Vicom SVE Service Manual For SUN Solaris Platform

SUN RELEASE

Document Identification:
Number: 310-606187

Preliminary Release: 2.5.3
November 15, 2001

Copyright

This document (and the information herein) is the property of Vicom Systems, Inc. It may not be copied or reproduced in whole or in part, or used or revealed to any person in any manner except to meet the purposes for which it was delivered. Additional rights and obligations regarding this document and its contents may be defined by a separate written agreement with Vicom Systems, Inc., and if so, such agreement shall be controlling.

Vicom reserves the right to make improvements and/or changes to this manual without incurring an obligation to incorporate such changes or improvements in units previously sold or shipped. This document has been carefully reviewed, but Vicom cannot be held responsible for unintentional errors or omissions. It is provided “as is” without express or implied warranty.

Vicom Systems Inc. 47281 Bayside Parkway Fremont, CA 94538	http://www.vicom.com ph: (510) 743 - 1130 fx: (510) 743 - 1131

Trademarks

SV Engine™, SV SAN Builder™, SV Zone Manager™, SV SNMP Agent™, Call Home™, and Instant Copy™ are trademarks of Vicom Systems, Inc.

Solaris® is a registered trademark of Sun Microsystems Corp.

Sun® is a registered trademark of Sun Microsystems Corp.

UNIX® is a registered trademark in the United States and other countries, exclusively licensed through X/ Open Company, Ltd.

Windows NT® is a registered trademark of Microsoft Corporation.

Adaptec® is a registered trademark of Adaptec, Inc.

Ethernet® is a registered trademark of Xerox.

CONTENTS

LIST OF FIGURES

PREFACE

Document Overview

The *Vicom SVE Service Manual For UNIX* describes troubleshooting and maintenance for the SVE 2.5/UNIX platform. This document, references the command line interface (CLI) and does not reference the graphical user interface (GUI), which designed for Windows. Information for the CLI can be found in *SV SAN Builder* - *Installation and User Guide and SV Zone Manager* - *Installation and User Guide*.

This document is designed for system administrators who have a working knowledge of the UNIX operating system. And is designed to be used in concert with all publication listed in "Related Publications" on page 13.

Chapter Overview

Chapter 1 provides an overview of the various SAN configurations using SVE 2.5 and UNIX platform.

Chapter 2 describes possible problems and solutions that may occur within the system.

Chapter 3 describes the maintenance of the SV Router FC-FC 3.

Chapter 4 describes the maintenance of the SV SAN Builder software.

Chapter 5 describes the maintenance of the SV Zone Manager software.

Chapter 6 describes the maintenance of the SV SNMP Manager software.

Chapter 7 describes the maintenance of all other components within a basic SAN configuration.

Chapter 8 provides a description of the basic commands that are used in this manual.

Appendix A provides a list of service numbers (SRNs and SNMP) and corrective action for each.

Appendix B provides a list of port numbers for communication.

Appendix C provides a list and corrective action for service codes.

Typographic Conventions

Typeface	Meaning	Examples
`AaBbCc 123`	• commands • files • on-screen computer inputs	• **`vdiskpool create`** • **`/svengine/sdus/svengine.cfg`** • type **`default`**
AaBbCc 123	Manual titles	*Vicom Systems' SV SAN Builder – Installation and User Guide*
blue font with quotes (pdf format only)	Hyperlink to another section of the manual	"SVE System Architecture" on page 16
blue font without quotes (pdf format only)	• Hyperlink to glossary • Hyperlink to Chapters	• SAN • Chapter 1

Related Publications

Vicom SV Router FC-FC 3 – Installation and User Guide (SUN RELEASE)	prt no. 310-606155
Vicom SV SAN Builder – Installation and User Guide (SUN RELEASE)	prt no. 310-605154
Vicom SV Zone Manager – Installation and User Guide (SUN RELEASE)	prt no. 310-605156
Vicom SV SNMP Agent – Installation and User Guide (SUN RELEASE)	prt no. 310-606157

Service and Support

Please fill out and mail or fax the warranty registration card furnished with the SV Router FC-FC 3 as soon as possible. Each installation must be registered in order to qualify for technical support.

Vicom provides 24x7x365 support. Customers may call: 1-877-868-4266 or 510-743-1427.

At any time, customer may request support via email at support@vicom.com. Responses to requests will be made during the following business day.

Before You Start

This manual relies heavily on the manuals of other devices. You should have on hand all manuals associated with each device used in the configuration of you storage system.

Feedback

In an effort to improve our products and documentation, Vicom wants to hear from its customers. Please send your feedback to:

customerfeedback@vicom.com

CHAPTER 1

INTRODUCTION

This chapter provides an overview of the SVE 2.5 system and configuration. It enables users to have a finer understanding of the detailed information in subsequent chapters.

- SVE System Architecture
- SAN Overview

SVE System Architecture

SVE is designed to provide advanced storage features, centralized management, and dynamic scalability and configuration of the SAN without effecting normal operations. SVE is composed of at least one hardware unit (SV Router FC-FC 3) and up to three software units (SV SAN Builder 2.5, SV Zone Manager 2.5, SV SNMP Agent 1.0).

The SV SAN Builder software builds, configures and maintains the SAN. The SV Zone Manager builds, configures, and maintains the zones. The SV SNMP Agent monitors the SAN and forwards the information to the SNMP manager. The SLIC deamon enables all communication between software and router. The daemon is installed and configured using the SAN Builder software. The software and the daemon reside in the remote management server(s), which manages up to 32 independent SANs.

Vicom's storage virtualization function enables an administrator to allocate storage on demand without disrupting normal operations. The SV Router, at the request of Vicom software, dynamically carves disk arrays or JBODs into smaller more manageable drives called virtual drives. Another part of Vicom's storage virtualization function is zoning, which enables an administrator to dynamically map an HBA to a specified drive. This allows an individual server or multiple servers access to an individual drive or to multiple drives, and prohibits unwanted server access to the same drive(s). Other SV Router features include disk mirroring (RAID 1), and disk concatenation.

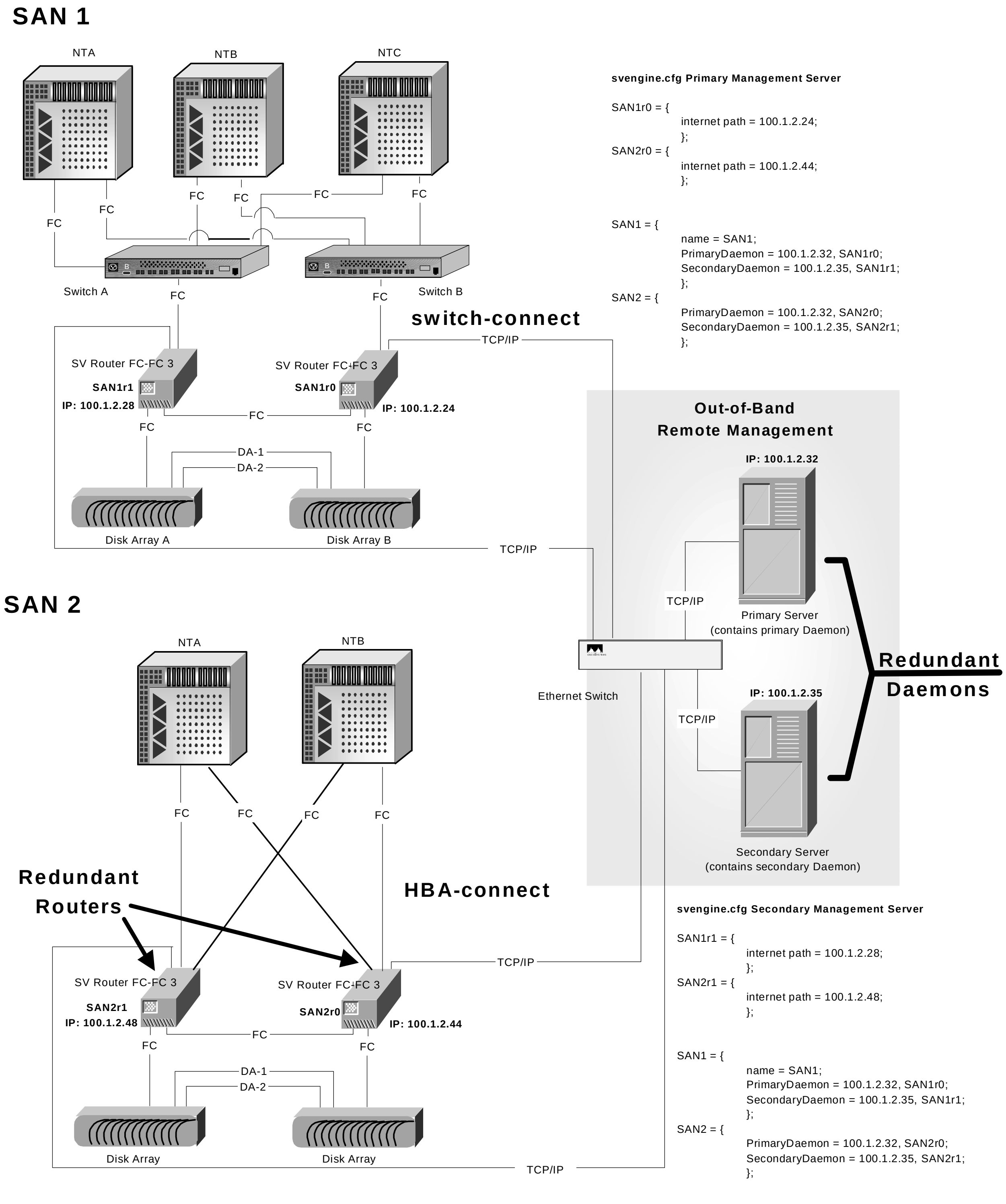
Note: *Certain configurations may or may not support the features listed above. For a detailed list of supported configurations, see Vicom Certified Solutions - Installation Guide series or contact your Vicom sales representative.*

SAN Overview

A SAN can be configured without redundancy, with partial redundancy, or with full redundancy. A fully redundant system is designed with redundant components throughout. Each component, within the system, performs a specific function. Each data server contains dual Host Bus Adapters (HBA) and software that supplies data path redundancy, as well as load balancing which equally spreads I/O through both HBAs. Switches permit multiple host attachment to the SV Routers. The redundant Vicom SV Routers enable remote management and monitoring of the SAN and the storage subsystem. The remote manager also provides redundancy. Because the SLIC daemon is the primary communication means between the remote manager and the SAN, its operation must not be disrupted. Therefore, a secondary server can be used for failover. It will be used for daemon failure, for daemon upgrades, or for adding additional SANs.

The following graphics on page 16 and 17 demonstrate various SAN configurations; redundant and standalone router configuration, redundant and standalone daemon configuration, HBA-connect and switch-connect. Without redundant routers the SAN is considered a standalone router configuration. With redundant routers the SAN is considered a redundant router configuration. For an HBA-connect, the SV Router connects directly to the server and can connect up to two servers. For a switch-connect, the router connects directly to a switch and can connect up to sixteen servers per router. Although placed between the data source and the destination source little or no reduction in throughput occurs.

Figure 1-1 Fully Redundant SVE System



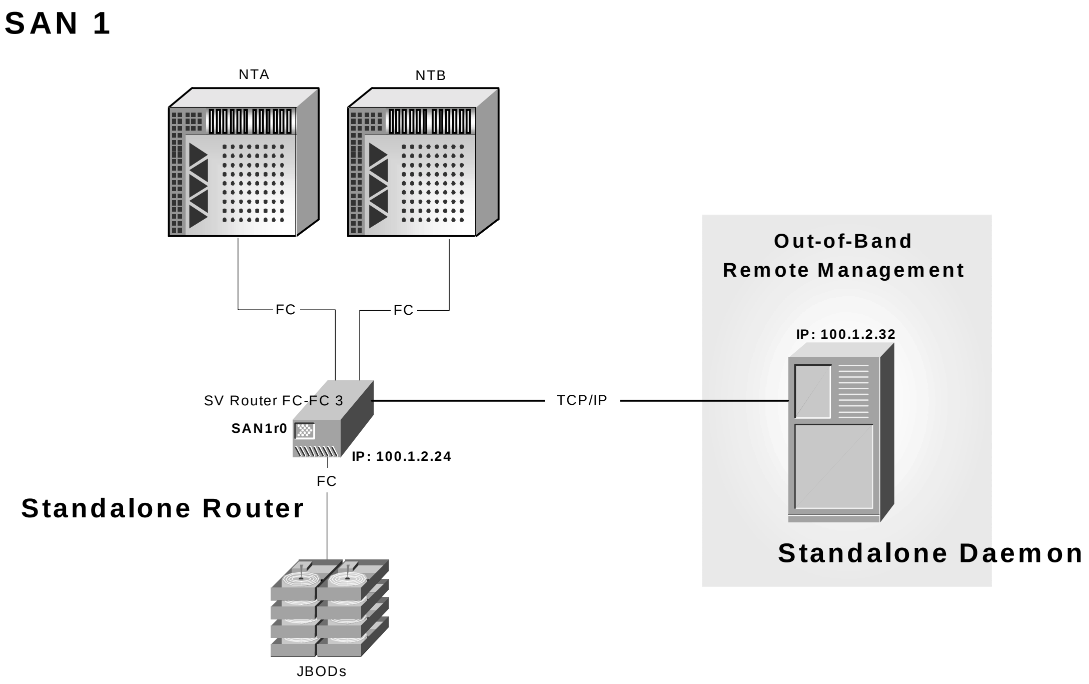
svengine.cfg Primary Management Server

```
SAN1r0 = {
                internet path = 100.1.2.24;
                };
SAN2r0 = {
                internet path = 100.1.2.44;
                };


SAN1 = {
                name = SAN1;
                PrimaryDaemon = 100.1.2.32, SAN1r0;
                SecondaryDaemon = 100.1.2.35, SAN1r1;
                };
SAN2 = {
                PrimaryDaemon = 100.1.2.32, SAN2r0;
                SecondaryDaemon = 100.1.2.35, SAN2r1;
                };
```

svengine.cfg Secondary Management Server

```
SAN1r1 = {
                internet path = 100.1.2.28;
                };
SAN2r1 = {
                internet path = 100.1.2.48;
                };


SAN1 = {
                name = SAN1;
                PrimaryDaemon = 100.1.2.32, SAN1r0;
                SecondaryDaemon = 100.1.2.35, SAN1r1;
                };
SAN2 = {
                PrimaryDaemon = 100.1.2.32, SAN2r0;
                SecondaryDaemon = 100.1.2.35, SAN2r1;
                };
```

Figure 1-2 Nonredundant SVE System



CHAPTER 2

SYSTEM DIAGNOSTICS

This chapter explains how to diagnose a system failure. It includes the following sections:

- Service Sources
- Retrieving Service Information
- Troubleshooting Process

Service Sources

Only the SAN and the storage subsystem are monitored by Vicom’s SVE. The SAN and the storage subsystem consist of the following:

- SV Router
- Storage subsystem or JBODs.
- Cabling among SV Router and storage.

Service Request Numbers

The service request numbers are employed to inform the user of storage subsystem activities. The SRNs are sent to:

- the SV SAN Builder.
- the SV SNMP manager.

Service and Diagnostic Codes

The SV Router’s service and diagnostic codes are employed to inform the user of subsystem activities. The codes are presented as an LED readout. See "Service Codes" on page 147 for the table of codes and actions to take. In some cases, you may not be able to receive SRNs or SNMP traps because the path is obstructed. If this occurs, you must read the SV Router LEDs to determine the problem. See "SV Router LEDs" on page 24 for information on LED reading.

Retrieving Service Information

SV SAN Builder

Once the SV SAN Builder program is installed, it is the SLIC daemon that communicates between the client and the SAN. The SLIC daemon periodically polls the SV Router for all subsystem errors and for topology changes. It then passes this information in the form of an SRN to the Error Log file.

Error Log Analysis Commands

Use the Error Log Analysis commands to analyze the error log and display the appropriate Service Request Numbers (SRN) for errors that need action. Data is returned in the following format:

```
TimeStamp:nnn.Txxxxx.uuuuuuuu  SRN=mmmmm
TimeStamp:nnn.Txxxxx.uuuuuuuu  SRN=mmmmm
TimeStamp:nnn.Txxxxx.uuuuuuuu  SRN=mmmmm
```

Time Stamp — Time and date when error occurred.

nnn — The name of the SLIC (already defined by user).

Txxxxx — The drive where the error occurred.

Note: Txxxxx may represent a physical drive or a logical drive.

uuuuuuuu — The unique ID of the drive or SV Router.

SRN=mmmmm — The SRN defined in numerical order (see "SRN and SNMP Reference" on page 141).

Accessing Error Log Analysis

1. Power on the management server and open a terminal.
2. Ensure the daemon is running. If not, see "Start and Stop Daemon" on page 66 if necessary.
3. Change to the sduc directory.

Example:

```
#/svengine/sduc
```

4. Using the **`Error Log Analysis`** command, display the error log file.
5. Determine corrective action by comparing the SRNs with the "SRN and SNMP Reference" on page 141.

SNMP Manager

The SNMP manager receives SRNs (Service Request Numbers) and trap messages sent from the Vicom SNMP Agent. Accessing the SRNs, depends on the type of SNMP manager that you use. Refer to your SNMP manager's user manual for more information. Determine corrective action by comparing the SRNs with the "SRN and SNMP Reference" on page 141.

SV Router LEDs

SV Router LEDs are shown in Figure 2-1. LED codes are listed in Table 2-1. Two LEDs located on the back of the router echo the functions of the Status and Fault LEDs (Figure 3-2).

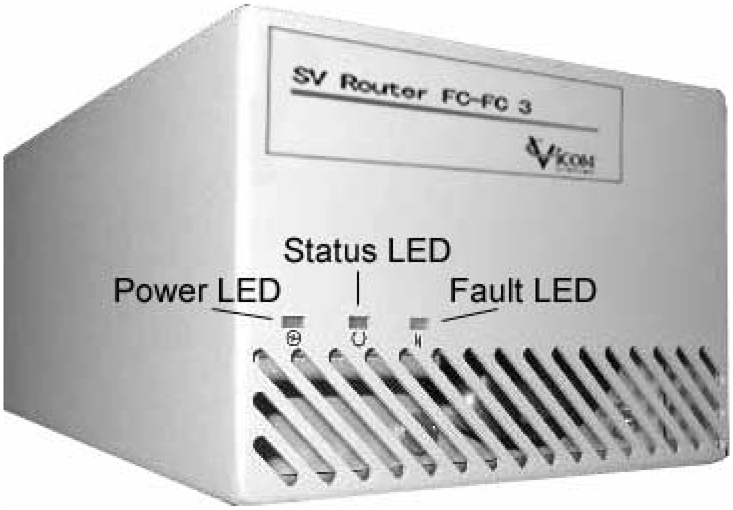
- Power LED (green)
  - When the Power LED is Solid On, it indicates that the SV Router is powered on.
- Status LED (green)
  - Solid on - normal operating mode.
  - Blink service code - A number of blinks to indicate a decimal number. The Status LED will blink a service code when the Fault LED is Solid On.

- Fault LED (amber) - when lit, the fault LED indicates a serious problem. Decipher the blinking of the status LED to determine the service code Reading Service and Diagnostic Codes below. Once you determine read out of the LED then look up the decimal number of the service code in“Appendix C: "Service Codes" on page 147.

Power LED (green)	Status LED (green)	Fault LED (amber)	Description
Solid On	Blinks Code	Solid On	Service Codes

Table 2-1 LED Quick Reference

Figure 2-1 Front Panel SV Router - LED Locations



Reading Service and Diagnostic Codes

Decimal numbers are presented by the Status LED. Each decimal number is represented by the number of blinks in series followed by a medium duration (two seconds) of LED Off.

0:	Fast Blink
1:	LED blinks once
2:	LED blinks twice, with one short duration (one second) between blinks
3:	LED blinks three times, with one short duration (one second) between each blink
. . .	
10:	LED blinks ten times, with one short duration (one second) between each blink

After the blink code presentation, a long duration (four seconds) of LED Off will follow, then the sequence will repeat. Figure 2-2 gives an example of blink code 060.

Rapid/fast blink	Medium Duration 2-seconds	Blinks 6 times Short duration between each blink	Medium Duration 2-seconds	Rapid/fast blink
0	OFF	6	OFF	0

Long Duration 4 - Seconds
OFF

Rapid/fast blink	Medium Duration	Blinks 6 times Short duration between each blink	Medium Duration	Rapid/fast blink
0	OFF	6	OFF	0

Figure 2-2 Example of Blink Code 060

Ethernet Port LEDs

Ethernet port LEDs are shown in Figure 2-1. They indicate the link’s speed, activity, and validity.

- Speed LED (amber)
  - Solid On - the link is 100base-TX.
  - Off - the link is 10base-T.
- Link/Activity LED (green)
  - Solid on - a valid link established.
  - Blink - normal operation, indicating data activity.

FC Link Error Status Report

Both the SV Router FC-FC 3's host-side and the device-side interfaces provide statistical data for the following:

- Link Failure Count

  This count reports the number of times the SV Router's Frame Manager detects a not operational state or other failure of N_Port initialization protocol.

- Loss of Synchronization Count

  This count reports the number of times that the SV Router detects a loss in synchronization.

- Loss of Signal Count

  This count reports the number of times that the SV Router's Frame Manager detects a loss of signal.

- Primitive Sequence Protocol Error

  This count reports the number of times that the SV Router's Frame Manager detects N_Port protocol errors.

- Invalid Transmission Word

  This count reports the number of times that the SV Router 8B/10B decorder did not detect a valid 10-bit code.

- Invalid CRC Count

  This count reports the number of times that the SV Router received frames with a bad CRC and a valid EOF. A valid EOF includes EOFn, EOFt, or EOFdti.

Checking FC Link Error Status

The SV Router’s power must be cycled to reset the counter. Therefore, you should check the accumulation of errors between a fixed time as detailed in the following steps:

1. Use the **`svstat`** command to take a reading. A Status report is given fo the host side ports and the device side ports.

Example:

```
sduc/svstat -d SANr1 -t i1
```

Note: *There are two host-side connectors and two device-side connectors. They are the interface for one host-side port and one device-side port.*

2. Within a few minutes, take another reading.
3. The number of new errors that occurred within that time frame represents the number of link errors.
4. If there is a high error rate on either the host-side or device-side port, check GBIC, switch, or cable. These are the most likely culprits. If you have replaced the host-side GBIC, switch and cable, and you have not found the problem then check the data server’s HBA. If the problem still exist then replace the SV Router, and check the Link Error Status again.

Figure 2-3 Example FC Link Error Status Report

```
I00001 Host Side FC Vital Statistics:
Link Failure Count                 1
Loss of Sync Count                 0
Loss of Signal Count               0
Protocol Error Count               0
Invalid Word Count                 18
Invalid CRC Count                  0


I00001 Device Side FC Vital Statistics:
Link Failure Count                 0
Loss of Sync Count                 0
Loss of Signal Count               0
Protocol Error Count               0
Invalid Word Count                 138
Invalid CRC Count                  0
```

Troubleshooting Process

Remote Manager Can Not Access SAN

If the Remote Manager can not access SAN, check for the following possibilities.

1. Cabling between remote management and SV Router down. See "Check Cabling and Connectors" on page 109 and "Ethernet Port LEDs" on page 26
2. Ethernet switch/HUB down.
   - Visually inspect Ethernet switch/HUB to determine if it is functioning properly.
   - If the switch/HUB is a strong suspect, but it still has power and if a spare Ethernet switch/HUB exist, swap it out and see if the remote manager can access the system.
3. SV Routers are powered off.
4. Access denied by the SV Router.
   - Check the SV Router's IP address. Ensure the same address is used in the SLIC daemon's config file and in the SV Router. While checking the SV Router's IP address, also check to ensure the subnet mask, and the gateway addresss are correct.
     - To check the SV Router, the subnet mask and the gateway IP address, see "Configure SV Router's Ethernet Settings" on page 57.
     - To check the config file, see "Daemon SignOn Path" on page 68.
   - Check the remote management server's IP address. Ensure the same address is used in the SLIC daemon's config file and in the SV Router.
     - To check the SV Router, see "Enable Daemon SignOn" on page 52.
     - To check the config file, see "Daemon SignOn Path" on page 68.
   - Ensure that the SignOn Path is correct. See "Daemon SignOn Path" on page 68.
   - Ensure that you have enable access of the SV Router by the daemon. See "Enable Daemon SignOn" on page 52.
   - Ensure that the remote management server's IP address is not blocked by the SV Router, see "Enable Password for Daemon SignOn" on page 53.

- Check daemon’s SignOn password. Ensure the same password is used in the SV Router, and in the password text file. Also ensure that the path to the text file, which is located in the config file, is correct.
    - To check the SV Router, see "Enable Password for Daemon SignOn" on page 53.
    - If you do not know the path or file name used to create the text file, see "Password Protection for Daemon-Router Communication" on page 71.

Other Problems

To determine problems within the SAN, access error message from the following locations.

- To check SNMP messages, see "SNMP Manager" on page 24. SNMP messages usually come with corrective action. If further help is needed, see "SRN/SNMP Single Point of Failure Table" on page 144.
- To retrieve SRNs, see "Service Request Numbers" on page 22. To determine action, see "SRN and SNMP Reference" on page 141.
- To check service code message, see "SV Router LEDs" on page 24. For further information, see “Appendix C: "Service Codes" on page 147.
- To check Link Errors, see "Checking FC Link Error Status" on page 28. Link Errors should be checked if you receive any abnormal FC events.

Because the SV Router only monitors activity between it and the storage, then problems concerning the activity between drives in a disk array, the data servers, and the switches, will not be reported by the SV Router. However, most devices contain an SNMP agent. Activate the agent in each device and monitor the entire system from the same SNMP manager.

CHAPTER 3

SV ROUTER MAINTENANCE

A Vicom developed hardware module in SVE, which serves as the fundamental building block in a SAN. It provides storage management functions that enable a Fibre Channel host to interface with, and control all storage-related elements in a SAN.

This chapter explains maintenance of the SV Routers within the system. It includes these sections:

- SV Router Communication Channels
- SV Router Microcode
- SV Router Replacement
- Clear SAN Database
- Emergency Recovery
- SV Router Configuration

SV Router Communication Channels

Associated manual: *SV Router FC-FC 3 – Installation and User Guide.*

The SV Router provides four methods of communication listed below. Each is password protected. This section explains how to establish each communication channel except for the SLIC daemon. The SLIC daemon is part of the SV SAN Builder software and all information pertaining to it can be found in, "SV SAN Builder and Daemon" on page 59.

- SLIC daemon
- Serial Port
- Telnet session
- FTP session

Serial Port Connection

Through this interface, you can:

- view SV Router settings, and vital product data.
- view disk status, and LUN mapping.
- download SV Router microcode.
- restrict local and remote daemon and server access and establish SV Router heartbeat.
- clear the error log file.
- configure the SV Router's three interfaces (host, device, and Ethernet).
- erase the SAN database table of the SV Router.

Necessary Components

- Computer (laptop recommended) with either PROCOMM PLUS or Window Hyperterminal installed. Vicom does not supply these components.
- DB9 serial port cable (must be purchased separately).

Set up Serial Port Communication Software

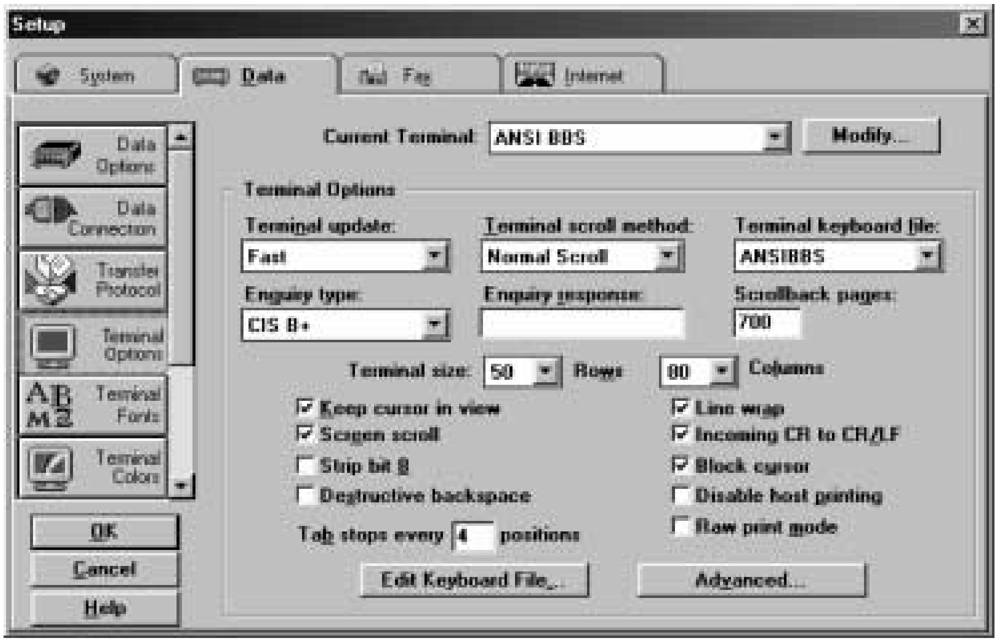
- The computer running the communication software will be used to configure each router's interface settings (host-side, device-side, and Ethernet).
- Associated manual: *SV Router FC-FC 3 – Installation and User Guide*.

Configure PROCOMM PLUS Communication Software

Install PROCOMM PLUS following the installation process in the PROCOMM PLUS manual.

1. Select **Setup** from the menu bar.
2. Select **Setup** from the pull-down menu.
3. Select the **Data** tab from the Setup dialog box.
4. Select the **Transfer Protocol** button.
5. Select **Xmodem** from the pull-down menu of the Current Transfer Protocol list.
6. Select the **Data Connection** button.
7. Select **57600** from the pull-down menu of the Modem Default Baud Rate list.
8. Select the **Terminal Options** button.
9. Ensure all settings match Figure 3-1 'PROCOMM PLUS Terminal Options Setting' below, and select the **OK** button.

Figure 3-1 PROCOMM PLUS Terminal Options Setting



Current Terminal: ANSI BBS

Terminal Options

Terminal update: Fast

Terminal scroll method: Normal Scroll

Terminal keyboard file: ANSIBBS

Enquiry type: CIS B+

Enquiry response:

Scrollback pages: 700

Terminal size: 50 Rows 80 Columns

☑ Keep cursor in view
☑ Screen scroll
☐ Strip bit 8
☐ Destructive backspace

Tab stops every 4 positions

☑ Line wrap
☑ Incoming CR to CR/LF
☑ Block cursor
☐ Disable host printing
☐ Raw print mode

Configure Windows Hyperterminal Communication Software

If necessary, install Windows Hyperterminal following the installation process in the Windows Hyperterminal manual.

Note: Windows Hyperterminal normally is included with Windows NT and Windows 98 operating systems.

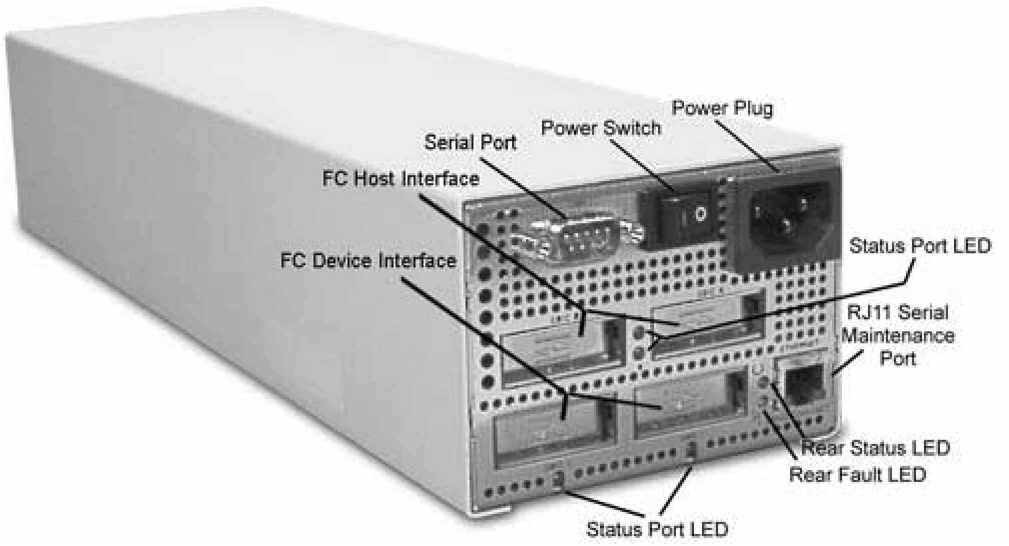
1. Select **File** from the menu bar.
2. Select **Properties** from the pull-down menu.
3. Select the **Change Icon** button.
4. Enter the name of the connection in the **Name** box, user defined.
5. Select the **OK** button.
6. Select the **Connect To** tab.
7. Select **Direct to Com1** from the pull-down menu of the Connect Using list.
8. Select the **Configure** button.
9. Select **57600** from the pull-down menu of the Bits per seconds list.
10. Select **8** from the pull-down menu of the Data bits list.

11. Select **None** from the pull-down menu of the Parity list.
12. Select **1** from the pull-down menu of the Stop bits list.
13. Select **None** from the pull-down menu of the Flow control list.
14. Select the **OK** button.
15. Select the **Settings** tab.
16. Select **VT100** from the pull-down menu of the Emulation list.
17. Select the **Terminal Setup** button.
18. Select **132 column mode** box.
19. Select **ASCII** from the pull-down menu of the Character set list.
20. Select the **ASCII Setup** button.
21. Select **Append line feeds to incoming line end** box and deselect all others.
22. Select the **OK** button.

Access Serial Port

1. Using a DB9 serial port cable, attach the serial port of the laptop computer, which contains the communication software, to the serial port of the SV Router.

Figure 3-2 SV Router Rear Interface



2. Power on the computer.

3. Using the AC power cord, plug the router into an 120VAC outlet and power on the SV Router.

4. Start the communication software. To configure communication software, see "Set up Serial Port Communication Software" on page 33.

5. Open the communication terminal and enter **hello**.

6. Enter **?** to display the following menu:

```
User Service Utility Key Assignments:

'?': Show User Service Utility Key Assignments Menu

'1': Show VPD

'2': Show LUN Map

'3': Download SVE Microcode from Local Computer

'4': View/Change Response to SV Router Management Programs

'5': Clear Error Log

'6': View/Change Interface Configuration

'9': Clear SAN Database

'B': Reboot Router

'Q': Quit Serial Port Service Utility
```

Telnet Session

Using a telnet session, you can have full access to the *User Service Utility* program.

You must configure the SV Router's Ethernet settings using the serial port before you can begin a telnet session. To configure the Ethernet port via the serial port, follow the steps below:

1. Access the *User Service Utility* program via the serial port interface and configure the Ethernet settings. See "Access Serial Port" above.

2. Open the *User Service Utility* menu and enter the number '6'

   ```
   '6': View/Change Interface Configuration
   ```

3. Enter the appropriate information for the following:

   - IP address.
   - Subnet mask.
   - Default gateway.
   - Server port number (5000-65535).
   - Password (up to 10 characters).

4. Press the enter button to accept the information, which you entered.

Establish Telnet Session

1. Using a management computer, enter the **`telnet`** command and the SV Router's IP address.

Example

```
mgtserver# telnet 10.1.1.200
```

2. If you assigned a password when configuring the Ethernet settings in the User Service Utility, enter it now. If you did not, press the enterkey. The User Service Utility menu should appear.

FTP Session

You must configure the SV Router's Ethernet settings using the serial port before you can begin an ftp session. To configure the Ethernet port, see "'Telnet Session"above.

To download the SV Router's microcode is the only legal activity for an ftp session.

1. Using a management computer, enter the **`ftp`** command and the SV Router's IP address.

Example

```
mgtserver# ftp 10.1.1.200
```

2. When prompted to login or enter a user name, enter **`vicomftp.`**

3. If you assigned a password when configuring the Ethernet settings in the User Service Utility, enter it now. If you did not, press the enterkey.

SV Router Microcode

- Approved Microcode Version 8.01.03 or later
- Related publication: *SV Router FC-FC 3 - Installation and User Guide*.

Determine SV Router Microcode Version

There are two ways to determine the router's microcode version; use the CLI or the *User Service Utility* menu (access to this menu can be gained via serial port or telnet) .

Command Line Interface

1. Start the daemon if not already running. See "Start and Stop Daemon" on page 66 if necessary.
2. Using the **svpd** command, view both SV Routers' microcode. See "Displaying VPD (Vital Product Data) [svpd]" on page 127.

Example

```
svpd –d SAN1r0 -t i1

svpd -d san1r0 -t i2r
```

Telnet

1. Telnet SV Router. See ""Telnet Session" on page 37 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. Enter **1** to show the router's VPD. The VPD will display the SV Router's microcode version.

SV Router Microcode Upgrade

1. Stop I/O to the SV Router. If it is a redundant router configuration, then stop I/O to the primary daemon's router.
2. Using the SV SAN Builder command **`sdnld,`** download the routers' microcode.

Example

```
sdnld –d SAN1r0 –f /svengine/microcode/microcode.new -t i1
```

3. SV Router will reboot automatically. Wait until the SV Router is fully initialized (green LED in rear solid-on), then resume I/O.
4. This completes a standalone router configuration. If you are using a redundant router configuration, complete steps 5 and 6.
5. Stop I/O to the secondary daemon's SV Router.
6. Repeat step 2-3 for secondary daemon's SV Router.
7. Perform T3 failback if necessary. See "T3 Disk Array Failback Procedure" on page 96.

SV Router Replacement

Indicators for SV Router Replacement

Because of the possible problems that can occur from improper router replacement, we strongly recommend that you contact Vicom before proceeding.

The following conditions indicate SVE hardware failure:

- After powering unit, LEDs do not light.
- Five seconds after powering unit, power LED lights but status and fault LED do not.
- Thirty seconds after power unit, both status and fault LED remain solid on.
- Service codes are also used to determine router replacement. See “Appendix C: Service Codes” for a list of service code and corrective action. See "Reading Service and Diagnostic Codes" on page 25 for information on retrieving service codes.

Replace Standalone Router

Because of the possible problems that can occur from improper router replacement, we strongly recommend that you contact Vicom before proceeding.

1. Stop I/O from data servers to the SV Router.
2. Power on the replacement SV Router.
3. Clear the SAN Database of the replacement routers. See "Clear SAN Database" on page 47 for directions.
4. Using the serial port, configure the SV Router’s settings. Use the same settings as the previous router. See "SV Router Configuration" on page 54 for configuration information.
5. Power off the replacement SV Router.
6. Power off and remove the failed SV Router.
7. Cable the replacement router to the system. Do not cable to the data server’s FC HBAs.
8. Power on the SV Router.
9. The daemon must be configured to talk with that router. See "Daemon SignOn Path" on page 68.

10. Start the daemon in the management server. See "Start Daemon" on page 66.

11. Using the **sanconfig write** command, download the drive configuration to the replacement router. See "Writing SAN Configuration File to SV Router" on page 122.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m
physical logical
```

12. After the download, cycle SV Router power.

13. Ensure the green LED is solid-on in the front of the powered-on SV Router.

14. Use the **showmap** command to view drive configurations and ensure they are restored. See "Listing Device Connections [showmap]" on page 113 for more information.

Example

```
showmap -d SAN1r0
```

15. Using the **sanconfig read** command, save the SAN configuration to file. See "Reading SAN Configuration File and Saving to File" on page 121 for more information.

Example

```
sanconfig read -d SAN1r0 -e /svengine/SANconf/T3SAN.san
```

16. Connect the data server FC HBAs to the replacement routers.

17. Using the **sadapter view** command, ensure the HBAs see the SV Router. See "Viewing Host Adapter Properties" on page 130 for more information.

Example:

```
sadapter view -d SAN1r0 -r I1
sadapter view -d SAN1r0 -r I2
```

18. Replacement is complete.

19. Using the **sanconfig read** command, save the SAN configuration to file.

20. Perform T3 failback if necessary. See "T3 Disk Array Failback Procedure" on page 96.

21. If you are running Vertias Volume Manager with DMP, type **vxdctl enable** to enable Veritas path. This should be done on each data server.

Replace One Router of a Redundant Pair

Because of the possible problems that can occur from improper router replacement, we strongly recommend that you contact Vicom before proceeding.

1. Using the **slicview** command, determine and record the offline SV Router's initiator number (I00001, I00002 etc.) The information will be used later. See"Viewing SV Router Zone Components [slicview]" on page 129 for more information.

Example

```
slicview view -d SAN1r0
```

2. Power on the replacement SV Router.

3. Clear the SAN Database of the replacement router. See "Clear SAN Database" on page 47 for directions.

4. Using the serial port, configure the replacement SV Router's settings. See "SV Router Configuration" on page 54 for configuration information.

5. Power off and remove the failed SV Router.

6. Power off the replacement SV Router.

7. Cable the replacement SV Router to the system. Do not cable to the data server's FC HBAs.

8. Power on the replacement SV Router. When powered on the new SV Router will download the SAN database from the existing router. However, it will not download its zone configuration. You must do this manually.

9. Using the **slicview** command, determine and record the new SV Router's initiator number.

10. Using the **sanconfig import** command, import zone configuration to the replacement SV Router. See "Importing SAN Zone Configuration" on page 123 for more information.

Example

```
sanconfig import -d SAN1r0 -e /svengine/SANconf/T3SAN.san -r i3 -j
i2
```

Usage

```
-r i3               new replacement router

-j i2               old failed router
```

Note: *The initiator numbers I00001 and I00002 can be written without zeroes (I1, I2, etc.)*

11. Power off the SV Router, and connect data server FC HBAs to the new SV Router.

12. Power on SV Router.

13. Using the **slicview view** command, view the router zone configuration information to ensure that all zones were assigned to their designated HBAs.

14. Using the **sadapter view** command, ensure the HBA sees its assigned drives. See "Viewing Host Adapter Properties" on page 130 for more information.

Example:

```
sadapter view -d SAN1r0 -r I2
```

15. Using the **sanconfig read** command, save SAN configuration in file. See "Reading SAN Configuration File and Saving to File" on page 121 for more information.

Example

```
sanconfig read -d SAN1r0 -e /svengine/SANconf/T3SAN.san
```

16. Replacement is complete.

17. Perform T3 failback if necessary. See "T3 Disk Array Failback Procedure" on page 96.

18. If you are running Vertias Volume Manager with DMP, type **vxdctl enable** to enable Veritas path. This should be done on each data server.

Replace Both SV Routers

Because of the possible problems that can occur from improper router replacement, we strongly recommend that you contact Vicom before proceeding.

1. Stop I/O from data servers to SV Routers.
2. Power on both replacement SV Routers.
3. Clear the SAN Database of both replacement routers. See "Clear SAN Database" on page 47 for directions.
4. Using the serial port, configure both SV Router's settings. Use the same settings as the previous routers. See "SV Router Configuration" on page 54 for configuration information.
5. Power off both replacement SV Routers.
6. Power off and remove both failed SV Routers.
7. Cable both replacement routers to the system. Do not cable to the data server's FC HBAs.
8. Power on only one SV Router.
9. The daemon must be configured to talk with that router. See "Daemon SignOn Path" on page 68.
10. Start the daemon in the management server. See "Start Daemon" on page 66.
11. Using the **sanconfig write** command, download the drive configuration to the replacement router. See "Writing SAN Configuration File to SV Router" on page 122.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m
physical logical
```

12. After the download, cycle SV Router power.
13. Ensure the green LED is solid-on in the front of the powered-on SV Router. Then power on the second SV Router.
14. Use the **showmap** command to view drive configurations and ensure they are restored. See "Listing Device Connections [showmap]" on page 113 for more information.

Example

```
showmap -d SAN1r0
```

15. Using the **sanconfig read** command, save the SAN configuration to file. See "Reading SAN Configuration File and Saving to File" on page 121 for more information.

Example

```
sanconfig read -d SAN1r0 -e /svengine/SANconf/T3SAN.san
```

16. Connect the data server FC HBAs to both replacement routers.

17. Using the **sadapter view** command, ensure the HBA sees both SV Routers. See "Viewing Host Adapter Properties" on page 130 for more information.

Example:

```
sadapter view -d SAN1r0 -r I1
sadapter view -d SAN1r0 -r I2
```

18. Replacement is complete.

19. Using the **sanconfig read** command, save the SAN configuration to file.

20. Perform T3 failback if necessary. See "T3 Disk Array Failback Procedure" on page 96.

21. If you are running Veritas Volume Manager with DMP, type **vxdctl enable** to enable Veritas path. This should be done on each data server.

Clear SAN Database

Clear SAN Database of a Standalone Router

Using this proceedure you may clear the SAN database of a standalone router in the SAN, or you may clear the SAN database of a router that is not connected to the SAN.

1. Stop I/O from data servers to SV Routers.
2. Telnet to one of the SV Routers, or use its serial port.
   - See ""Telnet Session" on page 37 for information on telnetting the router.
   - See "Access Serial Port" on page 36 for information on accessing serial port.
3. Enter the password. The *User Service Utility* menu will appear.
4. Enter 9 to Clear the SAN database. This will place the SV Router in a suspended state.
   - A successful command will read **`“SAN database has been cleared!”`** and service code 060 will flash.
   - An unsuccessful command will result in service code 051.
5. To take the SV Router out of the suspended state, cycle the SV Router’s power, or using the *User Service Utility* menu, reboot the SV Router.

Clear SAN Database of Mulitple Routers - Local Access

Clearing the SAN database of one router in a multi-router SAN, will not clear the SAN database stored in the other routers because each router is designed to import the SAN database from the other routers in the SAN.

Using this procedure you may clear the SAN database of a router in the SAN with mulitple routers. To clear the SAN database using local access, follow the directions below:

1. Stop I/O from data servers to the SV Routers.
2. Power off one router.
3. Telnet to one of the SV Routers, or use its serial port.
   - See "'Telnet Session" on page 37 for information on telnetting the router.
   - See "Access Serial Port" on page 36 for information on accessing serial port.
4. Enter the password. The *User Service Utility* menu will appear.
5. Enter 9 to Clear the SAN database. This will place the SV Router in a suspended state.
   - A successful command will read **`“SAN database has been cleared!”`** and service code 060 will flash.
   - An unsuccessful command will result in service code 051.
6. After the download is complete, power off the router.
7. Power on the other router.
8. Telnet to one SV Router, or use its serial port.
9. Enter the password. The *User Service Utility* menu will appear.
10. Enter 9 to Clear the SAN database.
11. Power off the SV Router.
12. You have now, using local access, cleared the SAN database in both SV Routers.

Clear SAN Database of Multiple Routers - Remote Access

Clearing the SAN database of one router in a multi-router SAN, will not clear the SAN database stored in the other routers because each router is designed to import the SAN database from the other routers in the SAN.

Using this procedure you may clear the SAN database of a router in the SAN with mulitple routers. To clear the SAN database using remote access, follow the directions below:

1. Stop I/O from data servers to the SV Routers.
2. Telnet to one of the SV Routers. See "'Telnet Session" on page 37 for information on telnetting the router.
3. Enter the password. The *User Service Utility* menu will appear.
4. Enter 9 to Clear the SAN database. This will place the SV Router in a suspended state.
   - A successful command will read **`“SAN database has been cleared!”`** and service code 060 will flash.
   - An unsuccessful command will result in service code 051.
5. Telnet to the other SV Router.
6. Enter the password. The *User Service Utility* menu will appear.
7. Enter 9 to Clear the SAN database.
8. At this point, both routers are in a suspended state. If there are more routers sharing the same backbone, then repeat steps 5-7 for each remaining SV Router.
9. Telnet each SV Router and using the *User Service Utility* menu reboot (Item B) each one.
10. You have now, using remote access, cleared the SAN database in multiple SV Routers sharing the same backbone.

Emergency Recovery

Single Router Configuration

1. Stop I/O from data servers to SV Router.

2. To perform emergency recovery:

    - with local access, use the *User Service Utility* menu to clear the SAN database. Then, cycle the router's power.

    - with remote access, telnet to the SV Router and use the *User Service Utility* menu to clear the SAN database. The SV Router will enter a suspended state, and it will flash service code 060. Then, use the *User Service Utility* menu to reboot the router. See "Establish Telnet Session" on page 38 for instructions on establishing a telnet session.

3. Start the daemon in the management station. See "Start and Stop Daemon" on page 66.

4. Using the **sanconfig write** command download the offline SAN configuration file to the SV Router. This will restore all of the drive configurations (mirror drives, virtual drives, etc.) from the last write, as well as any zone configurations (Zones, SV Domains, etc.). The physical SAN configuration must be exactly the same as it was when the backup was taken. If you do not select a -m option, the default (all three options) will be used. See "Writing SAN Configuration File to SV Router" on page 122 for parameters.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m
```

5. Use the **showmap** command to view drive configurations and ensure they are restored. See "Listing Device Connections [showmap]" on page 113 for more information.

Example

```
showmap -d SAN1r0
```

6. Using the **sadapter view** command, ensure the HBA sees both SV Routers. See "Viewing Host Adapter Properties" on page 130 for more information.

Example:

```
sadapter view -d SAN1r0 -r I1
sadapter view -d SAN1r0 -r I2
```

7. Recovery is complete.

Redundant Router Configuration Local Access

1. Stop I/O from data servers to SV Routers.

2. Power off both SV Routers.

3. Start the daemon in the management station. See "Start and Stop Daemon" on page 66.

4. Power on only one SV Router, clear its SAN database, and power off the router. See "Clear SAN Database" on page 47 if necessary.

5. Power on the other router, clear its SAN database, and cycle power.

   At this point, you should have cleared the SAN database in both routers and one router should be powered on.

6. Start the daemon in the management station. See "Start and Stop Daemon" on page 66.

7. Using the **sanconfig write** command, download the offline drive configuration file to the SV Router. This will restore all of the drive configurations (mirror drives, virtual drives, etc.) The physical setup must be exactly the same as it was when the backup was taken. See "Writing SAN Configuration File to SV Router" on page 122 for parameters.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m
physical logical
```

8. After the download, cycle SV Router power.

9. Ensure the green LED is solid-on in the front of the powered-on SV Router. Then power on the second SV Router. At this point, the second router will download the SAN database from the first router.

10. Use the **showmap** command to view drive configurations and ensure they are restored. See "Listing Device Connections [showmap]" on page 113 for more information.

Example

```
showmap -d SAN1r0
```

11. Using the **sanconfig write** command, download the offline zone configuration file to one SV Router. This will restore all of the zone configurations to both routers.The physical setup must be exactly the same as it was when the backup was taken. See "Writing SAN Configuration File to SV Router" on page 122 for parameters.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m zone
```

12. Using the **sadapter view** command, ensure the HBA sees both SV Routers. See "Viewing Host Adapter Properties" on page 130 for more information.

Example:

```
sadapter view -d SAN1r0 -r I1
sadapter view -d SAN1r0 -r I2
```

13. Recovery is complete.

14. Perform T3 failback if necessary. See "T3 Disk Array Failback Procedure" on page 96.

15. Enable dual multipathing if necessary. This should be done on each data server.

Redundant Router Configuration Remote Access

1. Stop I/O from data servers to SV Routers.

2. Telnet to one SV Router and use the *User Service Utility* menu to clear the SAN database. The SV Router will enter a suspended state, and it will flash service code 060. See "Establish Telnet Session" on page 38 for instructions on establishing a telnet session.

3. Start the daemon in the management station. See "Start and Stop Daemon" on page 66.

4. Using the **sanconfig write** command, download the offline drive configuration file to the functioning SV Router. It will overwrite the SAN database in the router, and restore all of the drive configurations (mirror drives, virtual drives, etc.) The physical SAN configuration must be exactly the same as it was when the backup was taken. See "Writing SAN Configuration File to SV Router" on page 122 for parameters.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m
physical logical
```

5. After the download is complete, use the *User Service Utility* menu in the suspended router and reboot it. When this router begins functioning, it will download the configuration file from the functioning router.

6. Use the **`showmap`** command to view drive configurations and ensure they are restored. See "Listing Device Connections [showmap]" on page 113 for more information.

Example

```
showmap -d SAN1r0
```

7. Using the **`sanconfig write`** command, download the offline zone configuration file to one SV Router. This will restore all of the zone configurations to both routers.The physical setup must be exactly the same as it was when the backup was taken. See "Writing SAN Configuration File to SV Router" on page 122 for parameters.

Example:

```
sanconfig write -d SAN1r0 -e /svengine/SANconf/T3SAN.san -m zone
```

8. Using the **`sadapter view`** command, ensure the HBA sees both SV Routers. See "Viewing Host Adapter Properties" on page 130 for more information.

Example:

```
sadapter view -d SAN1r0 -r I1
sadapter view -d SAN1r0 -r I2
```

9. Recovery is complete.

10. If this is a T3 configuration, perform T3 failback. See "T3 Disk Array Failback Procedure" on page 96.

11. Enable dual multipathing if necessary. This should be done on each data server.

SV Router Configuration

The following information is for basic router configuration. See *Vicom Certified Solutions - Installation Guide* series for special configurations or to learn more about each setting See *SV Router FC-FC 3 - Installation and User Guide*.

Enable Daemon SignOn

To configure this features using a telnet session you must first enable Ethernet access. This can only be done by configuring the Ethernet settings via the router's serial port. After you have established Ethernet access all edits or configurations can be done using a telnet session For detailed information on telnetting or accessing the router's serial port, see "SV Router Communication Channels" on page 32.

1. Enter the password. The *User Service Utility* menu will appear.
2. Enter **4** to View and/or Change Response to Router Management Programs.
    - Enable the Router Management Program Access.
    - 1/2 = Modify Host WWN Authentications.
        - Use escape to void access.
    - 3/4 = Modify IP Authentications.
        - Enter **3** and type the primary remote management server's IP address.

          This router will be the SignOn path of the primary daemon.
        - Enter **4** and enter 0.0.0.0 to block other servers from accessing this router.

          If you run a redundant router configuration, you will not enter the IP address of the secondary server in this router. You will enter it in the other router to allow the secondary daemon to SignOn through the secondary router. This process enables a secondary SignOn path.

Enable Password for Daemon SignOn

To configure this features using a telnet session you must first enable Ethernet access. This can only be done by configuring the Ethernet settings via the router's serial port. After you have established Ethernet access all edits or configurations can be done using a telnet session For detailed information on telnetting or accessing the router's serial port, see "SV Router Communication Channels" on page 32.

1. Enter the password. The *User Service Utility* menu will appear.
2. Enter **4** to View and/or Change Response to Router Management Programs.
   - Y/N = Enable/Disable Password Protection.
     - Enter **Y** to enable password protection.
     - Password protection in the daemon's config file is explained in ‘Configure Security Features’ on page 71.
   - A/I = Assign/Invalidate Password.
     - Enter **A** and type a password. This password must be the same password used in the daemon's config file.

Establish Heartbeat Between SV Routers

For a redundant router configuration, the user must establish a heartbeat between routers. To configure this features using a telnet session you must first enable Ethernet access. This can only be done by configuring the Ethernet settings via the router's serial port. After you have established Ethernet access all edits or configurations can be done using a telnet session For detailed information on telnetting or accessing the router's serial port, see "SV Router Communication Channels" on page 32.

Enter the password. The *User Service Utility* menu will appear.

3. Enter **4** to View and/or Change Response to Router Management Programs.
   - Enter **O** and type the other router's IP address. This establishes a heartbeat between the routers.

TroubleShooting
If you received a notice that this function is not supported, then you have the wrong microcode installed. • Go to ‘SV Router Microcode Upgrade’ on page 40 to update microcode.

   - Enter **V** and ensure that the settings are correct.

Configure SV Router’s Device-Side

To configure this features using a telnet session you must first enable Ethernet access. This can only be done by configuring the Ethernet settings via the router’s serial port. After you have established Ethernet access all edits or configurations can be done using a telnet session For detailed information on telnetting or accessing the router’s serial port, see "SV Router Communication Channels" on page 32.

1. Enter the password. The *User Service Utility* menu will appear.

2. Enter **6** to View and/or Change Interface Configuration

```
**** WARNING! ****
Upon committing to any changes made from the following menus,
the router will reboot and any active I/Os will be lost.
Continue? (Y/N) Y
```

3. Enter **D** to configure the router’s device side.

   - Enter **R** to ensure default settings are entered. Default settings are listed below:

```
Operating Mode:
        Current: Arb Loop mode.
                Loop id ==> take soft AL_PA
        Default: Arb Loop mode.
                Loop id ==> take soft AL_PA



Options:
        P = toggle Loop/Point-to-point mode
        L = set Loop ID (only if in Loop mode)
        ? = show settings as changed
        R = restore defaults
        <Esc> = restore entry settings (discard changes)
        <Enter> = accept and exit



Configure which interface?
        D = Device Side
        H = Host Side
        E = Ethernet
        <Enter> = doneList default settings
```

   - Press the **Enter** key to accept changes to the device side.
   - Press the **Enter** key to accept changes to all the router interfaces.

Caution ! ***If you reboot the router before saving your changes the second time, the changes will not be saved.***

Configure SV Router’s Host-Side

To configure this features using a telnet session you must first enable Ethernet access. This can only be done by configuring the Ethernet settings via the router’s serial port. After you have established Ethernet access all edits or configurations can be done using a telnet session For detailed information on telnetting or accessing the router’s serial port, see "SV Router Communication Channels" on page 32.

1. Enter the password. The *User Service Utility* menu will appear.

2. Enter **6** to View and/or Change Interface Configuration

   **** WARNING! ****

   Upon committing to any changes made from the following menus,

   the router will reboot and any active I/Os will be lost.

   Continue? (Y/N) Y

3. Enter **H** to configure the router’s host side.

   - Toggle **P** until you Set Operating Mode to **Pt-to-pt mode**.

     ```
     Operating Mode:
     Current: Pt-to-pt mode.
     Default: Arb Loop mode.
     ```

   - Press the **Enter** key to accept changes to the host side.

   - Press the **Enter** key to accept changes to all the router interfaces.

Caution ! ***If you reboot the router before saving your changes the second time, the changes will not be saved.***

Configure SV Router's Ethernet Settings

To configure this features using a telnet session you must first enable Ethernet access. This can only be done by configuring the Ethernet settings via the router's serial port. After you have established Ethernet access all edits or configurations can be done using a telnet session For detailed information on telnetting or accessing the router's serial port, see "SV Router Communication Channels" on page 32.

1. Enter the password. The *User Service Utility* menu will appear.
2. Enter **6** to View and/or Change Interface Configuration

```
**** WARNING! ****
Upon committing to any changes made from the following menus,
the router will reboot and any active I/Os will be lost.
Continue? (Y/N) Y
```

3. Enter **Y** to continue.
4. Enter **E** to configure the router's Ethernet settings.
   - Enter **A** and type the IP address of this router.
   - Press the **Enter** key.
   - Enter **M** and type the IP network's subnet mask address.
   - Press the **Enter** key.
   - Enter **G** and type the gateway IP address**.**
   - Press the **Enter** key.
   - Enter **N** and ensure default port number = 25000.
   - Enter **P** and type a password if you desire an added step of protection from unauthorized access by others ftping or telneting to this router.
   - Press the **Enter** key.
   - Press the **Enter** key to accept changes to the Ethernet settings.
   - Press the **Enter** key to accept changes to all the router interfaces.

Caution ! ***If you reboot the router before saving your changes the second time, the changes will not be saved.***

CHAPTER 4

SV SAN BUILDER AND DAEMON

Vicom SV SAN Builder software creates virtual drives and logical drives. Logical drives include composite drive, mirror drive, general spare, and Instant Copy.

This chapter explains maintenance of the SV SAN Builder and the SLIC daemon within the system. It includes these sections:

- Determine SV SAN Builder Software Version
- SV SAN Builder Installation
- SV SAN Builder Upgrade
- Start and Stop Daemon
- Edit Daemon Config File
- Text Files for Daemon Config File
- Update Daemon Config File

Determine SV SAN Builder Software Version

1. Read the SV SAN Builder CD label that was sent with the SV Router FC-FC 3.

   - Software versions should be 2.5 or later.

2. If you cannot find the SV SAN Builder CD, then boot up the management server. It should contain the software program.

3. Using most commands plus ‘--’ will display the SV SAN Builder Version.

Example

```
#/svengine/sduc/svpd --
```

4. To upgrade SV SAN Builder, see "SV SAN Builder Upgrade" on page 67.

SV SAN Builder Installation

Important Information

Related publication: *SV SAN Builder – Installation and User Guide.*

- SV SAN Builder installs:
  - The SLIC Daemon (or more commonly called daemon).
  - The Command Line Interface.

SUN Solaris Installation Server Package

The server package installs the daemon software.

1. Login as root.
2. Insert the Vicom SVE software module v.2.5 in the CD-ROM drive.
3. Mount the CD-ROM.
4. Type **`pkgadd -d . SUNWveser`**, and press enter. The default directory is **`/svengine`**.

   If the installation was successful, the following message is displayed; **`Installation of <SUNWveser> was successful.`**

Automated Daemon Reboot

This program forces the daemon to start automatically after server reboot.

To install:

1. Login as root.
2. Insert the Vicom SVE software module v.2.5 in the CD-ROM drive.
3. Mount the CD-ROM and change to that directory.
4. Type **`cdrom/<CD_name>/slicd_autostart install`**, and press enter.

Note: svengine.cfg must be properly configured before running the daemon. See "Edit Daemon Config File" on page 69 for more information.

To uninstall:

1. Login as root.
2. Insert the Vicom SVE software module v.2.5 in the CD-ROM drive.
3. Mount the CD-ROM.
4. Type **`cdrom/<CD_name>/slicd_autostart uninstall`**, and press enter.

SUN Solaris Installation Client Package

The client package installs only the application software (SV SAN Builder and SV Zone Manager). This may be installed on the management server that will run the daemon. To provide remote access to the management server, you may also install the client package on a server sharing the same network as the management server.

1. Login as root.
2. Insert the Vicom SVE software module v.2.5 in the CD-ROM drive.
3. Mount the CD-ROM.
4. Type **`pkgadd -d . SUNWveclt`**, and press enter. The default directory is **`/svengine`**.

   If the installation was successful, the following message is displayed: **`Installation of <SUNWveclt> was successful.`**

SUN Solaris Installation Reference Manual Package

The reference manual package installs only the man page software.

1. Login as root.
2. Insert the Vicom SVE software module v.2.5 in the CD-ROM drive.
3. Mount the CD-ROM.
4. Type **`pkgadd -d . SUNWveman`**, and press enter. The default directory is **`/svengine`**.

   If the installation was successful, the following message is displayed: **`Installation of <SUNWveman> was successful.`**

SUN Solaris Uninstall Server Package

This removes the server package, containing the daemon software.

- Type **`pkgrm SUNWveser`**, and press enter.

  If successful, the following message is displayed: **`Removal of <SUNWveser> was successful.`**

SUN Solaris Uninstall Client Package

This removes the client package, containing the application software (SV SAN Builder and SV Zone Manager).

- Type **`pkgrm SUNWveclt`**, and press enter.

  If successful, the following message is displayed: **`Removal of <SUNWveclt> was successful.`**

SUN Solaris Uninstall Reference Manual Package

This removes the reference manual package.

- Type **`pkgrm SUNWveman`**, and press enter.

  If successful, the following message is displayed: **`Removal of <SUNWveman> was successful.`**

SUN Solaris Server Package Information

Use this command to determine if the package is installed or to display package details.

- Type pkgparam -l SUNWveser, and press enter.

If successful, a message similar to the following is displayed:

```
CLASSES='none'
BASEDIR='/'
PKG='SUNWveser'
NAME='Vicom SVE Software Module -- Server Package'
DESC='Vicom Server, SVE module'
PRODNAME='Virtualization Engine'
PRODVERS='2.5'
VERSION='2.5, REV=2001.11.01.118'
ARCH='sparc'
CATEGORY='application'
VENDOR='Sun Microsystems, Inc.'
HOTLINE='Please contact your local service provider'
EMAIL=''
MAXINST='1000'
PSTAMP='sagem01122034'
PKGINST='SUNWveser'
INSTDATE='Nov 01 2001 18:06'
```

SUN Solaris Client Package Information

Use this command to determine if the package is installed or to display package details.

- Type **pkgparam -l SUNWveclt**, and press enter.

```
CLASSES='none'
BASEDIR='/'
PKG='SUNWveclt'
NAME='Vicom SVE Software Module -- Client Package'
DESC='Vicom Client, SVE module'
PRODNAME='Virtualization Engine'
PRODVERS='2.5'
VERSION='2.5, REV=2001.11.01.118'
ARCH='sparc'
CATEGORY='application'
VENDOR='Sun Microsystems, Inc.'
HOTLINE='Please contact your local service provider'
EMAIL=''
MAXINST='1000'
PSTAMP='sagem01122055'
PKGINST='SUNWveclt'
INSTDATE='Nov 01 2001 18:09'_)Fr ARCH='sparc'
CATEGORY=
```

Sun Solaris Reference Manual Package Information

Use this command to determine if the package is installed or to display package details.

- Type **pkgparam -l SUNWveman**, and press enter.

```
CLASSES='none'
BASEDIR='/'
PKG='SUNWveman'
NAME='Vicom SVE Software Module -- Reference Manual Package'
DESC='Vicom Reference Manual, SVE module'
PRODNAME='Virtualization Engine'
PRODVERS='2.5'
VERSION='2.5, REV=2001.11.01.118'
ARCH='sparc'
CATEGORY='application'
VENDOR='Sun Microsystems, Inc.'
HOTLINE='Please contact your local service provider'
EMAIL=''
MAXINST='1000'
PSTAMP='sagem01122317'
PKGINST='SUNWveman'
INSTDATE='Nov 01 2001 18:09'
```

SV SAN Builder Upgrade

Important Information

- Do not remove the old version of SV SAN Builder. The new version of SV SAN Builder will install over the old version.
- The daemon does not need to be shut down when installing SV SAN Builder in a remote client host.

Upgrade with Standalone Daemon

1. Stop the daemon. See "Start and Stop Daemon" on page 68 for instructions to stop and start the daemon.

   ```
   #/svengine/sdus/sdushutdown
   ```

2. Install the new SV SAN Builder software. The config file will not be changed. See "SV SAN Builder Installation" on page 61 for instructions on installation.
3. Start the daemon.

   ```
   #/svengine/sdus/slicd
   ```

Upgrade With Redundant Daemons

1. Stop the primary daemon. It will failover to the secondary daemon. See "Start and Stop Daemon" on page 68 for instructions to stop and start the daemon.

   ```
   #/svengine/sdus/sdushutdown
   ```

2. Install the new SV SAN Builder software. The config file will not be changed. See "SV SAN Builder Installation" on page 61 for instructions on installation.
3. Start the primary daemon.

   ```
   #/svengine/sdus/slicd
   ```

Start and Stop Daemon

Start Daemon

Related publication: *SV SAN Builder – Installation and User Guide*

1. Log in as root, and open a terminal.
2. Change to the directory that contains the sdus directory (default is **/svengine**).

   Example: **# cd /svengine/**
3. Change to the sdus directory.

   Example: **# cd /svengine/sdus/**
4. Type **ps –ef | grep slicd** to ensure that there is no other SLIC Daemon program running on the same system.

   Example with no SLIC Daemon program running:

   ```
   root 1802 213  1   21:36:22 console  0:00   grep slicd
   ```

   Example with SLIC Daemon program running:

   ```
   root 26352 26342  0 15:06:40 ?        0:00 ./slicd
   root 26347 26342  0 15:06:40 ?        0:00 ./slicd
   root 26345 26342  0 15:06:28 ?        0:00 ./slicd
   root 26342     1  0 15:06:28 ?        0:00 ./slicd
   root 26346 26342  0 15:06:28 ?        0:00 ./slicd
   root 26343 26342  0 15:06:28 ?        0:00 ./slicd
   root 26344 26342  0 15:06:28 ?        0:00 ./slicd
   ```

   Note: *When running the secondary daemon, the first SAN will display 7 processes. Every SAN after the first SAN will display 2 more processes.*
5. Type **./slicd** to start the daemon.

Stop Daemon

Related publication: *SV SAN Builder – Installation and User Guide.*

- For a local computer:

  ```
  #/svengine/sdus/sdushutdown
  ```

Edit Daemon Config File

Related publication: *SV SAN Builder –Installation and User Guide*.

In the configuration file, you may define:

- Daemon SignOn Path

  Establishes communication between daemon and SV Router to provide daemon management of the SAN(s).

- System specification or general SLIC daemon properties specifications

  Configurations defined in the system specification apply to all SANs associated with the daemon. System specifications contain the following feature configurations:

  - Call Home.
  - Security features.
    - Password protection for daemon-router communication.
    - IP Management Feature.
  - daemon retries establishment of daemon-router communication in startup process.

- SAN specification (Failover Settings for Redundant Daemons)

  Configurations defined in the SAN specification apply only to the SAN(s) defined within the SAN specification and associated with the daemon. SAN specifications contain the following feature configurations:

  - Security features.
    - IP Management Feature.

      Overrides IP Management features in system specifications.
    - Failover settings.

Daemon SignOn Path

SignOn Path for Standalone Daemon

A standalone daemon is a daemon that is not used in conjunction with another daemons for failover purposes.

1. Open and edit the config file svengine.cfg located in the sdus directory to name the daemon's SignOn path and reference the router's IP address.

2. Scroll down until you see the following information:

```
# r0 = {
# internet_path = 123.123.456.789;
# };
```

3. Copy the sample text in the file and paste it below the sample. Remove the comment line indicators (**#**), and substitute the following information as needed.

    - Where **r0** appears in the sample, enter the name of the SignOn path using one of the routers in SAN 1 (the example below uses SAN1r0) and enter that router's IP address. See example below.

Example of Standalone Daemon:

```
SAN1r0 = {
internet_path = 100.1.2.24;
};
r0 is a user defined name.
```

4. You must create a SignOn path for each SAN associated with the daemon.

SignOn Path for Redundant Daemons

1. Open and edit the config file svengine.cfg located in the sdus directory to name the daemon’s SignOn path and reference the router’s IP address.

2. Scroll down until you see the following information:

```
# r0 = {
# internet_path = 123.123.456.789;
# };
```

3. Copy the sample text in the file and paste it below the sample. Remove the comment line indicators (#), and substitute the following information as needed.

   - Where **r0** appears in the sample, enter the name of the SignOn path using one of the routers in SAN 1 (the example below uses SAN1r0) and enter that router’s IP address. See example below.

   - Create a second SignOn path using one of the routers in SAN 2, and enter that router’s IP address. See example below.

Example of Primary Daemon:

```
SAN1r0 = {
internet_path = 100.1.2.24;
};

SAN2r0 = {
internet_path = 100.1.2.44;
};
```

4. To edit the **Daemon SignOn Path** in the secondary daemon (located in the secondary management server) follow steps 1-3 but substitute the two remaining routers so that the config file resembles the following example.

Example of Secondary Daemon:

```
SAN1r1 = {
internet_path = 100.1.2.28;
};

SAN2r1 = {
internet_path = 100.1.2.48;
};
```

5. You must create a SignOn path for each SAN associated with the daemon. The path should use one of the routers in each SAN.

Configure Call Home Feature

The Call Home™ feature allows you to be notified via email when certain (user-designated) Service Request Numbers (SRNs), occur.

1. Open and edit the config file svengine.cfg located in the sdus directory to activate and assign an e-mail address for the Call Home feature.

2. Scroll down until you see the following information:

```
# system = {
#       email = myadmin@xyzcompany.com;
#       profile = "Microsoft Outlook";
#       srn = N7005x;
#       email_header_file = mailheader.txt;
# };
```

3. Copy the sample text in the file and paste it below the sample. (If you already have started system specifications then paste it under the last entry as seen in "Example of Final Config Files" on page 77.) Remove the comment line indicators (**#**), and substitute the following information as needed.

   - Where **myadmin@xyzcompany.com** appears, susbtitute your email address. If more than one, type the other addresses separated by a semicolon.

   - Where **profile = "Microsoft Outlook";** appears, remove the entire line (this is not used with UNIX-based management station).

   - Where **N7005x** appears, type the SRNs that you want to monitor via e-mail (**x** is a wild card). If more than one, substitute the other SRNs seperated by a semicolon.

   - Where mailheader.txt; appears, substitute the path and file name of a text file you have created to associate the SRNs with a particular customer and/or daemon. The text file will be treated as an attached email header. (No paramaters exist for the content of the text file. User defined.) See "Mail Header Text File" on page 79, for more information.

4. If you run a redundant daemon configuration then repeat steps 1-3 for the secondary daemon.

Configure Security Features

Password Protection for Daemon-Router Communication

Any SV Router in the SAN may be a SignOn path for the daemon. Anyone who can sign on to the SAN can make changes to the SAN. The *Password Protection for Daemon-Router Communication* provides a password-protected SignOn path that prevents unauthorized daemon access to the SAN.

1. Create a text file containing each SignOn path and its corresponding password. See "Password Text File" on page 80 for more information.

2. Open and edit the config file **`svengine.cfg`** located in the sdus directory to create a password-protected SignOn path.

3. Scroll down until you see the following information:

   ```
   #system = {
   #         password_file = TEXT_FILE_CONTAINING_PASSWORDS;
   #};
   ```

4. Copy the sample text in the file and paste it below the sample. (If you already have started system specifications then paste it under the last entry as seen in "Example of Final Config Files" on page 77.) Remove the comment line indicators (**#**), and substitute the following information as needed.

   - Where **`TEXT_FILE_CONTAINING_PASSWORDS`** appears, substitute the path and the name of the text file that was created in step 1 above.

5. If you run a redundant daemon configuration then repeat steps 1-4 for the secondary daemon.

IP Management Feature

The *IP Management Feature* provides protected access between client (computer used as remote manager) and host (management station) for those who decide to manage the management station remotely.

1. Open and edit the config file svengine.cfg located in the sdus directory to create a password-protected SignOn path.

2. Scroll down until you see the following information:

```
#system = {
#         RemoteClientAllowed = yes/no;
#         AnyRemoteClient= yes/no;
#         HostListFileName = FILENAME;
#         AuthorizedHosts = IP_HOST1, IP_HOST2;
#};
```

3. Copy the sample text in the file and paste it below the sample. (If you already have started system specifications then paste it under the last entry as seen in "Example of Final Config Files" on page 77.) Remove the comment line indicators (**#**), and substitute the following information as needed.

   - Enter **yes** for **RemoteClientAllowed**.
   - Enter **no** for **AnyRemoteClient.**
   - **HostListFileName** and **AuthorizedHosts** perform the same function.
     - Where **FILENAME** appears, substitute the path and filename of a text file containing a list of permitted clients' IP addresses.
     - Where **IP_HOST1** appears, substitute the IP address of the permitted client. If more than one, type the other addresses seperated by a comma.

4. If you run a redundant daemon configuration then repeat steps 1-3 for the secondary daemon.

Daemon-Router Communication

1. Open and edit the config file svengine.cfg located in the sdus directory to create a password-protected SignOn path.

2. Scroll down until you see the following information:

   ```
   #system = {
   #       retry_on_slic_signon_fail = yes/no;
   #};
   ```

3. Copy the sample text in the file and paste it below the sample. (If you already have started system specifications then paste it under the last entry as seen in "Example of Final Config Files" on page 77.) Remove the comment line indicators (**#**), and substitute the following information as needed.

   - Default setting is **`yes.`** The daemon will try to establish a SignOn path with the primary SV Router until stopped manually. Too many attempts to sign on may aggravate the system.

   - Enter **`no`** so that the daemon does not try to re-establish a SignOn path. If the primary daemon cannot sign on then the secondary daemon will activate and establish communication through its SV Router.

4. If you run a redundant daemon configuration then repeat steps 1-3 for the secondary daemon.

Configure the Failover Settings for Redundant Daemons

1. Scroll down until you see the following information:

```
#SAN_ENTRY_NAME = {
#       name = SAN_ENTRY_NAME;
#       PrimaryDaemon PRIMARY_SignOnPath_IP,SIGNON_PATH_PRIMARY;
#       SecondaryDaemon = SECONDARY_SignOnPATH_IP,SIGNON_PATH_OF_SECONDARY;
#
#       Optional SAN Properties Configuration...;
#     };
```

2. Copy the sample text in the file and paste it below the sample. (If you already have started system specifications then paste it under the last entry as seen in "Example of Final Config Files" on page 77.) Remove the comment line indicators (**#**), and substitute the following information as needed.

3. Where the SAN name (**`SAN1 and SAN2`**) appears, replace it with the name of your SAN.

4. Where the IP address of the **`PrimaryDaemon`** appears, replace it with the IP address of the primary server.

5. Where the daemon's SignOn path name (**`r0`**) appears, substitute the router that corresponds with that daemon as configured in the **`Router Sign On Path`**.

6. To configure the **`Failover Daemon Settings`** in the secondary daemon (located in the secondary management server), repeat steps 1 through 5. The secondary server's configuration is identical to the primary server's.

Example: Primary and Secondary Daemon Config File

```
SAN1 = {
name = SAN1;
PrimaryDaemon = 100.1.2.32, SAN1r0;
SecondaryDaemon = 100.1.2.35, SAN1r1;
};
SAN2 = {
name = SAN2;
PrimaryDaemon = 100.1.2.32, SAN2r0;
SecondaryDaemon = 100.1.2.35, SAN2r1;
};
```

Example of Final Config Files

Example of Final Configuration File (standalone daemon):

```
SAN1r0 = {
        internet_path = 100.1.2.24;
};
SAN2r0 = {
        internet_path = 100.1.2.44;
};
system = {
        email = me@vicom.com;
        srn = N7xxxx;
        email_header_file = \svengine\custlist\vicomsystems.txt;
        password_file = vicomsystemspassword.txt;
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 100.100.100.100, 110.110.110.110;
};

SAN1 = {
        name = SAN1;
        PrimaryDaemon = 100.1.2.32, SAN1r0;
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 100.100.100.100;
};
```

Note: SAN Specifications (SAN1) override system specifications of:

```
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 100.100.100.100, 110.110.110.110;
```

Example of Final Configuration File (redundant daemons):

```
SAN1r0 = {
        internet_path = 100.1.2.24;
};
SAN2r0 = {
        internet_path = 100.1.2.44;
};
system = {
        email = me@vicom.com;
        srn = N7xxxx;
        email_header_file = \svengine\custlist\vicomsystems.txt;
        password_file = vicomsystemspassword.txt;
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 100.100.100.100, 110.110.110.110;
};

SAN1 = {
        name = SAN1;
        PrimaryDaemon = 100.1.2.32, SAN1r0;
        SecondaryDaemon = 100.1.2.35, SAN1r1;
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 100.100.100.100;
};
SAN2 = {
        name = SAN2;
        PrimaryDaemon = 100.1.2.32, SAN2r0;
        SecondaryDaemon = 100.1.2.35, SAN2r1;
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 110.110.110.110;
};
```

Note: SAN Specifications (SAN1 and SAN2) override system specifications of:

```
        RemoteClientAllowed = yes;
        AnyRemoteClient= no;
        AuthorizedHosts = 100.100.100.100, 110.110.110.110;
```

Text Files for Daemon Config File

Mail Header Text File

No parameters exist for this text file. The text file is designed for you to associate the SRNs with a particular customer and/or daemon. Vicom provide an example below, but you may define all information included in the text file.

Example Text File for Mailheader (standalone daemon):

```
Customer: Vicom Systems
SANs: SAN 1 & 2
Daemon: 10.1.2.32
```

Example Text File for Mailheader (redundant daemons):

```
Customer: Vicom Systems
SANs: SAN 1 & 2
Primary Daemon: 10.1.2.32
Secondary Daemon: 10.1.2.35
```

Password Text File

Usage

- Text file name is user defined.
- SignOn Path
- The SignOn path should be typed first on the left-hand side of the text file. On the same line, create a space then type the password.
- The passwords must match the IP password defined in the router's *User Service Utility* menu item **'4': View and/or Change Response to Router Management Programs**.
- Maximum number of entries is 64.

Example Password Text File (standalone daemon)

```
SAN1r0            password
SAN2r0            password
```

Example Password Text File (redundant daemons)

```
SAN1r0            password
SAN1r1            password
SAN2r0            password
SAN2r1            password
```

Update Daemon Config File

Update for StandAlone Daemon

1. Stop the daemon. See "Start and Stop Daemon" on page 68for instructions to stop and start the daemon.

2. Edit the configuration file. See "Edit Daemon Config File" on page 69 for instructions to edit the configuration file.

3. Start the daemon.

Update for Redundant Daemon

1. Stop the primary daemon. It will failover to the secondary daemon.

   ```
   cd /svengine/sdus
   ./sdushutdown
   ```

2. Edit the configuration file. See "Edit Daemon Config File" on page 69 for instructions to edit the configuration file.

3. Start the daemon. See "Start and Stop Daemon" on page 68 for instructions to start the daemon.

4. Use the **setmasterdaemon** command, to restore the primary daemon for each SAN. This will ensure that the same primary daemon is used for each SAN. See "Setting the Master Daemon [setmasterdaemon]" on page 116 for more information.

Example

```
#svengine/sdus/setmasterdaemon -h 100.1.2.32 -d SAN1r0

#svengine/sdus/setmasterdaemon -h 100.1.2.32 -d SAN2r0

#svengine/sdus/setmasterdaemon -h 100.1.2.32 -d SAN3r0
```

5. Repeat steps 1-3 on all secondary Daemon.

Example of Normal Operating Status:

```
List of Daemons

ID   Host        Slic  SlicNumber   AssignedDaemon      DaemonStatus
-------------------------------------------------------------------------

0   100.1.2.32   SAN1r0    0          Primary Daemon       OK
1   100.1.2.35   SAN1r1    0          Secondary Daemon     Idle
2   100.1.2.32   SAN2r0    0          Primary Daemon       OK
3   100.1.2.35   SAN2r1    0          Secondary Daemon     Idle
```

Example of a Successful Failover

```
List of Daemons

ID   Host        Slic  SlicNumber   AssignedDaemon      DaemonStatus
-------------------------------------------------------------------------

0   100.1.2.32   SAN1r0    0          Primary Daemon       error
1   100.1.2.35   SAN1r1    0          Secondary Daemon     OK
2   100.1.2.32   SAN2r0    0          Primary Daemon       OK
3   100.1.2.35   SAN2r1    0          Secondary Daemon     Idle
```

CHAPTER 5

SV ZONE MANAGER

The Vicom SV Zone Manager enables the system administrator to map logical or physical storage to HBAs. This ability allows the administrator to allocate storage on demand.

This chapter explains maintenance of the SV Zone Manager within the system. It includes these sections:

- Determine SV Zone Manager Software Version
- SV Zone Manager Installation

Determine SV Zone Manager Software Version

1. Read the SV Zone Manager CD label that was sent with the SV Router FC-FC 3.
   - Software versions should be 2.5 or later.
2. If you cannot find the SV Zone Manager CD, then boot up the management server. It should contain the software program.
3. Using most commands plus ‘--’ will display the SV Zone Manager version.

Example

```
#/svengine/sduc/svpd --
```

4. To upgrade SV Zone Manager, see "SV Zone Manager Upgrade" on page 83.

SV Zone Manager Installation

Important Information

Related publication: *SV Zone Manager – Installation and User Guide.*

SV Zone Manager installs the Graphical User Interface (GUI) and the Command Line Interface (CLI) for configuring zones. Once installation is complete four files will appear:

- SLICView.
- SLICZone.
- Sdomain.
- Sadapter.

Installation for SUN

When you install the SV SAN Builder application software, you also install the SV Zone Manager. See "SV SAN Builder Installation" on page 61 for installation instructions.

SV Zone Manager Upgrade

- Do not remove the old version of SV Zone Manager. The new version of SV Zone Manager will install over the old version.
- The daemon does not need to be shut down when installing SV Zone Manager.
- For installation follow the steps in "SV Zone Manager Installation" on page 83.

CHAPTER 6

SV SNMP AGENT

Vicom SV SNMP Agent stores and retrieves data defined by the management information base (MIB) and signals the SNMP manager when an event occurs.

This chapter explains maintenance of the SV SNMP Agent within the system. It includes these sections:

- Determine SV SNMP Agent Software Version
- SV SNMP Agent Installation
- SV SNMP Agent Upgrade
- Start and Stop SV SNMP Agent
- Configure SAN List Specifications
- Configure Trap Client List Specification

Determine SV SNMP Agent Software Version

1. Read the SV SNMP Agent CD label that was sent with the SV Router FC-FC 3.
   - Software version should be 1.0 or later.
2. Start the software that will receive the SNMP traps.
   - When SV SNMP Agent starts, it will send the version number to the SNMP trap. However, to receive the information, the software that receives the SNMP traps must be running before SV SNMP Agent is started.
   - If SV SNMP Agent is started before the SNMP trap, then shut down the agent. See "Stop" on page 91
3. Start the SV SNMP Agent program. See "Start" on page 91.
   - If SV SNMP Agent has not been installed in the management station, then install it now. See "SV SNMP Agent Installation" on page 89.
4. To upgrade SV SNMP Agent See "SV SNMP Agent Upgrade" on page 90.

SV SNMP Agent Installation

Related publication: *SV Management SNMP Agent – Installation and User Guide.*

To install SV SNMP Agent on UNIX, follow these steps:

1. Ensure you have the latest software (1.0 or later). If you do not know how to determine the software version, see "Determine SV SNMP Agent Software Version" on page 88.
2. In the primary and/or secondary management server, login as root.
3. Insert the Vicom SV SNMP Agent v1.0 CD-ROM in the CD-ROM drive.
4. Mount the CD-ROM, and change to that directory.
5. Type **`./install.sh <user defined directory>`** and press enter. The default directory is **`/svengine`**.

SV SNMP Agent Upgrade

Important Information

- The daemon does not need to be shut down when installing SV SNMP Agent.
- Because the installation will override the configuration files (sanlist.cfg and trapclientlist.cfg), the files should be renamed.
- Do not remove the old version of SV SNMP Agent. It will install over the old version.

Upgrade

1. In the primary server, open the SNMPagent directory located in the svengine directory and change following file names:
    - sanlist.cfg
    - trapclientlist.cfg

Example

- sanlistA.cfg
- trapclientlistA.cfg

2. Install the new version of SV SNMP Agent. "SV SNMP Agent Installation" on page 89 for more information.
3. Delete the new configuration files.
4. Rename the old configuration files so that their names match the names of the new configuration files that were deleted in step 3.
5. Repeat steps 1-4 in the secondary daemon.

Start and Stop SV SNMP Agent

Start

- Enter `#svmgmtagent` to start the SNMP agent.

  ```
  #/svengine/SNMPagent/svmgmtagent
  ```

- If you changed the remote management server's UDP port setting, you can start the SNMP agent by entering `#svmgmtagent` and the new port setting.

Example:

```
#./svmgmtagent 4700
```

.

Troubleshooting

Error message: Transport in use SNMP port init failed (-21)

- Problem: Signifies SNMP Agent's UDP port is in use.
- Solution: Change SNMP Agent's UDP port setting.

Note: Server UDP port default setting is 161

Stop

1. Log in as root, and open a terminal.
2. View process number. Type `ps –aef | ./svmgmtagent.`

Example of process information

```
root 2704 2693 0  21:36:22  pts/9   0:00   grep svmgmtagent
```

3. Kill the process. Type `kill` and process number.

Example

```
#kill 2704
```

Configure SAN List Specifications

The maximum number of entries is 32.

1. Open the SNMPagent directory located in the svengine directory. It contains the following files:
    - svmgmtagent (executable file).
    - sanlist.cfg (user-configurable file for all SANs to be monitored).
    - trapclientlist.cfg (user configuration file for all trap clients to be monitored).
2. Open and edit the sanlist.cfg file.

Example:

```
#SAN_Name        Daemon_Name      Host_IPAddress     Tcp/Ip_Port

#SAN1            r0               123.123.456.789    default
SAN1             SAN1r0           100.1.2.32         default
```

- Directly under the sample given, under **#SAN1**, type the name of the SAN (**SAN1**)to be monitored (user-defined). Be sure to omit the comment line indicator (**#**).
- Under **Daemon_Names** type the Deamon SignOn path (SAN1**r0**).
- Under **Host_IPAddress** type the IP address of the server that contains the daemon.
- Under **Tcp/Ip_Port** type **default**. Default is 20000. Vicom highly recommends that you use the default port.

3. If you run a redundant daemon configuration then repeat steps 1-2 for the secondary daemon.

Configure Trap Client List Specification

The maximum number of entries is 32.

1. Open the SNMPagent directory located in the svengine directory. It contains the following files:
   - svmgmtagent (executable file).
   - sanlist.cfg (user-configurable file for all SANs to be monitored).
   - trapclientlist.cfg (user configuration file for all trap clients to be monitored).
2. Open and edit the trapclientlist.cfg file.

#TrapClient_IPAddress	**TrapClient_Port_Number**	**TrapClient_SeverityFilter_Number**
123.123.456.11	**162**	**6**

   - Directly under the sample given, under **#TrapClient_IPAddress**, enter the IP address of the host running SNMP Manager. It will receive SRNs (Service Request Numbers) and trap messages sent from the Vicom SNMP Agent. Be sure to omit the comment line indicator (**#**).
   - Under the **TrapClient_Port_Number**, enter the UDP port number of the SNMP Manager. For most hosts running the SNMP Manager, the default UDP setting is 162.
   - Enter the severity filter number. One represents the most severe (worst-case), and six the least severe.
3. If you run a redundant daemon configuration then repeat steps 1-2 for the secondary daemon.

CHAPTER 7

OTHER COMPONENT MAINTENANCE

This chapter explains maintenance of non-Vicom related components within the system. It includes these sections:

- T3 Disk Array Maintenance
- Ethernet Switch/HUB Maintenance
- Fibre Channel Switch Maintenance
- Data Server Maintenance
- Management Server Maintenance
- Cabling and Connections Maintenance

T3 Disk Array Maintenance

T3 Disk Array Failback Procedure

Important Information

- The T3 partner group represents two LUN (L0 and L1). If the SV Router sends I/O to L0 and the primary path to L0 is down, then the secondary path to L0 is used. When the SV Router uses the secondary path, T3 LUN failover occurs. This process is the same for both LUNs.
- Failback uses the same concept. However, you must re-establish the primary path, issue the command **`mpdrive failback,`** and send I/O to one of the LUNs via its primary path. This is an automatic function once I/O transmission begins.
- Because the T3 must flush the cache, failover/failback can take 3-5 minutes.

Failback Procedure

1. Repair the disrupted primary path by replacing or repairing failed component.
2. If the SV Router's fault LED is flashing, cycle the power.
3. Using CLI **`mpdrive view,`** determine the T3 controller number (**`-j`** used in the example for step 4.) See "Viewing MultiPath Drive Properties" on page 119.

Example

```
mpdrive view -d SAN1r0
```

Note: *The T3 partner group will report only one controller number.*

4. Using the **`mpdrive failback`** command, cause the secondary path to the T3 to failback to the primary path.

Example

```
mpdrive failback -d SAN1r0 -j 2000000100000123
```

5. Resume I/O to enable failback.

Failover Scenarios for Host-Side Switch Configuration

- Cable or GBIC at either end of cable D1 fails:

  Both SV Router FC-FCs remain functioning properly. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- Cable or GBIC at either end of cable D2 fails:

  Both SV Router FC-FCs remain functioning properly. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

- Cable or GBIC at either end of cable SV-AB fails and SV Router FC-FC A was master:

  SV Router FC-FC A remains functioning properly. SV Router FC-FC B will shut down to avoid T3 ping-pong effect. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

- Cable or GBIC at either end of cable SV-AB fails and SV Router FC-FC B was master:

  SV Router FC-FC B remains functioning properly. SV Router FC-FC A will shut down to avoid T3 ping-pong effect. All IO will be directed to T3(A). T3 failover triggers. IO to L0 will go through its secondary path.

- SV Router FC-FC A fails and SV Router FC-FC A was master:

  SV Router FC-FC B remains functioning properly and it will promote itself to master. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- SV Router FC-FC A fails and SV Router FC-FC B was master:

  SV Router FC-FC B remains functioning properly. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

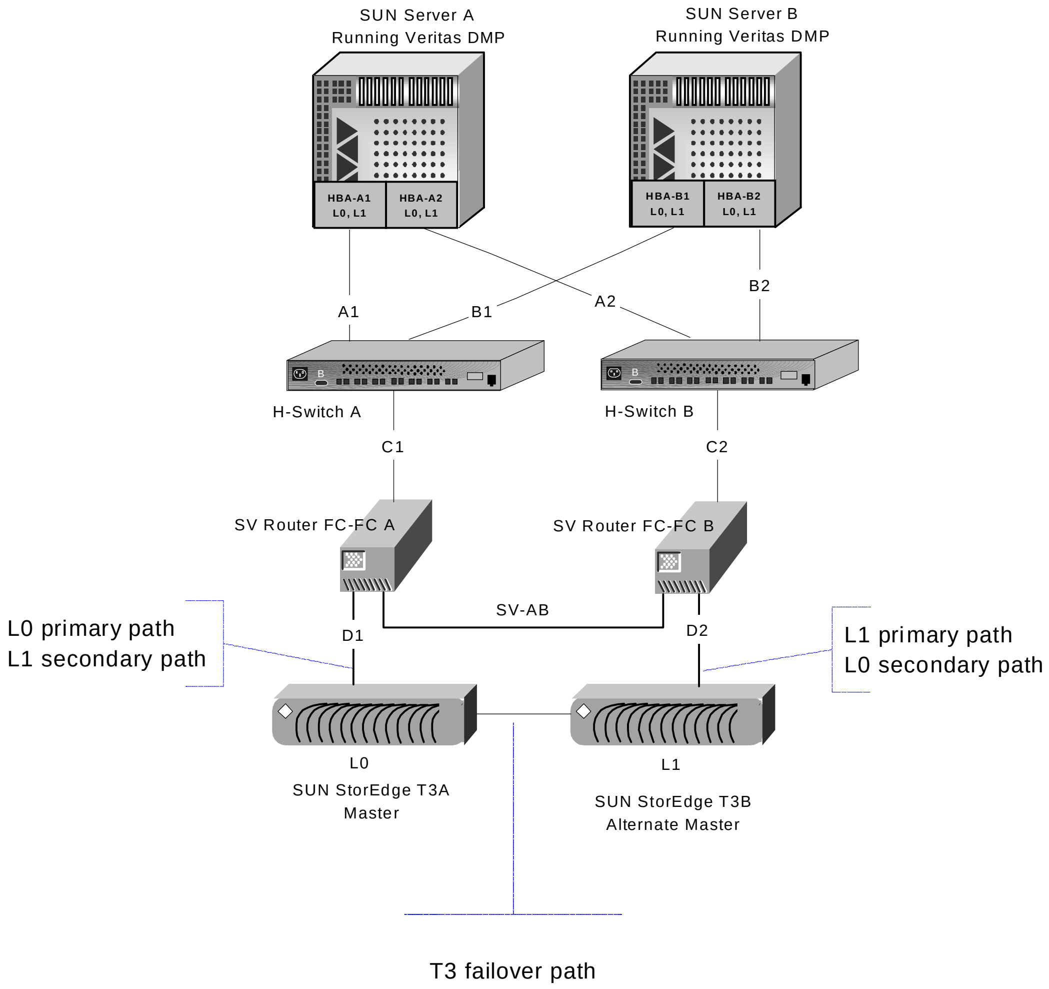
- SV Router FC-FC B fails and SV Router FC-FC B was master:

  SV Router FC-FC A remains functioning properly and it will promote itself to master. All IO will be directed to T3(B). T3 failover triggers. IO to L1 will go through its secondary path.

- SV Router FC-FC B fails and SV Router FC-FC A was master:

  SV Router FC-FC A remains functioning properly. All IO will be directed to T3(B). T3 failover triggers. IO to L1 will go through its secondary path.

Figure 7-1 Host-Side Switch Configuration



Failover Scenarios for Host/Device-Side Switch Configuration

- Cable E1 or GBIC of either end of cable E1 fails:

  Both SV Router FC-FCs remain functioning properly. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- Cable E2 or GBIC of either end of cable E2 fails:

  Both SV Router FC-FCs remain functioning properly. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

- Cable F1 or GBIC of either end of the cable F1 fails and SV Router FC-FC A was master:

  SV Router FC-FC A remains functioning properly. SV Router FC-FC B will shut down to avoid T3 ping-pong effect. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

- Cable F1 or GBIC of either end of cable F1 fails and SV Router FC-FC B was master:

  SV Router FC-FC B remains functioning properly. SV Router FC-FC A will shut down to avoid T3 ping-pong effect. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- SV Router FC-FC A fails and SV Router FC-FC A was master:

  SV Router FC-FC B remains functioning properly and it will promote itself to master. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- SV Router FC-FC A fails and SV Router FC-FC B was master:

  SV Router FC-FC B remains functioning properly. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- SV Router FC-FC B fails and SV Router FC-FC B was master:

  SV Router FC-FC A remains functioning properly and it will promote itself to master. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

- SV Router FC-FC B fails and SV Router FC-FC A was master:

  SV Router FC-FC A remains functioning properly. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

- Cable A1 or GBIC of either end of cable A1 fails:

  SV Router FC-FC B remains functioning properly. SV Router FC-FC A will shut down.

- Cable D2 or GBIC of either end of cable D2 fails:

  SV Router FC-FC A remains functioning properly. SV Router FC-FC B will shut down.

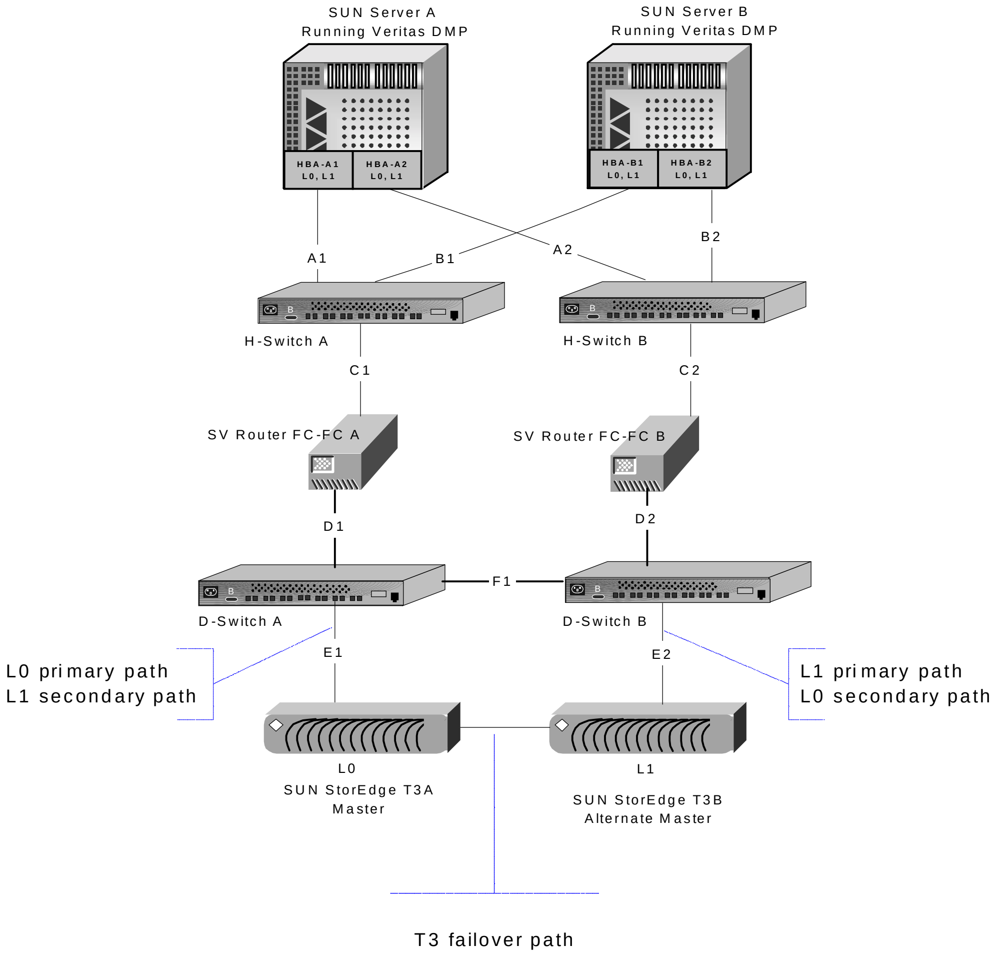
- D-SwitchA fails:

  SV Router FC-FC B remains functioning properly. SV Router FC-FC A will shut down to avoid T3 ping-pong effect. All IO will be directed to T3(B). T3 failover triggers. IO to L0 will go through its secondary path.

- D-SwitchB fails:

  SV Router FC-FC A remains functioning properly. SV Router FC-FC B will shut down to avoid T3 ping-pong effect. All IO will be directed to T3(A). T3 failover triggers. IO to L1 will go through its secondary path.

Figure 7-2 Host/Device-Side Switch Configuration



T3 Drive Replacement

Please refer to the *Sun StorEdge T3 Disk Tray Installation, Operation, and Service Manual* for complete instructions on T3 disk tray service and function.

- Only remove one drive at a time from the T3 disk tray at any time. Ensure this drive is replaced and fully enabled before removing another drive.
- Replace drives when the T3 disk tray is fully enabled and powered on. Drives that are replaced when the disk tray is powered off or not fully enabled may not be detected properly by the T3 monitoring system.
- Disk drive spin-up takes about 30 seconds. Disk drive rebuild (reconstruction of data on new drive) takes about an hour.

Ethernet Switch/HUB Maintenance

Refer to the service manual associated with the Ethernet switch/HUB for maintenance information.

Ethernet Switch/HUB Replacement

- Replacement of the Ethernet switch/HUB is a plug-and-play action and will not have an effect on the SAN.
- If using only one Ethernet switch/HUB, then communication between SV Routers and management station will be lost temporarily.

Fibre Channel Switch Maintenance

Refer to the service manual associated with the FC switch for maintenance information.

Replacing a Switch in a Host-Side Switch Configuration

- If a standalone router configuration is used, then I/O must be stopped before replacement can begin.
- If a redundant router and switch configuration is used, I/O will be routed to the remaining FC switch temporarily. Replacement of the FC switch is a plug-and-play action and will have a minimal effect on the SAN.

Data Server Maintenance

Refer to the service manual associated with the servers for maintenance information.

Data Server/FC HBA Replacement for Zones

If you are not using zones in your system configuration then HBA replacement becomes a plug and play action.

1. Install HBAs.

2. Cable the server to the switches if it is an indirect connect or to the routers if it is a direct connect.

3. Using remote management, check the connection:

   - Switch-connect telnet each switch to view the UIDa of all devices connected to that switch.

   - HBA-connect, go to step 4.

4. In each SV Router, if more than one, use the **`slicview view`** command, view the router zone configuration information.See "Viewing SV Router Zone Components [slicview]" on page 129 for more information.

   You should see in each SV Router the replacement HBA, the failed HBA and if the original configuration included more than one HBA per server, you will see those HBA(s) as well.

Example

```
slicview view -d SAN1r0
```

5. In each SV Router, if more than one, using the **`sadapter alias`** command, assign aliases for the new HBAs.

    - Limit alias to 12 characters. See "Creating or Changing the Host Adapter Alias" on page 132 for more information.
    - To ensure that conflict does not occur, do not use an existing HBA alias for the replacement HBAs.

Example for One Server

```
sadapter alias -d SAN1r0 -r I1 -u 2137845600000005 -n e450E
sadapter alias -d SAN1r0 -r I2 -u 2137845600000006 -n e450F
```

Note: *The initiator numbers I00001 and I00002 can be written without zeroes (I1, I2, etc.)*

6. In each SV Router, if more than one, using the **`sliczone view`** command, determine the zone(s) of failed HBA.

Example

```
sliczone view -d SAN1r0
```

7. In each SV Router, if more than one, using the **`sliczone add`** command, add new HBAs to each zone. See "Adding Members to a Zone" on page 135 for more information.

Example

```
sliczone add -a e450E -z e450zone
sliczone add -a e450F -z e450zone
```

Usage

```
-a                        Name of new HBA
-z                        Zone name
```

8. In each SV Router, if more than one, using the **`sadapter view`** command, view the devices assigned an HBA. The new HBA should see the same number of drives and the same drive map as the old HBA. See "Viewing Host Adapter Properties" on page 130 for more information.

Example

```
adapter view -r I1
adapter view -r I2
```

Troubleshooting

If the view of the old HBA and the new HBA do not match, repeat steps 6-8.

9. In each SV Router, if more than one, using **`sliczone del`** command, delete the old HBA from the zone. See "Deleting Members from a Zone" on page 136 for more information.

Example

```
sliczone del -a e450A -z e450zone
sliczone del -a e450B -z e450zone
```

Usage

```
-a                       Name of old HBA
-z                       Zone name
```

10. Using the **`sanconfig read`** command, save the SAN configuration to file. See "Reading SAN Configuration File and Saving to File" on page 121 for more information.

Example

```
sanconfig read -d SAN1r0 -e /svengine/SANconf/T3SAN.san
```

Management Server Maintenance

Management Server Replacement

- Install the replacement server.
- Copy the daemon configuration file **`(svengine.cfg)`**, and paste it in the **`sdus`** directory located in the **`svengine`** directory.

  `#/svengine/sdus`

- Copy the SAN list specification file **`(sanlist.cfg)`**, and paste it in the **`SNMPagent`** directory located in the **`svengine`** directory.

  `#svengine/SNMPagent/`

- Copy the trap client list file **`(trapclientlist.cfg),`** and paste it in the **`SNMPagent`** directory located in the **`svengine`** directory.

  `#svengine/SNMPagent/`

Cabling and Connections Maintenance

Check Cabling and Connectors

1. Be sure to power off the device to which the connector is attached before removing it.
2. Visually study the end of both connectors on the cable. Ensure that pins are not broken, bent, or pushed in.
3. If a connector is damaged, replace the connector, and power on the device.
4. Ensure that the connector is fastened to the device securely. A loose connection can cause termination problems.
5. Ensure the cable does not exceed recommended length.
    - For Ethernet cabling, see "Ethernet Requirements" on page 109.
    - For optical cabling, see "FC Requirements" on page 110.
    - For serial cabling on SV Routers, "Serial Requirements" on page 110
6. If problems still exist, power off the device and replace the cable.

Ethernet Requirements

SV Router.

- Speed: 10base-T/100base-TX
- Connector RJ-45
- Topology: Transmission Control Protocol - Internet Protocol (TCP-IP).
- Maximum distance between devices: 100 meters (328 feet).

FC Requirements

SV Router.

- Finisar GBIC connector (recommended).
- Short-wavelength optical cable.
  - Data Rate: 100 Mbytes/sec burst
  - Cable: 50 or 62.5 micron fiber optic
  - Connector: Dual SC
  - Distance: 500 m (1640 ft) or 172 m (564 ft)
- Long-wavelength optical cable.
  - Data Rate: 100 Mbytes/sec burst
  - Cable: 9 micron fiber optic
  - Connector: Dual SC
  - Distance: 10 km (6.2 miles)
- Copper cable.
  - Data Rate: 100 Mbytes/sec burst
  - Cable: Twinax
  - Connectors: Two DB-9 or HSSDC
  - Distance: 30 m (98 ft) equalized, 20 m (65.6 ft) non-equalized

Serial Requirements

SV Router.

- Topology: Serial Transmission
- Speed: 56K baud
- Connector DB-9

CHAPTER 8

BASIC COMMAND LINE INTERFACE

This chapter explains only the commands used with this manual. It includes these sections:

- Getting Started
- Listing Device Connections [showmap]
- SLIC Daemon Commands
- MultiPath Drive Commands [mpdrive]
- SLIC (SV Router) Commands
- Error Log Analysis Commands
- Command Line Diagnostic Commands
- Viewing SV Router Zone Components [slicview]
- Host Adapter Commands [sadapter]
- Zone Commands [sliczone]

Getting Started

Related publications: *SV SAN Builder – Installation and User Guide* and *SV Zone Manager – Installation and User Guide*

The following commands can be used to administer the storage subsystem and its components. They are accessed from the operating system's command prompt.

1. Open a terminal for prompt.
2. Change to the directory that contains the sduc directory (default is **`svengine`**).

   UNIX Example: **`# cd /svengine/sduc`**

Listing Device Connections [showmap]

Use the **showmap** command to list all the physical and logical devices present in the SAN. The SignOn path is always required.

The lists of physical and logical devices are presented in tables:

1. The List of SLICs table may have one or two entries: SLICs in Initiator Mode and/or SLICs in Initiator Mode. Each of these tables displays the SLIC/Initiator Number, Alias, UID or WWN, and Type for each individual SV Router within the SAN. Offline SV Routers will be placed in the List of Offline Devices Table, and will not be displayed in this table.

   The ‘*’ denotes the Master SV Router.

   ```
   List of SLICs in Initiator Mode:
   SLIC Number SLIC Name        SLIC UID          TYPE Version
   I00001                       28000060-22000073 FCFC 08.04     *
   I00002                       28000060-220000CC FCFC 08.04

   List of SLICs in Target Mode:
   SLIC Number SLIC Name        SLIC UID          TYPE Version
   ```

2. The List of Target Devices table provides you with the Target Number, UID or WWN, LUN (native), VPD, Type, and Capacity of each physical target device. Offline physical target devices will be placed in the List of Offline Devices Table, and will not be displayed in this table.

   ```
   List of Target Devices:
   Target   Target UID        LUN      VPD             TYPE Capacity
   Number
   T00003   50020F20-00009CC3 0001     SUN   T300       DISK 488641  MB
   T00004   50020F20-00009C08 0000     SUN   T300       DISK 488641  MB
   T00005   50020F20-00009C08 0001     SUN   T300       DISK 488641  MB
   T00006   50020F20-00009BED 0000     SUN   T300       DISK 488641  MB
   T00007   50020F20-00009BED 0001     SUN   T300       DISK 488641  MB
   ```

3. The List of Logical Devices table provides you with the Target Number, Name, Serial Number, and Capacity for each logical device.

   ```
   List of Logical Devices:
   Target  Complex Name   TYPE       Serial Number   Capacity
   Number
   T49152  VMPDR000 MULTIPATH DRV  62526964-30305A54 488641 MB
   T49153  VMPDR001 MULTIPATH DRV  62526964-30305A55 488641 MB
   T49154  VMPDR002 MULTIPATH DRV  62526964-30305A56 488641 MB
   T49155  VMPDR003 MULTIPATH DRV  62526964-30305A57 488641 MB
   ```

4. The Map table lists all physical and logical devices that have been mapped and displays their SCSI/FC ID and LUN, Target Number, and UID/Complex Name. The maps listed in this table are global SAN maps and not the localized SV Router zone maps.

```
FC Map:
FC       Target   UID/Complex Name
MAP      Number
00-000   T49152   VMPDR000
00-001   T49153   VMPDR001
00-002   T49154   VMPDR002
00-003   T49155   VMPDR003
```

5. The List of Unmapped Drives table provides the Target Number and UID/Complex Name of any target devices that have not been mapped globally.

```
List of Unmapped Drives:
Target   UID/Complex Name
Number
T00000       50020F20-000093B5 0000
```

6. The List of General Spare Drives table provides the Target Number and UID of any target devices that have been allocated as general spares.

```
List of General Spare Drives:
Target   UID
Number
T00002       50020F20-000093B5 0002
```

7. The List of Offline Devices table provides the Target or SLIC/Initiator Number, UID or WWN, and Type of any physical devices that are offline.

```
List of Offline Devices:
SLIC/Target  UID                      Type
Number
T00001       50020F20-000093B5 0001
```

Usage:

```
showmap -d Cx {-m [lists_option] -f File_Name -h Host -v}
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-m [lists_option]	Optional. Selective display of tables. If this parameter is not specified, the program will display all tables relevant to the physical and logical devices in the SAN.

all	Output map showing all tables.
target	Output map of all target devices.
fc	Output global FC map table.
slic	Output List of SV Routers table.
physical	Output List of all physical device tables.
spare	Output List of General Spare Drives table.
offline	Output List of Offline Devices table.
unmapped	Output List of Unmapped Drives table.

-h Host	Optional. The name or IP address of the host running the daemon.
-f File_Name	Optional. Print maps to the file **File_Name**.
-v	Optional. Print maps to console (default).

Examples:

The following example will display all tables. The **showmap** command is executed on a server running the daemon (r0).

```
showmap -d r0
```

The following example will display the general spare drives. The **showmap** command is executed on a server running the daemon (r0).

```
showmap -d r0 -m spare
```

The following example will display all tables. The **showmap** command is executed remotely from the the daemon (r0) running on server (myhost).

```
showmap -d r0 -h myhost
```

SLIC Daemon Commands

Listing SLIC Daemons [sgetname]

Use the **`sgetname`** command to list the SignOn paths for the daemon processes running on each host.

Usage:

```
sgetname -h Host
```

-h Host	The name or IP address of the host running the daemon.

Examples:

The following example will display the SignOn paths for the SLIC Daemon processes running on host 205.119.173.113.

```
sgetname -h 205.119.173.113
```

Setting the Master Daemon [setmasterdaemon]

The SetMasterDaemon command is used to set the master daemon in the SAN. After failover, the primary daemon no longer acts as the master daemon. Run this command to reset the primary daemon back to the master daemon. This command can be executed only from the sdus directory in the daemon server.

Note: **`setmasterdaemon`** is only used in a failover daemon environment.

If there are any users connected to the current daemon, resetting back to the master daemon will cause them to be disconnected. The system will display the following message:

```
# users connected to daemon. Proceed? (Y or N):.
```

Type **`Y`** to disconnect the other users and continue setting the master daemon; type **`N`** to abort the command.

Caution ! ***Please wait until all I/O activity is completed before running this command. Otherwise this may cause lost I/Os and system panic.***

Usage:

```
setmasterdaemon -d Cx {-h Host -f}
```

-d Cx Cx is the SignOn path, as specified in the config file.

-h Host Optional. The name or IP address of the host running the daemon.

-f Optional. Bypass user confirmation step.

Examples:

The following example will set the primary daemon (c0) to become the master daemon. The **setmasterdaemon** command is executed remotely from the daemon (c0) running on server (myhost).

```
setmasterdaemon -d c0 -h myhost
```

Listing SAN Communication Properties [signoninfo]

The **signoninfo** command displays how communication between the daemon and the SV Router has been established. It lists the SignOn SLIC (SV Router) UID and the IP address of the router.

Usage:

```
signoninfo –d Cx {–h Host}
```

-d Cx Cx is the SignOn path, as specified in the config file.

-h Host Optional. The name or IP address of the host running the daemon.

Example

The following example will display the SignOn SLIC (SV Router) UID and the IP address of the router connected to the server running the daemon (c0).

```
signoninfo -d c0
```

MultiPath Drive Commands [mpdrive]

The **`mpdrive`** command is used to configure and manage MultiPath drives. MultiPath drive functionality is supported only in conjunction with the Sun StorEdge™ T3 Array.

Using MultiPath Drive Failback

Use the **`mpdrive failback`** command to switch between the active and passive paths by specifying the storage system's controller serial number. Use the **`mpdrive view`** command to obtain the controller serial number associated with the MultiPath drive.

Caution ! ***Please wait until all I/O activity is completed in the selected drives before running this command. Otherwise this may cause lost I/Os and system panic.***

Usage:

```
mpdrive failback -d Cx -j UID {-h host -v}
```

`-d Cx` Cx is the SignOn path, as specified in the config file.

`-j UID` The controller serial number of the MultiPath drive. This must be entered in upper case. See 'Viewing MultiPath Drive Properties' on page 123 to find the controller serial number.

`-h Host` Optional. The name or IP address of the host running the daemon.

`-v` Optional. User confirmation required.

Examples:

The following example will perform a failback on the set of MultiPath drives (after a prior failover incident has occurred on the array with controller serial number 20000001000001FE). The **`mpdrive`** command is executed remotely from the daemon (r0) running on server (100.2.34.120).

```
mpdrive failback -d r0 -j 20000001000001FE -h 100.2.34.120
```

Viewing MultiPath Drive Properties

Use the **`mpdrive view`** command to display the name, target number, drive capacity, active and passive paths, and controller serial number of a MultiPath Drive.

Usage:

```
mpdrive view -d Cx {-m Txxxxx -h Host}
```

`-d Cx`	Cx is the SignOn path, as specified in the config file.
`-m Txxxxx`	Optional. The target Number of MultiPath drive.
`-h Host`	Optional. The name or IP address of the host running the daemon.

Examples:

The following example will display the MultiPath drive (T49154) properties. The **`mpdrive`** command is executed on a server running the daemon (r0).

```
mpdrive view -d r0 -t t49154
```

SLIC (SV Router) Commands

Download Microcode [sdnld]

Use the sdnld command to download the microcode for the SV Router. This function can be used to download microcode to all the SV Routers in the SAN.

Caution ! ***Do not download new microcode to the SV Router FC-FC 3 if it is being used by the operating system. The SV Router will reset itself after the download is complete, which can cause lost I/Os and system panic.***

Usage:

```
sdnld -d Cx -t [s/Ixxxxx/sa] -f File_Name {-h Host}
```

-d Cx		Cx is the SignOn path, as specified in the config file.
-t [s/Ixxxxx/sa]		Initiator/SLIC number of the SV Router.
	s	SignOn SV Router.
	sa	All SV Routers in the SAN.
	Ixxxxx	Initiator number of the SV Router.
-f File_Name		Name of the microcode file.
-h Host		Optional. The name or IP address of the host running the daemon.

Examples

The following example will download microcode (fcfc3.ima) to SV Router I00002. The **sdnld** command is executed on a server running the daemon (r0).

```
sdnld -d r0 -t i2 -f fcfc3.ima
```

The following example will download microcode (fcfc3.ima) to all the SV Routers in the SAN. The **sdnld** command is executed remotely from the daemon (r0) running on server (123.123.123.111).

```
sdnld -d r0 -t sa -f fcfc3.ima -h 123.123.123.111
```

SAN Configuration File (Backup and Emergency Recovery) [sanconfig]

The **sanconfig** command allows you to save the SAN configuration file to an offline file, and then download the file to the SV Router if needed for emergency recovery.

You should save the SAN configuration periodically for effective Emergency Recovery.

Reading SAN Configuration File and Saving to File

Use the **sanconfig read** command to read the SAN configuration file from the SV Routers in the SAN to an offline file. To prevent losing drive configuration information, you should make a copy of this file whenever the configuration changes.

If you do not select a -m option, the default (all three options) will be used.

Usage:

```
sanconfig read -d Cx -e FileName {-m SANCfgType -h host -v}
```

-d Cx — Cx is the SignOn path, as specified in the config file.

-e FileName — The SAN configuration file name.

-m SANCfgType — Optional. SAN Configuration type. Choose one or more of the options. The default includes all three options (physical, logical, and Zone configuration information).

- **physical** — Physical components in the SAN (i.e. SV Routers and drives).
- **logical** — Logical drive configuration in the SAN.
- **zone** — SAN Zone Configuration.

-h host — Optional. The name or IP address of the host running the daemon.

-v — Optional. User confirmation required.

Examples:

The following example will save the SAN configuration to a file (SanFile.san) stored locally in the management server. The **sanconfig** command is executed on a server running the daemon (r0).

```
sanconfig read -d r0 -e SanFile.san
```

Writing SAN Configuration File to SV Router

Use the **`sanconfig write`** command to download the offline SAN configuration file to the SV Routers in the SAN. This will restore all of the drive configurations (simple drives, virtual drives, etc.) from the last save, as well as any zone configurations (Zones, SV Domains, etc.). The physical setup must be exactly the same as it was when the backup was taken.

If you do not select a -m option, the default (all three options) will be used.

Caution ! ***Please wait until all I/O activity is completed before running this command. Otherwise this may cause lost I/Os and system panic.***

Usage:

```
sanconfig write -d Cx -e FileName {-m SANCfgType -h host -v}
```

`-d Cx` Cx is the SignOn path, as specified in the config file.

`-e FileName` The SAN configuration file name.

`-m SANCfgType` Optional. SAN Configuration type. Choose one or more of the options. The default includes all three options (physical, logical, and Zone configuration information).

`physical`	Physical components in the SAN (i.e. SV Routers and drives).
`logical`	Logical drive configuration in the SAN.
`zone`	SAN Zone Configuration.

`-h host` Optional. The name or IP address of the host running the daemon.

`-v` Optional. User confirmation required.

Examples:

The following example will download the physical and logical components of the SAN from a SAN configuration file to the SV Routers. The **`sanconfig`** command is executed on a server running the daemon (r0).

```
sanconfig write -d r0 -e SanFile.san -m physical logical
```

Importing SAN Zone Configuration

Use the **sanconfig import** command to upload Zone information to an SV Router that has been replaced in a multi-router environment.

Note: This is only necessary when there are Zones and more than one SV Router in the configuration. The SV Routers will sync together to get the drive information, but the zone information must be imported.

Caution ! ***Please wait until all I/O activity is completed before running this command. Otherwise this may cause lost I/Os and system panic.***

Usage:

```
sanconfig import -d Cx -e FileName -r NewSLIC# -j CurrentSLIC# {-h
Host -v}
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-e FileName	The SAN configuration file name.
-r NewSLIC#	The new SV Router's Initiator/SLIC number.
-j CurrentSLIC#	The current SV Router's Initiator/SLIC number.
-h host	Optional. The name or IP address of the host running the daemon.
-v	Optional. User confirmation required.

Examples:

The following example will import the zoning information from SV Router I00002 to SV Router I00003. The sanconfig command is executed on a server running the daemon (r0).

```
sanconfig import -d r0 -e SanFile.san -r i3 -j i2
```

SV Router FC Statistics

Use the **svstat** command to view the SV Router vital statistics. If the SV Router (**-t Ixxxxx**) is not specified, the program will display the vital statistics of all the SV Routers in the SAN.

Both the SV Router FC-FC 3's host-side and the device-side interfaces provide statistical data for the following:

Link Failure Count	This count reports the number of times the SV Router's Frame Manager detects a not operational state or other failure of N_Port initialization protocol.
Loss of Synchronization Count	This count reports the number of times that the SV Router detects a loss in synchronization.
Loss of Signal Count	This count reports the number of times that the SV Router's Frame Manager detects a loss of signal.
Primitive Sequence Protocol Error	This count reports the number of times that the SV Router's Frame Manager detects N_Port protocol errors.
Invalid Transmission Word	This count reports the number of times that the SV Router 8B/10B decorder did not detect a valid 10-bit code.
Invalid CRC Count	This count reports the number of times that the SV Router received frames with a bad CRC and a valid EOF. A valid EOF includes EOFn, EOFt, or EOFdti.

The SV Router's power must be cycled to reset the counter. Therefore, you should check the accumulation of errors between a fixed time.

Usage:

```
svstat -d Cx {-t Ixxxxx -h Host}
```

-d Cx Cx is the SignOn path, as specified in the config file.

-t Ixxxxx Optional. Initator/SLIC number of the SV Router.

-h host Optional. The name or IP address of the host running the daemon.

Examples:

The following example will display the vital statistics for SV Router I00001. The **svstat** command is executed remotely from the daemon (r0) running on server (100.1.1.193).

```
svstat -d r0 -t I1 -h 100.1.1.193
```

Error Log Analysis Commands

The **`sreadlog`** command is used to read and display the error or event logs.

The SLIC Daemon creates an error log file (SignOnPath_SLICERR.LOG) to track all of the errors and events in the SAN. The sreadlog command analyzes the error log and displays the appropriate Service Request Number (SRN) for errors or events that need action. Log entries are returned in the following general format:

```
TimeStamp:nnn.Txxxxx.uuuuuuuu.SRN=mmmmm
```

TimeStamp	Time and date when event occurred.
nnn	SignOn Path.
Txxxxx	The device that reported this event.
uuuuuuuu	Unique ID of the device.
mmmmm	The SRN associated with this event (see Appendix A ‘SRN and SNMP Reference’ on page 145).

Note: Do not remove or move the error log file (SignOnPath_SLICERR.LOG) while the SLIC Daemon is activated.

Caution ! ***Do not remove or move the error log file (`CO_slicerr.log`) while the SLIC Daemon is activated.***

Reading the Error Log [sreadlog]

Use the **sreadlog** command to read the error log.

Usage:

```
sreadlog -d Cx {-f File_Name -h Host -v}
```

-d Cx Cx is the SignOn path, as specified in the config file.

-h Host Optional. The name or IP address of the host running the daemon.

-f File_Name Optional. Output event logs to File_Name..

-v Optional. Print event logs to console.

Examples:

The following example will display the event logs. The **sreadlog** command is executed on a server running the daemon (r0).

```
sreadlog -d r0
```

The following example will output the event logs to a file (mylog.txt). The **sreadlog** command is executed remotely from the daemon (r0) running on server (myhost).

```
sreadlog -d r0 -f mylog.txt -h myhost
```

Command Line Diagnostic Commands

Displaying VPD (Vital Product Data) [svpd]

Use the **svpd** command to display important information (Vital Product Data or VPD) for the physical device selected.

```
Vendor ID - xxxxxx
Product Type - xxxx
Model Number - xxx
Microcode Revision - xxxx
Unit Serial Number - xxxxxxxx
Unique ID – xxxxxxxxxxxxxxxx
```

Note: **svpd** only displays the information for a physical device. No logical information is given.

Usage:

```
svpd –d Cx –t [s/Txxxxx] {–f File_Name -h host –v}
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-t [s/Txxxxx]	Target number of the physical device or the SignOn

Router.

s	SignOn Router.
Txxxxx	Target number of the physical device.

-f File_Name	Optional. Output VPD to File_Name.
-h Host	Optional. The name or IP address of the host running the daemon.
-v	Optional. Print VPD to console.

Examples:

The following example will display the VPD of T00005. The **svpd** command is executed on a server running the daemon (r0).

```
   svpd -d r0 -t t5
```

The following example will display the VPD of the SignOn router. The **svpd** command is executed on a server running the daemon (r0).

```
   svpd -d r0 -t s
```

The following example will display the VPD of the SignOn router. The **svpd** command is executed remotely from the daemon (r0) running on server (myhost).

```
svpd -d r0 -t s -h myhost
```

Viewing SV Router Zone Components [slicview]

Use the **`slicview view`** command to view information about the SV Router and all drives and host adapters that are accessible from it.

If an SV Router initiator is specified, then only the information pertaining to that particular SV Router is displayed. When no SV Router initiator is specified, the complete list of SV Routers in the SAN and their accessible drives and host adapters is displayed.

If the host is specified the SV Router initiator number is not required.

Usage:

```
slicview view -d Cx {-r Ixxxxx -h Host -v}
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r Ixxxxx	Optional. Initiator/SLIC Number of the SV Router.
-h Host	Optional. The name or IP address of the host running the daemon.
-v	Optional. Show public zone information.

Examples:

The following example will display the zoning information of SV Router I00003. The **`slicview`** command is executed on a remote server (MYHost) running the daemon (r0).

```
slicview view -d r0 -r I3 -h MyHost
```

The following example will display the zoning information of all the SV Routers in the SAN. The **`slicview`** command is executed on a server running the daemon (r0).

```
slicview view -d r0
```

Host Adapter Commands [sadapter]

The **`sadapter`** command is used to add a host adapter to a SV Router, assign or change alias to a host adapter, or view properties of the host adapters connected to a SV Router.

Viewing Host Adapter Properties

Use the **`sadapter view`** command to view the active/inactive drive list of host adapters connected to the SV Router selected. When a host adapter is specified (either by UID or name), it displays the active/inactive drives for that particular host. If no host adapter is specified, it displays the complete list of hosts and their active/inactive drive list.

Note: When viewing a host adapter's properties, use either -a HostName or -u HostUID to specify the host adapter. If no alias is defined for a host adapter, -u HostUID should be used to identify the host adapter.

Usage:

```
sadapter view -d Cx -r Ixxxxx {-a HostName -u HostUID} {-h Host}
```

`-d Cx` Cx is the SignOn Path, as specified in the config file.

`-r Ixxxxx` Initiator/SLIC Number of the SV Router.

`-a HostName` The name assigned to the host adapter. Not needed if **`-u HostUID`** is used.

`-u HostUID` UID or WWN of the host adapter. Not needed if **`-a HostName`** is used.

`-h Host` Optional. The name or IP address of the host running the daemon.

Examples:

The following example will display the properties of host adapter HBA_A on SV Router I00002. The **`sadapter`** command is executed on a server running the daemon (r0).

```
sadapter view -d r0 -r I2 -a HBA_A
```

The following example will display the properties of host adapter 213784FE74A93DC1 on SV Router I00003. The **`sadapter`** command is executed on a server running the daemon (r0).

```
sadapter view -d c0 -r I3 -u 213784FE74A83DC1
```

The following example will display the properties of all host adapters connected to SV Router I00002. The **`sadapter`** command is executed on a server running the daemon (r0).

```
sadapter view -d r0 -r I2
```

Creating or Changing the Host Adapter Alias

Host adapters are identified by their 16-digit Unique IDs (UID). The UID, also called the worldwide name, cannot be changed. Use **`sadapter alias`** to create an alias to identify a host adapter or to change an existing host adapter alias.

Note: When changing a host adapter's alias, use either the -a HostName or the -u HostUID to specify the host adapter. If no alias is defined for a host adapter, the -u HostUID should be used to identify the host adapter.

Usage:

```
sadapter alias -d Cx -r Ixxxxx -n NewHostName {-a HostName -u
HostUID} {-h Host -v}
```

`-d Cx` Cx is the SignOn Path, as specified in the config file.

`-r Ixxxxx` Initiator/SLIC Number of the SV Router.

`-n NewHostName` The new host adapter name to be assigned.

`-a HostName` The name assigned to the host adapter. Not needed if **`-u HostUID`** is used.

`-u HostUID` UID or WWN of the host adapter. Needed when creating the alias for the first time. When changing the alias, it is not needed if **`-a HostName`** is used.

`-h Host` Optional. The name or IP address of the host running the daemon.

`-v` Optional. User confirmation required.

Examples:

The following example will create an alias (HBA_A) for HBA 213784FE74A83DC1 on SV Router I00002. The **`sadapter`** command is executed on a server running the daemon (r0).

```
sadapter alias -d r0 -r I2 -n HBA_A -u 213784FE74A83DC1
```

The following example will change the alias Data_Host on SV Router I00003 to DB_Host. The **`sadapter`** command is executed on a server running the daemon (r0).

```
sadapter alias -d r0 -r I3 -a Data_Host -n DB_Host
```

Zone Commands [sliczone]

The **`sliczone`** command is used to configure and manage the zones for all the SV Routers in a SAN. All zone commands require the SV Router initiator number.

Creating a Zone

Use the **`sliczone create`** command to create zones. A zone must contain at least one host adapter, which you can use either **`-a HostName`** or **`-u HostUID`** to specify. One or more drives can be included in this zone during the creation process.

A zone is part of an SV domain. If you do not specify an SV domain it will default to the primary SV Domain.

If you do not select the -m option, this program will generate the map in sequence, filling in any gaps in the sequence (similar to the **`-m auto`** behavior).

Usage:

```
sliczone create -d Cx -r Ixxxxx -z ZoneName {-a HostName -u
HostUID} {-t Txxxxx -g DomainName -m [auto/global] -h Host -v}
```

-d Cx Cx is the SignOn Path, as specified in the config file.

-r Ixxxxx Initiator/SLIC Number of the SV Router.

-a HostName The name assigned to the host adapter. Not needed if **-u HostUID** is used.

-u HostUID The UID or WWN of the host adapter. Not needed if **-a HostName** is used.

-z ZoneName The new zone name to be assigned. If not specified, a zone name will be assigned automatically.

-t Txxxxx Optional. The target number of the drive.

-g DomainName Optional. The name of the SV domain.

-h Host Optional. The name or IP address of the host running the daemon.

-m auto/global Optional. Zone map generation.

- **auto** Auto assigns LUN maps in sequence.
- **global** Retains the global map of the drives.

Note: If you do not select the **-m** option, Zone Manager will use the **-m auto** function by default.

-v Optional. User confirmation required.

Examples:

The following example will create a zone (ZONE_NY) with HBA HBA_NY on SV Router I00002. No drive is included in this zone. The **sliczone** command is executed on a server running the daemon (r0).

```
sliczone create -d r0 -r I2 -a HBA_NY -z ZONE_NY
```

The following example will create a zone (ZONE_CA) with HBA HBA_CA and two drives (T16384 and T16385) on SV Router I00002. The **sliczone** command is executed on a server running the daemon (r0).

```
sliczone create -d r0 -r I2 -a HBA_CA -z ZONE_CA -t t16384 t16385
```

Adding Members to a Zone

Use the **sliczone add** command to add members (drives (**-t Txxxxx**)) and/or host adapters (use either **-a HostName** or **-u HostUID**) to a zone. You must specify the name of the zone to which these component members will be added.

Usage:

```
sliczone  add  -d  Cx  -r Ixxxxx -z ZoneName {-t Txxxxx -a HostName
-u HostUID} {-m[auto/global] -h Host -v}
```

-d Cx Cx is the SignOn Path, as specified in the config file.

-r Ixxxxx Initiator/SLIC Number of the SV Router.

-t Txxxxx The target number of the drive.

-a HostName The name assigned to the host adapter. Not needed if **-u HostUID** is used.

-u HostUID The UID or WWN of the host adapter. Not needed if **-a HostName** is used.

-z ZoneName The name of the zone.

-h Host Optional. The name or IP address of the host running the daemon.

-m auto/global Optional. Zone map generation.

- **auto** Auto assigns LUN maps in sequence.
- **global** Retains the global map of the drives. If there are any duplicates, the command will fail.

Note: If you do not select the **-m** option, Zone Manager by default will save the existing zone maps and then fill in any gaps in sequence before proceeding incrementally.

-v Optional. User confirmation required.

Examples:

The following example will add a drive (T16386) to a zone (Zone_NY) on SV Router I0002. The sliczone command is executed on a server running the daemon (r0).

```
sliczone add -d r0 -r I2 -z ZONE_NY -t t16386
```

Deleting Members from a Zone

Use the **`sliczone del`** command to delete existing members from a zone. Members may be host adapters (specified using either **`-a HostName`** or **`-u HostUID`**) or target drives (**`-t Txxxxx`**). You must specify the name of the zone.

Note: Zones must contain at least one host adapter. To delete all host adapters, you must remove the zone (see ‘Removing Zones’).

Usage:

```
sliczone del -d Cx -r Ixxxxx -z ZoneName {-t Txxxxx -a HostName -u
HostUID} {-h Host -v}
```

`-d Cx`	Cx is the SignOn Path, as specified in the config file.
`-r Ixxxxx`	Initiator/SLIC Number of the SV Router.
`-t Txxxxx`	The target number of the drive.
`-a HostName`	The name assigned to the host adapter. Not needed if **`-u HostUID`** is used.
`-u HostUID`	UID or WWN of the host adapter. Not needed if **`-a HostName`** is used.
`-z ZoneName`	The name of the zone.
`-h Host`	Optional. The name or IP address of the host running the daemon.
`-v`	Optional. User confirmation required.

Examples:

The following example will delete one drive (T16385) from a zone (ZONE_CA) on SV Router I0002. The **`sliczone`** command is executed on a server running the daemon (r0).

```
sliczone del -d r0 -r I2 -z ZONE_CA -t t16385
```

Mapping Drives in a Zone

Use the **`sliczone map`** command to re-map the members of a zone—the target drives as viewed by the host adapter. You must specify the name of the zone to map.

This command has no terminal output.

Usage:

```
sliczone map -d Cx -r Ixxxxx -z ZoneName {-h Host -v}
```

`-d Cx` Cx is the SignOn Path, as specified in the config file.

`-r Ixxxxx` Initiator/SLIC Number of the SV Router.

`-z ZoneName` The name of the zone.

`-h Host` Optional. The name or IP address of the host running the daemon.

`-v` Optional. User confirmation required.

Examples:

The following example will remap the drives in a zone (ZONE_NY) on SV Router I00003. The **`sliczone`** command is executed on a server running the daemon (r0).

```
sliczone map -d r0 -r I3 -z Zone_NY
```

Viewing Members of a Zone

The **sliczone view** command is used to view the members of a zone: the host adapters, target drives, and any other devices present. Specify the name of the zone to be viewed.

Usage:

```
sliczone view -d Cx -r Ixxxxx -z ZoneName {-h Host}
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r Ixxxxx	Initiator/SLIC Number of the SV Router.
-z ZoneName	The name of the zone.
-h Host	Optional. The name or IP address of the host running the daemon.

Examples:

The following example will display the properties of a zone (ZONE_NY) on SV Router I00002. The **sliczone** command is executed on a server running the daemon (r0).

```
sliczone view -d r0 -r I2 -z ZONE_NY
```

Removing Zones

Use the **`sliczone remove`** command to remove a zone entirely. Specify the name of the zone to be removed.

Usage:

```
sliczone remove -d Cx -r Ixxxxx -z ZoneName {-h Host -v}
```

`-d Cx`	Cx is the SignOn Path, as specified in the config file.
`-r Ixxxxx`	Initiator/SLIC Number of the SV Router.
`-z ZoneName`	The name of the zone.
`-h Host`	Optional. The name or IP address of the host running the daemon.
`-v`	Optional. User confirmation required.

Examples:

The following example will remove a zone (ZONE_CA) from SV Router I0002. The **`sliczone`** command is executed on a server running the daemon (r0).

```
sliczone remove -d r0 -r I2 -z ZONE_CA
```

APPENDIX A

SRN AND SNMP REFERENCE

SRN	Description	Corrective Action
1xxxx	Disk drive Check Condition status. xxxx is the Unit Error Code. (The Unit Error Codes are returned by the drive in Sense Data bytes 20-21 in response to the SCSI ***Request Sense*** command.)	If too many check conditions are returned then check the link status page 28.
70000	SAN Configuration has changed.	
70001	Rebuild process has started.	
70002	Rebuild is completed without error.	
70003	**Rebuild is aborted with a read error.** This means that the drive copying information can not read from the primary drive.	If a spare drive is available, it will be brought in and used to replace the failed drive. If no spare is available, replace the failed drive with a new drive.
70004	**Write error is reported by follower.** If the initiator is master, then its follower has detected a write error on a member within a mirror drive.	If a spare drive is available, it will be brought in and used to replace the failed drive. If no spare is available, replace the failed drive with a new drive.
70005	**Write error is detected by master.** If the initiator is master, then it has detected a write error on a member within a mirror drive.	If a spare drive is available, it will be brought in and used to replace the failed drive. If no spare is available, replace the failed drive with a new drive.
70006	Router to router communication has failed.	Internal error. Update firmware.
70007	**Rebuild is aborted with write error.** This means the primary drive can not write to the drive being built.	If a spare drive is available, it will be brought in and used to replace the failed drive. If no spare is available, replace the failed drive with a new drive.

Table A-1 Explanation of Service Request Numbers

70008	**Read error is reported by follower.** If the initiator is master, then its follower has detected a read error on a member within a mirror drive.	If a spare drive is available, it will be brought in and used to replace the failed drive. If no spare is available, replace the failed drive with a new drive.
70009	**Read error is detected by master.** If the initiator is master, then it has detected a read error on a member within a mirror drive.	If a spare drive is available, it will be brought in and used to replace the failed drive. If no spare is available, replace the failed drive with a new drive.
70010	CleanUp configuration table is completed.	
70020	SAN physical configuration changed.	If unintentional, check condition of drives.
70021	Drive is offline.	If unintentional, check condition of drives.
70022	SV Router is offline.	If unintentional, check condition of drives.
70023	Drive is unresponsive.	Check condition of drives.
70024	For T3 pack: Master Router has detected the partner SV Router's IP Address.	
70025	For T3 pack: Master Router is unable to detect the partner SV Router's IP Address.	Check the Ethernet connection between the two SV Routers.
70030	SAN configuration changed by SV SAN Builder.	
70040	Host zoning configuration has changed.	
70050	MultiPath drive Failover.	Check MultiPath drive.
70051	MultiPath drive Failback.	
70098	Instant Copy degrade.	If no spare is available, replace the failed drive with a new drive.
70099	Degrade because the drive has disappeared.	Reinsert the missing drive, or replace it with a drive of equal or greater capacity.
7009A	**Read degrade recorded.** A mirror drive was written to, causing it to enter the degrade state.	Reinsert the missing drive, or replace it with a drive of equal or greater capacity
7009B	**Write degrade recorded.** If a spare drive is available, it will be brought in and used to replace the failed drive.	The removed drive needs to be (if good) reinserted or (if bad) replaced.
7009C	**Last primary failed during rebuild**. This is a "multi-point failure" and is very rare.	Backup drive data. Destroy mirror drive where failure has occurred. Format (mode 14) drives. Create new mirror drive. Re-assign old SCSI ID and LUN to mirror drive. Restore data.
71000	Router to Router communication has recovered.	

Table A-1 Explanation of Service Request Numbers

71001	This is a generic error code for the SLIC. It signifies communication problems between the SV Router and the daemon.	1. Check the condition of the SV Router. 2. Check cabling between router and daemon server. 3. Error halt mode also forces this SRN.
71002	This indicates that the SLIC was busy.	1. Check the condition of the SV Router. 2. Check cabling between router and daemon server. 3. Error halt mode also forces this SRN.
71003	SLIC Master unreachable.	Check conditions of the SV Routers in the SAN.
71010	The status of the SLIC daemon has changed.	
72000	Primary/Secondary SLIC daemon connection is active.	
72001	Failed to read SAN Drive Configuration.	
72002	Failed to lock on to SLIC daemon.	
72003	Failed to read SAN SignOn Information.	
72004	Failed to read Zone Configuration.	
72005	Failed to check for SAN changes.	
72006	Failed to read SAN event log.	
72007	SLIC daemon connection is down.	Wait for 1-5 minutes for backup daemon to come up. If it doesn’t, check the network connection, for SV Router error halt, or hardware failure.

Table A-1 Explanation of Service Request Numbers

SRN	SNMP Description	Corrective Action	SRN after Corrective Action
70020 70030 **70050*** 70021	• SAN topology has changed. • Global SAN configuration has changed. • SAN configuration has changed. • A physical device is missing.	• Check SAN cabling and connections between T3 and SV Routers page 110 and page 109. • Perform T3 failback if necessary.	70020 70030 **70051****
70025	Partner's Router's IP is not reachable.	Check Ethernet cabling and connections page 109.	None.
70020 70030 70050 **70025** 70021 70022 **Readings** 72007 72000	• SAN topology has changed. • Global SAN configuration has changed. • SAN configuration has changed. • Partner Router's IP is not reachable. • A physical device is missing. • A SLIC Router is missing. **when error halt on SV Router (not master)** • SLIC daemon connection is inactive - Failed to check for SAN changes. daemon error, check the SLIC Router. • Secondary daemon connection is active.	• Check cabling and connections between SV Routers page 110 and page 109. • Cycle power on failed SV Router if fault LED flashes. • Perform T3 failback if necessary. • Enable VERITAS path.	70020 70030 70050 **70024** 70021 70022
*	T3 LUN Failover.		
**	T3 LUN Failback.		

Table A-2 SRN/SNMP Single Point of Failure Table

APPENDIX B

PORT COMMUNICATION

Port	Port	Port Number
Daemon	Management Programs	20000
Daemon	Daemon	20001
Daemon	Router	25000
Router	Router	25001

Table 8-1 Port Communication Table

APPENDIX C

SERVICE CODES

View these codes by reading the SV Routers LEDs. See 'Reading Service and Diagnostic Codes' on page 25 for more information.

If you do not find a matching service code in the following table, contact Vicom for corrective action. See 'Service and Support' on page 13.

Code Number	Cause	Corrective Action
005	PCI Bus parity error.	Replace router, page 41.
024	The attempt to report one error resulted in another error.	Cycle power to the router. If problem persists, contact Vicom, page 13.
040	Corrupt database.	• Clear SAN database, page 47. • Cycle power to the router. • Import SAN zone configuration, page 127.
041	Corrupt database.	• Clear SAN database, page 47. • Cycle power to the router. • Import SAN zone configuration, page 127.
042	Zone mapping database corruption.	Import SAN zone configuration, page 127.

Code Number	Cause	Corrective Action
050	This message indicates that an attempt to write a value into non-volatile storage failed. It could be a hardware failure, or it could be that one of the databases stored in Flash memory could not accept the entry being added.	• Clear SAN database, page 47. • Cycle power to the router. • If problem persists, contact Vicom, page 13.
051	Can not erase FLASH memory.	Replace router, page 41.
053	Unauthorized cabling configuration.	• Check cabling. Ensure server/ switch connects to host-side and storage connects to device-side of router. • If necessary, clear SAN database, page 47.. • If necessary, cycle router power. • If necessary, Import SAN zone configuration, page 127.
054	Unauthorized cabling configuration.	Check cabling.
057	Too many HBAs attempting to log in.	Check cabling.
060	SAN database successfully cleared.	No action needed.
126	Too many Routers in SAN.	• Remove the extra router. • Cycle router power.
130	Heartbeat connection between routers is down.	• Correct problem. • Cycle the power on the follower router.
400-599 Device side interface driver errors:		
409	FC device-side type code invalid.	• Cycle power • If problem persists, replace router, page 41.
434	Too many elastic store errors to continue. Elastic store errors result from a clock mismatch between transmitter and receiver, and indicates an unreliable link. This error can also occur if a device in the SAN loses power unexpectedly.	• Check for faulty component and replace. • Cycle the power on the follower router.
462	Too many hosts tried to log in.	Check cabling.

Code Number	Cause	Corrective Action
502	Too many ports logged in with fabric.	Check cabling.
539	Too many SV Routers in the SAN	• Remove extra router. • Cycle the power on the follower router.
542	Target has too many LUNs	Check subsystem setup
543	Too many total LUNs (all targets together)	Check cabling.
550	Too many devices logged in with us.	Check cabling.
600-699 Ethernet driver errors:		
601-608	Ethernet port down.	Replace router, page 41.
609-610 612-615 617	Ethernet port down.	• Replace router, page 41. • Send router to Vicom for examination.
618	Corrupt firmware	• Replace router, page 41. • Send router to Vicom for examination.
621	Too many Telnet sessions open.	• Cycle power • If problem persists, contact Vicom, page 13.
624-626	Telnet server down.	• Cycle power • If problem persists, contact Vicom, page 13.
634 638 643 650	TCP down.	• Cycle power • If problem persists, contact Vicom, page 13.
700-899 Host side interface driver errors:		
709 715	FC host-side type code invalid.	• Cycle power • If problem persists, replace router, page 41.
734/434	FC host-side connection error.	Check cabling and connections on both ends, page 109.

GLOSSARY

async alert

A signal sent by a drive or a storage area router to inform the user that an error has occurred with the originator of the signal.

auto rebuild

The storage router automatically replaces the failed drive with the spare drive. Router then copies the data from the primary drive to the spare drive, which is now a member of the mirror drive.

available drive pool

A list of usable, functional drives. This includes composite, simple, and general spare drives.

command line interface

A program that accepts commands as typed-in phrases for both UNIX and NT operating systems.

complex drive

A group of storage drives that contains a single ID and LUN. Complex drives can be mirror, composite, mirror composite or multipath.

composite drive

A combination of multiple drives that are seen by the host computer as one. The host sees one drive with the capacity of all the drives combined. Maximum number of drives that a user may combine is eight. When writing to this drive, the information is written in a sequential manner.

concatenation

See composite drive.

configuration file (config file)

The configuration (config) file defines the function of the SLIC daemon.

daemon

See SLIC daemon.

daemon server

The server used to run the SLIC daemon.

dedicated spare

A drive assigned to replace any failed drive within a designated mirror set.

delete Instant Copy

Removes Instant Copy member from a mirror drive.

device router

The router connected to the storage loop.

disk partition

A designated section of memory created on a disk drive.

disk pool

The disk pool is a group of drives from which virtual drives are created. The group of drives that make up the disk pool are called pool drives. Pool drives are created from mapped drive(s), unmapped drive(s), spare drive(s), or multipath drive(s).

DMP

An acronym for dynamic multi-pathing. A software based process that provides and manages multiple data paths. It provides load balancing across multiple I/O channels and if a path fails, it redirects the data through an alternate route.

encapsulation technique

Creating a partition on a drive for use by the storage router.

Ethernet communication

Also called out-of-band communication. SAN connection where control-related signals are transmitted through TCP, rather than in-band with the data.

failover

Automatic and seamless possession of a device’s operations when it fails.

FC-AL

An acronym for Fibre Channel – Arbitrated loop. A form of Fibre Channel network in which up to 127 nodes are connected in an arbitrated loop topology. All devices share the same bandwidth and only two devices can communicate with each other at the same time.

FC Node

Fibre Channel Architecture. Any device on the FC-AL loop.

GBIC

An acronym for Gigabit Interface Converter. An interface that converts serial optical signals to serial electrical signals and vice versa. The GBIC is designed to transmit signals via Fibre Channel and Ethernet protocol. It can be designed for use with an optical or copper path. The GBIC is also hot-swappable.

general spare

A spare drive prepared to replace any failed mirror drive.

heartbeat

A signal used to identify and ensure that paired failover devices in the network are functioning. Once the partner no longer detects the heartbeat signal then the device will perform failover.

heterogeneous

Dissimilar. In storage it usually refers to servers or storage that have differing protocol (SCSI, FC, SSA etc.) and exist within the same network.

host

The computer that is coordinating the functions of the (local) SV Router in use.

host bus adapter

A device that connects one or more peripheral units to a computer.

host router

The router connected to the host computer.

host server

The computer that is coordinating the functions of the target router in use.

hot plugging (hot swapping)

The connection and disconnection of peripherals or other components without interrupting system operation.

in-band communication

SAN connection where both control-related signals and data are transmitted through the same path.

initiator

A device that originates a signal or a command.

Instant Copy

An Instant Copy drive will duplicate the data on any mirror drive (two-way or three-way) without interrupting normal operating functions.

IOCB

I/O Control Block. It restricts the number of I/O commands sent from the Host Buffer. When the IOCB count is reached, it will issue a “Queue Full” message to the corresponding HBA. Limiting the Queue Depth keeps the host adapters from issuing too many commands, which can slow down system performance.

IOPS

Input/Output Per Second. It is the number of inputs and outputs or read/writes per second.

Ixxxxx

The initiator’s identification number.

local SLIC

The SV Router that is attached to the host computer running the daemon.

logical drive

A group of drives that contain a single ID and LUN. Logical drives can be mirror, composite, mirror composite, Instant Copy or multipath.

logical volume

A designated section of memory created on a disk drive.

logical unit number (LUN)

The SCSI identifier of a logical unit within a target. Each SCSI ID can be divided into eight (0-7) logical units. These logical units can represent whole disks. This identifying number determines the device’s priority.

LUN mapping

The ability to change the virtual LUN number as presented to the server from the storage. This allows such benefits as the ability for a server to boot from the SAN without the requirement of a local disk drive. Each server requires LUN 0 to boot.

LUN masking

Enables an administrator to dynamically map an HBA to a specified LUN. This allows an individual server or multiple servers access to an individual drive or to multiple drives, and prohibits unwanted server access to the same drive(s).

management information base

See MIB.

mapped drive

A drive that is assigned an ID and/or LUN for addressing purposes.

mapping table

See SAN database.

master SLIC (master router)

This is the SV Router that controls the storage loop including the drive configuration. All changes to drives must come through this master.

member drive

A drive within a complex drive. Within a Mirror drive, a member can be a simple or a composite drive.

media

The permanent storage area of a drive.

MIB

Acronym for Management Information Base. A database that describes the objects of the a device monitored by SNMP agent.

microcode

An instructional program to enable the proper operations between electrical functions of the computer and its corresponding device(s).

mirror composite drive

A combined group of drives seen as one drive by the host and mirrored or copied by another drive or combined group of drives.

mirror drive

A group of two or three members that contain the same information. A member of a mirror drive can be a simple or a composite drive.

mirroring

Writing identical information to separate drives simultaneously. Also known as RAID Level 1.

multipath drive

A logical LUN or drive created to hide, from the data server, the active and passive paths to a disk array that does not support multi-initiator attach.

node

Any device on the storage loop.

node mapping table

See SAN database.

node table

See SAN database.

offline

Describes a device that is not connected to or not installed in the storage subsystem. A drive could be connected physically to the SAN, but if it is not turned on or not in ready mode, it is considered offline.

owner

The SV Router or SV Routers that have access to the corresponding drive.

one-way mirror

A drive that contains only one mirror member. A one-way Mirror Drive is designed specifically to transmit data from a physical or a composite drive to an Instant Copy drive. This feature is only useful with the Instant Copy command.

out-of-band communication

SAN connection where both control-related signals and data are transmitted through separate paths.

physical drive

A drive that exist in the storage subsystem. They can be mapped or unmapped drives.

primary member

The drive that is copied via mirroring by other drives.

pool drives

The name for drives in the disk pool.

private drive

A simple drive or a complex drive that can be accessed only by an authorized storage router.

public drive

A drive (simple or complex) that can be accessed by any router on the storage loop.

quick initialize

Prompts SV SAN Builder to write zeros to the first block of the disk. After this process is complete, the drive appears new to the host. The host then will review the drive’s configuration again. It is not a full initialization.

RAID Level 5

Data is striped across three or more drives for performance, and parity bits are used for fault tolerance. The parity bits from two drives are stored on a third drive.

RMBPS

An acronym for Read MegaBytes Per Second. Displays the rate at which data is read from a specific drive within the storage loop.

SAN

Acronym for Storage Area Network. A high-speed network that connects storage devices. The SV Routers are the foundation of the Vicom SAN. They share a common backbone and enable communication between storage device such as; data servers, switches, and disk arrays. In certain cases, the combination of all these devices may also be referred to as a SAN. See "Fully Redundant SVE System" on page 18.

SAN database

A data reference source for the configuration of the SAN. The database is shared among all the SV Routers in the SAN, and each SV Router retains a copy of the database. Each time a change occurs in the SAN, all SV Routers are updated.

SLIC

An acronym for Serial Loop IntraConnect. Often used to represent SV Router.

SCSI-FC Extender

Extends SCSI connectivity to 500 meters, overcoming the SCSI distance constraint.

SCSI ID

An acronym for Small Computer Serial Interface Identification. A unique number, given to each device on the SCSI bus. This identifying number determines the device’s priority. The numbers range from 0-15, with 7 reserved for the host.

SCSI topology

A map or view of all the complex drives on the storage loop.

service and diagnostic codes

A code composed of numbers referring to problems and events within the storage subsystem. Presented through an LED readout on the SV Router.

service request number

See SRN.

serial loop

A loop of devices connected via fibre channel or SSA protocol.

SignOn drive

The logical or physical drive containing all the configuration data that is located on the storage or serial loop. The host communicates with the SAN through this drive.

SignOn path

The path that points to the location of the SLIC Partition on the sign-on drive.

SignOn router

The router attached to the host computer running the SLIC daemon, through which communication to the SAN is established.

simple drive

One storage drive that contains an ID and LUN. It is not a complex drive.

SLIC daemon

A software agent running on the host (either a local or remote server) that permits communication between the client and the subsystem (SV Routers and Drives).

SNMP

An acronym for Simple Network Management Protocol. A network protocol. Used with software (SNMP agent and manager) that monitors the network and transmit the information to the network administrator.

spare drive

See general spare.

SRN

An acronym for Service Request Number. A number used to notify the user of changes or problems that occur within the storage system

SSA

An acronym for Serial Storage Architecture. A storage loop from IBM with speeds that can reach 160 Mbps. The loop’s design provides added security. If one drive fails, access to the storage loop is maintained.

SSA node

Any device on the SSA (Serial Storage Architecture) loop.

SSA topology

A map of the nodes on the SSA loop.

standby drive

An unmapped drive that is a member of a disk pool.

storage subsystem

A combination of disk drives and controllers.

storage capacity

The amount of data that can be stored on each drive or complex drive.

storage virtualization

The secure and dynamic pooling of diverse storage equipment across heterogeneous servers and clients.

SV Router

A Vicom developed hardware module in SVE, which serves as the fundamental building block in a SAN. It provides storage management functions that enable a Fibre Channel host to interface with and control all storage-related elements in a SAN.

SV SAN Builder

A Vicom developed software module in SVE, which creates virtual drives and logical drives on the SAN. Logical drives can be composite drive(s), mirror drive(s), general spare drives, and Instant Copy drives.

SV SNMP Agent

A Vicom developed software module in SVE, which stores and retrieves data from the SAN, and signals the SNMP manager when an event occurs.

SV Zone Manager

A Vicom developed software module in SVE, which enables the system administrator to map logical or physical storage to an HBA. This ability allows the administrator to allocate storage on demand.

target

The recipient of a command or a signal sent by the initiator.

target number

A number assigned to each drive on the loop, except unmapped drives.

target router

The router attached to the host computer.

three-way mirror

Triplicate drives that are created either by data simultaneously written to three separate drives or by data copied from one drive to another drive. Either method ensures that they become duplicates.

two-way Mirror

Duplicate drives that are created either by data simultaneously written to two separate drives or by data copied from one drive to another drive. Either method ensures that they become duplicates.

Txxxxx

The Target’s identification number.

unmapped drive

A drive that has not been assigned an ID and/or LUN for addressing purposes.

virtual drive

A logical drive created from the free space of a disk pool.

VPD

An acronym for Vital Product Data. Information about a device that is stored on the device itself. It allows the device to be administered at a system or network level. Typical VPD information includes a product model number, a unique serial number, product release level, maintenance level, and other information specific to the device type.

web walk The process of a device scanning the storage subsystem.

WMBPS Acronym for Write MegaBytes Per Second. Displays the rate at which data is written to a specific drive within the storage loop.

zone A dedicated path between a LUN and the HBA to which it is mapped.

zoning The act of mapping a LUN(s) to an HBA(s).

INDEX