SVE SUN T3 SOLUTION PACK

Installation

and

Service Manual

For
Command Line Interface
Management

Document Identification:
Number: 310-606114

Revision: 1.3
August 14, 2001

Copyright

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

Trademarks

CONTENTS

LIST OF FIGURES

PREFACE

Document Overview

The *SVE Sun T3 Solution Pack Installation and Service Manual* describes the configuration and troubleshooting of the SVE Sun T3 Solution Pack. The use of the command line interface (CLI), zoning features, and MultiPath drives are specific to this configuration. All other information associated with those features can be found in related publications. See 'Related Publications' on page 15 for a list of related publications.

This document is designed for system administrators who have a working knowledge of the Solaris operating system. Knowledge of Brocade Silkworm switches, Vicom routers, and Emulex HBAs is a plus.

Chapter Overview

Chapter 1 provides an overview of the SVE Sun T3 Solution Pack.

Chapter 2 details installation and configuration of the SVE Sun T3 Solution Pack.

Chapter 3 describes the maintenance of the SV SAN Builder software within the SVE Sun T3 Solution Pack.

Chapter 4 describes the maintenance of the SV Zone Manager software within the SVE Sun T3 Solution Pack.

Chapter 5 describes the maintenance of the SV SNMP Manager software within the SVE Sun T3 Solution Pack.

Chapter 6 describes the maintenance of the SV Router FC-FC 3 within the SVE Sun T3 Solution Pack.

Chapter 7 describes the maintenance of all other components within the SVE Sun T3 Solution Pack.

Chapter 8 provides information for each command in the CLI interface. The commands that are listed are used either in the installation or the maintenance of the SVE Sun T3 Solution Pack.

Chapter 9 describes possible problems and solutions that may occur within the system.

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 (pdf)	Hyperlink	'System Specifications' on page 18

Related Publications

SV Router FC-FC 3 – Installation and User Guide	prt no. 310-606074
SV SAN Builder – Installation and User Guide	prt no. 310-605995
SV Zone Manager – Installation and User Guide	prt no. 310-605996
SV SNMP Agent – Installation and User Guide	prt no. 310-606074
Sun StorEdge T3 Disk Tray Installation, Operation, and Service Manual	prt no. 806-1062-11
Sun StorEdge T3 Disk Tray Administrator's Guide	prt no. 806-1063-11
All associated SUN Server Manuals	
All associated Brocade SilkWorm Switch 2050 rev. 2.2 Manuals	
All associated Veritas Volume Manager 3.1/DMP Manuals	

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 each device listed in 'Related Publications' on page 15. You should have on hand all manuals associated with each device used in the Virtual T3 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 needed information about the system to be installed. It enables users to have a finer understanding of the detailed information in subsequent chapters.

- System Specifications
- System Components
- System Architecture

System Specifications

Out-of-band, remote management features include:

- Two daemons.
  - One primary daemon (located in primary server)
  - One secondary daemon (located in secondary server)
- Up to 32 SANs per active daemon.

SAN features include:

- Up to 2 SV Routers per SAN.
- Up to 6 SUN servers (2 HBAs per server).
- One T3 partner group per SAN (two T3 disk arrays per partner group).
- Up to 32 virtual drives per SAN.

Zoning features include:

- Up to 2 SV Domains per router (only one active at a time).
- Up to 128 targets per SV Routers.
- Up to 128 devices per zone.

System Components

- Components used in this configuration can be interchanged with tested components. For a list of tested components, see "Appendix D" on page 185.
- Ensure you have one laptop computer with either PROCOMM PLUS or Windows Hyperterminal installed. Vicom does not supply these components.
- Two SUN 450 servers in the SAN
  - Solaris 8
  - Solaris 8 Patches
    - Solaris 8 Update 3 and Installation Guide (CD included with the Solaris 8 OS software).
    - 110383-01
    - 108528-06
    - 110255-04
  - Veritas Volume Manager 3.1 with DMP for UNIX (supplied with each Sun StorEdge T3 Array for the Enterprise).
  - Four Emulex 7000 Host Bus Adapters [lpfc2: Firmware Rev. 3.02 (S2F3.02)]
  - Four optical cables with eight GBICs.
- Two SUN Ultra 30 servers for out-of-band, remote management.
    - Solaris 8

      Solaris 8 Update 3 and Installation Guide (CD included with the Solaris 8 OS software.)

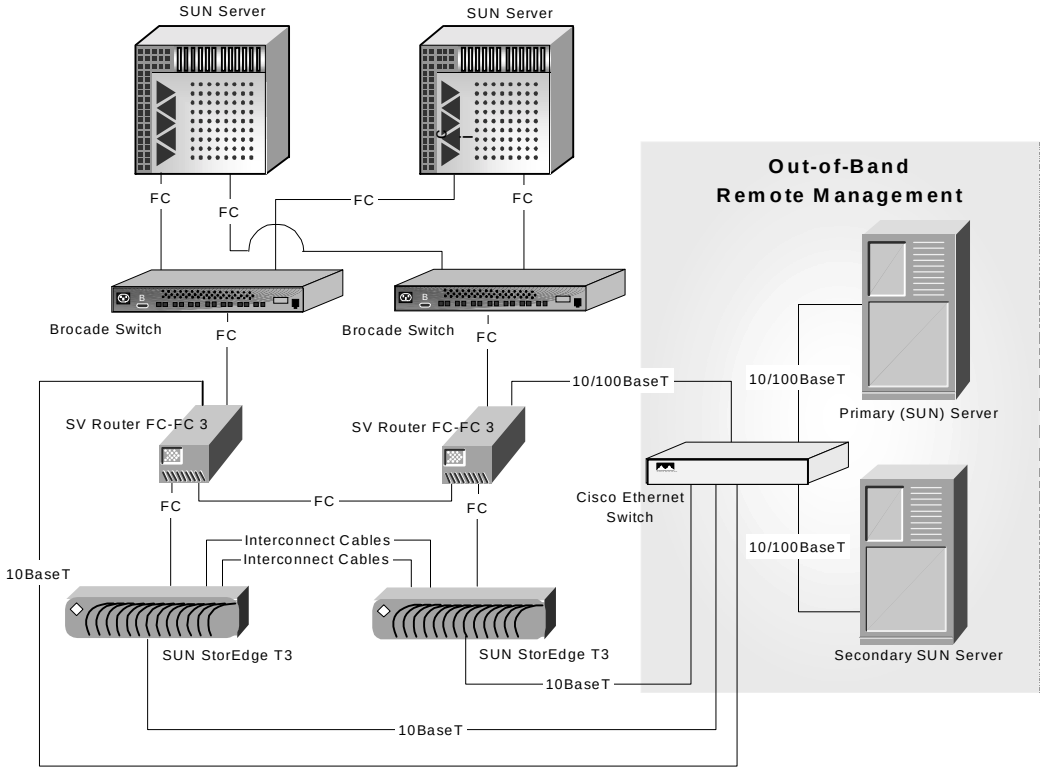
      Other patches are not necessary.
  - SV SAN Builder 2.5 or later software
  - SV Zone Manager 2.5 or later software
  - SV SNMP Agent 1.0 or later software
  - Two 10BaseT or 100BaseT cables

- Two Brocade Silkworm 2050 Switches (tested
  - Kernel: 5.3.1
  - Fabric OS: v2.2.1a
  - Made on: Fri Feb 2 17:45:23 PST 2001
  - Flash: Fri Feb 2 17:46:54 PST 2001
  - BootProm: Wed Sep 22 13:48:55 PDT 1999
- Two SV Routers.
  - Firmware (FC-FC 3 router H Firmware Revision : 8.01.03 or later).
  - Two AC power cords (one per unit, one packaged with each unit).
  - Two DB9 serial port cables (must be purchased separately).
  - Two 10BaseT or 100BaseT cables (must be purchased separately).
  - Three optical cables, with six GBICs (must be purchased separately).

  Note: *If you wish to purchase parts, contact your Vicom service representative. Refer to the SV Router FC-FC 3 – Installation and User Guide for a complete parts list.*

- Two SUN StorEdge T3 Disk Arrays.
  - Firmware Rev. 1.17A or later.
  - Interconnect cables
  - Power Cord
  - Media interface adapter (MIA), one per unit
- Cisco Catalyst 3524-PWR XL Stackable 10/100 Ethernet Switch.
- You must have an IP address, a subnet mask address, and a gateway address for the following components:
  - Two management servers
  - Two SV Routers
  - Two T3 disk arrays

Figure 1-1 SVE SUN T3 Solution Pack System Diagram



System Architecture

The design of the system is to enable one remote manager to manage up to 32 independent SANs. Each SAN will feature no-single-point of failure. For this reason, each SAN is designed with redundant components, dual data paths and RAID Level 5. The remote manager is also designed for 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 is used for failover. It will be used for Daemon failure, for daemon upgrades, or for adding additional SANs. See Figure 1-1 ‘SVE SUN T3 Solution Pack System Diagram’ above.

SUN did not design the T3 partner group to support multiple initiators. To enable this feature, the SV Router was added. It creates multipath drives, which hide, from the data server, the active and passive paths to the T3. If the paths were not hidden, the host would route data to both the paths causing the T3 to be placed in an endless failover loop.

The SV Router not only enables multi-initiator attach, but it also improves storage utilization. It provides virtual drive capability, which allow the T3 partner group, seen as two large LUNs, to be carved into much smaller more manageable drives. The SV Router also provides zoning capability, which maps 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).

Each component, within the system, performs a specific function. Each server contains dual Host Bus Adapters (HBA) and Veritas Volume Manager with DMP software. The DMP software supplies data path redundancy, as well as increased performance by equally spreading I/O through both HBAs. The Brocade switches permit multiple host attachment to the SV Routers. The paired Vicom SV Routers enable remote management and monitoring of the SAN and the storage subsystem. The programs that monitor the system are the SLIC Daemon, and the SNMP Agent. Next, the routers directly connect to the T3 partner group, which provide fault tolerant storage.

CHAPTER 2

SYSTEM INSTALLATION

This chapter first describes the installation and activation of one SAN with remote, out-of-band management. The addition of more SANs, while the system is running, is detailed last.

Step One: StorEdge T3 Setup

The following information is necessary for proper understanding of the T3 setup:

- This manual does not provide step-by-step information needed to configure and install the T3 partner group. The information given, is a general overview of the type of T3 configuration needed with the *SVE SUN T3 Solution Pack*. After reviewing this section, Step One: StorEdge T3 Setup, refer to the *SUN StorEdge T3 Disk Tray Installation, Operation, and Service Manual* for detailed information on T3 configuration and installation.
- Repeat StorEdge T3 Setup for each SAN established.

StorEdge T3 Setup Overview

The first step in the setting up the *SVE SUN T3 Solution Pack* is to configure the StorEdge T3 disk array. This includes:

- creating T3 partner group.
- establishing T3 Ethernet access.
- configuring T3 drives.

Create T3 Partner Group Overview

You will combine two StorEdge T3 disk trays to produce a single StorEdge T3 partner group. The two trays are connected via the “T3 failover path” (as seen in Figure 2-1 below). This connection establishes a data path between trays. When the primary path fails, it is used as part of the secondary path for data access.

Once partnered:

- its official name becomes *SUN StorEdge T3 Array for the Enterprise*.
- it makes one disk tray functions as master and the other as alternate master.
- it provides redundant controller cards. A single disk tray contains only one.
- it provides: RAID 5 with hot-swap capability, redundant unit interconnect cards, redundant power units, and redundant cooling units.
- its storage can expand up to 1.3 TB.

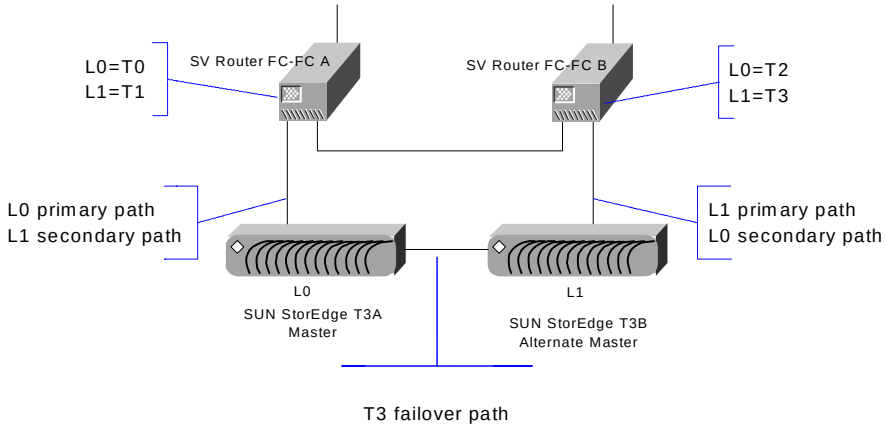
Establish T3 Ethernet Access Overview

To configure and manage the partner group, you must use the T3's Ethernet (10BaseT) connection. You will need the following information: T3 IP Address; Subnet Mask; Gateway IP Address. Connect both Ethernet cables to the Ethernet switch, which will be used for remote management access. Only the master T3 will be accessible under these conditions. However, the alternate master should also be connected in case the master T3 fails.

Configure T3 Drives Overview

For full redundancy, you will configure each disk tray as 8 disk RAID 5 with one spare and dual data paths. To establish dual data paths, you must configure each disk tray as a single LUN.

Figure 2-1 T3 Setup Overview



Components for T3 Setup

- Components used in this configuration can be interchanged with tested components. For a list of tested components, see "Appendix D" on page 185.
- Two SUN StorEdge T3 Disk Arrays.
  - Firmware revision 1.17A or later.
  - Interconnect cables.
  - Power cords.
  - Media Interface Adapter (MIA), one per unit.

T3 Installation and Configuration

Refer to the installation process in the *SUN StorEdge T3 Disk Tray Installation, Operation, and Service Manual*.

After performing SUN's disk tray inspection and following SUN's electrical requirements, edit the host files. Be sure to follow all cautionary notes in the SUN manual.

- Check firmware revision level to ensure correct firmware and patch are installed by typing the telnet command **`ver.`**
- Assign the IP address to the T3 controllers.
- T3 configuration requirements are as follows:
  - T3 must be configured as a "partner group." See *SUN StorEdge T3 Disk Tray Installation, Operation, and Service Manual*, page 2-37, steps 1-8.
  - Establish Alternate Pathing on the Host. See *SUN StorEdge T3 Disk Tray Installation, Operation, and Service Manual*, page 2-44, steps 2 and 3.
  - Configure the T3 for MultiPath Read/Write mode (MP r/w).
  - Configure each disk tray to represent one LUN with one hot spare. See Table 2-1 below.

Volume 1	Volume 2	Hot Spare
8 disk RAID 5	None	X

Table 2-1 Volume Configuration

Step Two: SV Router Setup

SV Router Setup Overview

The second step in the setting up the *SVE SUN T3 Solution Pack* is to configure and cable the SV Routers. This includes:

- enabling SLIC Daemon access to the SV Router
- configuring the device-side of the SV Router
- configuring the host-side of the SV Router
- enabling Ethernet access to the SV Router
- cabling the SV Router

Access SV Router for Configuration Overview

To configure the SV Router, you must use the *User Service Utility* menu located in the SV Router. There are two ways to access this menu.

- The first is through the serial port, using communication software such as; PROCOMM PLUS or Windows Hyperterminal.

  Note: *Because the SV Routers are usually located in a different location from the management server, the communication software is best installed in a laptop computer.*

- The second, is to establish a telnet session using the Ethernet port. However, before you establish Ethernet communication you must first enable Ethernet access to the SV Router.

Enable SLIC Daemon Access Overview

The *Router Management Program* menu, a submenu of *User Service Utility* menu, enables and defines SLIC Daemon access to the SV Router. The menu allows the user to:

- enable out-of-band communication between the router and the SLIC Daemon.
- enable password protection for SLIC Daemon access.

Configure Device-Side Overview

The SV Router's FC port are the two lower FC ports on the rear of the router. See Figure 2-4 on page 33. To enable router compatibility with differing devices, the user may change the device-side FC topology. Here the device-side will be configured for: arbitrated loop mode, and soft loop ID (soft AL-PA). Both are default settings.

Configure Host-Side Overview

The SV Router's FC port are the two upper FC ports on the rear of the router. See Figure 2-4 on page 33. To enable router compatibility with differing host, the user may change the host-side FC topology and mapping algorithms. Here the host-side will be configured for: point to point mode, command queue depth of 736 (default), and direct LUN mapping (default).

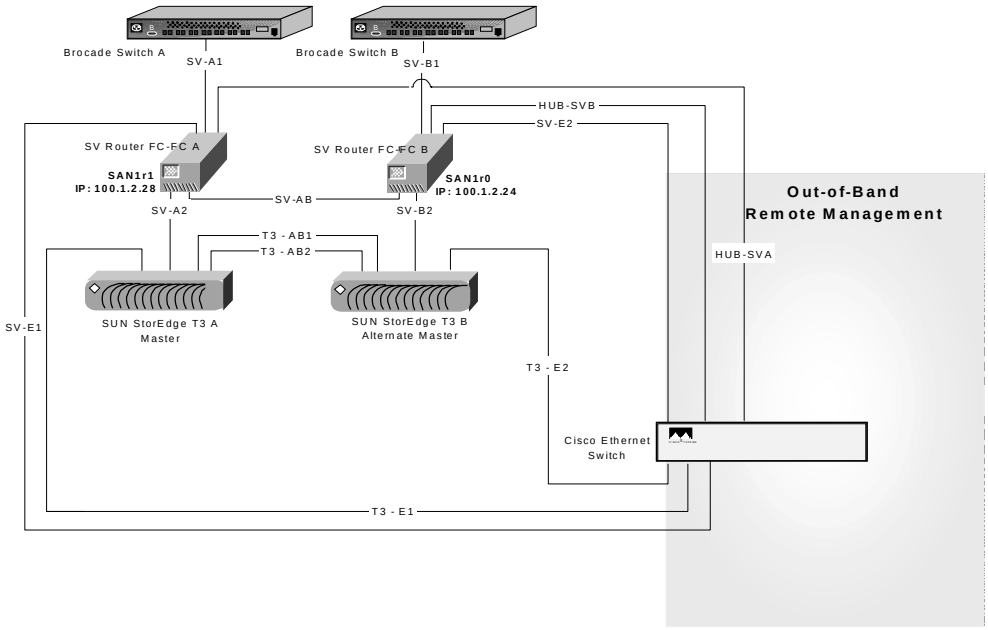
Enable Ethernet Access Overview

The SV Router's Ethernet port is in the lower right-hand corner of the rear of the router. See Figure 2-4 on page 33. By enabling Ethernet access, you will be able to enter the *User Service Utility* menu remotely using a telnet session. It will also be used to establish a heartbeat between the two routers. If one router dies, the heartbeat will activate failover to the live one. To configure the Ethernet settings, you will enter: the IP address, the subnet mask address, the gateway address, the port number 25000 (default), and if needed, the password to secure telnet and ftp access.

Cable SV Router Overview

With optical cabling, you will connect the device-side of each SV Router to one T3 disk tray (E1, E2). You will connect the routers together with the remaining device-side ports (D1). This establishes the SV Router heartbeat. The SV Router will monitor this connection. If a heartbeat is not detected then the slave router will shut down and the master router will send an SRN indicating the problem.

Figure 2-2 SV Router Setup Overview



System Components

- Components used in this configuration can be interchanged with tested components. For a list of tested components, see "Appendix D" on page 185.
- Ensure you have one laptop computer with either PROCOMM PLUS or Window Hyperterminal installed. Vicom does not supply these components.
- Two SV Routers.
  - Firmware (FC-FC 3 router H Firmware Revision : 8.01.03 or later).
  - Two AC power cords (one per unit, one packaged with each unit).
  - Two DB9 serial port cables (must be purchased separately).
  - Two 10BaseT or 100BaseT cables (must be purchased separately).
  - Three optical cables, with six GBICs (must be purchased separately).

  Note: *If you wish to purchase parts, contact your Vicom service representative. Refer to the SV Router FC-FC 3 – Installation and User Guide for a complete parts list.*

Set up Serial Port Communication Software

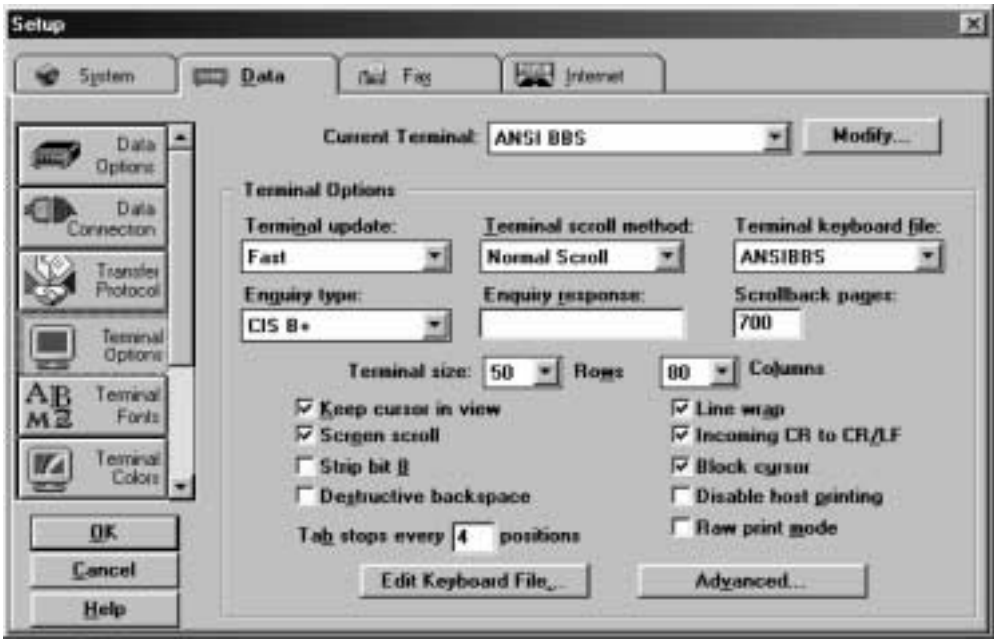
- The computer running the communication software will be used to configure each router's interface settings (host-side, device-side, and Ethernet).
- Associated manual: *SV Router FC-FC 3 – Installation and User Guide*.

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 2-3 "PROCOMM PLUS Terminal Options Setting" below, and select the **OK** button.

Figure 2-3 PROCOMM PLUS Terminal Options Setting



Configure Windows Hyperterminal Communication Software

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

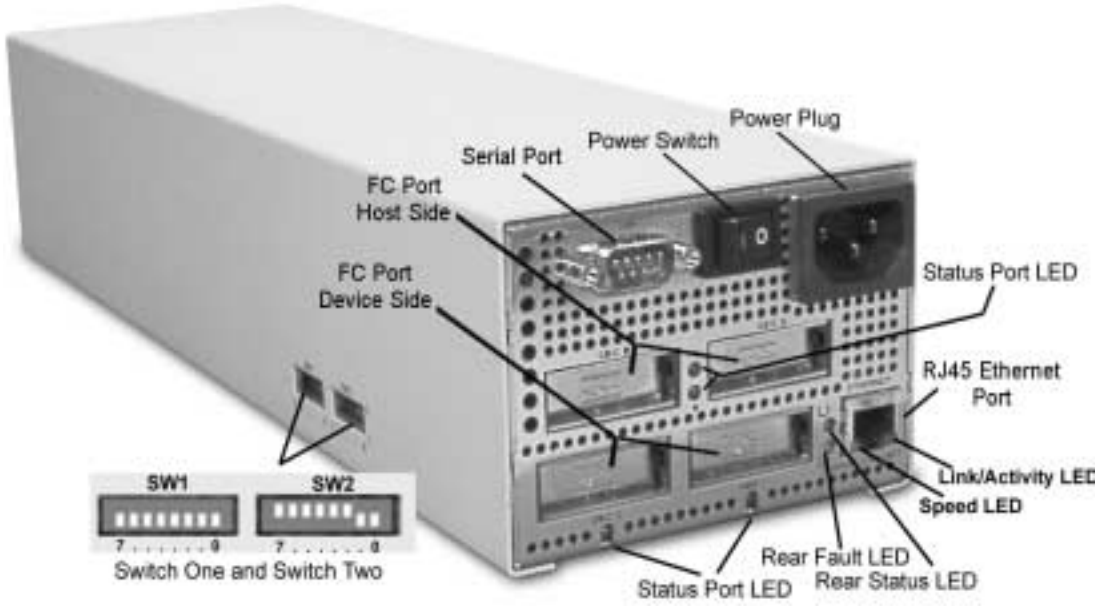
> ***Note:*** *Windows Hyperterminal normally is included with Windows NT and Windows 98 operating systems.*

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.

Configure SV Routers

You must configure one router at a time. After you have configured the first router then repeat all the steps listed under this section (“Configure SV Routers”) to configure the remaining router.

Figure 2-4 SV Router FC-FC 3 Hardware Interfaces



Switch Settings

1. Power off the SV Router. See Figure 2-4 "SV Router FC-FC 3 Hardware Interfaces" for power switch and DIP switch location.
2. DIP switch 1 is unused.
3. Set mode 3 (03h) on DIP switch 2 (SW2) as shown below.

4. The proper switch mode is now set.

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. For interface location, see Figure 2-4 on page 33.
2. Power on the laptop 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.
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 Management Programs

'5': Clear Error Log

'6': View/Change Interface Configuration

'7': Virtual Drive Utility

'9': Clear SAN Database

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

Initial Router Configuration

1. Enter **1** to show the router's VPD. The VPD will display the SV Router's microcode.
   - FC-FC 3 SVE H Firmware Revision : 8.01.03 or later.
2. Enter 9 to Erase the mapping table.
   - A successful command will read **`"SAN database has been cleared!"`**
   - An unsuccessful command will cause the fault LED to light and the status LED to blink. If this occurs, cycle power and try again.
3. 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. WWN is only used to enablein-band communication between the router and the SLIC Daemon. It will not be used in this configuration.
   - 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.

       You will not enter the IP address of the secondary server in this router. You will enter it in the partner router.
   - Y/N = Enable/Disable Password Protection.
     - Enter **Y** to enable password protection.
     - Enter **N** to disable password protection.

       If you do not want a password, do not create a password in the daemon's config file.
     - Password protection in the daemon's config file is explained in "Configure Security Features" on page 79.
   - 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.

- Enter **O** and type the other router's IP address. This establishes a heartbeat between the routers.

Trouble Shooting

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 105 to update microcode.

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

Configure Device-Side, Host-Side, and Ethernet Settings

1. 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

2. Enter **Y** to continue.

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.

4. 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.
5. 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.

Cable SV Routers to T3 Partner Group

From this point forward, to ease confusion, the routers will be referred to as router A and router B, as depicted in Figure 2-5 "SVE SUN T3 Solution Pack Diagram" on page 39. And the remote management servers will be referred to as primary or secondary.

1. Ensure you power off all devices before connecting them.
2. Using an optical cable, connect the device side of router A's FC port to one T3 partner group port. See Figure 2-4 "SV Router FC-FC 3 Hardware Interfaces" on page 33 to determine the location of the router's device side port.
3. Using an optical cable, connect the device side of router B's FC port to the other T3 partner group port.
4. Using an optical cable, connect the two remaining device side FC ports of router A and router B together.

Connection Test

1. Power on the T3 Partner Group then the SV Routers.
2. Start the communication software.
3. Open the communication terminal, and type **hello**.
4. Enter **?** to display the **`User Service Utility Key Assignments:`**
5. Enter **2**

   `'2': Show LUN Map`
6. Each router should see four LUNs (T0, T1, T2, T3).
7. Repeat steps 1-4 for both routers.

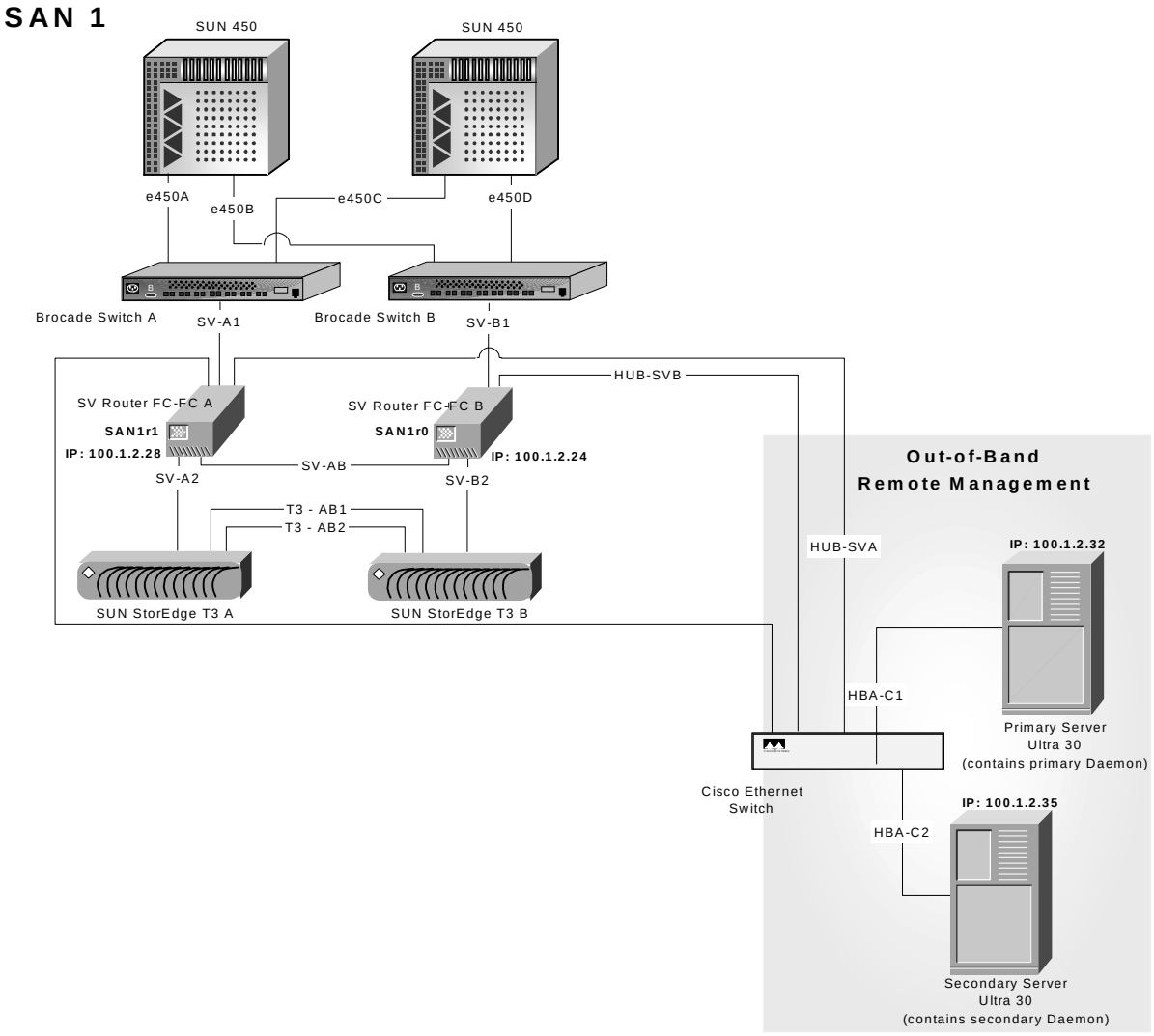
Cable SAN and Remote Management

1. Ensure you power off all devices before connecting them.
2. Using a 10/100BaseT cable, connect the Cisco Ethernet switch to the primary server's Ethernet adapter port. See "Ethernet Port LEDs" on page 172 for information concerning proper LED function.
3. Using a 10/100BaseT cable, connect the Cisco Ethernet switch to the secondary server's Ethernet adapter port.
4. Using a 10/100BaseT cable, connect router B's Ethernet serial port to the Cisco Ethernet switch.
5. Using a 10/100BaseT cable, connect router A's Ethernet serial port to the Cisco Ethernet switch.
6. Power on router A, router B, Cisco Ethernet switch, primary server and secondary server.
7. Using the primary server's and then the secondary server's terminal, ping router A then router B to ensure Ethernet communication is established between both servers and both routers.

Troubleshooting

If communication can not be established by ping, then:
- Check all cabling and connectors between the servers, Ethernet switch, and routers.
- Check TCP/IP settings (IP, Gateway, and Subnet mask addresses).

Figure 2-5 SVE SUN T3 Solution Pack Diagram



Step Three: Setup Remote Management

Remote Management Setup Overview

Because this system configuration is based on high redundancy, the remote management is composed of a primary server and a secondary server. If the primary router, Daemon, or server fails then the secondary router, Daemon, and server take over

In this section, you will install the management software, and use it to configure the SAN. The management software is composed of the following three software programs:

- the SV SAN Builder software. It installs the SLIC Daemon, which monitors and manages the SAN, and most of the Command Lines, which configure the drives and perform basic operations of the SAN.
- the SV Zone Manager software. It installs the remaining Command Lines (primarily commands associated with zoning).
- The SV SNMP Agent software. It delivers information to the SNMP manager concerning the storage subsystem devices. (The SNMP manager is not part of Vicom's software. It must be purchased separately.)

After you have installed the SV SAN Builder software, which installs the SLIC Daemon, you will edit the config file. There you will define:

- the SignOn path, which enables communication between the management server and the storage subsystem.
- the failover settings between the two management servers.

In this chapter, only the SignOn path and the failover configuration are explained. The config file also defines the following information:

- Call Home service, which notifies you via email when a specific service request number (SRN) is sent. SRNs are user defined.
- password protection, which authorizes Daemon SignOn to the SAN.
- IP management features, which prevent unathorized users from accessing the Daemon.

  Note: *Configuration for these features is explained in* "Edit Config File" on page 77*.*

Lastly, you will create two multipath drives. These drives are used to enable multi-initiator attach for the T3 partner group. The SV Router hides, from the data server, the active and passive paths to the T3. If the paths were not hidden, the host would route data to both the paths causing the T3 to be placed in an endless failover loop. See Figure 2-6 "Creation of MultiPath Drives" below.

System Components

- Components used in this configuration can be interchanged with tested components. For a list of tested components, see "Appendix D" on page 185.
- Two SUN Ultra 30 servers for out-of-band, remote management.
  - Solaris 8 OS with *Solaris 8 Update 3 and Installation Guide* (This a CD included with the Solaris 8 OS software)
  - SV SAN Builder 2.5 or later software.
  - SV Zone Manager 2.5 or later software.
  - SV SNMP Agent 1.0 or later software.
  - Two 10BaseT or 100BaseT cables.

Change TCP Settings in Solaris

1. To quickly restart the daemon you need to change the TCP parameters for two kernel device drivers in the primary server.

   ```
   ndd -set /dev/tcp tcp_time_wait_interval 30000
   ndd -set /dev/tcp tcp_fin_wait_2_flush_interval 30000
   ```

2. Wait a few minutes for the changes to take effect.

3. Check changes made by typing the following commands. Returned values will be in milliseconds.

   ```
   ndd /dev/tcp tcp_time_wait_interval
   ndd /dev/tcp tcp_fin_wait_2_flush_interval
   ```

4. Repeat process for secondary server.

Note: *Changes will remain until manually revised or computer reboot.*

Install and Configure SV SAN Builder Software

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

1. In the primary server, login as root.

2. Insert the Vicom SV SAN Builder v2.5 CD-ROM in the CD-ROM drive.

3. Mount the CD-ROM, and change to that directory.

4. Type **`./install.sh <user defined directory>`** and press enter. The default directory is **`/svengine`**.

5. Repeat process for secondary server.

Edit the SLIC Daemon Configuration File

Configure Router SignOn Path

Only the configuration of the SignOn Path and the failover settings will be discussed in this section and the next. To configure other specifications see "SLIC Daemon Config File" on page 74.

1. In the primary server, open and edit the config file svengine.cfg located in the sdus directory to name the router's SignOn path and reference the router's IP address.

   # **/svengine/sdus/svengine.cfg**

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.

   - In the text file, the sample text names the first SignOn path for the router '**r0**' as seen above in step 2. Where **r0** appears, susbstitute the name of the SignOn path for one of the routers in SAN 1 (the example below uses SAN1r0) and enter that same router's IP address. See example below.

Example of Primary Daemon:

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

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

Example of Secondary Daemon:

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

Note: *Only one SignOn path per daemon can be configured. If the router for the primary daemon fails, then failover will occur. The secondary daemon will become active and use its router as the SignOn path.*

Configure the Failover Settings

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. Remove the comment line indicators (**#**), and substitute the following information as needed.

3. Where the SAN name (**SAN1)** appears, replace it with the name of your SAN (user defined).

4. Where the IP address of the **PrimaryDaemon** appears, substitute the IP address of the primary server.

5. Where the router's SignOn path name (SAN1**r0**) appears, substitute the router that corresponds with that daemon as configured in the **Router Sign On Path**.

6. Where the IP address of the **SecondaryDaemon** appears, substitute the IP address of the secondary server.

7. Where the router's SignOn path name (SAN1**r1**) appears, substitute the router that corresponds with that daemon as configured in the **Router Sign On Path** file.

8. To configure the **Failover Daemon Settings** in the secondary daemon (located in the secondary 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;
};
```

Install SV Zone Manager Software

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

1. In the primary server, login as root.
2. Insert the Vicom SV Zone Manager v2.5 CD-ROM in the CD-ROM drive.
3. Mount the CD-ROM, and change to that directory.
4. Type **`./install.sh <user defined directory>`** and press enter. The default directory is **`/svengine`**.
5. Repeat process for secondary server.

Start the Daemon

1. In the primary server, 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 daemon program running

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

Example with 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.

6. Repeat process for secondary server.

Note: *To shut down the daemon see* "Stop Daemon" on page 73.

Test the Failover Configuration

1. In the primary server, run the command line **`slicd`** from the svengine directory to start the primary daemon.

```
# ./slicd
```

2. In the secondary server, run the **`slicd`** command from the svengine directory, to start the secondary daemon.

3. In the primary server, run the command line **saninfo.** Where **SAN1r0** appears, substitute the name of one of the routers' SignOn path that you entered in the config file.

   # /svengine/sduc/saninfo -d SAN1r0

   - This program provides a list of all the daemons running and their status.
   - The example below shows the normal status of the primary and secondary daemons.

Example:

```
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
```

4. Power off the router associated with the primary daemon (**SAN1r0**).

5. Run the **saninfo** command.

Below is an example of a successful failover.

#/svengine/sduc/saninfo -d SAN1r0

Example:

```
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
```

6. Power on the router that was powered off in step 4.

7. Restore primary daemon by running the **setmasterdaemon** executable file.

   #/svengine/sdus/setmasterdaemon -d SAN1r0

8. Run the **saninfo** command to ensure that you have restored the primary daemon.

   #/svengine/sduc/saninfo -d SAN1r0

The example below shows the normal status of the primary and secondary daemons.

Example:

```
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
```

Install SV SNMP Agent in Both Servers

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

1. In the primary server, login as root.
2. Insert the Vicom SV SNMP Agent v1.0 CD-ROM in the CD-ROM drive.
3. Mount the CD-ROM, and change to that directory.
4. Type **./install.sh <user defined directory>** and press enter. The default directory is **/svengine**.
5. Repeat process for secondary server.

Configure the SAN List Specifications

The SAN List provides the SV SNMP Agent with the proper information needed to access and monitor the storage subsystem. The maximum number of entries is 32.

1. In the primary server, 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 example 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 router SignOn path (SAN1**r0**) listed in the **PrimaryDaemon** path in "Configure the Failover Settings" on page 44.
- Under **Host_IPAddress** type the IP address listed in the **PrimaryDaemon** path in "Configure the Failover Settings" on page 44.
- Under **Tcp/Ip_Port** type **default**. Default is 20000. Vicom highly recommends that you use the default port.

3. Repeat process for secondary server.

Configure the Trap Client List Specification

The Trap Client List provides the SV SNMP Agent with the proper information needed to send storage subsystem information to the SNMP manager in the form of MIBs. The maximum number of entries is 32.

1. In the primary server, return to the **SNMPagent** directory.
2. Open and edit the trapclientlist.cfg file.

```
#TrapClient_IPAddress    TrapClient_Port_Number    TrapClient_SeverityFil
                                                   ter_Number

123.123.456.11           162                       6
```

- Directly under the example 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.
- 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

3. Repeat process for secondary server.

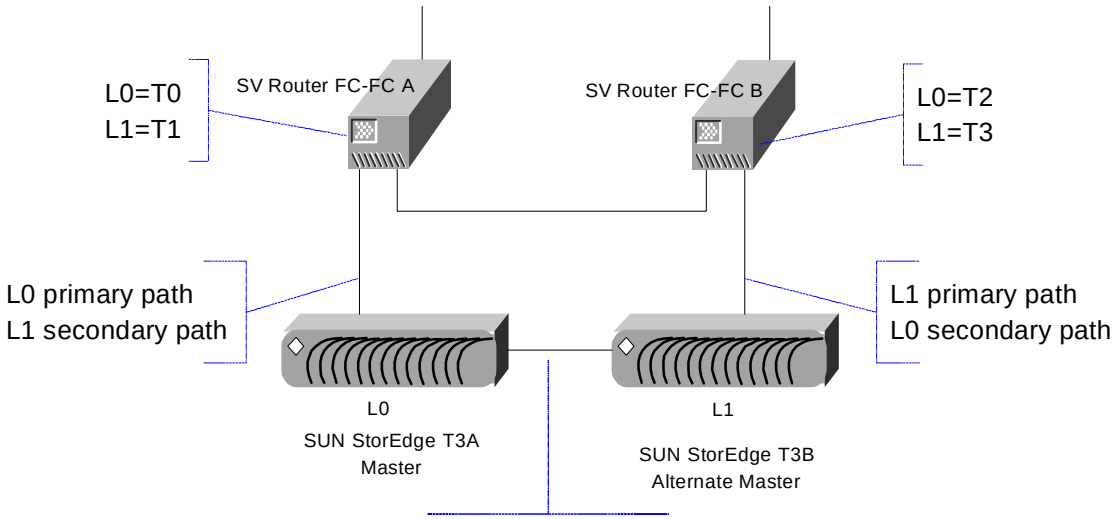
Create Multipath Drives

For a complete list of commands, refer to the Command Line Interface section in the *SV SAN Builder – Installation and User Guide* and the *SV Zone Manager – Installation and User Guide.*

For a list of commands associated with the following functions, See "Basic Command Line Interface" on page 131.

1. Power on the T3 partner group, the routers, the Ethernet switch, and the remote management servers.
2. Ensure that the router in each SAN can see all four T3 LUNs. Using the laptop computer, access the serial port to view the T3 LUNs. If you configured each T3 to represent only one LUN (as detailed in "T3 Installation and Configuration" on page 26) then each SV Router instead of mapping two LUNs will map four LUNs (T0, T1, T2, T3). SeeFigure 2-6 below.
   - Start communication software.
   - Type **`hello`**
   - Enter **`?`**
   - Enter **`2:Show LUN Map`**

Figure 2-6 Creation of MultiPath Drives



3. Change to the sdus directory.

   Example: **`# cd /svengine/sdus/`**

4. Type **`ps –ef | grep slicd`** to ensure that the primary SLIC Daemon program is running in the primary server.

Example with 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.*

Example with no daemon program running

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

Note: *If not running, See* "Start the Daemon" on page 45.

5. Type **`ps –ef | grep svmgmtagent`** to ensure that the primary SNMP Agent program is running in the primary server.

Example SNMP Agent program running

```
root 26352 26342  0 15:06:40 ?        0:00 ./svmgmtagent
```

Example SNMP Agent program not running

```
root 1155 1148 0  14:40:57 pts/8    0:00   grep svmgmtagent
```

Note: *If not running, See* "Start" on page 95.

6. Ensure that the secondary daemon and the SNMP Agent are activated in the secondary server.
7. Change to the sduc directory.

Example:

```
#/svengine/sduc
```

8. Using the **`mpdrive autocreate`** command, create MultiPath drives. Each T3 tray will become a MultiPath drive producing a total of 2 MultiPath drives.

   See "Autocreating a MultiPath Drive" on page 145 for more information.

Example for SAN 1

```
mpdrive autocreate -d SAN1r0
```

Usage

```
mpdrive autocreate -d SAN1r0
```

-d SAN1r0	SAN1r0 is the SignOn path, as specified in the config file.

9. Using the **`mpdrive view`** command, view the SV Router map to determine the target numbers associated with each MultiPath drive. See "Viewing MultiPath Drive Properties" on page 147 for more information.

Example Command

`#/svengine/sduc/mpdrive view -d SAN1r0`

The first line of the information returned contains the target number of the MultiPath drive.

`Property of Dynamic MultiPath Drive T49152`

Note: *SV SAN Builder automatically generates target numbers (t49152, t49153) for the new MultiPath drives created.*

10. Using the **`vdiskpool create`** command, create a disk pool and place the MultiPath drives in the pool.

    The **`vdiskpool create`** command creates one disk pool out of drives belonging to the SAN. See "Creating a Disk Pool" on page 137 for more information.

Example for SAN 1

`#/svengine/sduc/vdiskpool create -d SAN1r0 -t t49152 t49153 -n poolSAN1`

Usage

-d SAN1r0	SignOn Path
-n	[PoolName] The name of the disk pool.
-t	Optional. Add a particular drive, add all spare drivesf1

Step Four: Setup Servers and Switches

Servers and Switches Setup Overview

In this section, you will install the servers and switches, and configure and zone the drives.

Setup Server Overview

First you will install and cable the HBAs and the switches. Test the switches to ensure the HBAs are connected. This is done by accessing each switch and viewing the WWNs of the HBAs connected. Determine which HBA belongs to which server. This information is used later when you create zones.

Next you will install the Veritas Volume Manager in each server within the SAN. In the config file (vxdmp.conf) you must list the name of the virtual drives. This process enables Veritas Volume Manager to perform dynamic multi-pathing (DMP) to the virtual drives.

Configure and Zone the Drives Overview

Finally you must create a disk pool, virtual drives, and zones.

- 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).
- The virtual drive command divides the T3 partner group, which are two large LUNs, into multiple smaller LUNs. The LUNs can be as small as a half a gigabyte and as many as 32 per SAN. In the example given, the new LUNs or virtual drives are created one at a time, allowing you to determine the size of each drive. To automatically create drives you can use the command **`vlun autocreate.`** See "Autocreating a Virtual Drive" on page 142 for more information. This process automatically creates the same sized drives, until all the LUN's free space is used.
- The zoning process maps a virtual drive to an HBA, allowing that HBA to have full access to that virtual drive. This access is private unless you map other HBAs to the same drive. To begin the zoning process, you will first assign an alias to each HBA, this will help you remember the name instead of the UID of each HBA. Next, you will create a zone and then add the drive(s) and the HBA(s). If the HBA and the drive share the same zone then they are considered mapped to each other. Drives can be physical, logical or virtual. In this case, all the drives will be virtual. You may zone each HBA to all the disk drives or to various disk drives.

After you have completed this section you will have a fully functional T3 Solution Pack. However, you will probably want to add additional SANs (up to 32) to the remote management station. This process is explained in the next section, "Step Five: Adding Additional SANs" on page 64.

System Components:

- Components used in this configuration can be interchanged with tested components. For a list of tested components see "Appendix D" on page 185.
- Two SUN 450 servers in the SAN.
  - Solaris 8
  - Solaris 8 Patches
    - Solaris 8 Update 3 and Installation Guide (The CD included with the Solaris 8 OS software.)
    - 110383-01
    - 108528-06
    - 110255-04
  - Veritas Volume Manager 3.1 with DMP
  - Four Emulex 7000 Host Bus Adapters [lpfc2: Firmware Rev. 3.02 (S2F3.02)]
  - Four optical cables with eight GBICs
- Two Brocade Silkworm 2050 Switches
  - Kernel: 5.3.1
  - Fabric OS: v2.2.1a
  - Made on: Fri Feb 2 17:45:23 PST 2001
  - Flash: Fri Feb 2 17:46:54 PST 2001
  - BootProm: Wed Sep 22 13:48:55 PDT 1999

Setup Servers

Install Emulex 7000 HBA

Referring to the SUN and Emulex service manuals, install the Emulex 7000 HBAs.

1. Edit **`lpfc.conf`** file located in **`/kernel/drv/`** and set the topology to **`point-to-point mode`**.

   lpfc.conf is located in the driver installation directory and contains all the variables that control driver initialization.

Example:

```
# topology:  link topology for initializing the Fibre Channel connection.
#            0 = attempt loop mode, if it fails attempt point-to-point mode
#            2 = attempt point-to-point mode only
#            4 = attempt loop mode only
#            6 = attempt point-to-point mode, if it fails attempt loop mode
# Set point-to-point mode if you want to run as an N_Port.
# Set loop mode if you want to run as an NL_Port.
topology=2;
```

2. Edit the Config.file the **`lun-queue-depth.`** Use the formula below to determine the proper queue depth.

LUN-Queue-Depth Formula

736 ÷ (n Virtual Drives) x (2 HBAs) = # of queues for each HBA

Note: *736 is the IOCB size on the host side interface of the SV Router*

Example

- 32 Virtual Drives
- 2 HBAs (constant)

736 ÷ (32 x 2) = 11

```
# lun-queue-depth: the default value lpfc will use to limit
# the number of outstanding commands per FCP LUN. This value is
# global, affecting each LUN recognized by the driver, but may be
# overridden on a per-LUN basis (see below). RAID arrays may want
# to be configured using the per-LUN tunable throttles.
lun-queue-depth=92;
```

3. Edit **sd.conf** file in each server so that the HBAs scan the LUNs.

   To allow the system to scan 32 LUNs (from LUN = 0 to LUN = 31) from Target 0, make the following changes in sd.conf:

Example:

```
# cd /kernel/drv
# vi sd.conf

name="sd" parent="lpfc" target=0 lun=0;
name="sd" parent="lpfc" target=0 lun=1;
name="sd" parent="lpfc" target=0 lun=2;
name="sd" parent="lpfc" target=0 lun=3;
name="sd" parent="lpfc" target=0 lun=4;
name="sd" parent="lpfc" target=0 lun=5;
name="sd" parent="lpfc" target=0 lun=6;
name="sd" parent="lpfc" target=0 lun=7;
name="sd" parent="lpfc" target=0 lun=8;
name="sd" parent="lpfc" target=0 lun=9;
name="sd" parent="lpfc" target=0 lun=10;
name="sd" parent="lpfc" target=0 lun=11;
name="sd" parent="lpfc" target=0 lun=12;
name="sd" parent="lpfc" target=0 lun=13;
name="sd" parent="lpfc" target=0 lun=14;
name="sd" parent="lpfc" target=0 lun=15;
name="sd" parent="lpfc" target=0 lun=16;
name="sd" parent="lpfc" target=0 lun=17;
name="sd" parent="lpfc" target=0 lun=18;
name="sd" parent="lpfc" target=0 lun=19;
name="sd" parent="lpfc" target=0 lun=20;
name="sd" parent="lpfc" target=0 lun=21;
name="sd" parent="lpfc" target=0 lun=22;
name="sd" parent="lpfc" target=0 lun=23;
name="sd" parent="lpfc" target=0 lun=24;
name="sd" parent="lpfc" target=0 lun=25;
name="sd" parent="lpfc" target=0 lun=26;
name="sd" parent="lpfc" target=0 lun=27;
name="sd" parent="lpfc" target=0 lun=28;
name="sd" parent="lpfc" target=0 lun=29;
name="sd" parent="lpfc" target=0 lun=30;
name="sd" parent="lpfc" target=0 lun=31;
```

4. Install in the remaining server following the process above.

Cable Switches and Servers

Refer to Brocade service manual, and assign an IP address for each switch.

Refer to Figure 2-5 "SVE SUN T3 Solution Pack Diagram" on page 39 for naming convention.

1. Ensure you power off all devices before connection.
2. Using an optical cable, connect e450A to Brocade Switch A.
3. Using an optical cable, connect e450B to Brocade Switch B.
4. Using an optical cable, connect e450C to Brocade Switch A.
5. Using an optical cable, connect e450D to Brocade Switch B.

Check Configuration and Retrieve WWNs

From the management station, telnet to each switch and ensure all the appropriate devices are connected to that switch. The devices are represented by World Wide Names (WWNs).

Record the HBA's WWNs. You will use the WWNs in section, "Create and Configure Zones" on page 59.

```
#switchshow
```

Install Veritas Volume Manager

1. Edit **`vxdmp.conf`** file located in **`/kernel/drv/`** and type the name of the virtual drives in the dmp_jbod field. This enables the Veritas DMP to recognize the virtual drives created by SAN Builder. The name or names used must be consistent with the names of the virtual drives created in "Create and Allocate Virtual Drives" on page 61.

Example:

```
name="vxdmp" parent="pseudo" instance=0
dmp_jbod="VICOMSVD0";"VICOMSVD1";"VICOMSVD2";"VICOMSVD3";
```

Note: *You may use one name in place of multiple names for the virtual drives. However, you will have to rely on the target numbers of the drives for identification when managing them.*

2. Install Veritas Volume Manager in the remaining server following the process above.

Create and Configure Zones

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

You must use the management station to create and configure zones for the servers.

1. Change to the sduc directory.

Example:

```
#/svengine/sduc
```

2. Using the **showmap** command, view the SV Router map to determine the initiator number automatically assigned to each SV Router (I00001, I00002, etc.) as seen below in the Example for One Server in SAN 1. See "Listing Device Connections [showmap]" on page 133 for more information.

Example:

```
showmap -d SAN1r0 -m slic
```

Usage:

-d SAN1r0	SignOn Path
-m slic	Output List of SV Routers table. See Figure 8-1 "List of SLICs Table – Initiator & Target Mode" on page 134 for an example of the table.

3. Using the **`sadapter alias`** command, assign an alias for each HBA. Limit alias to 12 characters.

   This command is used to create an alias for the HBA of the servers. See "Create or Change Alias of Host Adapter" on page 149 for more information.

   Telnet each switch **`#switchshow`** to determine the WWN of the HBA. See "Check Configuration and Retrieve WWNs" on page 58 for more information.

Example for One Server in SAN 1

```
sadapter alias -d SAN1r0 -r I1 -u 2137845600000001 -n e450A
sadapter alias -d SAN1r0 -r I2 -u 2137845600000002 -n e450B
sadapter alias -d SAN1r0 -r I1 -u 2137845600000003 -n e450C
sadapter alias -d SAN1r0 -r I2 -u 2137845600000004 -n e450D
```

Usage:

-r I1	The SV Router initiator number.
-u **`2137845600000001`**	The host adapter UID.
-n e450A	The new host adapter name to be assigned.

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

4. Using the **`sliczone create`** command, create a zone and add the HBAs in both routers (i.e., two HBAs per server). See "Create Zone" on page 151 for more information.

Example of zone created for each HBA in one server

```
sliczone create -d SAN1r0 -r I1 -a e450A -z e450Zone
sliczone create -d SAN1r0 -r I2 -a e450B -z e450Zone
sliczone create -d SAN1r0 -r I1 -a e450C -z e450ZoneB
sliczone create -d SAN1r0 -r I2 -a e450D -z e450ZoneB
```

Usage:

-a e450A	The name assigned to the host adapter.
-z e450Zone	The new zone name to be assigned.

5. Using the **`sanconfig read`** command, save the SAN configuration to a file. The user must specify the name of the file and the path. See "Reading SAN Configuration File and Saving to File" on page 158 for more information.

Example

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

Usage:

-e /SANconf/T3SAN.san The SAN configuration file name (including path).

6. Using the **`slicview view`** command, to view the router zone configuration information to ensure that all zones were assigned to their designated HBAs. See "View Properties of SLIC" on page 163 for more information.

Example

```
slicview view -d SAN1r0
```

Create and Allocate Virtual Drives

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

Use remote management to create and allocate drives for the data servers.

1. Change to the sduc directory.

Example:

```
#/svengine/sduc
```

2. Using the **`vlun create`** command, create virtual drives.

   See "Creating a Virtual Drive" on page 141 and "Autocreating a Virtual Drive" on page 142 for more information.

Example

```
vlun create -d SAN1r0 -l 10 -t t49152 -n VICOMSVD0
```

(This will create a 10GB virtual drive named VICOMSVD0 from the MultiPath drive t49152.)

```
vlun create -d SAN1r0 -l 20 -t t49153 -n VICOMSVD1
```

(This will create a 20GB virtual drive named VICOMSVD0 from the MultiPath drive t49153.)

Usage:

-l [size]	New virtual drive size in GB.
-n [VdriveName]	Optional. The name of the virtual drive.
-t [Txxxx]	Optional. The target number of the physical drive in the disk pool to be used.

Note: *"-n VICOMSVD0" enables the Veritas DMP to recognize the virtual drives created by SAN Builder. It is the name of the virtual drives created above. The name or names used must be consistent with the names of the virtual drives in the Veritas configuration file in* "Install Veritas Volume Manager" on page 58*.*

3. Using the **`vdiskpool`** command, determine the virtual drives' target numbers.

Example

```
vdiskpool view -d SAN1r0
```

4. Using the **sliczone add** command, add newly created drives to the each zone.

   See "Adding Zone Components" on page 152 for more information.

Example

```
Newly created drives are T16384 T16385 T16386 T16387.
sliczone add -d SAN1r0 -r I1 -t T16384 T16385 -z e450Zone
sliczone add -d SAN1r0 -r I2 -t T16384 T16385 -z e450Zone
sliczone add -d SAN1r0 -r I1 -t T16386 T16387 -z e450ZoneB
sliczone add -d SAN1r0 -r I2 -t T16386 T16387 -z e450ZoneB
```

Usage:

-d SAN1r0	SignOn Path
-r I1	[PoolName] The name of the disk pool.
-t T16384	Optional. Add a particular drive, add all spare drives.
-z e450Zone	The new zone name to be assigned.

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

Example

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

6. Using the **vdiskpool view** command, view a disk pool to ensure virtual drives were added successfully.

   See "Viewing a Disk Pool" on page 140 for more information.

Example:

```
vdiskpool view -d SAN1r0
```

7. Using the **sadapter view** command, view the devices that are assigned to each HBA.

   See "View Properties of Host Adapter" on page 148 for more information.

Example:

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

Step Five: Adding Additional SANs

Up to 32 SANs per active daemon.

1. Perform "Step One: StorEdge T3 Setup" on page 24.
2. Perform "Step Two: SV Router Setup" on page 27.
3. Configure SignOn path for additional SANs. See "Configure Router SignOn Path" on page 43 if necessary.

Example for Primary Server

```
SAN1r0 = {
        internet_path = 100.1.2.24;
};
SAN2r0 = {
        internet_path = 100.1.2.44;
};
SAN3r0 = {
        internet_path = 100.1.2.64;
};
```

Example for Secondary Server

```
SAN1r1 = {
        internet_path = 100.1.2.28;
};
SAN2r1 = {
        internet_path = 100.1.2.48;
};
SAN3r1 = {
        internet_path = 100.1.2.68;
};
```

4. Configure failover settings for additional SANs. See "Configure the Failover Settings" on page 44 if necessary.

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;
        };
SAN3 = {
        name = SAN3;
        PrimaryDaemon = 100.1.2.32, SAN3r0;
        SecondaryDaemon = 100.1.2.35, SAN3r1;
        };
```

Note: *The secondary server's configuration is identical to the primary server's.*

5. Start the primary daemon. See "Start and Stop Daemon" on page 73 for more information.

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

6. Using the **setmasterdaemon** command, 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 156 for more information.

Example

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

#svengine/sdus/setmasterdaemon -d SAN2r0

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

7. To configure the secondary daemon (located in the secondary server), repeat steps 1-6 above.

8. Test failover. See "Test the Failover Configuration" on page 46. The examples below represent a configuration using three SANs.

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
4   100.1.2.32    SAN3r0   0          Primary Daemon       OK
5   100.1.2.35    SAN3r1   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
2   100.1.2.32    SAN3r0   0          Primary Daemon       OK
3   100.1.2.35    SAN3r1   0          Secondary Daemon     Idle
```

9. Update SAN list specifications. See "Configure the SAN List Specifications" on page 48 if necessary. The examples below represent a configuration using three SANs.

Example:

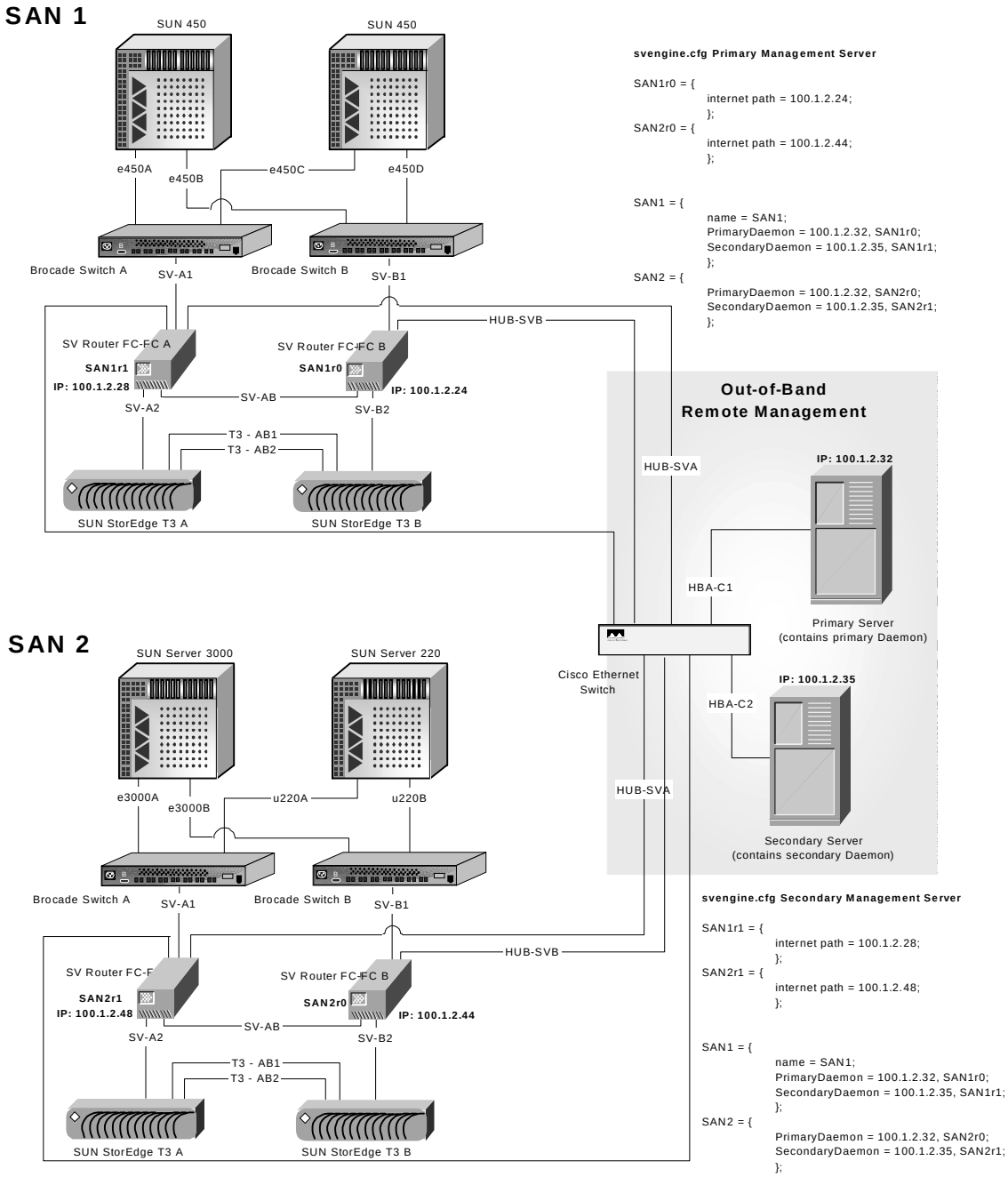
```
#SAN_Name       Daemon_Name      Host_IPAddress     Tcp/Ip_Port

#SAN1           r0               123.123.456.789    default
SAN1            SAN1r0           100.1.2.32         default
SAN2            SAN2r0           100.1.2.32         default
SAN3            SAN3r0           100.1.2.32         default
```

10. Initialize the additional SAN. See "Create Multipath Drives" on page 50.

11. Perform "Step Four: Setup Servers and Switches" on page 54.

Figure 2-7 Multiple SAN Configuration



CHAPTER 3

SV SAN BUILDER

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 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
- SLIC 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 at least one of the servers used in the management station. It should contain the software program.
   - If SV SAN Builder has not been installed in the management station, install it now. See "SV SAN Builder Installation" on page 71.
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 Installation" on page 71.

Note: *The version displayed represents both SV SAN Builder and SV Zone Manager.*

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.

Install

1. Ensure you have the latest software (2.5 or later). If you do not know how to determine the software version, see "Determine SV SAN Builder Software Version" on page 70.
2. Login as root.
3. Insert the Vicom SV SAN Builder v2.5 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 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

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

   #/svengine/sdus/sdushutdown

2. Install the new SV SAN Builder software. The config file will not be changed.
3. Start the primary daemon. See "SV SAN Builder Upgrade" on page 72 for more information.

   #/svengine/sdus/slicd

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 156 for more information.

Example

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

#svengine/sdus/setmasterdaemon -d SAN2r0

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

5. Repeat steps 1-3 for secondary daemon.

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`

SLIC Daemon Config File

Important Information

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

Remote management maximums:

- Two daemons.
  - One primary daemon (located in the primary server).
  - One secondary daemon (located in the secondary server).
- Up to 32 SANs per active daemon.

In the configuration file, you will define:

- "Daemon SignOn Path" on page 77.

  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 (“Configure the Failover Settings” on page 81).

  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.

Example of Final Configuration File:

```
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;
```

Edit Config File

Daemon SignOn Path

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 Configuration File:" on page 76.) 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 84, for more information.

Example Text File for Mailheader:

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

4. Repeat steps 1-3 for each daemon installed.

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 84 for more information.

Example Password Text File

```
SAN1r0            first password
SAN1r1            second password
SAN2r0            third password
SAN2r1            fourth password
```

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 Configuration File:" on page 76.) 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.

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 Configuration File:" on page 76.) 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.

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 Configuration File:" on page 76.) 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.

Configure the Failover Settings

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 Configuration File:" on page 76.) 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;
};
```

Update Config File

Important Issues

Remote management maximums:

- Two daemons per remote management
  - One primary daemon (located in primary server)
  - One secondary daemon (located in secondary server)

Update

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

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

2. Edit the configuration file. See "SLIC Daemon Config File" on page 74 for instructions to edit the configuration file.

3. Start the daemon. See "SV SAN Builder Upgrade" on page 72 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 156 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
```

Text Files

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:

```
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.
- The SignOn Path is the same as the ones that you defined in "Configure Router SignOn Path" on page 43.
- 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 will be the same as the ones that you defined in "Initial Router Configuration" on page 35.
- Maximum number of entries is 64.

Example Password Text File

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

CHAPTER 4

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

If the SV SAN Builder version is 2.5 or later, then the SV Zone Manager version is also correct. See "Determine SV Zone Manager Software Version" on page 86 to determine the proper version.

SV Zone Manager Installation

Important Information

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

SV Zone Manager installs the CLI for configuring zones. Once installation is complete four files will appear:

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

Install

1. Ensure you have the latest software (2.5 or later). If you do not know how to determine the software version, see "Determine SV Zone Manager Software Version" on page 86.
2. Login as root.
3. Insert the Vicom SV Zone Manager v2.5 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 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 "Install SV Zone Manager Software" on page 45.

Start and Stop SV Zone Manager

Start

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

SV Zone Manager is composed primarily of zone commands. Because the daemon handles all software commands, ensure that the daemon is running. See "Start and Stop Daemon" on page 73.

Stop

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

SV Zone Manager is composed primarily of zone commands. Because the daemon handles all software commands, stopping the daemon stops Zone Manager. See "Stop Daemon" on page 73.

CHAPTER 5

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

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 95
3. Start the SV SNMP Agent program. See "Start" on page 95.
   - If SV SNMP Agent has not been installed in the management station, then install it now. See "SV SNMP Agent Installation" on page 93.
4. To upgrade SV SNMP Agent See "SV SNMP Agent Upgrade" on page 94.

SV SNMP Agent Installation

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

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 92.
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 93 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 router SignOn path (SAN1**r0**) listed in the **PrimaryDaemon** path in "Configure the Failover Settings" on page 44.
- Under **Host_IPAddress** type the IP address listed in the **PrimaryDaemon** path in "Configure the Failover Settings" on page 44.
- Under **Tcp/Ip_Port** type **default**. Default is 20000. Vicom highly recommends that you use the default port.

Install in the secondary server by repeating steps 1 and 2.

Configure Trap Client List Specification

The maximum number of entries is 32.

1. Return to the SNMPagent directory.
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.
- Enter **#./svmgmtagent** to start the SNMP agent.

  #svengine/SNMPagent/svmgmtagent
- If you changed the remote management server's UDP port setting, you can start 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

Install in the secondary server by repeating steps 1 and 2.

CHAPTER 6

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

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" on page 69.

- 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 node mapping table data base table of the SV Router.

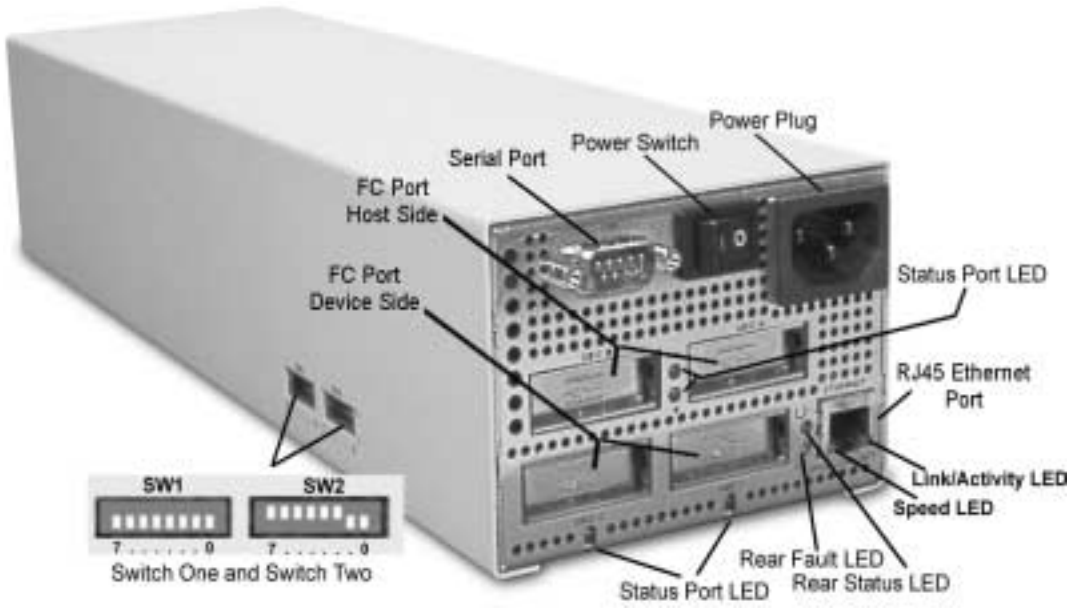
Necessary Components

- 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).

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 6-1 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 30.
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 Router Microcode from Local Computer

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

'5': Clear Error Log

'6': View/Change Interface Configuration

'7': Virtual Drive Utility

'9': Erase Node Table

'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.

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

Command Line Interface

1. Start the daemon. See "SV SAN Builder Upgrade" on page 72 if necessary.
2. Using the **svpd** command, view both SV Routers' microcode. See "Displaying VPD (Vital Product Data) [svpd]" on page 164.

Example

```
svpd –d SAN1r0 -t i1

svpd -d san1r0 -t i2
```

Telnet

1. Telnet SV Router. See "Telnet Session" on page 102 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 primary daemon's SV Router.
2. Using the **sdnld** command, download 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. Stop I/O to the secondary daemon's SV Router.
5. Repeat step 2-3 for secondary daemon's SV Router.

   Perform T3 failback if necessary. See "T3 Disk Array Failback Procedure" on page 116.

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 171 for information on retrieving service codes.

Replace One SV Router

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 the offline SV Router’s initiator number (I00001, I00002 etc.) The information will be used later. See "View Properties of SLIC" on page 163 for more information.

Example

```
slicview view -d SAN1r0
```

2. Power on the replacement SV Router.
3. Using the serial port, configure the replacement SV Router’s settings. See "Configure SV Routers" on page 33 for configuration steps.
    - Switch Settings
    - Initial Router Configuration
    - Configure Devic-Side, Host-Side, and Ethernet Settings
4. Power off and remove the failed SV Router.

5. Power off the replacement SV Router.
6. Cable the replacement SV Router to the T3 disk array. See "Cable SV Routers to T3 Partner Group" on page 37.
7. Cable the replacement SV Router to the management station. "Cable SAN and Remote Management" on page 38.
8. Power on the replacement SV Router.
9. Using the **`slicview`** command, determine 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 160 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 HBAs to the new SV Router. "Cable Switches and Servers" on page 58.
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 "View Properties of Host Adapter" on page 148 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 158 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 116.

18. 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. Using the serial port, configure both SV Router's settings. Use the same settings as the previous routers. See "Configure SV Routers" on page 33 for configuration steps.
   - Switch Settings
   - Initial Router Configuration
   - Configure Devic-Side, Host-Side, and Ethernet Settings
4. Power off both replacement SV Routers.
5. Power off and remove both failed SV Routers.
6. Cable both replacement routers to the T3 disk array. See "Cable SV Routers to T3 Partner Group" on page 37.
7. Cable both replacement routers to the management station. "Cable SAN and Remote Management" on page 38.
8. Power on only one SV Router.
9. The daemon must be configured to talk with that router. See "Edit the SLIC Daemon Configuration File" on page 43.
10. Start the daemon in the management station. See "Start the Daemon" on page 45.
11. Using the **`sanconfig write`** command, download the drive configuration to the replacement router. See "Writing SAN Configuration File to SV Router" on page 159.

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 133 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 158 for more information.

Example

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

16. Connect the HBAs to both replacement routers. "Cable Switches and Servers" on page 58.
17. Using the **sadapter view** command, ensure the HBA sees both SV Routers. See "View Properties of Host Adapter" on page 148 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 116.
21. Type **vxdctl enable** to enable Veritas path. This should be done on each data server.

Erase the Node Mapping Table

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. Enter 9 to Erase the mapping table.
   - A successful command will read **“Node Table has Erased !”**
   - An unsuccessful command will result in an error halt. The service code is 051.

Enable Daemon SignOn

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. 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.

       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

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. 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 79.
   - 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

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. 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 105 to update microcode.
   - Enter **V** and ensure that the settings are correct.

Configure SV Router's Device-Side

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. 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

4. 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.

Configure SV Router’s Host-Side

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. 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
4. 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.

Configure SV Router’s Ethernet Settings

1. Telnet SV Router. See "Telnet Session" on page 102 for more information.
2. Enter the password. The *User Service Utility* menu will appear.
3. 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

4. Enter **Y** to continue.
5. 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.

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

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. See Figure 7-1 "T3 Paths" below.
- 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.
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 147.

Example

```
mpdrive view -d SAN1r0
```

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

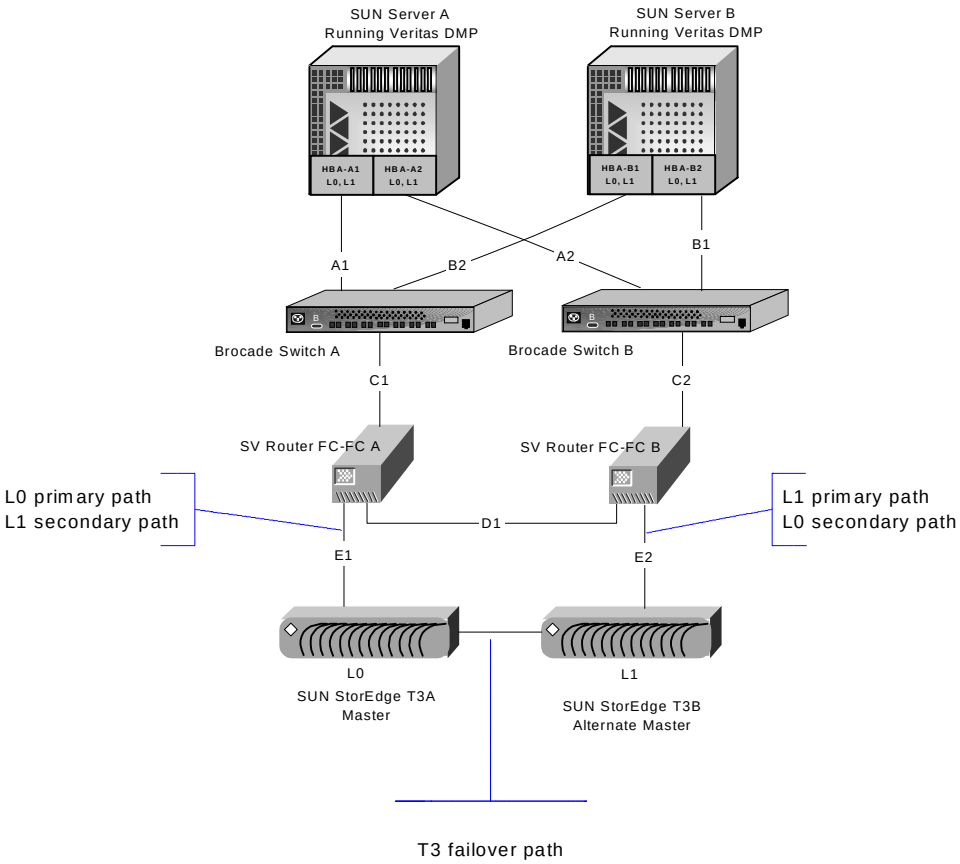
4. Using the **`mpdrive failback`** command, cause the secondary path to the T3 to failback to the primary path. See "Using MultiPath Drive Failback" on page 146 for more information.

Example

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

5. Resume I/O to enable failback.

Figure 7-1 T3 Paths



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.

Important Information

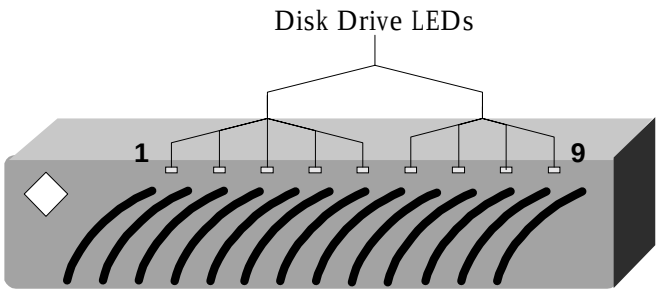
- Only remove one drive at a time from the T3 disk tray at any time. Ensure this drive is replaced and fully enabled before removing another drive.
- Replace drives when the T3 disk tray is fully enabled and powered on. Drives that are replaced when the disk tray is powered off or not fully enabled may 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.

Replacing Drive

1. Check LED activity to determine drive failure (see section "Reading T3 Drive LEDs" on page 119).
2. Verify FRU (Field Replacement Unit) status.
3. See SUN StorEdge T3 service manual for proper drive replacement.

T3 Drive LEDs

Figure 7-2 Disk Drive LED Location



Reading T3 Drive LEDs

Drive Activity (green)	Drive Status (amber)	Description	Corrective Action
Off	Off	• No drive. • Drive not recognized.	None.
Slow blink	Off	Drive spin-up or spin-down.	None.
Solid	Off	Drive OK, idle.	None.
Flashing	Off	Drive OK, I/O activity.	None.
n/a	Solid	• Drive data rebuild. • Firmware download.	None.
n/a	Slow Blink	Drive failure.	Replace drive.

Table 7-1 Drive LED Activity

Ethernet Switch Maintenance

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

Ethernet Switch Replacement

- Replacement of the Ethernet switch is a plug-and-play action and will not have an effect on the SAN.
- If using only one Ethernet switch, 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.

Fibre Channel Switch Replacement

- Replacement of the FC switch is a plug-and-play action and will have a minimal effect on the SAN.
- I/O will be routed to the remaining FC switch temporarily.

Data Server Maintenance

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

Server Replacement

1. Install Emulex HBAs. See "Install Emulex 7000 HBA" on page 56.
2. Cable the server to the switches. See "Cable Switches and Servers" on page 58.
3. Using remote management, telnet to each switch to show the UIDa of all devices connected to that switch. This will test the connection.

   `#switchshow`

4. In both SV Routers, using the **`slicview view`** command, view the router zone configuration information.See "View Properties of SLIC" on page 163 for more information.

   You should see in both SV Routers the existing HBA(s), the new HBA and the old HBA.

Example

```
slicview view -d SAN1r0
```

5. In both SV Routers, using the **`sadapter alias`** command, assign aliases for the new HBAs.
   - Limit alias to 12 characters. See "Create or Change Alias of Host Adapter" on page 149 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 both SV Routers, using the **`sliczone view`** command, determine the zone(s) of failed HBA.

Example

```
sliczone view -d SAN1r0
```

7. In both SV Routers, using the **`sliczone add`** command, add new HBAs to each zone. See "Adding Zone Components" on page 152 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 both SV Routers, 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 "View Properties of Host Adapter" on page 148 for more information.

Example

```
slicadapter view -r I1
slicadapter view -r I2
```

Troubleshooting

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

9. In both SV Routers, using **`sliczone del`** command, delete the old HBA from the zone. See "Deleting Zone Components" on page 153 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 158 for more information.

Example

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

Veritas Maintenance

Enable Veritas Path

1. Veritas automatically enables the path. Wait at least five minutes after system configuration/change to determine if it automatically enables. If I/O transmission begins, the path is enabled.
2. If the path does not enable, check within the data server to determine if the path is enabled. Type **`vxdisk`** to view the disk.
3. If path is not enabled, enable path. Type **`vxdctl enable.`**

Management Server Maintenance

Management Server Replacement

- Follow the installation process in Chapter 2. See "Step Three: Setup Remote Management" on page 40.
- 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 daemon configuration file **(trapclientlist.cfg),** and paste it in the **SNMPagent** directory located in the **svengine** directory.

  #svengine/SNMPagent/

Cabling and Connections Maintenance

Ethernet Requirements

- Topology: Transmission Control Protocol - Internet Protocol (TCP-IP).
- Maximum distance between devices: 100 meters (328 feet).
- SV Router.
  - Speed: 10base-T/100base-TX
  - Connector RJ-45
- T3 Disk Array (refer to *Sun StorEdge T3 Disk Tray Installation, Operation, and Service Manual*).

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
- T3 Disk Array (refer to *Sun StorEdge T3 Disk Tray Installation, Operation, and Service Manual*).

Serial Requirements

- SV Router.
  - Topology: Serial Transmission
  - Speed: 56K baud
  - Connector DB-9
- T3 Disk Array (refer to *Sun StorEdge T3 Disk Tray Installation, Operation, and Service Manual*).

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 127.
    - For optical cabling, see "FC Requirements" on page 128.
    - For serial cabling on SV Routers, "Serial Requirements" on page 128
6. If problems still exist, power off the device and replace the cable.

CHAPTER 8

BASIC COMMAND LINE INTERFACE

This chapter explains only the commands used with the installation or service of this system. It includes these sections:

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 always is required; the host name of the server that attaches directly to the SV Router is needed for remote access.

Usage:

```
showmap -d Cx {-h Host} -m [all/target/fc/SLIC/physical/spare/
offline/unmapped] {–f File_Name –v}
```

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

-m [all/target/fc/SLIC/physical/spare/offline/unmapped]

all	Output map showing all tables.
target	Output map for all target devices.
fc	Output FC map table.
slic	Output List of SV Routers table.
physical	Output List of Target Devices and List of SLICs 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. Name or IP address of host to which the SV Router is connected.

-f File_Name — Optional. Print maps to File_Name.

-v — Optional. Print maps to console (default).

Example:

```
showmap -d c0 -h venus -m slic
```

This function displays and/or prints (to a file) a number of tables that display information about the SV Routers and target devices in the storage subsystem.

Tables displayed are:

1. The List of SLICs table may have one or two entries: SLICs in Target Mode and/or SLICs in Initiator Mode. Each of these tables displays the initiator number, alias, UID, and type for each individual SV Router within the loop (see Figure 8-1).

Figure 8-1 List of SLICs Table – Initiator & Target Mode

```
List of SLICs in Initiator Mode:
SLIC Number SLIC Name        SLIC UID           TYPE Version
I00001                       28000060-220000DC FCFC 08.00
I00002                       28000060-220000DD FCFC 08.00     *

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, LUN (native), VPD, type, and capacity of each physical target device (see Figure 8-2).

Figure 8-2 List of Target Devices Table

```
List of Target Devices:
Target    Target UID         LUN      VPD                TYPE Capacity
Number
T00000    20000060-22876543 0000      IBM    DCHC09B     DISK 8689  MB
T00001    20000060-22876543 0001      IBM    DCHC09B     DISK 8689  MB
T00002    20000060-22876543 0002      IBM    DCHC09B     DISK 8689  MB
T00003    20000060-22876543 0003      IBM    DCHC09B     DISK 8689  MB
T00004    20000060-22876543 0004      IBM    DCHC09B     DISK 8689  MB
T00005    20000060-22876543 0005
T00006    20000060-22876543 0006      IBM    DFHCC4C     DISK 4303  MB
T00007    20000060-22876543 0007      IBM    DCHC09B     DISK 8689  MB
T00008    20000060-22876543 0008      IBM    DCHC09B     DISK 8689  MB
T00009    20000060-22876543 0009      IBM    DCHC09B     DISK 8689  MB
T00010    20000060-22876543 0010      IBM    DCHC09B     DISK 8689  MB
T00011    20000060-22876543 0011      IBM    DCHC09B     DISK 8689  MB
T00012    20000060-22876543 0012      IBM    DCHC09B     DISK 8689  MB
T00013    20000060-22876543 0013      IBM    DCHC09B     DISK 8689  MB
T00014    20000060-22876543 0014      IBM    DCHC09B     DISK 8689  MB
T00015    20000060-22876543 0015      IBM    DCHC09B     DISK 8689  MB
```

3. The List of Logical Devices table provides you with the target number, complex name, type, serial number, and capacity for each logical device (see Figure 8-3).

Figure 8-3 List of Logical Devices Table

```
List of Logical Devices:
Target   Complex Name     TYPE              Serial Number     Capacity
Number
T33025   VicomC01         COMPOSITE         62526B74-30303046 17378 MB
T33026   VicomC02         COMPOSITE         62526B74-30303047 17378 MB
T33539   VicomM03         MIRROR            62526B74-30303048 8689  MB
T33540   VicomM04         MIRROR            62526B74-30303049 8689  MB
T41989   VicomI05         INSTANT COPY      62526B74-3030304A 8689  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 (see Figure 8-4).

Figure 8-4 FC Map Table

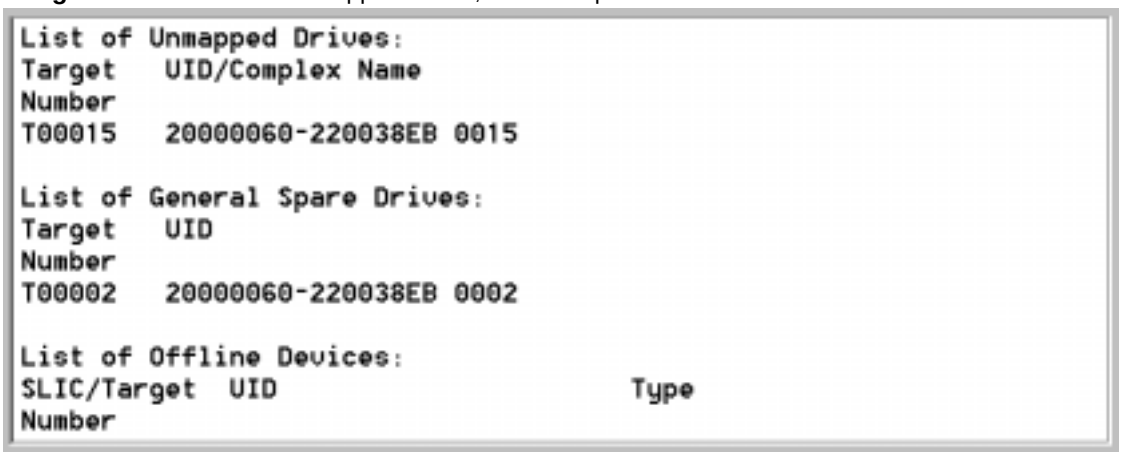
```
FC Map:
FC       Target   UID/Complex Name
MAP      Number
00-000   T00000   20000060-220038EB 0000
00-001   T00001   20000060-220038EB 0001
00-002   T41989   VicomI05
00-003   T33025   VicomC01
00-005   T33539   VicomM03
00-006   T33026   VicomC02
00-007   T33540   VicomM04
00-012   T00012   20000060-220038EB 0012
00-015   T00015   20000060-220038EB 0015
00-016   T00012   20000060-220038EB 0012
```

5. The List of Unmapped Drives table provides the target number and UID/complex name of any target devices that have not been mapped (see Figure 8-5).

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.

7. The List of Offline Devices table provides the target number, UID, and type of any target devices that are offline.

Figure 8-5 Lists of Unmapped Drives, General Spares and Offline Devices



Virtual Drive Commands [vdiskpool / vlun]

The following commands are used to create and manipulate virtual drives. Only mapped drive(s), unmapped drive(s), spare drive(s), or multipath drive(s) drives can be used in LUN carving. Before the drives can be carved, they must be added to a disk pool in a SAN. At this point, each drive in the disk pool can be carved into as many as 32 virtual drives of at least 0.5 GB each.

Creating a Disk Pool

The **`vdiskpool create`** command creates one disk pool out of drives belonging to the SAN. Only simple drives or general spare drives can be used in a disk pool.

Usage:

`vdiskpool create -d Cx -n PoolName {-t [Tx/allspare] -v}`

-d Cx	Cx is the SignOn path, as specified in the config file.
-n [PoolName]	The name of the disk pool.
-t [tnum.../allspare]	Optional. Add a particular drive, add all spare drives
-v	Optional. Verbose mode. User confirmation required.

Example:

`vdiskpool create -d c0 -t all -n MyPool -v`

Adding Drives to a Disk Pool

The **vdiskpool add** command adds one or more drives to an existing disk pool. If there is more than one pool, the pool name must be specified.

Usage:

vdiskpool add -d Cx -t [Tx/allspare/all] {-h host -p PoolName -v}

-d Cx	Cx is the SignOn path, as specified in the config file.
-t [tnum.../allspare/all]	Add a particular drive, add all spare drives, add all drives.
-h [host]	Optional. The name of the host.
-p [PoolName]	Optional. The name of the disk pool.
-v	Optional. Verbose mode. User confirmation required.

Example:

vdiskpool create -d c0 -t allspare -h MyHost -p MyPool -v

Deleting Drives from a Disk Pool

The **vdiskpool del** command deletes one or more drives from the disk pool. Any data on virtual drives created from these will be lost.

Usage:

vdiskpool del -d Cx -t [Tx/all] -p PoolName {-v}

-d Cx	Cx is the SignOn path, as specified in the config file.
-t [tnum/all]	Delete a particular drive or delete all drives.
-p [PoolName]	The name of the disk pool.
-v	Optional. Verbose mode. User confirmation required.

Example:

vdiskpool del -d c0 -t all -p MyPool -v

Removing a Disk Pool

The **vdiskpool remove** command removes the entire disk pool.

Usage:

vdiskpool remove -d Cx -p PoolName {-h host -v}

-d Cx	Cx is the SignOn path, as specified in the config file.
-p [PoolName]	The name of the disk pool.
-h [host]	Optional. The name of the host.
-v	Optional. Verbose mode. User confirmation required.

Example:

vdiskpool remove -d c0 -p MyPool -h MyHost -v

Renaming a Disk Pool

The **vdiskpool change** command changes the name of a pool.

Usage:

vdiskpool change -d Cx -p PoolName -n NewPoolName {-h host -v}

-d Cx	Cx is the SignOn path, as specified in the config file.
-p [PoolName]	Current pool name.
-n [NewPoolName]	New pool name.
-h [host]	Optional. The name of the host.
-v	Optional. Verbose mode. User confirmation required.

Example:

vdiskpool change -d c0 -p MyPool -n MyNewPool -h MyHost -v

Viewing a Disk Pool

The **`vdiskpool view`** command shows all drives that belong to a particular disk pool.

Usage:

`vdiskpool view -d Cx -p PoolName {-m [physical/logical/all]}`

-d Cx	Cx is the SignOn path, as specified in the config file.
-p [PoolName]	The name of the disk pool.
-m [physical/logical/all]	Optional. Allows selection of physical drives, logical drives, or all drives combined.

Example:

`vdiskpool view -d c0 -p MyPool -m physical`

Creating a Virtual Drive

The **`vlun create`** command carves one virtual drive from the existing disk pool.

Usage:

```
vlun create -d Cx -l size -p PoolName {-n VdriveName -s map -h host
-t Txxxx -v}
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-l [size]	New virtual drive size in GB.
-p [PoolName]	The name of the disk pool.
-n [VdriveName]	Optional. The name of the virtual drive.
-s [map]	Optional. The map of the virtual drive.
-h [host]	Optional. The name of the host.
-t [Txxxx]	Optional. The target number of the physical drive in the disk pool to be used.
-v	Optional. Verbose mode. User confirmation required.

Example:

```
vlun create -d c0 -l 10 -p MyPool -n MyVDrive -s L23 -h MyHost -t
T1 -v
```

Autocreating a Virtual Drive

The **`vlun autocreate`** command carves several virtual drives from the existing disk pool at one time. All drives must be the same size. If a drive name is specified, all drives created will share the same name.

Usage:

```
vlun autocreate -d Cx -l size -p PoolName -c #LUN {-n MyVDrive -h
host -v}
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-l [size]	New virtual drive size in GB.
-c [count]	Number of virtual drives to be created.
-p [PoolName]	The name of the disk pool.
-n [VdriveName]	Optional. The name of the virtual drive.
-h [host]	Optional. The name of the host.
-v	Optional. Verbose mode. User confirmation required.

Example:

```
vlun autocreate -d c0 -l 10 -p MyPool -c 5 -h MyHost -v
```

Removing a Virtual Drive

The **`vlun remove`** command turns the virtual drive into free space within the disk pool.

Usage:

`vlun remove -d Cx -p PoolName -t Txxxxx -h host -v`

-d Cx	Cx is the SignOn path, as specified in the config file.
-p [PoolName]	The name of the disk pool.
-t [Txxxxx]	Target number of virtual drive.
-h [host]	Optional. The name of the host.
-v	Optional. Verbose mode. User confirmation required.

Example:

`vlun remove -d c0 -p MyPool -t T16385 -h MyHost -v`

Changing a Virtual Drive

The **`vlun change`** command changes the name and the global map of a virtual drive.

Usage:

`vlun change -d Cx -t Txxxxx -p pool -n VdriveName -h host -s map -v`

-d Cx	Cx is the SignOn path, as specified in the config file.
-t [Txxxxx]	Target number of virtual drive.
-p [PoolName]	The name of the disk pool.
-n [VdriveName]	New virtual drive name.
-s [map]	The map of the virtual drive.
-h [host]	Optional. The name of the host.
-v	Optional. Verbose mode. User confirmation required.

Example:

`vlun change -d c0 -n NewDriveName -t T16386`

Viewing Virtual Drive Properties

The **`vlun view`** command shows the properties of the LUN.

Usage:

`vlun view -d Cx {-p PoolName -t Txxxxx -h host -v}`

-d Cx	Cx is the SignOn path, as specified in the config file.
-p [pool name]	The name of the disk pool.
-t [Txxxxx]	Target number of virtual drive.
-h [host]	Optional. The name of the host.
-v	Optional. Verbose mode. User confirmation required.

Example:

`vlun view -d c0 -p MyPool -t T16387 -h MyHost -v`

MultiPath Drive Commands [mpdrive]

MultiPath Drive functionality is supported only in conjunction with the Sun StorEdge™ T3 Array.

Autocreating a MultiPath Drive

The **`mpdrive autocreate`** command checks to see if a MultiPath drive can be created, reads the active and passive paths, and creates the MultiPath drive. It assigns a name and a map to the new drive and displays the target number.

Usage:

`mpdrive autocreate -d Cx -h host -v`

-d Cx	Cx is the SignOn path, as specified in the config file.
-h [host]	Optional. Name or IP address of SLIC Daemon host.
-v	Optional. User Confirmation Mode.

Example:

`mpdrive autocreate -d c0 -h 100.2.34.120 -v`

Removing a MultiPath Drive

The **`mpdrive remove`** command removes a MultiPath drive.

Usage:

`mpdrive remove -d Cx -h host -m Txxxxx -v`

-d Cx	Cx is the SignOn path, as specified in the config file.
-m [Txxxxx]	Target number of MultiPath drive.
-h [host]	Optional. Name or IP address of SLIC Daemon host.
-v	Optional. User Confirmation Mode.

Example:

`mpdrive remove -d c0 -h 100.2.34.120 -m t49154`

Using MultiPath Drive Failback

The **`mpdrive failback`** command is used to switch between the active and passive paths.

Usage:

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

-d Cx	Cx is the SignOn path, as specified in the config file.
-h [host]	Optional. Name or IP address of SLIC Daemon host.
-j [UID]	The controller number of the MultiPath drive.
-v	Optional. User Confirmation Mode.

Example:

`mpdrive failback -d c0 -h 100.2.34.120 -j 2000000100000123`

Replacing a MultiPath Drive

The **`mpdrive replace`** command is used in case the target SV Router needs to be replaced; it loads all the information to the SV Router so that the MP drive will function correctly.

Usage:

`mpdrive replace -d Cx -h host -f -v`

-d Cx	Cx is the SignOn path, as specified in the config file.
-h [host]	Optional. Name or IP address of SLIC Daemon host.
-f	Force replace.
-v	Optional. User Confirmation Mode.

Example:

`mpdrive replace -d c0 -h 100.2.34.120 -f`

Changing MultiPath Drives

The **`mpdrive change`** command allows you to change the map of the MultiPath drive.

Usage:

`mpdrive change -d Cx -h host -m Txxxxx -s map -v`

-d Cx	Cx is the SignOn path, as specified in the config file.
-m [Txxxxx]	Target number of MultiPath drive.
-s [map]	Optional. Mapping set.
-h [host]	Optional. Name or IP address of SLIC Daemon host.
-v	Optional. User Confirmation Mode.

Example:

`mpdrive change -d c0 -h 100.2.34.120 -m t49154 -s L15`

Viewing MultiPath Drive Properties

The **`mpdrive view`** command displays the name, target number, map, active and passive paths, and controller serial number of a MultiPath Drive.

Usage:

`mpdrive view -d Cx -m Txxxxx`

-d Cx	Cx is the SignOn path, as specified in the config file.
-m [Txxxxx]	Target number of MultiPath drive.

Example:

`mpdrive view -d c0 -m t49154`

Basic HBA Commands [sadapter]

View Properties of Host Adapter

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.

Usage:

```
sadapter view -d Cx -r SLIC# -a HostName -u HostUID -h Host
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-a HostName	The name assigned to the host adapter.
-u HostUID	The host adapter UID.
-h Host	Optional. The name or IP address of the host running the SLIC Daemon.

Examples:

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

sadapter view -d c0 -r I5

sadapter view -d c0 -r I4 -h 127.13.21.141 -a Web_Host
```

Create or Change Alias of Host Adapter

Host adapters are identified by their 12-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.

Usage:

```
sadapter alias -d Cx -r SLIC# -a HostName -u HostUID -n NewHostName
-h Host -v
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-a HostName	The name assigned to the host adapter.
-u HostUID	The host adapter UID.
-n NewHostName	The new host adapter name to be assigned.
-h Host	Optional. The name or IP address of the host running the SLIC Daemon.
-v	Optional. User confirmation mode.

Example:

```
sadapter alias -d c0 -r I0 -a Data_Host -n DB_Host
```

Add Host Adapter

Use the **`sadapter add`** command to add a host adapter to the SV Router. You must specify the host adapter UID, and you also can assign an alias for the host adapter.

Usage:

```
sadapter add -d Cx -r SLIC# -u HostUID -n NewHostName -h Host -v
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-u HostUID	The host adapter UID.
-n NewHostName	The new host adapter name to be assigned.
-h Host	Optional. The name or IP address of the host running the SLIC Daemon.
-v	Optional. User confirmation mode.

Example:

```
sadapter add -d c0 -r I3 -u 213784FE74A83DC1 -n MyServer
sadapter add -d c0 -r I3 -u 213784FE74A83DC1 -v
```

Basic Zone Commands [sliczone]

All zone commands require the SV Router initiator number.

Create Zone

Use the **`sliczone create`** command to create each zone. Each zone must contain at least one host adapter, but it can contain multiple host adapters. It also may contain one or more drives.

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

Usage:

```
sliczone create -d Cx -r SLIC# -t Txxxxx -a HostName -u HostUID -g
DomainName -z ZoneName -h Host -m auto/global -v
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-t Txxxxx	The target number of the drive.
-a HostName	The name assigned to the host adapter.
-u HostUID	Required. The host adapter UID.
-g DomainName	Optional. The name of the SV domain.
-z ZoneName	The new zone name to be assigned. If unspecified, a zone name will be assigned automatically.
-h Host	Optional. The name or IP address of the host running the SLIC Daemon.
-m auto/global	Optional. Zone map generation.
auto	Automatically generates the map in sequence, filling in any gaps in the sequence.
global	Retains the global map of the drives in the zone mapping.

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

-v	Optional. User confirmation mode.

Example:

```
sliczone create -d c0 -r I0 -t T1 T2 -a MyHost -g MyDomain -m
global -z MyZone

sliczone create -d c0 -r I0 -t T00000 -a MyHost -g MyDomain -v
```

Adding Zone Components

Use the **sliczone add** command to add members (drives and/or host adapters) to each zone. You must specify the name of the zone to which these component members will be added.

Specify the target drive number, the host adapter name, or the host adapter UID.

Usage:

```
sliczone add -d Cx -r SLIC# -t Txx...x -a HostName -u HostUID -z
ZoneName -h Host -m auto/global -v
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-t Txx...x	The target number of the drive.
-a HostName	The name assigned to the host adapter.
-u HostUID	The host adapter UID.
-z ZoneName	Required. The name of the zone.
-h Host	Optional. The name or IP address of the host running the SLIC Daemon.
-m auto/global	Optional. Zone map generation.
auto	Resets all maps in the modified zone and replaces them in sequence. All zone mapping will be lost.
global	Retains both the zone mapping and the global mapping 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 mode.

Example:

```
sliczone add -d c0 -r I4 -z MyZone -t T00004 T00005 -a MyHost
```

Deleting Zone Components

Use the **sliczone del** command to delete existing members from a zone. Members may be host adapters or target drives. You must specify the name of the zone.

Note: *Zones must contain at least one host adapter. To delete all host adapters, you must delete the zone.*

Specify the target drive number, the host adapter name, or the host adapter UID.

Note: *When deleting a virtual drive you must delete the virtual drive from all zones and then remove the virtual drive.*

Usage:

```
sliczone del -d Cx -r SLIC# -t Txx...x -a HostName -u HostUID -z
ZoneName -h Host -v
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-t Txx...x	The target number of the drive.
-a HostName	The name assigned to the host adapter.
-u HostUID	The host adapter UID.
-z ZoneName	Required. The name of the zone.
-h Host	Optional. The name or IP address of the host running the SLIC Daemon.
-v	Optional. User confirmation mode.

Example:

```
sliczone del -d c0 -r I2 -z MyZone -t T00001 -a MyHost
```

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 SLIC# -z ZoneName -v

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-z ZoneName	Required. The name of the zone.
-v	Optional. User confirmation mode.

Example:

sliczone map -d c0 -r I3 -z MyZone

Viewing Zone Components

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 SLIC# -z ZoneName

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-z ZoneName	The name of the zone.

Example:

sliczone view -d c0 -r I3 -z Data_Zone

Removing Zones

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

Deleting a zone may affect communications between the SV Router and SLIC Daemon.

Note: If the zone contains both the SignOn host and SignOn drive, deleting it could result in a loss of communications with the SV Router (for in-band management only).

Usage:

```
sliczone remove -d Cx -r SLIC# -z ZoneName -v
```

-d Cx	Cx is the SignOn Path, as specified in the config file.
-r SLIC#	SLIC# is the SV Router initiator number.
-z ZoneName	The name of the zone.
-v	Optional. User confirmation mode.

Example:

```
sliczone remove -d c0 -r I0 -z MyZone
```

Basic SLIC Daemon Commands

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 is acting as the master daemon. Run this command to reset the primary daemon back to the master daemon.

Usage:

setmasterdaemon -d Cx -h Host –o

-h Host	Host is the network name or IP address of the host computer to which the SV Router is connected.
-d Cx	Cx is the SignOn path, as specified in the config file.
-o	User Confirmation.

Example:

setmasterdaemon -d c0 -h 10.10.20.180 –o

Listing SAN Communication Properties [signoninfo]

The **signoninfo** command displays how communication between the SLIC Daemon and the SV Router has been established. For Ethernet communication, it displays the SignOn SLIC (SV Router) UID and the IP address of the router. For in-band management, it displays the SignOn drive ID and LUN, the target number, the SignOn SLIC (SV Router) UID, and the SLIC Partition. If more than one SLIC Partition was created, one will be displayed as an Alternate SLIC Partition.

Usage:

signoninfo {–h Host} –d Cx

-d Cx	Cx is the SignOn path, as specified in the config file.
-h Host	Optional. Host system name (e.g. venus) or IP address (e.g. 204.118.9.9).

Example

signoninfo -d c0

Listing SLIC Daemon Configuration Information [saninfo]

The **saninfo** command displays the SLIC Daemon configuration information. If the SignOn path is not specified, it will display the configuration information for all SANs the daemon is controlling.

Usage:

saninfo -d Cx -h host

-d Cx	Optional. Cx is the SignOn path, as specified in the config file.
-h host	Optional. The name or IP Address of the host.

Example:

saninfo -d c0 -h 10.10.20.224

Basic SAN Configuration File Commands

SAN Configuration File (Emergency Recovery) [sanconfig]

These commands allow 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

The **`sanconfig read`** command reads the SAN configuration file from the SV Router and saves it to an offline file. To prevent losing drive configuration information, you should make a copy of this file whenever the configuration changes.

Usage:

```
sanconfig read -d Cx -h host -e FileName -v
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-e FileName	The SAN configuration file name.
-h host	Optional. The name or IP Address of the host.
-v	Optional. User confirmation mode.

Example:

```
sanconfig read -d c0 -e SanFile.san -h 123.123.123.224
```

Writing SAN Configuration File to SV Router

The **`sanconfig write`** command downloads 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 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.

Usage:

```
sanconfig write -d Cx -h host -e FileName -v
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-e FileName	The SAN configuration file name.
-h host	Optional. The name or IP Address of the host.
-v	Optional. User confirmation mode.

Example:

```
sanconfig save -d c0 -e SanFile.san -h 123.1.10.224
```

Importing SAN Zone Configuration

The **`sanconfig import`** is used in a multi-SLIC environment to upload zone information to the SV Router that was replaced.

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.

Usage:

```
sanconfig import -d Cx -r NewSLIC# -j CurrentSLIC#-h host -e
FileName -v
```

-d Cx	Cx is the SignOn path, as specified in the config file.
-e FileName	The SAN configuration file name.
-r NewSLIC#	New SLIC initiator number.
-j ReplacedSLIC#	Replaced SLIC initiator number.
-h host	Optional. The name or IP Address of the host.
-v	Optional. User confirmation mode.

Example:

```
sanconfig import -d c0 -e san08.san -r i3 -j i2
```

SAN Import [sanimport]

The **sanimport** command imports the SAN configuration file from the source SAN to the destination SAN, based on the import configuration file defined.

Usage:

sanimport haimport -e FileName -v

-e FileName	The SAN configuration file name.
-v	Optional. User confirmation file.

Example:

sanimport haimport -e FCsan08haimport.cfg -v

The import configuration file is a text file that contains the following information:

```
[SAN Parameters]
DB2Import=yes
DB4Import=yes
SourceHostName=100.123.123.221
SourceSlicName=c0
SourceSlicInitiatorNumber=1
DestinationHostName=10.10.20.37
DestinationSlicName=c0
DestinationSlicInitiatorNumber=1
[Host Adapter Info]
SourceHostAdapterUID=200000E08B0138ED

DestinationHostAdapterUID=20000000C923839C
```

Basic SLIC (SV Router) Commands

Download Microcode [sdnld]

This function is used to update the microcode for the SV Router and for the storage drives. In the normal mode, the download function will not download microcode unless it is a newer version than what is in the drive. The force option overrides this safeguard. Only the microcode for a local SV Router can be downloaded in a multi-SV Router environment.

Usage:

`sdnld {–h Host} –d Cx –t [s/Ixxxxx/sa] –o [F/N] –f File_Name`

-h Host	Host system name (e.g. venus) or IP address (e.g. 204.118.9.9).
-d Cx	Cx is the SignOn path, as specified in the config file.
-t [s/Ixxxxx/sa]	
s	Local SV Router.
sa	All SV Routers in the SAN.
Ixxxxx	SV Router/Initiator number of remote SV Router.
-o [F/N]	
F	Force download.
N	Normal download (default).
-f File_Name	Name of the microcode file.

Caution ! ***Do not download new microcode to the SV Router if the SV Router 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.***

View Properties of SLIC

The **`slicview view`** command is used to view the SLIC information. It displays all the accessible drives and host adapter information. If a SLIC initiator is specified, then only the information pertaining to that particular SLIC is displayed. When no SLIC initiator is specified, the complete list of SLICs in the SAN and their accessible drives and host adapters, is displayed. If a host is specified, then the SLIC initiator number is not required.

Usage:

`slicview view -d Cx -r SLIC# -h Host`

-d Cx	Cx is the SignOn path, as specified in the config file.
-r SLIC#	Optional. SLIC# is SLIC initiator number.
-h Host	Optional. Host is name or IP address of SLIC host.

Example:

`slicview view -d c0 -r I3 -h MyHost`

Displaying VPD (Vital Product Data) [svpd]

The **svpd** command is used to display important information (Vital Product Data or VPD) for the device selected.

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

Note: VPD only displays the information for a physical drive. No logical information is given.

Usage:

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

-h Host	Host system name (e.g. venus) or IP address (e.g. 204.118.9.9).
-d Cx	Cx is the SignOn path, as specified in the config file.
-t [s/Txxxxx]	Optional. Two possible variables:
s	Sign-On Drive.
Txxxxx	Target number of a drive that the host can access.
-f File_Name	Optional. Write VPD to File_Name.
-v	Optional. Print VPD to console.

Diagnostic CLI

Reading the Error Log [sreadlog]

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

Usage:

sreadlog {–h Host} –d Cx {–f File_Name –v}

-h Host	Host system name (e.g. venus) or IP address (e.g. 204.118.9.9).
-d Cx	Cx is the SignOn path, as specified in the config file.
-f File_Name	Optional. Write the Log Analysis to File_Name.
-v	Optional. Print the Log Analysis to console.

Clearing the Check Mode [sclrlog]

Use the **sclrlog** command to clear the check status (CK) or power cooling (PC) in the SLIC topology of the selected device. After running sclrlog, the entries in the error log file under the selected device will be marked as old. Old entries are not displayed the next time you run the sreadlog command.

Usage:

sclrlog {–h Host} –d Cx –t[all/Txxxxx]

-h Host	Host system name (e.g. venus) or IP address (e.g. 204.118.9.9).
-d Cx	Cx is the SignOn path, as specified in the config file.
-t [all/Txxxxx]	Two mutually exclusive parameter choices:
all	Clears the check mode (CK) of all the drives.

- Txxxxx — Target number of a drive that the host can access.

CHAPTER 9

SYSTEM DIAGNOSTICS

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

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:

- Both SV Routers.
- Sun StorEdge T3 Array for the Enterprise.
- Cabling between the SV Routers and between the T3 partner group.

Service Request Numbers

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

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

Service and Diagnostic Codes

The service and diagnostic codes are employed to inform the user of subsystem activities. Only the SV Routers provide an LED readout of these codes. See "Service Codes" on page 181 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 170 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.

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 175).

Accessing Error Log Analysis

1. Power on the remote management server and open a terminal.
2. Change to the sduc directory.

Example:

```
#/svengine/sduc
```

3. Using the **`Error Log Analysis`** command, display the error log file.
4. Determine corrective action by comparing the SRNs with the SRN and SNMP Reference" on page 175.

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 175.

SV Router LEDs

SV Router LEDs are shown in Figure 9-1. LED codes are listed in Table 9-1. Two LEDs located on the back of the router echo the functions of the Status and Fault LEDs (Figure 2-4).

- 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 181.

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

Table 9-1 LED Quick Reference

Figure 9-1 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 9-2 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 9-2 Example of Blink Code 060

Ethernet Port LEDs

Ethernet port LEDs are shown in Figure 9-1. 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.

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 129.
2. Ethernet Switch down.
   - Visually inspect Ethernet switch to determine if it is functioning properly.
   - If the switch is a strong suspect but it still has power and if a spare Ethernet switch 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 113.
     - To check the config file, see "Daemon SignOn Path" on page 77.
   - 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 110.
     - To check the config file, see "Daemon SignOn Path" on page 77.
   - Ensure that the SignOn Path is correct. See "Daemon SignOn Path" on page 77.
   - Ensure that you have enable access of the SV Router by the Daemon. See "Enable Daemon SignOn" on page 110.
   - Ensure that the remote management server's IP address is not blocked by the SV Router, see "Enable Password for Daemon SignOn" on page 110.

- 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 110.
  - 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 79.

Other Problems

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

- To check SNMP messages, see "SNMP Manager" on page 170. SNMP messages usually come with corrective action. If further help is needed, see "SRN/SNMP Single Point of Failure Table" on page 178.
- To retrieve SRNs, see "Service Request Numbers" on page 168. To determine action, see "SRN and SNMP Reference" on page 175.
- To check service code message, see "SV Router LEDs" on page 170. For further information, see “Appendix C: Service Codes" on page 181.

Because the SV Router only monitors activity between it and the storage, then problems concerning the activity between drives, the data servers, and the brocade switches, will not be reported by the SV Router. However, the user can activate the SNMP agent in each device. Have the agent send the messages to the same SNMP manager that the SV SNMP Agent is using and monitor the entire system from a central location.

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.)	
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 128 and page 129. • Perform failback if necessary page 116.	70020 70030 **70051****
70025	Partner's Router's IP is not reachable.	Check Ethernet cabling and connections page 127.	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 128 and page 129. • Cycle power on failed SV Router if fault LED flashes. • Perform failback if necessary page 116. • Enable VERITAS path page 125.	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 9-2 Port Communication Table

APPENDIX C

SERVICE CODES

View these codes by reading the SV Routers LEDs. See ‘Reading Service and Diagnostic Codes’ on page 171 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 15.

Code Number	Cause	Corrective Action
005	PCI Bus parity error.	Replace router, page 104.
24	The attempt to report one error resulted in another error.	Cycle power to the router. If problem persist, contact Vicom, page 15.
40	Corrupt database.	• Erase the node mapping table, page 109. • Cycle power to the router. • Import SAN zone configuration, page 160.
41	Corrupt database.	• Erase the node mapping table, page 109. • Cycle power to the router. • Import SAN zone configuration, page 160.
42	Zone mapping database corruption.	Import SAN zone configuration, page 160.
051	Can not erase FLASH memory.	Replace router, page 104.

Code Number	Cause	Corrective Action
53	Unauthorized cabling configuration.	• Check cabling. Ensure server/ switch connects to host-side and storage connects to device-side of router. • If necessary, erase the node mapping table, page 109. • If necessary, cycle router power. • If necessary, Import SAN zone configuration, page 160.
54	Unauthorized cabling configuration.	Check cabling.
57	Too many HBAs attempting to log in.	Check cabling.
60	Node mapping table cleared using SW2.	No action needed.
62	Improper SW2 setting.	• Correct SW2 setting. • Cycle router power.
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 persist, replace router, page 104.
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.
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.

Code Number	Cause	Corrective Action
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 104.
609-610 612-615 617	Ethernet port down.	• Replace router, page 104. • Send router to Vicom for examination.
618	Corrupt firmware	• Replace router, page 104. • Send router to Vicom for examination.
621	Too many Telnet sessions open.	• Cycle power • If problem persist, contact Vicom, page 15.
624-626	Telnet server down.	• Cycle power • If problem persist, contact Vicom, page 15.
634 638 643 650	TCP down.	• Cycle power • If problem persist, contact Vicom, page 15.
700-899 Host side interface driver errors:		
709 715	FC host-side type code invalid.	• Cycle power • If problem persist, replace router, page 104.
734/434	FC host-side connection error.	Check cabling and connections on both ends, page 129.

APPENDIX D

TESTED COMPONENTS

Table 9-3 Tested Hardware

Hardware	Vendor	Model	Detail
Storage	SUN Systems	SUN StorEdge T3 Partner Group	Firmware: 1.17A
Router	Vicom Systems	SV Router FC-FC 3	Firmware: 8.01.03
Server(s)	SUN Systems	• SUN Enterprise Ultra 60 • SUN Enterprise 220R • SUN Enterprise 3500 • SUN Enterprise 450	Represent the three major bus architecture for SUN Servers
Management Server(s)	SUN Systems	• SUN Enterprise Ultra 30 • SUN Enterprise 3500 • SUN Enterprise 450	Represent the three major bus architecture for SUN Servers
Switch(es)	Brocade	• Silkworm 2050 • Silkworm 2250 • Silkworm 2800	Firmware: 2.21A
HBA(s)	Emulex	• LP7000 • LP8000	Firmware: v.3.20.a10 for Solaris
Peripherals/ Networking	Cisco Systems	Catalyst 3524-PWR XL Stackable 10/100 Ethernet Switch	Represent the three major bus architecture for SUN Servers

Table 9-4 Tested Software

Vendor	Software	Version	Patches	Detail
SUN Systems	Solaris OS	8	• Solaris 8 Update 3 and Installation Guide • 110383-01 • 108528-06 • 110255-04	Solaris 8 Update 3 and Installation Guide is included as a CD with the Solaris 8 OS software.
SUN Systems	Solaris OS	7		
SUN Systems	Solaris OS	6		
Veritas	Veritas Volume Manager	3.10		
Veritas	Veritas File System	3.3.3		
Vicom Systems	SV SAN Builder	2.5		
Vicom Systems	SV Zone Manager	2.5		
Vicom Systems	SV SNMP Agent	1.0		

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.

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.
lxxxxx	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 determine which servers are exposed to and have access to a particular LUN, and to allocate to specific servers. LUN masking allows servers not to see or view each other's LUN.
management information base	See MIB.
mapped drive	A drive that is assigned an ID and/or LUN for addressing purposes.
mapping table	See node mapping table.
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	A data reference source for the configuration of the SAN.
node table	See node mapping table.
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.
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 'SVE SUN T3 Solution Pack System Diagram' on page 21.

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

T

V

Z