CHAPTER 1

SNMP Overview

Simple Network Management Protocol (SNMP) is the protocol governing network management and monitoring of network devices. This guide describes how to use SNMP to manage and monitor the Cisco MDS 9020 Fabric Switches. Specifically, this reference describes the SNMP agent that resides on the switch.

The following topics are covered in this chapter:

SNMP Interface Objectives

The objectives of the SNMP Interface are as follows:

- Connect to the SNMP agent that resides on the switch using a management workstation.
- Support of Fabric Element Management Information Bases (FE-MIB) (rfc2837) and Fibre Alliance Management Information Bases (FA-MIB) draft.
- Support of version 1 and 2 traps.
- The SNMP agent supports SNMPv1 and SNMPv2c.

Manager and Agent

The two primary elements of SNMP are:

- Manager - the application that runs on the management workstation.
- Agent - the daemon application that runs on the switch.

The manager is the application through which the network administrator performs network management functions. The SNMP agent is the direct interface on the switch for any SNMP manager connecting to the switch using the SNMP protocol. The agent will be started by the script files responsible for switch initialization when the switch powers up or when the switch is reset.

When an SNMP request arrives at the agent, the agent will compose a message and pass it on to Switch Management to process the message and provide a response to the agent. The agent then provides a response to the originator of the SNMP request. The SNMP agent does not have direct access to the internal database of the switch.

Traps

Traps are notification messages sent from the switch to a registered manager when a change of state occurs within the switch. A change of state can be an alarm condition or simply a configuration change. The Fibre Alliance MIB defines a trap table configurable through SNMP. A trap table may have up to 5 entries, and can be configured using the SNMP manager, the Cisco MDS 9000 Family FabricWare software, or the command-line interface.

A trap event is reported when the incoming error has a severity level less than or equal to the configured severity level. The trap event types and trap severity levels are listed in Table 1-1.

Table 1-1 Trap Severity Levels

Event Type	Severity Level
Unknown	1
Emergency	2
Alert	3
Critical	4
Error	5
Warning	6
Notify	7
Info	8
Debug	9
Mark	10

Management Information Base

Management Information Bases (MIBs) define the properties of the managed object within the device to be managed. Every managed device keeps a database of values for each definition written in the MIB. It is not the actual database itself; it is implementation dependant. Definition of the MIB conforms to the Structure of Management Information (SMI) given in Request For Comment (RFC) 1155. The latest Internet MIB is given in RFC 1213, and is sometimes called MIB-II.

User Datagram Protocol

Cisco MDS 9020 Fabric Switches support the following User Datagram Protocol (UDP) settings:

- Agents “listen” on UDP port 161.
- Responses are sent back to the originating Network Management Station (NMS) port from a dynamic port, although many agents use port 161 also for this target.
- The maximum SNMP message size is 65,507 octets (maximum UDP message size).
- The minimum receive packet size for SNMP implementations is 484 octets in length.
- Agent and Network Monitoring Systems are responsible for determining error recovery.

Numbering System Conventions

The conventions for numbering systems in this guide are as follows:

- Decimal = 101
- Hexadecimal = 0x101
- Binary = 101b