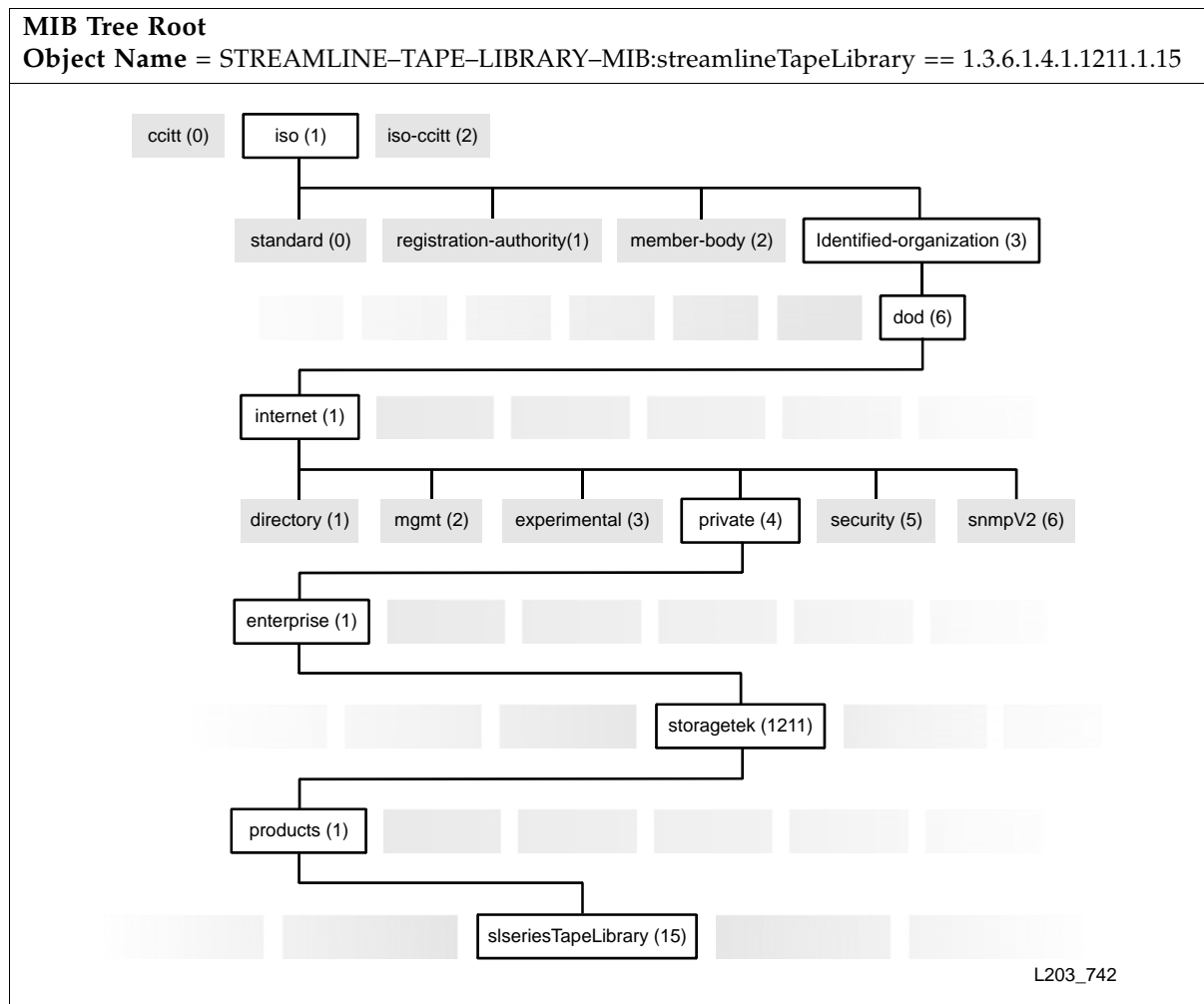
**Note** – Customers can download the MIB through the StorageTek Library Console, but it cannot be directly viewed from the console itself. However, because the MIB is a plain ASCII text file, it can be viewed from any readily available text editor.

# 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

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

**TABLE 2-1** Library Type

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

### Library Location

**sLibLocation** provides information about the location of the library.

**TABLE 2-2** Library Location

Content	Description
sLibLocatContact	Primary contact for administration
sLibLocatStreet	Location/site – Street address
sLibLocatState	Location/site – State/province
sLibLocatZip	Location/site – ZIP code or other data
sLibLocatCountry	Location/site – Country
sLibLocatDescr	Location/site – Description or other data
sLibLocatCity	Location/site – City

### Library Date

**sLibDate** provides information about the date and time-of-day.

**TABLE 2-3** Library Date and Time of Day

Content	Description
sLibDateString	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:

- [Agent](#)
- [Agent Trap Recipients](#)
- [Agent Trap Recipient for Version 2](#)
- [Agent Trap Recipient for Version 3](#)
- [Cartridge Access Ports](#)
- [Cleaning](#)
- [Controller](#)
- [Elevator](#) (see note)
- [Physical Hardware](#)
- [Inventory](#)
- [Library State](#)
- [Library Configurations](#)
- [Media Events](#)
- [Network](#)
- [Pass-thru Ports](#) (see note)
- [Power Supply](#)
- [Robot](#)
- [Safety Door](#) (see note)
- [Statistics](#)
- [Storage](#)
- [Tape Drives](#)
- [Versions](#)

**Note** – This information is from the standard MIB for all StorageTek libraries; therefore, the SL500 library may not support all of these variables.

## Agent

**slAgent** provides information about the agent.

**TABLE 2-4** Agent Data

Content	Description
slAgentRevision	Firmware version of the embedded agent
slAgentBootDate	Date and time when the agent initialized
slAgentURL	URL for Web based management
slAgentPort	UDP port number where the agent is listening
slAgentCommunity	The agent default community

## Agent Trap Recipients

**slAgentTrapRecipient** provides information about the recipients.

**TABLE 2-5** Trap Recipients

Content	Description
slAgentTrapRecipientClearAll	Set to 2 to clear all the trap recipients in list
slAgentTrapRecipientCount	Number of trap recipients in the table

## Agent Trap Recipient for Version 2

**slAgentTrapRecipientV2** provides information about Version 2 recipients.

**TABLE 2-6** Version 2 Trap Recipients

Content	Description
slAgentTrapRecipientV2	Version 2c Trap recipients table
slAgentTrapRecipientV2ClearAll	Set to 2 to clear all the trap recipients in list
slAgentTrapRecipientV2Count	Number of trap recipients in the table
slAgentTrapRecipientV2Table	Version 2 trap recipients table
slAgentTrapRecipientV2Entry	Trap recipients table entry
slAgentTrapRecipientV2TableIndex	Index into the trap recipients table
slAgentTrapRecipientV2Filter	Set to specify the traps to filter on (such as, * = all, errors, warnings, info)
slAgentTrapRecipientV2Host	Trap recipient's host name or IP address
slAgentTrapRecipientV2Port	UDP port for the recipient to receive notification
slAgentTrapRecipientV2Community	Trap recipient's community string
slAgentTrapRecipientV2ClearEntry	Set to 2 to clear or remove this trap from the recipient entry

## Agent Trap Recipient for Version 3

**slAgentTrapRecipientV3** provides information about Version 3 recipients, such as: UDP port, recipient table, security and encryption levels.

**TABLE 2-7** Version 3 Trap Recipients

Content	Description
slAgentTrapRecipientV3ClearAll	Set to 2 to clear all the trap recipients in list.
slAgentTrapRecipientV3Count	Number of trap recipients in the table
slAgentTrapRecipientV3Table	Version 3 trap recipients table
slAgentTrapRecipientV3Entry	Trap recipients table entry
slAgentTrapRecipientV3TableIndex	Index into the trap recipients table
slAgentTrapRecipientV3Filter	Set to specify the traps to filter on (0 = none, 1 = error, 2 = warning, 3 = info)
slAgentTrapRecipientV3Host	Trap recipient's host name or IP address
slAgentTrapRecipientV3Port	UDP port for the recipient to receive notification
slAgentTrapRecipientV3SecLevel	Security level: <ul style="list-style-type: none"> <li>■ noAuthNoPriv: match on user name for authentication</li> <li>■ authNoPriv: MD5 or SHA authentication</li> <li>■ authPriv: MD5 or SHA authentication</li> <li>■ DES or AES encryption.</li> </ul>
slAgentTrapRecipientV3Auth	Authentication algorithm: MD5 or SHA
slAgentTrapRecipientV3AuthPass	MD5 or SHA authentication pass phrase. This object is write-only.
slAgentTrapRecipientV3Priv	Encryption algorithm: DES or AES.
slAgentTrapRecipientV3PrivPass	DES or AES encryption pass phrase. This object is write-only.
slAgentTrapRecipientV3RemoteId	Remote engine ID. This object is write-only.
slAgentTrapRecipientV3ClearEntry	Set to 2 to clear / remove this trap recipient entry

- **MD5** = Message-Digest algorithm 5, a widely used cryptographic hash function with a 128-bit hash value
- **SHA** = Secure Hash Algorithm functions refer to five FIPS-approved algorithms for computing a condensed digital representation
- **DES** = Data Encryption Standard, a cipher or method for encrypting information
- **AES** = Advanced Encryption Standard, a block cipher method for encrypting information

## Cartridge Access Ports

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

**TABLE 2-8** Cartridge Access Port Data

Content	Description
sICapCount	Number of the CAPs in the CAP table
sICapTable	Table of cartridge access ports (CAPs)
sICapEntry	Cartridge access port
sICapIndex	Integer index into the CAP table
sICapAddress	CAP device address
sICapAccessibility	Accessibility of a CAP (for example: open, allow/prevent)
sICapAccessStateEnum	Access state of the CAP presented as an enumeration
sICapState	Physical state of the CAP
sICapStatusEnum	Operational status of the CAP presented as an enumeration
sICapName	CAP name
sICapRotations	CAP rotation count
sICapRotationRetries	Number of rotation retries performed by the CAP
sICapRotationFails	Number of rotation failures performed by the CAP
sICapIPLs	Number of IPL's performed by the CAP

## Cleaning

**sLibCleaning** provides information about cleaning, such as: library features, thresholds, labels, plus the number of and type of cleaning cartridges.

**TABLE 2-9** Cleaning

Content	Description
sLibCleanEnabled	Auto clean feature configuration. Not all libraries support this feature, refer to user documentation for more information.
sLibCleanNumCartTypes	Number of unique cartridge types supported
sLibCleanWarnTable	Table of clean count warning thresholds
sLibCleanWarnEntry	Clean count warning thresh table entry
sLibCleanWarnIndex	Index into clean warning threshold table
sLibCleanWarnCartType	Cleaning cartridge type (for example: SDLT, 9840, LTO and T10000)
sLibCleanWarnCount	Configured warning count threshold
sLibCleanNumCarts	Count of the clean cartridges in the library
sLibCleanCartTable	Table of cleaning cartridges in the library
sLibCleanCartEntry	Cleaning cartridge
sCleanCartIndex	Integer index into the cleaning cartridge table
sCleanCartLabel	Clean cartridge label
sCleanCartType	Cleaning cartridge type (for example: SDLT, 9840, and LTO)
sCleanCartLocationElementID	Clean cartridge location – Element ID
sCleanCartHostAccessible	Indication of host accessible status
sCleanCartUsageCount	Number of times that the cartridge has been used to clean a tape drive



## Controller

**slController** provides information about the library controller, such as: type, quantity, code, firmware, versions, and serial number.

**TABLE 2-10** Library Controller Data

Content	Description
slControllerCount	Count of the controllers in the controller table
slControllerTable	Table of controllers
slControllerEntry	Controller entry (HBC, HBCR, RLC, HBT, etc)
slControllerIndex	Controller's Card Index
slControllerElementID	Element ID/Address of the controller
slControllerSerialNum	Controller card serial number
slControllerStatus	Controller state (for example: okay, error, and warning)
slControllerFaultLED	Controller Fault LED state
slControllerSafeToRemoveLED	Controller safe to remove LED state
slControllerStatusEnum	Controller operational status in enumerated form
slControllerCodeVer	Controller code version
slControllerVersion	Controller version
slControllerFirmwareVer	Controller firmware version
slControllerHAState	Controller High Availability Status (active=0 and standby=1)

## Elevator

**sLElevator** provides information about elevators.

**Note** – This information is from the standard MIB for StorageTek Libraries; however, the SL500 library does not have an Elevator; therefore, the information in this variable is not applicable.

**TABLE 2-11** Elevator

Content	Description
sLElevatorCount	Number of elevators in elevator table
sLElevatorTable	Table of elevators
sLElevatorEntry	Elevator entry
sLElevatorIndex	Elevator index
sLElevatorElementID	Element ID / Address of elevator
sLElevatorPositionOn	Physical position of elevator
sLElevatorHandCartStatus	Elevator hand state (cartridge = 1, no cartridge = 0)
sLElevatorSerialNum	Elevator serial number
sLElevatorState	Elevator state (such as idled, moving, in-operative)
sLElevatorFaultLED	Elevator Fault LED state
sLElevatorStatusEnum	Elevator operational status in enumerated form
sLElevatorCodeVer	Elevator code version
sLElevatorVersion	Elevator version
sLElevatorFirmwareVer	Elevator firmware version
sLElevatorGetRetries	Number of mount retries performed to the elevator
sLElevatorPutRetries	Number of dismount retries performed to the elevator

## Physical Hardware

**slPhysHardware** provides information about the physical components of the library, such as host connections, controller card, cooling fans and temperature.

**TABLE 2-12** Hardware Components

Content	Description
slHostInterfaceCount	Count of interface cards.
slHostInterfaceTable	Table of host interfaces
slHostInterfaceEntry	Host interface entry (such as Fiber or SCSI)
slHostInterfaceIndex	Integer index into the table of host interface cards
slHostInterfaceFibreCount	Number of active fibres in this host interface card
slHostInterfaceAWWN	Fibre A – World Wide Name (WWN)
slHostInterfaceA1AddressingMode	Port A1 – Addressing mode
slHostInterfaceA1PortEnabled	Port A1 – Port enabled
slHostInterfaceA1LoopId	Port A1 – Loop ID
slHostInterfaceA1PortSpeed	Port A1 – Port speed
slHostInterfaceA2AddressingMode	Port A2 – Addressing mode
slHostInterfaceA2PortEnabled	Port A2 –Port enabled
slHostInterfaceA2LoopId	Port A2 – Loop ID
slHostInterfaceA2PortSpeed	Port A2 – Port speed
slHostInterfaceBWWN	Fibre B – World Wide Name
slHostInterfaceB1AddressingMode	Port B1 – Addressing mode
slHostInterfaceB1PortEnabled	Port B1 – Port enabled
slHostInterfaceB1LoopId	Port B1 – Loop ID
slHostInterfaceB1PortSpeed	Port B1 – Port speed
slHostInterfaceB2AddressingMode	Port B2 – Addressing mode
slHostInterfaceB2PortEnabled	Port B2 – Port enabled
slHostInterfaceB2LoopId	Port B2 – Loop ID
slHostInterfaceB2PortSpeed	Port B2 – Port speed
slHostInterfaceElementID	Element ID / Address of the controller
slHostInterfaceSerialNum	Controller card serial number
slHostInterfaceStatus	Controller state (okay, error, warning)
slHostInterfaceFaultLED	Controller Fault LED state
slHostInterfaceSafeToRemoveLED	Controller safe to remove LED state
slHostInterfaceStatusEnum	Controller operational status in enumerated form
slHostInterfaceCodeVer	Controller's code version

**TABLE 2-12** Hardware Components (Continued)

<b>Content</b>	<b>Description</b>
slHostInterfaceVersion	Controller's version
slHostInterfaceFirmwareVer	Controller's firmware version
slHostInterfaceHAState	Controller's High Availability Status (active=0 and standby=1)
slTempSensorCount	Number of temperature sensors in the library
slTempSensorTable	Table of the library's temperature sensors
slTempSensorEntry	Temperature sensor
slTempSensorIndex	Integer index into the temperature sensor table
slTempSensorName	Name of the temperature sensor
slTempSensorCurrentTemp	Current / Present temperature reading
slTempSensorHighTemp	Storage area peak temp since last machine boot
slTempSensorWarnThreshold	Temperature threshold for automated warning
slTempSensorFailThreshold	Temperature threshold for automated library shutdown
slFanCount	Number of monitored fans in the library
slFanTable	Table of the library's fans
slFanEntry	Fan entry
slFanIndex	Integer index into the fan table
slFanName	Name of the fan
slFanOperational	Operational state of the fan
slPowerSupplyCount	Number of power supplies installed in the library
slPowerSupplyTable	Table of the library power supplies
slPowerSupplyEntry	Power supply
slPowerSupplyIndex	Integer index into the power supply table
slPowerSupplyName	Name of the power supply
slPowerSupplyInstalled	Indicates if the supply is installed (2) or not (1)
slPowerSupplyOperational	Indicates if the supply is OK (2), meaningless if not-installed

## Inventory

**sInventory** provides information about the contents of the library, such as: number of and types of cartridges and labels in the library.

**TABLE 2-13** Library Inventory

Content	Description
sTapeCount	Number of the cartridges in the inventory table
sTapeTable	Table of data cartridges (tapes) in the library
sTapeEntry	Cartridge
sTapeIndex	Integer index into the inventory table
sTapeLabel	Cartridge label
sTapeType	Cartridge type
sTapeLocationElementID	Cartridge location – Element ID
sTapeHostAccessible	Indication of host accessible status

## Library State

**sLibLSMState** provides information about the library storage modules (LSMs).

**TABLE 2-14** Library State

Content	Description
sLibLSMCount	LSM count
sLibLSMStateTable	LSM states
sLibLSMStateEntry	LSM state entry
sLibLSMStateIndex	LSM state index
sLibLSMStatus	LSM operational state – reported as a string (for example: offline, online, or maintenance)
sLibLSMStatusEnum	LSM operational state – reported as an enumeration

## Library Configurations

**sLibLSMConfig** provides configuration information about the library storage modules, such as: number of LSMs, hands, CAPs, and tape drives.

**TABLE 2-15** Library Configurations

Content	Description	
sLibLSMConfigCount	Number of LSM's installed	
sLibLSMConfigTable	LSM configurations	
sLibLSMConfigEntry	LSM configuration entry	
sLibLSMConfigIndex	LSM configuration index	
sLibLSMConfigNumPanels	Number of physical panels	
sLibLSMConfigNumHandCells	Number of physical hands	
sLibLSMConfigMinHandAddr	Minimum Element ID or Address of physical hands	
sLibLSMConfigMaxHandAddr	Maximum Element ID or Address of physical hands	
sLibLSMConfigNumSystemCells	Number of system and reserved cells	
sLibLSMConfigNumRestrictedCells	Number of customer restricted cells	
sLibLSMConfigMinSystemAddr	Minimum Element ID or Address of system cells	
sLibLSMConfigMaxSystemAddr	Maximum Element ID or Address of system cells	
sLibLSMConfigNumCaps	Number of cartridge access ports (CAPs)	
sLibLSMConfigNumCapColumns	Number of columns within CAPs	
sLibLSMConfigNumCapCells	Number of CAP cells	
sLibLSMConfigMinCapAddr	Minimum Element ID or Address of CAP cells	
sLibLSMConfigMaxCapAddr	Maximum Element ID or Address of CAP cells	
sLibLSMConfigNumDriveColumns	Number of drive columns	
sLibLSMConfigNumDrives	Number of tape drives	
sLibLSMConfigMinDriveAddr	Minimum Element ID or Address of tape drives	
sLibLSMConfigMaxDriveAddr	Maximum Element ID or Address of tape drives	
sLibLSMConfigNumStorageCells	Number of storage cells	
sLibLSMConfigMinStorageAddr	Minimum Element ID or Address of storage cells	
sLibLSMConfigMaxStorageAddr	Maximum Element ID or Address of storage cells	
sLibLSMConfigNumPtps	Number of pass-thru ports (PTPs)—	SL500 only
sLibLSMConfigNumPtpColumns	Number of columns within the PTPs	
sLibLSMConfigNumPtpCells	Number of PTP cells	
sLibLSMConfigMinPtpAddr	Minimum Element ID or Address of PTP cells	
sLibLSMConfigMaxPtpAddr	Maximum Element ID or Address of PTP cells	

## Media Events

**sLibMediaEvents** provides information about the media—data cartridges—such as: volume IDs or serial numbers (VOLSERs), the labels and barcode, tape drive types, plus errors and statistics.

**TABLE 2-16** Media Events

Content	Description
sLibMediaEventCount	Number of media statistics in the table
sLibMediaEventTable	Table of media statistics
sLibMediaEventEntry	Media error statistic
sLibMediaEventIndex	Index into the media error statistic table
sLibMediaEventVolid	Volume ID of the optical barcode
sLibMediaEventDomain	Domain of the optical barcode
sLibMediaEventType	Type of the optical barcode
sLibMediaEventDriveSerialNum	Electronics serial number of the drive
sLibMediaEventDriveType	Type of tape drive
sLibMediaEventDateTime	Log entry date and time in this format: MM:DD:YYYY HH:MM:SS
sLibMediaEventEnum	Type of media error – reported as an enumeration
sLibMediaEventOccurrenceCount	Occurrence count for media statistic

## Network

**sLibNetwork** provides information about the network, such as: host names, IP addresses, gateways and netmasks, and packet transmissions.

**TABLE 2-17** Network Information

Content	Description
sNetworkCount	Count of all the Ethernet ports
sNetworkTable	Table of network interfaces
sNetworkEntry	Network interface entry
sNetworkIndex	Index into the table
sLibNetworkInterfaceName	Interface name used by the library software
sLibNetworkIpAddr	Library IP address
sLibNetworkGateway	Library network internet gateway
sLibNetworkEthAddr	Library physical 48 bit ethernet address
sLibNetworkName	Library network host name
sLibNetworkNetmask	Library network internet address netmask
sLibNetworkDhcpEnabled	DHCP IP address / name client lookup service status—SL500 only
sLibNetworkDomainName	Library network domain name
sLibNetworkPrimaryDNS	Library network's primary DNS server
sLibNetworkSecondaryDNS	Library network's secondary DNS server
sLibNetworkRXPackets	Number of packets received
sLibNetworkTXPackets	Number of packets transmitted
sLibNetworkErrors	Number of errors on this interface
sLibNetworkDropped	Number of dropped packets on this interface
sLibNetworkOverruns	Number of overrun packets on this interface
sLibNetworkFrame	Number of frame packets on this interface
sLibNetworkCollisions	Number of collisions on this interface



## Pass-thru Ports

**slPtp** provides information about pass-thru ports (PTP).

**Note** – This information is from the standard MIB for StorageTek libraries; however, the SL500 library does not have a Pass-thru Port; therefore, the information in this variable is not applicable.

**TABLE 2-18** Pass-thru Port Data

Content	Description
slPtpCount	Count of the pass-through ports in the library
slPtpTable	Table of pass-thru ports
slPtpEntry	Pass-thru port entry
slPtpIndex	Integer index into the PTP table
slPtpAddress	PTP device address
slPtpState	State of the PTP
slPtpStatusEnum	PTP operational state reported as an enumeration
slPtpSerialNumber	PTP controller serial number
slPtpPartNumber	PTP controller part number
slPtpFirmwareVersion	PTP embedded firmware version
slPtpFirmwareDate	PTP embedded firmware build date
slPtpSoftwareResetCount	Number of times the PTP firmware has been initialized
slPtpDoorOpenCount	Number of times a service door has been opened (either library)
slPtpInitializationCount	Number of times the PTP has been initialized
slPtpInoperativeCount	Number of times PTP has been inoperative
slPtpGoodCommandCount	Number of commands successfully processed by the PTP
slPtpFailCommandCount	Number of failed commands processed by the PTP
slPtpGoodEmptyMotionCount	Number of successful PTP motions with empty elements
slPtpFailEmptyMotionCount	Number of unsuccessful PTP motions with empty elements
slPtpGoodPartMotionCount	Number of successful partially populated PTP motions
slPtpFailPartMotionCount	Number of unsuccessful partially populated PTP motions
slPtpGoodFullMotionCount	Number of successful fully populated PTP motions
slPtpFailFullMotionCount	Number of unsuccessful fully populated PTP motions

**TABLE 2-18** Pass-thru Port Data (Continued)

Content	Description
slPtpCompLibNetworkIpAddr	Companion library IP Address
slPtpCompLibNetworkName	Companion library's network host name
slPtpCompLibSerialNumber	Companion library's controller serial number
slPtpCompLibPartNumber	Companion library's controller part number
slPtpCompLibVendorName	Companion library's vendor name
slPtpCompLibModelName	Companion library's model name
slPtpCompLibFirmwareVersion	Companion library's embedded firmware version
slPtpCompLibFirmwareDate	Companion library's embedded firmware build date

## Power Supply

The **slPowerSupply** variable provides information about the power supplies in the SL500 library.

**TABLE 2-19** 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 2-20** 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

## Safety Door

**slSafetyDoor** provides information about the library safety door.

**Note** – This information is from the standard MIB for StorageTek libraries; however, the SL500 library does not have a Safety Door; therefore, the information in this variable is not applicable.

**TABLE 2-21** Safety Door

Content	Description
slSafetyDoorCenterCount	Safety door center completion count
slSafetyDoorRetries	Number of total Safety Door retries
slSafetyDoorIPLs	Number of IPL's performed by the Safety Door

## Statistics

**slLibStatistics** provides statistics about functions of the library, such as: IPLs, retries, failures, mounts, puts, and gets.

**TABLE 2-22** Library Statistics

Content	Description
slLibStatsNumBoots	Number of library initializations
slLibStatsNumDoorOpens	Number of times the service door has been opened
slLibStatsNumGetRetries	Total number of get retries
slLibStatsNumGetFails	Total number of get failures
slLibStatsNumPutRetries	Total number of put retries
slLibStatsNumPutFails	Total number of put failures
slLibStatsNumLabelRetries	Total number of label read retries
slLibStatsNumLabelFails	Total number of label read failures
slLibStatsNumTargetRetries	Total number of target read retries
slLibStatsNumTargetFails	Total number of target read failures
slLibStatsNumMoves	Total number of cartridge moves
slLibStatsNumMounts	Total number of mounts
slLibStatsNumTargetReads	Total number of target reads
slLibStatsNumEmptyReads	Total number of empty cell reads
slLibStatsNumLabelReads	Total number of label reads
slLibStatsGetTotals	Sum of all Get operations of individual robots
slLibStatsPutTotals	Sum of all Put operations of individual robots
slLibStatsCumMachUptime	Cumulative machine up time in <i>seconds</i>
slLibStatsUpTimeSinceLastBoot	In seconds

## Storage

**slStorage** provides information about the storage elements, such as: cells, slots, cartridges, and labels within the library.

**TABLE 2-23** Storage Elements

Content	Description
slCellCount	Count of the storage elements in the cell table
slCellStorageFreeCells	Number of available (empty) storage cells in the library
slCellStorageRestrictedFreeCells	Number of available restricted (empty) storage cells in the library
slCellTable	Table of storage elements in the library
slCellEntry	Storage element
slCellIndex	Integer index into the storage cell table
slCellElementID	Physical Element ID / Address of the storage cell
slCellHostAccessible	Indication of host accessible status
slCellContentStatus	The status of the cell (such as EMPTY, READABLE)
slCellContentLabel	The label of the cartridge in the cell (zero length string if empty, '?????' if unreadable)
slCellContentType	The type of the cartridge in the cell (zero length string if empty)
slCellGetRetryCount	Number of get retries performed from this cell
slCellPutRetryCount	Number of put retries performed to this cell
slCellHostType	The type of cell (system, restricted, data)

## Tape Drives

`slDrive` provides information about the tape drives.

**TABLE 2-24** Tape Drive Data

Content	Description
<code>slDriveCount</code>	Count of the drives in the drive table
<code>slDriveTable</code>	Table of drives
<code>slDriveEntry</code>	Tape drive entry
<code>slDriveIndex</code>	Integer index into the drive table
<code>slDriveElementID</code>	Element ID/Address of the drive
<code>slDriveType</code>	Drive type (for example: STK9840, LTO4, DLT-S4)
<code>slDriveVendor</code>	Drive vendor (for example: STK, HP, and IBM)
<code>slDriveSerialNum</code>	Drive electronic serial number
<code>slDriveInterfaceType</code>	Drive physical data transport type
<code>slDriveID</code>	Drive SCSI ID or Fibre Port assignment
<code>slDriveState</code>	Drive state (such as: empty, loaded, needs cleaning)
<code>slDriveLED</code>	Drive Tray LED state (0=off and 1=on)
<code>slDriveStatusEnum</code>	Drive operational status in enumerated form
<code>slDriveCodeVer</code>	Drive code version
<code>slDriveVersion</code>	Drive version
<code>slDriveFirmwareVer</code>	Drive firmware version
<code>slDriveGetRetries</code>	Number of mount retries performed to the drive
<code>slDrivePutRetries</code>	Number of dismount retries performed to the drive
<code>slDriveCommandClean</code>	Signal to clean or cancel cleaning of the drive
<code>slDriveCellStatusEnum</code>	Drive cell presented as an enumeration
<code>slDriveCellStatusText</code>	Drive cell status
<code>slDriveCellContentLabel</code>	Label of the cartridge in the drive (zero length string if empty, '?????' if unreadable)
<code>slDriveCellContentType</code>	Type of cartridge in the drive (zero length string if empty)
<code>slDriveIdleSeconds</code>	Number of seconds that the drive has been idle (un-mounted)
<code>slDriveNumMounts</code>	Number of mounts to the drive
<code>slDriveFibreNodeName</code>	Drive Fibre node name

**TABLE 2-24** 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 2-25** 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





## 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.

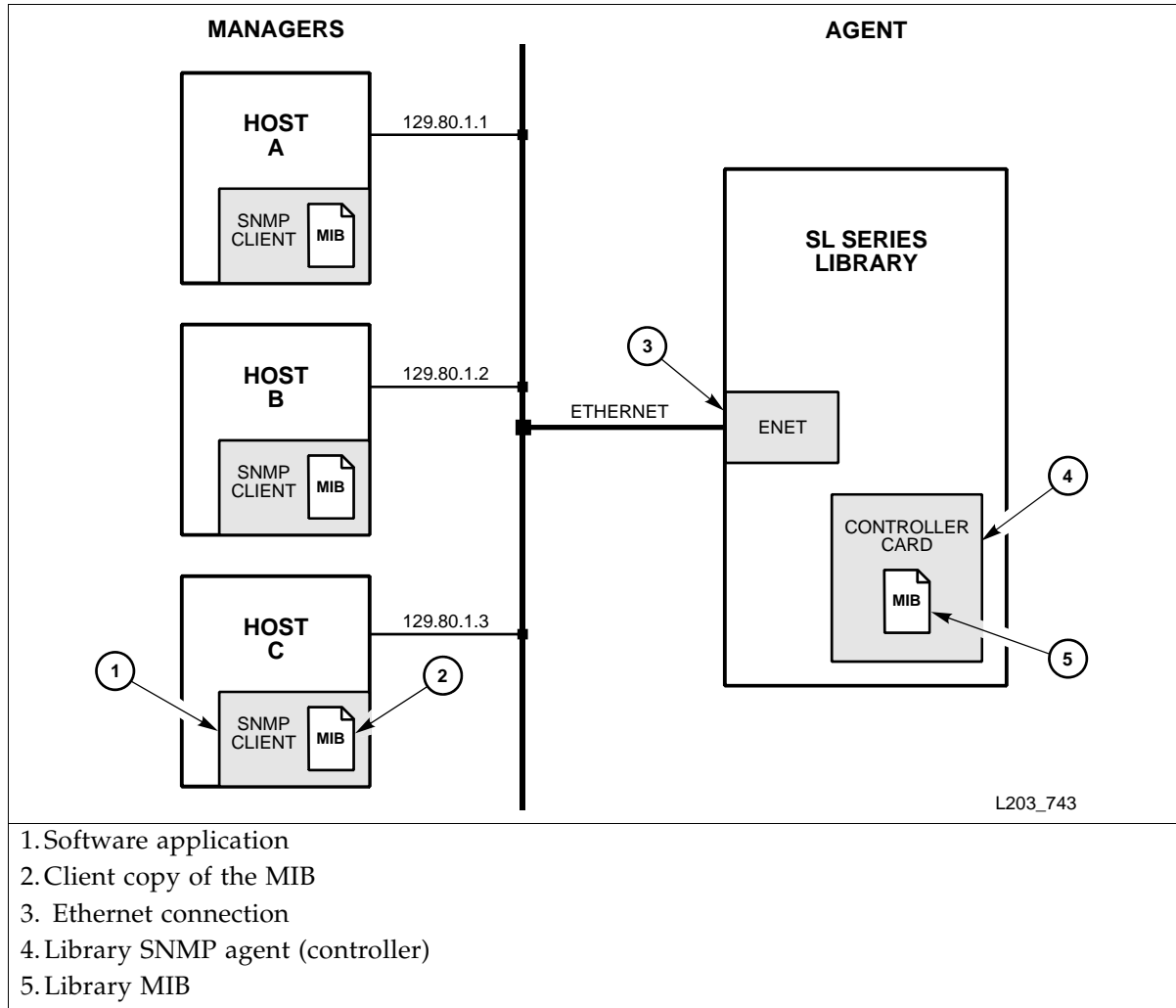
**TABLE 3-1** SNMP Default Settings

Setting	Default	Description
Port ID	Disabled	Agent trap requests are sent and received over the RLC card port: <ul style="list-style-type: none"> <li>■ 1B = standard, public port</li> </ul>
Socket number <sup>1</sup>	161	Agent requests are sent and received on the enabled port.
Socket number <sup>1</sup>	162	Traps are sent to this socket on the host port.
SNMPv2c users string <sup>2</sup>	Public	Community String Public Agent Community. Use this field (setting) to <i>read-only</i> MIB data.
SNMPv3 users string <sup>2</sup>	Empty	Community String Public Agent Community. Use this field (setting) to both <i>read</i> and <i>write</i> 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 <a href="#">page 36</a> for information.
SNMP (agent)	Disabled	Enabled or disabled through CLI command <i>only</i> .
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 2. MIB Location**



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 Transfer File 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:

```
ADVSRV>> addUser
```

- b. Configure trap recipients:

```
ADVSRV>> addTrapRecipient
```

- c. Double check that the information was entered correctly, using:

```
ADVSRV>> listTrapRecipients and
```

```
ADVSRV>> listUsers
```

- d. Enable the agent:

```
ADVSRV>> 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 44:](#)

```
ADVSRV>> 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 “authpass” instead of “authPass” 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 (*ADVSRV>>*) indicates the library login (such as MFG, Service, or Advanced Service - ADVSRV).

# Help

Using the Help command provides supporting information about the command syntax

```

ADVSRV>> 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 digit or a comma separated
list of digits 1,2,3,4,... or *
and <hostName | hostAddr> need to be fully qualified.
The engine ID shall be string of at most 31 hex characters,
preceded with 0x.
snmp addUser
    version <v2c community <communityString>
        |
        v3 name <trapUserName>
        auth <MD5 | SHA>
        authPass <authPassPhrase>
        [priv <DES | AES>
         privPass <privPassPhrase>]
snmp deleteTrapRecipient
    <id <index>
        |
        host <hostName | hostAddr>
        version <v2c community <communityString>
            |
            v3 name <trapUserName> > >
The <hostName | hostAddr> need to be fully qualified
snmp deleteUser
    <id <index>
        |
        version <v2c community <communityString>
            |
            v3 name <userName> > >
snmp disable port<portID>
snmp enable port<portID>
    where <portID> is 1B, public, or 1A
Notes:
- Ethernet ports: port1B = public, port1A = private
- Ports 2A, and 2B are currently unavailable on this library

snmp listTrapRecipients
snmp listUsers

OK
ADVSRV>>

```

## Adding Trap Recipients

```

ADVSRV>> 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 SNMPv2c to monitor four trap levels—error, warning, informational, and agent start—for an SL500 library would be:

```

ADVSRV>> 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
ADVSRV>>

```

As another example, here is this CLI entry monitoring the same trap levels, but using SNMPv3 protocol with additional “secure” parameters:

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

```
ADVSRV>> 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
ADVSRV>>
```

**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

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

Adding an SNMPv2c user to a public community string would be:

```
ADVSRV>> 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
ADVSRV>>
```

Another example of adding an SNMPv3 user with a security name of "stkAgentV3," a mixed level of security, MD5 authentication, and DES encryption, would be:

```
ADVSRV>> 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
ADVSRV>>
```



## Deleting Trap Recipients

```
ADVSRV>> 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:

```
ADVSRV>> 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
ADVSRV>>
```

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

```
ADVSRV>> 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
ADVSRV>>
```

## Deleting Users

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

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

```
ADVSRV>> snmp deleteUser id 1

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

    Failure Count 0

    Success Count 1
COMPLETED
OK
ADVSRV>>
```

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

```
ADVSRV>> 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
ADVSRV>>
```

## Disabling portID

```
ADVSRV>> snmp disable port<portID>
           disables SNMP for <portID>
```

Where: <portID> is 1A or 1B

SL500 ports: Currently, only Port 1B (or Public) provides the host connection to the library.

An example to disable Port 1B on an SL500 would be:

```
ADVSRV>> snmp disable port1B
      requestId
      requestId      53
      Device         1,0,0,0
      Success        true
      Done
Failure Count 0
Success Count 1
COMPLETED
OK
ADVSRV>>
```

### Notes:

- There is no space between the word 'port' and the value for the 'portID'. For example: `snmp disable port1B` is the correct syntax for this command. The same applies for the `snmp enable` command.
- Ethernet ports: port1B = Public, port1A = Private.

## Enabling portID

```
ADVSRV>> snmp enable port<portID>
           enables SNMP for <portID>
```

Where: <portID> is 1A or 1B

SL500 ports: Currently, only Port 1B (or Public) provides the host connection to the library.

An example to enable Port 1B on an SL500 would be:

```
ADVSRV>> snmp enable port1B
      requestId
      requestId      53
      Device         1,0,0,0
      Success        true
      Done
Failure Count 0
Success Count 1
COMPLETED
OK
ADVSRV>>
```

## Listing Trap Recipients

```
ADVSRV>> snmp listTrapRecipients
```

To list information about the trap recipients, enter:

```
ADVSRV>> 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
ADVSRV>>
```

## Listing Users

```
ADVSRV>> snmp listUsers
```

To list information about the users, enter:

```
ADVSRV>> 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
ADVSRV>>
```

## 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 ( ' ' )

```
ADVSRV>> 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:

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

# Traps, Events, and Notifications

---

This chapter lists the supported SNMP traps—also known as events or notifications—and the supporting data for the SL500 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](#), for more information.

### Organization

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

- 1 through 10 = Generic traps
  
- 11 through 20 = Agent *specific* related traps
- 21 through 100 = Device *specific* related traps
  - 21 through 27 = Library status change
  - 41 through 45 = Drive status change
  - 61 through 65 = Cartridge access port (CAP) status change
- 101 and above = Media *specific* related traps

**Note** – 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.

## 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



## 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. <i>Device inoperable:</i> Refers to the entire system. Failure of a sub-unit or redundant component is not a Category 1.	<a href="#">TABLE 4-3</a>
2	slTrapWarning	A device condition which may need attention has been encountered. <i>Device degraded:</i> Refers to recoverable failures that may allow the system to remain in use, but only in a degraded mode.	<a href="#">TABLE 4-4</a>
3	slTrapInformation	Information is presented for activity monitoring. <i>Device activity:</i> A device has reported activity. This information is used to monitor normal activity and messages.	<a href="#">TABLE 4-5</a>
4	slTrapConfiguration	Configuration information is presented. <i>Device configuratiion:</i> A device has reported configuration activity.	<a href="#">TABLE 4-6</a>

## Error Trap

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

**TABLE 4-3** Error Trap

<b>MIB Name</b>	sITrapError
<b>Level</b>	1
<b>Objects</b>	sITrapLibrarySerialNumber sITrapDeviceId sITrapDeviceTime sITrapDeviceAddress sITrapDeviceUserName sITrapDeviceInterfaceName sITrapDeviceActivity sITrapDeviceRequestId sITrapDeviceSeverity sITrapDeviceResultCode sITrapDeviceFreeFormText

## Warning Trap

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

**TABLE 4-4** Warning Trap

<b>MIB Name</b>	sITrapWarning
<b>Level</b>	2
<b>Objects</b>	sITrapLibrarySerialNumber sITrapDeviceId sITrapDeviceTime sITrapDeviceAddress sITrapDeviceUserName sITrapDeviceInterfaceName sITrapDeviceActivity sITrapDeviceRequestId sITrapDeviceSeverity sITrapDeviceResultCode sITrapDeviceFreeFormText

## Information Trap

An information trap presents information for activity monitoring.

**TABLE 4-5** Information Trap

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

## Configuration Trap

A configuration trap reports configuration activity.

**TABLE 4-6** Configuration Trap

<b>MIB Name</b>	slTrapConfiguration
<b>Level</b>	4
<b>Objects</b>	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	<a href="#">TABLE 4-8</a>
21	slTrapLibStatusGood	Library status changes to Good.	<a href="#">TABLE 4-9</a>
25	slTrapLibStatusCheck	Library status changes to a check condition (degraded, non-operational).	<a href="#">TABLE 4-10</a>
27	slTrapEnvHdwCheck	Library environmental or hardware condition changes.	<a href="#">TABLE 4-11</a>
41	slTrapDrvStatusGood	Drive status changes to Good.	<a href="#">TABLE 4-12</a>
45	slTrapDrvStatusCheck	Drive status changes to a check condition (error, warning, unknown).	<a href="#">TABLE 4-13</a>
61	slTrapCapStatusGood	CAP status changes to Good.	<a href="#">TABLE 4-14</a>
63	slTrapCapStatusOpen	CAP status changes to Open.	<a href="#">TABLE 4-15</a>
65	slTrapCapStatusCheck	CAP status changes to a check condition (error, warning, unknown).	<a href="#">TABLE 4-16</a>

## Agent Boot Date

An SNMP agent starts.

**TABLE 4-8** Agent Boot (Start) Date

<b>MIB Name</b>	sIAgentBootDate
<b>Level</b>	11
<b>Objects</b>	sIAgentBootDate

## Library Status Good

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

**TABLE 4-9** Library Status Good

<b>MIB Name</b>	sITrapLibStatusGood
<b>Level</b>	21
<b>Objects</b>	sILibraryTopLevelCondition sILibStkBaseModel sILibSerialNumber

## 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

<b>MIB Name</b>	sITrapLibStatusCheck
<b>Level</b>	25
<b>Objects</b>	sILibraryTopLevelCondition sILibStkBaseModel sILibSerialNumber

## Environmental Hardware Check

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

**TABLE 4-11** Environmental Hardware Check

<b>MIB Name</b>	slTrapEnvHdwCheck
<b>Level</b>	27
<b>Objects</b>	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

<b>MIB Name</b>	slTrapDrvStatusGood
<b>Level</b>	41
<b>Objects</b>	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

<b>MIB Name</b>	slTrapDrvStatusCheck
<b>Level</b>	45
<b>Objects</b>	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

<b>MIB Name</b>	sITrapCapStatusGood
<b>Level</b>	61
<b>Objects</b>	sLibSerialNumber sCapState sCapAddress

## CAP Status Open

This trap sent when a CAP status changes to Open.

**TABLE 4-15** CAP Status Open

<b>MIB Name</b>	sITrapCapStatusOpen
<b>Level</b>	63
<b>Objects</b>	sLibSerialNumber sCapState sCapAddress

## 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

<b>MIB Name</b>	sITrapCapStatusCheck
<b>Level</b>	65
<b>Objects</b>	sLibSerialNumber sCapState sCapAddress



# 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 Sun StorageTek 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” on page 32](#) 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 Entries on page 34](#) and
- [Configure the SNMP Service Information on page 37](#)

# 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 SL500 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 SL500 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 SL500 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: resu  
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:** sITrapWarning  
**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:** sITrapInformation  
**Category:** status alarms  
**Severity:**  
normal (green)  
**Message:** Trapped an informational message. Variables: \$\*

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

**Event name:** sITrapAgentStart  
**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

**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: \$\*

## 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 Sun StorageTek 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](#)” on [page 32](#) 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 Sun StorageTek service representative log in and use the:
  - [Command Line Interface Entries](#) on [page 34](#) and
  - [Configure the SNMP Service Information](#) on [page 37](#)

## 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” on page 63](#).

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

---

## A

- access control, 7
- add trap recipient, 36
- add users, 38
- additional variables, 10
- address, street location, 9
- administrative password, 7
- agent, 11
  - firmware versions, 11
- architecture, SNMP, 1
- ASCII text file, 2
- authentication algorithms, 12
- authentication protocol, 33, 55, 61

## B

- barcode, 21
- basic variables, 9

## C

- cartridges, 21, 27
- cell table, 27
- cells, 20, 27
- city, 9
- CLI
  - service information settings, 44
  - SNMP commands, 31
- commands, list, 6
- communications protocol, 5
- config print, 44
- config serviceInfo set, 44
- config serviceInfo set entries, 44
- configurations
  - service information, 44
- configurations, default settings, 31
- controller, 15

- country, 9

## D

- data cartridges, 21
- date, 9
- default settings, 31
- delete trap recipients, 39
- disable port ID, 41
- door, safety, 25
- drives, 28

## E

- enable port ID, 41
- encryption algorithms, 12
- encryption, capabilities in SNMP, 7
- errors
  - media, 21
- Ethernet ports, 22

## F

- Fibre ports, 29
- filters, recipients, 11
- firmware versions, 7
- framework for SNMP, 1

## G

- gateway, 22
- gateways, IP addresses, 22

## H

- HandBots, 25
- hardware data, 17
- host interfaces, 17

## I

IETF, 3  
Internet Engineering Task Force, 3  
inventory, 19

## L

labels, 19, 21, 27  
library  
    contents, 19  
    controller data, 15  
    inventory, 19  
    location, 9  
    model number, 9  
    state, 19  
    storage elements, 27  
library configuration data, 20  
library default settings, 31  
library statistics, 26  
library storage modules, 19  
list trap recipients, 42  
list users, 43  
location, 9  
LSM configuration, 20

## M

managed device, 1  
management information base, 2, 5  
Management Information Base. *See* MIB  
management station, description, 1  
manager, description, 1  
media, 21  
MIB  
    additional variables, 10  
    basic variables, 9  
    description, 8  
    hierarchy, 8

## N

netmasks, 22  
network, 22  
notifications  
    description, 6  
    destinations, 33, 55, 61

## O

object identifiers, 5  
organization  
    trap levels, 45  
overview of SNMP, 1

## P

pass-thru ports, 23  
PDUs, 6  
physical hardware data, 17  
ports, 29  
ports, UDP, 4  
protocol comparisons, TCP/IP and OSI, 4  
protocol data units, 6  
PTPs, 23

## R

recipients, 11  
Request for Comments, 3  
required versions, 7  
RFCs, 3  
robotic data, 25

## S

safety door, 25  
security levels, 12  
service information settings, 44  
Simple Network Management Protocol, 1  
slAgentTrapRecipientV3, 12  
slots, 20, 27  
SNMP  
    access control, 7  
    agent, 6  
    architecture, 1  
    configuration, 31  
    default settings, 31  
    definition, 1  
    MIB diagram, 8  
    settings, 31  
    terms, 67  
    trap organization, 45  
    versions, 3  
state of the library, 19  
statistics, 26  
storage elements, 27

StreamLine library settings, 31  
street address, 9

## T

TallBots, 25  
tape cartridges, 21  
tape drives, 28  
    quantity, 20  
time-of-day, 9  
TOD, 9  
transports, 28  
trap  
    description, 6  
    destinations, 33, 55, 61  
trap recipients table, 11  
traps  
    agent, 11  
    agents, 11  
    configuration, library, 20  
    controller, 15  
    date, 9  
    doors, safety, 25  
    filter, 11  
    library configuration, 20  
    library data, 9  
    library location, 9  
    library statistics, 26  
    location, 9  
    network, 22  
    pass-thru ports, 23  
    PTPs, 23  
    recipients, 11  
    robotic data, 25  
    safety door, 25  
    statistics, library, 26  
    storage, 27  
    time-of-day, 9  
    version 2 agents, 11  
    version 3 agents, 12  
    versions, 29

## U

UDP, 4  
UDP port recipients, 11  
UDP ports, 4  
user datagram protocol, 4

## V

variables, 9, 10  
version 2 agents, 11  
version 3 agents, 12  
versions, 3, 29  
VOLID, 21

## Z

ZIP code, 9







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