



Solaris SFS Driver

User Manual

Copyright© 2007 Emulex Corporation. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Emulex Corporation.

Information furnished by Emulex Corporation is believed to be accurate and reliable. However, no responsibility is assumed by Emulex Corporation for its use; or for any infringements of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent or patent rights of Emulex Corporation.

Emulex, AutoPilot Installer, BlockGuard, cLAN, FabricStream, FibreSpy, Giganet, HBAnyware, InSpeed, IntraLink, LightPulse, MultiPulse, SAN Insite, SBOD and Vixel are registered trademarks, and AutoPilot Manager, EZPilot, SLI and VMPilot are trademarks, of Emulex Corporation. All other brand or product names referenced herein are trademarks or registered trademarks of their respective companies or organizations.

Emulex provides this manual "as is" without any warranty of any kind, either expressed or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Emulex Corporation may make improvements and changes to the product described in this manual at any time and without any notice. Emulex Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties that may result. Periodic changes are made to information contained herein; although these changes will be incorporated into new editions of this manual, Emulex Corporation disclaims any undertaking to give notice of such changes.

Last Updated June 14, 2007

Installation	1
Introduction	1
Compatibility	1
Known Issues	2
Minimum Driver for Firmware Installation on LPe11000 and LPe11002 HBAs ...	2
Special Circumstances for Installing Solaris SFS Driver Version 2.12 or later ...	2
Installing the Solaris SFS Driver	3
Downloading and Installing the Driver for Solaris 8 or 9	3
Method 1: Using the Install_it Script (recommended)	3
Method 2: Using Individual Patches	3
Downloading and Installing the Driver for Solaris 10 (Sparc, X64 and x86)	4
Installing the FCA Utilities and the HBAnyware Utility	5
Unpacking the Utility Files	5
Installing the FCA Utilities	5
Installing or Updating the FCA Utilities Using the emlXu_install Script	5
Installing the HBAnyware Utility, Web Launch and Security Configurator	7
Installing the HBAnyware Utility	7
Installing the HBAnyware Utility with Web Launch	8
Installing the HBAnyware Utility Security Configurator	9
Installing or Updating the Utilities Package Manually	9
Removing the Utilities Using the emlXu_remove Script	10
Removing the Utilities Package Manually	11
Configuration	12
Introduction	12
Driver Parameters	13
Solaris SFS and Ipfc Driver Parameter Cross-Reference Table	14
Using the HBAnyware Utility	18
Starting the HBAnyware Utility	18
Starting HBAnyware with Web Launch	18
Starting the HBAnyware Security Configurator	18
Prerequisites	18
Procedure	18
Starting the HBAnyware Utility from the Command Line	19
Changing Management Mode	19
The HBAnyware Utility Window Element Definitions	20
The Menu Bar	20
The Toolbar	20
The Toolbar Buttons	21
The Discovery-Tree	21
Property Tabs	22
Status Bar	22
Using the HBAnyware Utility Command-Line Interface	22
Using the CLI Client	23
Discovering HBAs	38
Configuring Discovery Settings	39
Sorting HBAs	40
Sorting by Host Name	40
Sorting by Fabric Address	40
Sorting Local HBAs Only	40

Viewing HBA Information	41
Viewing Discovery Information	41
Viewing Host Information	42
The Host Information Tab	42
The Host Driver Parameters Tab	43
Viewing General HBA Attributes	44
Adapter Summary Field Definitions	44
Adapter Status Area Field Definitions	45
Viewing Detailed HBA Information	46
Adapter Details Field Definitions	46
Port Attributes Field Definitions	46
Loop Map Table Definitions	47
Viewing Fabric Information	47
Discovery Information Field Definitions	48
Viewing Target Information	48
Viewing LUN Information	49
LUN Information Field Definitions	49
Viewing Port Statistics	50
Port Statistics Field Definitions	51
Viewing Firmware Information	52
Firmware Field Definitions	52
Viewing Target Mapping	53
Target Mapping Field Definitions	53
Resetting HBAs	54
Updating Firmware	55
Prerequisites	55
Procedure	55
Updating Firmware (Batch Mode)	58
Prerequisites	58
Procedure	58
Enabling or Disabling the BIOS	59
Prerequisites	59
Procedure	59
Setting Driver Parameters	60
Setting Driver Parameters for an HBA	61
Setting Driver Parameters for a Host	62
Creating the Batch Mode Driver Parameters File	64
Assigning Batch Mode Parameters to HBAs	64
Setting Up Persistent Binding	65
Adding New Targets Using sd.conf for Solaris 8, 9 and 10	68
Changing Parameters or Bindings for Solaris 8, 9 and 10	68
Setting Up Target/LUN Blocking Using sd.conf	69
No-Reboot Firmware Updates	69
Loading or Unloading the Driver Without Rebooting	69
Performing Diagnostic Tests	70
Running a Quick Test	70
Running a POST Test	71
Using Beacons	71
Creating Diagnostic Dumps	72
Displaying PCI Registers and Wakeup Information	72
Running Advanced Diagnostic Tests	73
Running Loopback Tests	74
Running End-to-End (ECHO) Tests	75
Saving the Log File	76

Out-of-Band SAN Management	77
Adding a Single Host	78
Adding a Range of Hosts	79
Removing Hosts	80
HBAnyware Security	80
Introduction	80
Starting the Security Configurator for the First Time: Creating the First ACG, Designating the MSC and Selecting Systems in the FC Network	82
Prerequisites	82
Procedure	82
Access Control Groups	84
Introduction	84
Adding a Server to the ACG	86
Deleting a Server from the ACG	87
Removing Security from all Servers in the ACG	88
Generating New Security Keys	89
Restoring the ACG to Its Last Saved Configuration	90
Accessing a Switch	91
Access Sub-Groups	92
Introduction	92
Creating an ASG	93
Adding a Server to an ASG	95
Deleting an ASG	95
Restoring an ASG to Its Last Saved Configuration	96
Editing an ASG	97
About Offline ASGs	98
Backup Masters	99
Introduction	99
Creating a Backup Master	100
Reassigning a Backup Master as the New MSC from the Old MSC	101
Reassigning a Backup Master as the New MSC from the Backup Master	103
Using the emlxadm Utility	104
Modes of Operation (emlxadm)	104
Interactive Mode (emlxadm)	104
CLI Mode (emlxadm)	105
Command Descriptions (emlxadm)	107
get_num_devs	107
get_dev_list	107
get_logi_params <wwpn>	108
get_host_params	108
get_sym_pname	109
set_sym_pname <"string">	109
get_sym_nname	109
set_sym_nname <"string">	109
dev_login <wwpn>	109
dev_logout <wwpn>	110
get_state <wwpn>	110
dev_remove <wwpn>	110
link_status <d_id>	110
get_fcode_rev	110
download_fcode <filename>	111
get_fw_rev	111
download_fw <filename>	111

get_boot_rev	112
download_boot <filename>	112
get_dump_size	112
force_dump	112
get_dump <-t filename.txt or -b filename.bin>	112
get_topology	113
reset_link <wwpn or zero for local link>	113
reset_hard	113
reset_hard_core	114
diag <test [parameters]> or diag code <cmd_code (hex)>	114
ns	115
parm_get_num	115
parm_get_list	116
parm_get <label>	118
parm_set <label> <value>	118
msgbuf all or <number> [-i interval]	119
get_host_attrs	119
get_port_attrs <index>, <wwn> or all	120
get_path <index>	121
get_vpd	122
boot_code [enable or disable]	122
q	122
h	122
hba	123
p	123
Using the emlxdrv Utility	124
Modes of Operation (emlxdrv)	124
Interactive Mode (emlxdrv)	124
CLI Mode (emlxdrv)	125
Command Descriptions (emlxdrv)	126
set_emlxs <alias>	126
set_emlxs_sun	126
set_emlxs_all	126
set_lpfc <alias>	127
set_lpfc_nonsun	127
clear_dev <alias>	127
clear_lpfc	128
clear_emlxs	128
clear_sun	129
clear_nonsun	129
clear_all	130
q	130
Troubleshooting	131
Introduction	131
Situations That Involve HBAnyware	131
General Situations	131
Security Configurator Situations - Access Control Groups (ACG)	133
Security Configuration Situations - Access Sub-Groups (ASG)	134
HBAnyware Security Configurator Situations - Backup Masters	135
Error Message Situations	136
Master Security Client Situations	137

Console and Log Messages	139
Introduction	139
Severity Levels	140
Message Log Example	140
Miscellaneous Events	141
Driver Events	142
HBA Initialization Events	143
Memory Management Events	145
Service Level Interface (SLI) Events	146
Mailbox Events	148
Node Events	148
Link Events	150
ELS Events	151
General I/O Packet Events	152
FCP Traffic Events	154
IP Traffic Events	154
Solaris SFS Events	155
IOCTL Events	157
Firmware Download Events	158
Common Transport Events	159
 Appendix	 161
Introduction	161
Use Cases	161
Migrating from the Solaris lpfc Driver to the Solaris SFS Driver	162
Operational Differences Between lpfc and SFS	162
Sample Script File Details	162
start_emlxs_migration.sh	162
finish_emlxs_migration.sh	163
Migrating a Configuration without FC Boot	164
Migrating Automatically	164
Prerequisites	164
Procedure	164
Migrating Manually	165
Migrating a Configuration with FC Boot	166
Migrating Non-emlxs HBAs to emlxs HBAs	166
Migrating an lpfc Configuration to emlxs – Adding Sun-Branded HBAs	168

Installation

Introduction

Compatibility

The StorEdge SAN Foundation Software (SFS) driver and utilities support the following operating systems:

- Solaris 8 SPARC
- Solaris 9 SPARC
- Solaris 10 SPARC
- Solaris 10 x64 and x86

The following table specifies the host bus adapters (HBAs) supported by the Solaris SFS driver and the Emulex Fibre Channel Adapter Utilities (FCA Utilities).

Table 1: HBA Compatibility

HBA	Solaris SFS Driver	HBAnyware Utility	FCA Utilities	
			emlxadm	emlxdrv
SG-XPCI1FC-EM4-Z**	X	X	X	N/A
SG-XPCI2FC-EM4-Z**	X	X	X	N/A
SG-XPCIE1FC-EM4**	X	X	X	N/A
SG-XPCIE2FC-EM4**	X	X	X	N/A
SG-XPCI1FC-EM2**	X	X	X	N/A
SG-XPCI2FC-EM2**	X	X	X	N/A
LP11002	X	X	X	X
LP11000	X	X	X	X
LPe11002*	X	X	X	X
LPe11000*	X	X	X	X
LP10000ExDC	X	X	X	X
LP10000DC	X	X	X	X
LP10000	X	X	X	X
LP9802	X	X	X	X
LP9002DC	X	X	X	X
LP9002L	X	X	X	X
LP9002S	X	X	X	X

* Special driver and firmware installation considerations may apply. See the Known Issues section of this manual for more information.

** Special firmware installation considerations apply. See *Updating Firmware* on page 55 for more information.

Known Issues

Minimum Driver for Firmware Installation on LPe11000 and LPe11002 HBAs

You cannot install firmware version 2.70 or later on an LPe11000 or an LPe11002 HBA that is running a driver version earlier than 2.11i (Sun patch revision -12). (If you are installing driver version 2.12 [Sun patch revision -15] or later, continue reading the next section.)

Special Circumstances for Installing Solaris SFS Driver Version 2.12 or later

If you want to update the driver to version 2.12 (Sun patch revision -15) through 2.20h (Sun patch revision -18) and both of the following conditions are true, follow one of the sets of special installation procedures in this section.

- An LPe11000 or an LPe11002 HBA is installed
- A firmware version earlier than 2.70 is installed

If the above conditions are true and you do not want to enable support for multiple interrupt MSI mode, follow the instructions in Procedure 1 to install the driver and, optionally, to update the firmware.

If the above conditions are true and you do want to enable support for multiple interrupt MSI, follow the instructions in Procedure 2 to install the driver and update the firmware (you must update the firmware to version 2.70 or later for multiple interrupt MSI support).

Procedure 1

1. Download and install the driver version 2.12 or later patch from the Sun Web site. Do not reboot the server after the installation is finished.
2. Add "msi-mode=1;" to the /kernel/drv/emlxs.conf file. This step enables single interrupt MSI mode.
3. Perform a reconfiguration reboot of the server.
4. If desired, download firmware version 2.70 or later from the Emulex Web site and install it on each HBA port. No reboot is required. (Installing firmware version 2.70 or later is not mandatory.)

Procedure 2

1. Download and install the driver version 2.12 or later patch from the Sun Web site. Do not reboot the server after the installation is finished.
2. Add "msi-mode=1;" to the /kernel/drv/emlxs.conf file. This step enables single interrupt MSI mode. (You will enable multiple interrupt MSI support later.)
3. Perform a reconfiguration reboot of the server.
4. Download firmware version 2.70 or later from the Emulex Web site and install it on each HBA port (this step is not optional for multiple interrupt MSI support). No reboot is required.
5. Remove the "msi-mode=1;" entry from the /kernel/drv/emlxs.conf file to enable multiple interrupt MSI support.
6. Perform a reconfiguration reboot of the server.

Installing the Solaris SFS Driver

Caution: Before installing the Emulex utilities package, you must first install the Sun StorEdge SAN Foundation Software package and all the recommended patches as described in the *Sun StorEdge SAN Foundation Software Installation Guide* provided by Sun.

Downloading and Installing the Driver for Solaris 8 or 9

The Emulex FCA driver and the Solaris SFS prerequisites can be acquired in two ways. Method 1, Using the Install_it Script (the recommended method) or method 2, Using Individual Patches.

Method 1: Using the Install_it Script (recommended)

Note: Install_scripts may be available a few days after the individual patches are available.

To obtain and install the Install_it script:

1. Go to <http://www.sun.com/download/index.jsp?tab=2>, scroll down and click **StorageTek SAN 4.4**.
2. Log in with your user name and password, and accept the license agreement.
3. Select and download "Install_it Script SAN 4.4.12, English".
4. Select and download "Install_it Script SAN 4.4.x Readme, English", and follow the instructions.

Method 2: Using Individual Patches

To obtain and install individual patches:

1. Go to <http://www.sun.com/download/index.jsp?tab=2>, scroll down and click **StorEdge SAN 4.4**.
2. Log in with your user name and password, and accept the license agreement.
3. For Solaris 8:
 - a. Select "Solaris 8 SFS Base Packages, English" and follow the instructions.
 - b. Go to <http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>. Enter and download the following required patches:
 - 111095
 - 119913
 - 111413
 - c. Follow the instructions to install each patch.
 - d. For additional functionality, install the following optional patches:
 - 111096 (FCIP)
 - 111412 (mpxio)
 - 113767 and 113766 (Common HBA API)
 - 114475 (FCSM)

For Solaris 9:

- a. Select "Solaris 9 SFS Base Packages, English" and follow the instructions.

- b. Go to <http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>. Enter and download the following required patches:
 - 113040
 - 119914
 - 113043
- c. Follow the instructions to install each patch.
- d. For additional functionality, install the following optional patches:
 - 113041 (FCIP)
 - 113039 (mpxio)
 - 114478 and 114477 (Common HBA API)
 - 114476 (FCSM)

Downloading and Installing the Driver for Solaris 10 (Sparc, X64 and x86)

If the Solaris SFS driver is not already installed, obtain and install the Solaris 10 packages.

To obtain and install the Solaris 10 packages:

1. Go to <http://www.sun.com/download/products.xml?id=42c4317d> and click **Download**.
2. Log in with your user name and password, and accept the license agreement.
3. Select and download the driver package.
4. Select and download the readme file, and follow its instructions.

To finish the installation (or if the Solaris SFS driver was already installed), install the driver by obtaining and installing individual patches:

1. Go to <http://sunsolve.sun.com/pub-cgi/show.pl?target=patchpage>. Enter and download the following required patches:
 - For SPARC systems:
 - 119130
 - 120222
 - For x64 and x86 systems:
 - 119131
 - 120223
2. Follow the instructions to install each patch.
3. For additional functionality, install the following optional patches:
 - For SPARC systems:
 - 119470 (Sun Enterprise Network Array firmware and utilities)
 - 119715 (scsi_vhci patch)
 - For x64 and x86 systems:
 - 119471 (Sun Enterprise Network Array firmware and utilities)
 - 119715 (scsi_vhci patch)

Installing the FCA Utilities and the HBAnyware Utility

Unpacking the Utility Files

The FCA Utilities and the HBAnyware utility are packaged together in one application kit tar file.

To unpack the tar file:

1. Log in as root, or su to root.
2. Copy the application kit tar file from your distribution medium into a directory, referred to here as <directory>. The .tar file is named something similar to Solaris-3.2a13-1.01c-1a.tar.
3. Change to the directory where you put the kit tar file by typing:

```
cd <directory>
```

4. Extract and unpack the FCA Utilities and the HBAnyware utility files from the tar by typing:

```
tar xf Solaris-3.2a13-1.01c-1a.tar
```

Both of the following tar kits will be placed in the specified directory:

- Solaris-3.2a13-1.01c-1a-i386.tar
- Solaris-3.2a13-1.01c-1a-sparc.tar

Each of these .tar files contains the following:

- readme.first.txt
- eml_xu_kit-1.01c-<platform>.tar - The eml_xu_kit files contain the FCA Utilities.
- EmlxApps300b-12-Solaris.tar - This file contains the HBAnyware utility.

5. Untar the Solaris-3.2a13-1.01c-1a-<platform>.tar:

```
tar xvf Solaris-3.2a13-1.01c-1a-<platform>.tar
```

Installing the FCA Utilities

The FCA Utilities are comprised of the eml_xadm utility and the eml_xdrv utility.

- The eml_xadm utility provides an interface to the Fibre Channel input/output (FCIO) interface provided by the Sun StorEdge SFS.
- The eml_xdrv utility temporarily associates or binds the Emulex eml_xs Solaris SFS driver and the Solaris lpfc driver to the various models of Emulex FC HBAs during migration from the Solaris lpfc driver to the Solaris SFS driver.

Installing or Updating the FCA Utilities Using the eml_xu_install Script

Although it is possible to install eml_xu onto one or more clients from a server, that procedure is not covered in this document; refer to the Solaris documentation.

Note: If an earlier version of the eml_xu utilities package is already installed on the system, the eml_xu_install script will remove the old version before installing the new version.

Prerequisites

- Before installing the Emulex emlxu utilities package, you must completely install:
 - The Sun StorEdge SAN Foundation Software package.
 - All the recommended patches as described in the *Sun StorEdge SAN Foundation Software Installation Guide* provided by Sun.
 - The Emulex-Sun Fibre Channel adapter SUNWemlxs driver package.

Procedure

To install the utilities kit using the emlxu_install script:

1. Untar the emlxu_kit-1.01c-<platform>.tar file.

```
tar xvf emlxu_kit-1.01c-<platform>.tar
```

The emlxu_install script is available.
2. Install the FCA Utilities by typing:

```
emlxu_install
```
3. The script removes any earlier version of the emlxu utilities package. (If an earlier package is not found, this fact is indicated; skip to step 9.) The following text is displayed:

```
<Removing old EMLXemlxu package>
```
4. If an old package is installed, you are prompted to remove it:

```
Do you want to remove this package? [y,n,?,q]
```
5. Enter **y**. The following message is displayed:

```
Removal of <EMLXemlxu> was successful.
```
6. The script expands the utilities kit .tar file and begins installing the new package. A message similar to the following message will be displayed:

```
<Expanding emlxu_kit-1.01c-sparc.tar>  
<Adding new package>
```
7. The script installs the emlxu utilities package. The package is prepared for installation and you are prompted for confirmation by the following message:

```
Do you want to continue with the installation of <EMLXemlxu> [y,n,?]:
```
8. Enter **y**. The installation package provides running commentary on the installation process.
9. Examine the output for any errors or warnings. If the installation is successful, the following message is displayed near the end of the process:

```
Installation of <EMLXemlxu> was successful.
```
10. The script performs some cleanup and displays the following messages:

```
<Cleaning directory>  
<emlxu_install complete>  
<Execute "emlxu_remove" when ready to uninstall>
```
11. The script leaves a copy of the emlxu_remove script in your working directory with the original utilities kit tar file. You can remove this script, or leave it in the directory if you may want to uninstall the emlxu utilities from your system in the future. See *Installing or Updating the Utilities Package Manually* on page 9 for more details.

The emlxu utilities installation is complete. The utility package's programs are located in the /opt/EMLXemlxu/bin directory.

You do not need to reboot your system to run a utility program, but you must either enter the program's full path name, or add the package's bin directory (/opt/EMLXemlxu/bin) to your environment's search path. To use the man pages provided by the package, you must also add the package's man directory (opt/EMLXemlxu/man) to your environment's man path.

For further information on installing and removing packages, consult the Solaris system administration documentation and the pkgadd(1M) and pkgrm(1M) manual pages.

Installing the HBAnyware Utility, Web Launch and Security Configurator

Known Issues

- Starting with the HBAnyware utility version 3.2, Emulex provides support for LightPulse adapters that are reprogrammed with WWPNs outside the typical Emulex range, such as Hewlett-Packard's upcoming Virtual Connect for Fibre Channel on the BladeSystem c-Class platform. In such environments, the HBAnyware utility version 3.2, must be deployed across all servers on the SAN, as well as any other management console used for out-of-band management, so that all adapters appear in the Discovery Tree.

Installing the HBAnyware Utility

Prerequisites

- The FCA Utilities must be installed prior to installing the HBAnyware utility.
- Java Runtime Environment:

Version 5 of the Java Runtime Environment (JRE) must be installed. The HBAnyware utility will not run under earlier versions of the JRE.

Caution: The utilities require the java runtime binaries and libraries, so their path must be included at the beginning of the PATH environment variable to avoid conflicts with possible earlier versions of java that may still be installed on the system. For example, if the java runtime binaries are in /usr/java/bin, then include this path in the PATH environment variable.

For example: (bash> export PATH="/usr/java/bin:\$PATH")

The JRE and instructions for installation can be found at <http://java.sun.com/downloads/index.html>.

Procedure

To install the HBAnyware utility from the tar file:

- Untar the EmlxApps tar file:

```
tar xvf EmlxApps-300b12-Solaris.tar
```
- Run the unpack script to obtain the correct package version. Type:

```
./unpack_apps
```
- Unzip the HBAnyware package file. Type:

```
gunzip HBAnyware-<version>-<platform>.tar.gz
```
- Untar the HBAnyware package file. Type:

```
tar -xvf HBAnyware-<version>-<platform>.tar
```
- Run the pkgadd utility. Type:

```
pkgadd -d .
```

6. When prompted by pkgadd, choose to install the HBAnyware utility.
7. When prompted by pkgadd, answer the HBAnyware installation questions.

Installing the HBAnyware Utility with Web Launch

Prerequisites

Before installing the HBAnyware utility with Web Launch, ensure your systems meet the following requirements.

- The system on which you are installing the Web Launch services package (the server) requires that the HTTP Web server be configured to handle the JNLP MIME file type. Follow these steps:
 - a. Change your working directory to the directory containing the Apache configuration files for example: `/etc/apache` or `/etc/apache2`.
 - b. Edit the file "mime.types".
 - c. Add the following line to the file:

```
application/x-java-jnlp-file jnlp JNLP
```
 - d. Save the file.
 - e. Stop and restart the HTTP Web server (to enable the Web server to detect this change).
- The system on which you are running the browser (the client) requires the Java Runtime Environment (JRE) 5.0 or later must be installed on the browser host. Below are the specific requirements:
 - Sun 32-bit JRE 5.0 or later for Intel based systems (x86 and IA64)
 - Sun 32-bit JRE 5.0 or later x86-64

Refer to the appropriate vendor documentation for detailed instructions about configuring and starting the HTTP server and installing the JRE.

- The HBAnyware utility must be installed before installing HBAnyware with Web Launch.

Procedure

To install HBAnyware with Web Launch:

1. Log on as 'root'.
2. Navigate to the HBAnyware directory. Type:

```
cd /usr/sbin/hbanyware
```
3. Run the install script. Type:

```
./wsinstall
```
4. When prompted, enter the Web server's document root directory. For example:

```
/srv/www/htdocs
```
5. You are provided with the IP address of the host and asked if that is the IP address that is being used by your Web server. Answer Y or N as appropriate. If you answer N, you are prompted for the IP address you wish to use.
6. You are asked if your web server listening on the normal default HTTP port (80)? Answer Y or N as appropriate. If you answer N, you are prompted for the port you wish to use.

You are notified the installation of the HBAnyware Web Launch package has completed.

Installing the HBAware Utility Security Configurator

Follow these instructions to install the Security Configurator on your system.

Prerequisites

- The HBAware utility must be installed on the system.
- Java Runtime Environment:
Version 5 of the Java Runtime Environment (JRE) must be installed. The lputil and HBAware utilities will not run under earlier versions of the JRE.
The JRE and instructions for installation can be found at:
<http://java.sun.com/downloads/index.html>.

Procedure

To install the HBAware utility Security Configurator from a tar file:

1. If you have not already done so, untar the EmlxApps tar file and run the unpack script to obtain the correct package version:

```
tar xvf EmlxApps-300b12-Solaris.tar  
./unpack_apps
```
2. Unzip the HBAwareSSC package file:

```
gunzip HBAwareSSC-<version>-<platform>.tar.gz
```
3. Untar the HBAwareSSC package file. Type:

```
tar xvf HBAwareSSC-<version>-<platform>.tar
```
4. Run the pkgadd utility. su to 'root'.

```
pkgadd -d
```
5. When prompted by pkgadd, choose to install HBAwareSSC.
6. If prompted by pkgadd, answer the HBAwareSSC installation questions.

Installing or Updating the Utilities Package Manually

Compatibility

- The HBAware utility can be used with Solaris 10 Update 4 or later, or with SFS driver version 2.20i (Sun patch revision -19) or later

Prerequisites

- Before installing the Emulex utilities package, you must completely install:
 - The Sun StorEdge SAN Foundation Software package.
 - All the recommended patches as described in the *Sun StorEdge SAN Foundation Software Installation Guide* provided by Sun.
- If an earlier version of the emlXu utilities package is already installed on the system and you want to install a different version, follow the instructions in *Removing the Utilities Package Manually* on page 11, then return to this section to install the new utilities package.

Procedure

To install the emlxu utilities package manually:

1. Log in as root, or su to root.
2. Copy the utilities kit from your distribution medium into a directory, referred to here as <directory>. The utilities kit is a .tar file named something similar to emlxu_kit-1.01c-sparc.tar.
3. Change to the directory where you put the kit tar file by typing:

```
cd <directory>
```
4. Extract the installation images from the tar file by typing:

```
tar xvf emlxu_kit-1.01c-sparc.tar
```
5. Install the EMLXemlxu utilities package by typing:

```
pkgadd -d . EMLXemlxu
```
6. The package is prepared for installation, and you are prompted to confirm the installation with the following message:

```
Do you want to continue with the installation of <EMLXemlxu> [y,n,?]
```
7. Enter **y**. The installation package provides running commentary on the installation process.
8. Examine the output for any errors or warnings. If the installation is successful, the following message is displayed near the end of the process:

```
Installation of <EMLXemlxu> was successful.
```

The emlxu utilities installation is complete. The utility package's programs are located in the /opt/EMLXemlxu/bin directory.

You do not need to reboot your system to run a utility program, but you must either enter the program's full path name, or add the package's bin directory (/opt/EMLXemlxu/bin) to your environment's search path. To use the man pages provided by the package, you must also add the package's man directory (opt/EMLXemlxu/man) to your environment's man path.

Removing the Utilities Using the emlxu_remove Script

You can uninstall the utilities kit using the emlxu_remove script. If you do not have the emlxu_remove script and you do not have the original emlxu utilities kit tar file, you must uninstall the emlxu package manually; follow the instructions in *Removing the Utilities Package Manually* on page 11. If you are updating the emlxu utilities to a newer version and you have the new utilities kit tar file, you do not need to use the emlxu_remove script; the emlxu_install script removes any old version as it installs the newer version; see *Installing or Updating the FCA Utilities Using the emlxu_install Script* on page 5 for more details.

To uninstall the utilities package (without updating them):

Note: All emlxu files are removed.

1. Go to the directory where the emlxu_remove script is located, or to the directory where the original utilities kit tar file is located, by typing:

```
cd <directory>
```
2. If you have the emlxu_remove script, skip to step 4. If you do not have the emlxu_remove script but you do have the original emlxu utilities kit tar file, extract the emlxu_remove script from the tar file by typing:

```
tar xf emlxu_kit-1.01c-sparc.tar emlxu_remove
```

3. Remove the emlXu utilities package by typing:

```
emlXu_remove
```

4. The script locates the EMLXemlXu utilities package, and the following message is displayed:

```
<Removing EMLXemlXu package>
```

Note: If no package is installed, the following message is displayed:

```
pkgrm: ERROR: no package associated with <EMLXemlXu>
```

5. You are prompted to remove the package with the following message:

```
Do you want to remove this package? [y,n,?,q]
```

6. Enter **y**. The following message is displayed:

```
Removal of <EMLXemlXu> was successful.
```

7. The script performs some cleanup and displays the following message:

```
<Removing emlXu scripts>
```

```
<emlXu_remove complete>
```

The utilities package has been removed. If you want to install another version of the emlXu utilities package, do so now by following the instructions in one of the following sections:

- *Installing or Updating the FCA Utilities Using the emlXu_install Script* on page 5
- *Installing or Updating the Utilities Package Manually* on page 9

For additional information on installing and removing packages, see the Solaris system administration documentation and the pkgadd(1M) and pkgrm(1M) manual pages.

Removing the Utilities Package Manually

To remove the emlXu utilities package:

1. Remove the EMLXemlXu utilities package by typing:

```
pkgrm EMLXemlXu
```

2. You are prompted to confirm the removal by the following message:

```
Do you want to remove this package? [y,n,?,q]
```

3. Enter **y**. The package is prepared for removal, and you are prompted again for confirmation:

```
Do you want to remove this package? [y,n,?,q]
```

4. Enter **y**. The following message is displayed:

```
Removal of <EMLXemlXu> was successful.
```

The utilities package has been removed.

For additional information on installing and removing packages, see the Solaris system administration documentation and the pkgadd(1M) and pkgrm(1M) manual pages.

Configuration

Introduction

The HBAnyware utility is launched directly from your Web browser. The utility is client/server based and allows you to perform configuration, update and management tasks locally and remotely (inband - host systems on the same FC SAN or out-of-band - from IP addresses of remote machines). The HBAnyware Web Launch feature enables you to download and launch the HBAnyware user interface by specifying the URL of a server that is hosting the HBAnyware Web Launch software. You only need a standard web browser, or some other application capable of making HTTP requests.

Note: Only the HBAnyware Web Launch GUI is being exported to the requesting client. All HBA discovery and remote management operations are performed by resources running on the remote host that served up the GUI component. Therefore, the SAN "view" displayed by the GUI is not from the perspective of the client running the GUI, but rather from the perspective of the host from which this GUI was retrieved.

Use the HBAnyware utility to do any of the following:

- Discover local and remote hosts, HBAs, targets and LUNs
- Reset HBAs
- Set HBA driver parameters locally, simultaneously to multiple HBAs (using Batch Update) and globally
- Update firmware on a single HBA or multiple HBAs using Batch Update
- Update FC boot code (BootBIOS, OpenBoot or EFIBoot) on the local HBA or on remote HBAs
- Enable or disable the system BIOS
- Run diagnostic tests on HBAs
- Manage local, in-band remote and out-of-band remote HBAs

Note: Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

- Locate HBAs using beaconing
- The Solaris SFS utility allows you to make changes to the driver initialization.
- The Emulex FCA utilities consist of the emlxadm utility and the emlxdrv utility:
 - The emlxadm utility provides an interface to the FCIO interface provided by the Sun StorEdge SFS.
 - The emlxdrv utility temporarily associates or binds the Emulex emlxs Solaris SFS driver and the Solaris lpfc driver to the various models of Emulex FC HBAs during migration from the Solaris lpfc driver to the Solaris SFS driver.

Driver Parameters

- The `emlxs.conf` file contains all the parameters necessary to initialize the Solaris SFS driver.

In the `emlxs.conf` file, all adapter-specific parameters have `emlxsX`-prefix (where `X` is the driver instance number); e.g. setting `emlxs0-link-speed=4` makes 4 the default link speed setting for the zero instance of the driver. Changes to the `emlxs.conf` file require you to unload and reload the driver.

- The `lpfc.conf` file contains all the parameters necessary to initialize the Solaris `lpfc` driver.

In the `lpfc.conf` file, all adapter-specific parameters have `lpfcX`-prefix (where `X` is the driver instance number); e.g., setting `lpfc0-lun-queue-depth= 20` makes 20 the default number of maximum commands which can be sent to a single logical unit (disk) for the zero instance of the `lpfc` driver. Changes to the `lpfc.conf` file require you to unload and reload the driver.

Note: If you want to override a driver parameter for a single driver-loading session, you can specify it as a parameter to the `modload` command. For example: `# modload /kernel/drv/lpfc automap=0` (for 32-bit platforms) or `modload/kernel/drv/sparcv9/lpfc automap=0` (for 64-bit platforms). This will load Emulex's SCSI support driver with `automap` set to 0 for this session.

- The `HBAnyware` utility reflects the Solaris SFS driver parameters.

The following table is a cross-reference of the Solaris SFS driver parameters and the corresponding or related `lpfc` driver parameters. The values for the `lpfc` driver parameters and the Solaris SFS driver parameters default to enable migration from the Solaris `lpfc` driver to the Solaris SFS driver.

Note: If any of the default parameter values were changed, verify that this change will not impact the migration **before** you migrate.

Solaris SFS and Ipfc Driver Parameter Cross-Reference Table

Table 1: Solaris SFS and Ipfc Driver Parameter Cross-Reference

Solaris SFS/ HBAnyware Parameter	Solaris SFS/HBAnyware Min/Max, Defaults and Description	Related Ipfc Parameter	Ipfc Min/Max, Default and Description	Comments
ack0	0 = Off 1 = On Default: 0 Description: Use ACK0 for class 2. If ACK0 is 1, the HBA tries to use ACK0 when running Class 2 traffic to a device. If the device doesn't support ACK0, then the HBA uses ACK1. If ACK0 is 0, only ACK1 is used when running Class 2 traffic.	ack0	0 = Off 1 = On Default: 0 Description: Use ACK0 for class 2. If ACK0 is 1, the HBA tries to use ACK0 when running Class 2 traffic to a device. If the device doesn't support ACK0, then the HBA uses ACK1. If ACK0 is 0, only ACK1 is used when running Class 2 traffic.	
adisc-support	0 = No support. Flush active I/O's for all FCP target devices at link down. 1 = Partial support. Flush I/O's for non-FCP2 target devices at link down. 2 = Full support. Hold active I/O's for all devices at link down. Default: 1 Description: Sets the level of driver support for the FC ADISC login I/O recovery method.	use-adisc	0 = Off 1 = On Default: 0 Description: Controls the ELS command used for address authentication during rediscovery upon link-up. The driver will always use ADISC for FCP-2 devices and re-discovery due to an registered state change notification (RSCN).	If there are tape devices on the SAN that support FCP2, set the use-adisc parameter to 1 and the adisc-support parameter to 1 (partial support) or 2 (full support).
assign-alpa	Min:0x00 Max:0xef Default:0x00 (valid ALPA's only) Description: This is only valid if topology is loop. A zero setting means no preference. If multiple adapter instances on the same host are on the same loop, you should set this value differently for each adapter.	N/A	N/A	

Table 1: Solaris SFS and Ipfc Driver Parameter Cross-Reference (Continued)

Solaris SFS/ HBAnyware Parameter	Solaris SFS/HBAnyware Min/Max, Defaults and Description	Related Ipfc Parameter	Ipfc Min/Max, Default and Description	Comments
cr-delay	Min:0 Max:63 Default:0 Description: Specifies a count of milliseconds after which an interrupt response is generated if the cr-count has not been satisfied. This value is set to 0 to disable the Coalesce Response feature as default.	cr-delay	Min:0 Max:63 Default:0 Description: Specifies a count of milliseconds after which an interrupt response is generated if the cr-count has not been satisfied. This value is set to 0 to disable the Coalesce Response feature as default.	Setting this value can minimize CPU utilization by reducing the number of interrupts that the driver generates to the operating system.
cr-count	Min:1 Max:255 Default:1 Description: Specifies a count of I/O completions after which an interrupt response is generated. This feature is disabled if cr-delay is set to 0.	cr-count	Min:1 Max:255 Default:1 Description: Specifies a count of I/O completions after which an interrupt response is generated. This feature is disabled if cr-delay is set to 0.	The parameter setting is often determined by your OEM. This parameter sets the number of I/Os to be queued in the operating system's driver before an interrupt is initiated. The driver default settings are roughly a 1:1 I/O to interrupt ratio. If you change this parameter, performance varies per application.
link-speed	0 = auto select 1 = 1 Gigabaud 2 = 2 Gigabaud 4 = 4 Gigabaud Default: 0 Description: Sets the link speed setting for initializing the FC connection.	link-speed	0 = auto select 1 = 1 Gigabaud 2 = 2 Gigabaud 4 = 4 Gigabaud Default: 0 Description: Sets link speed.	This variable can be changed to a specific link speed to optimize the link initialization process for a specific environment.

Table 1: Solaris SFS and Ipfc Driver Parameter Cross-Reference (Continued)

Solaris SFS/HBAnyware Parameter	Solaris SFS/HBAnyware Min/Max, Defaults and Description	Related Ipfc Parameter	Ipfc Min/Max, Default and Description	Comments
network-on	Min:0 (Disables) Max:1 (Enables) Default:1 Description: Enables or disables IP networking support in the driver.	network-on	Min:0 (Disables) Max:1 (Enables) Default:1 Description: Controls whether Ipfc provides IP networking functionality over FC. This variable is Boolean: when zero, IP networking is disabled: when non-zero, IP networking is enabled.	The Ipfc parameter enables or disables FCIP on the Emulex HBA.
num-iocbs	Min:128 Max:1024 Default = 1024 Description: Sets the number of iocb buffers to allocate.	num-bufs	Min:64 Max:128 Default = 128 Description: Specifies the number of command buffers to allocate. These buffers are used for Fibre Channel Extended Link Services (ELS) and one for each FCP command issued in SLI-2 mode. If you want to queue lots of FCP commands to the adapter, then you should increase num-bufs for better performance. These buffers consume physical memory and are also used by the device driver to process loop initialization and rediscovery activities. Important: The driver must always be configured with at least several dozen ELS command buffers; Emulex recommends at least 128.	
num-nodes	Min:2 Max:512 Default:512 Description: Number of FC nodes (NPorts) the driver will support.	N/A	N/A	

Table 1: Solaris SFS and Ipfc Driver Parameter Cross-Reference (Continued)

Solaris SFS/HBAnyware Parameter	Solaris SFS/HBAnyware Min/Max, Defaults and Description	Related Ipfc Parameter	Ipfc Min/Max, Default and Description	Comments
pm-support	0 = Disables power management support in the driver. 1 = Enables power management support in the driver. Default: 0 Description: Enable/Disable power management support in the driver	N/A	N/A	
topology	0 = loop, if it fails attempt pt-to-pt 2 = pt-to-pt only 4 = loop only 6 = pt-to-pt, if it fails attempt loop Default: 0 Description: Link topology for initializing the Fibre Channel connection. Set pt-to-pt if you want to run as an N_Port. Set loop if you want to run as an NL_Port.	topology	0x0 = loop, if it fails attempt pt-to-pt 0x2 = pt-to-pt only 0x4 = loop only 0x6 = pt-to-pt, if it fails attempt loop Default: 0 Description: Controls the FC topology expected by Ipfc at boot time. FC offers pt-to-pt, fabric and arbitrated loop topologies. To make the adapter operate as an N_Port, select pt-to-pt mode (used for N_Port to F_Port and N_Port to N_Port connections). To make the adapter operate as an NL_Port, select loop mode (used for private loop and public loop topologies). The driver will reject an attempt to set the topology to a value not in the above list. The auto-topology settings 0 and 6 will not work unless the adapter is using firmware version 3.20 or higher.	The topology parameter controls the protocol (not physical) topology attempted by the driver.
ub-bufs	Min:40 Max:16320 Default:1000 Description: Sets the number of unsolicited buffers to be allocated.	N/A	N/A	

Using the HBAnyware Utility

Starting the HBAnyware Utility

Note: The HBAnyware utility can only discover and manage remote HBAs on hosts running the HBAnyware utility's elxhamgr daemon.

Note: Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

To start the HBAnyware utility:

1. Login as or su to 'root'.
2. Run the script:

```
/usr/sbin/hbanyware/hbanyware
```

Starting HBAnyware with Web Launch

After the HBAnyware Web Launch software has been installed and the Web Launch server has been initialized, you can launch the HBAnyware utility directly with your Web browser.

To launch the HBAnyware utility with your Web browser:

1. Open your Web browser.
2. Enter the URL of an HBAnyware.jnlp file. Make sure that the URL specifies a remote server which has the HBAnyware Web Launch software installed and running. For example:

```
http://138.239.20.30/hbanyware.jnlp
```

Note: If the browser window displays "Emulex Corporation HBAnyware Demo of HBAnyware WebStart web n.n.n.n ..." when attempting to start HBAnyware with Web Launch, refer to the "Troubleshooting" section on page 131.

Starting the HBAnyware Security Configurator

Prerequisites

- Make sure that all of the systems that are part of, or will be part of, the security configuration are online on the network so that they receive updates or changes made to the security configuration.
- Before running the security configurator out-of-band, you must set up the OOB hosts so they will be seen by the security configurator. For more information, see *Out-of-Band SAN Management* on page 77

Procedure

If this is the first time you are starting the configurator, see *Starting the Security Configurator for the First Time: Creating the First ACG, Designating the MSC and Selecting Systems in the FC Network* on page 82.

To start the HBAnyware Security Configurator for Solaris:

1. Login as or su to 'root'.
2. Run the script:

```
/usr/sbin/hbanyware/ssc
```

Starting the HBAnyware Utility from the Command Line

To launch the HBAnyware utility from the command line:

1. Type `/usr/sbin/hbanyware/hbanyware`. This starts the HBAnyware utility running in in-band access. You can also start the HBAnyware utility running in out-of-band access by adding an argument in the form “`h=<host>`”. The `<host>` argument may be either the IP address of the host or its system name. The call will use a default IP port of 23333, but you can override this by optionally appending a colon (:) and the IP port number.

Note: Remember that not all HBAs for a specific host may be running in-band. Therefore, running that host out-of-band may display HBAs that do not appear when the host is running in-band.

Examples of Modifications

- HBAnyware `h=138.239.82.2`
The HBAnyware utility will show HBAs in the host with the IP address 138.239.82.2.
- HBAnyware `h=Util01`
The HBAnyware utility will show HBAs in the host named Util01.
- HBAnyware `h=138.239.82.2:4295`
The HBAnyware utility will show HBAs in the host with the IP address 138.239.82.2 using IP Port 4295.
- HBAnyware `h=Util01:4295`
The HBAnyware utility will show HBAs in the host named Util01 using IP port 4295.

Run this modified command line to launch the HBAnyware utility for a single, remote host in local mode.

Changing Management Mode

During installation a management mode was selected, however you can change it if the “Allow users to change management mode from the utility” box was checked. HBAnyware enables you to choose from three types of host/HBA management.

To change HBAnyware management mode:

1. Run the `set_operating_mode` script:

```
/usr/sbin/hbanyware/set_operating_mode
```

The following appears:

```
1 Local Mode - HBAs on this Platform can be managed by HBAnyware clients on this Platform Only.
```

```
2 Managed Mode - HBAs on this Platform can be managed by local or remote HBAnyware clients.
```

```
3 Remote Mode - Same as "2" plus HBAnyware clients on this Platform can manage local and remote HBAs.
```

```
Enter the number '1', '2' or '3'.
```

2. Enter desired management mode.
3. Press **<Enter>**.
4. Click **OK**.

The HBAnyware Utility Window Element Definitions

The HBAnyware utility window contains five basic components: the menu bar, the toolbar, the discovery-tree, the property tabs and the status bar.

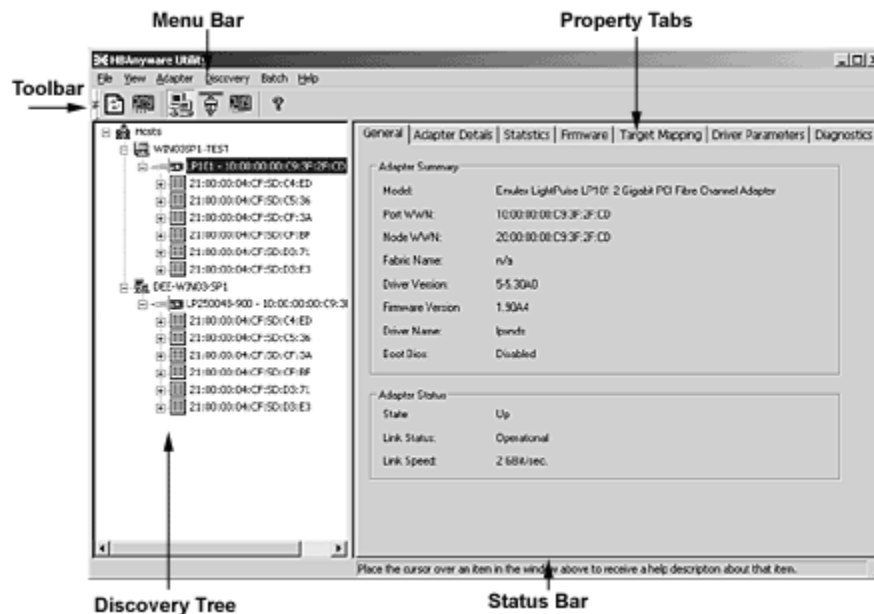


Figure 1: HBAnyware Utility Window with Element Call Outs

Note: The element you select in the discovery-tree determines whether a menu item or toolbar icon is active. For example, if you select the local host or other system host, the Reset Adapter item on the Adapter menu is unavailable. The Reset Adapter toolbar button is unavailable as well.

The Menu Bar

The menu bar contains command menus that enable you to perform a variety of tasks such as exiting the HBAnyware utility, resetting host bus adapters and sorting items in the discovery-tree view. Many of the menu bar commands are also available from the toolbar.

The Toolbar

The toolbar contains buttons that enable you to refresh the discovery-tree, reset the selected HBA and sort the discovery-tree. Many of the toolbar functions are also available from the menu bar.



Figure 2: The HBAnyware Toolbar

The toolbar is visible by default. Use the Toolbar item in the View menu to hide the toolbar. If the item is checked, the toolbar is visible.

The Toolbar Buttons

The toolbar buttons perform the following tasks:



Click the **Rediscover** button to refresh the discovery-tree display.



Click the **Reset** button to reset the selected HBA.

Sort Toolbar Buttons

You can sort discovered adapters by host name or fabric addresses. You can also choose to display only local or remote HBAs. See page 40 for details on sort buttons.



Sort by Host Name button (default)



Sort by Fabric ID button



Local HBAs Only button



Help button

The Discovery-Tree

The discovery-tree (left pane) has icons that represent discovered network (SAN) elements (local host name, system host names and all HBAs active on each host). Targets and LUNs, when present, are also displayed.

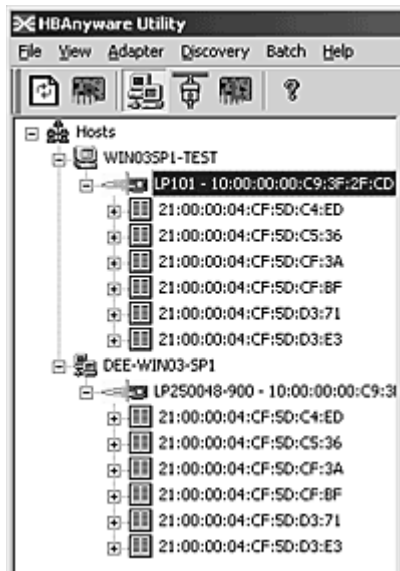


Figure 3: HBAAnyware Utility, Discovery-tree

Discovery-Tree Icons

Discover- tree icons represent the following:



This icon represents the local host.



This icon represents other hosts connected to the system.



A green HBA icon with black descriptive text represents an online HBA.

A red HBA icon with red descriptive text represents an offline or otherwise temporarily inaccessible HBA. Several situations could cause the HBA to be offline or inaccessible:

- The HBA on a local host is not connected to the network, but is still available for local access.
- The HBA on a local host is malfunctioning and is inaccessible to the local host as well as to the network.
- The HBA on a local host is busy performing a local download and is temporarily inaccessible to the local host as well as to the network.



The Target icon represents connections to individual storage devices.



The LUN icon represents connections to individual LUNs.

Property Tabs

The property tabs display configuration, statistical and status information for network elements. The set of available tabs is context-sensitive, depending on the type of network element or HBA currently selected in the discovery-tree.

Status Bar

As you navigate through the menu bar or the toolbar, help messages appear on the status bar near the bottom of the HBAnyware window.

The status bar is visible by default. Use the Status Bar item in the View menu to hide the status bar. If checked, the status bar is visible.

Using the HBAnyware Utility Command-Line Interface

The Command Line Interface (CLI) Client component of the HBAnyware utility provides access to the capabilities of the Remote Management library from a console command prompt. This component is intended for use in scripted operations from within shell scripts, batch files, or the specific platform equivalent.

Note: The HBAnyware utility can only discover and manage remote HBAs on hosts running the HBAnyware utility's elxhbmgr daemon.

Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

Using the CLI Client

The CLI Client is a console application named `hbacmd`. Each time you run this application from the command line, a single operation is performed.

The first parameter of this command is the requested operation. When the specified operation is completed, the command prompt is displayed. Most operations retrieve information about an entity on the SAN and display that information on the console.

Most of the CLI Client commands require one or more additional parameters that specify the nature of the command. A parameter used by many `hbacmd` commands specifies the World Wide Port Name (WWPN) of the HBA that is the target of the command. For example, the following command shows the port attributes for the HBA with the specified WWPN:

```
/usr/sbin/hbanyware/hbacmd portattrib 10:00:00:00:c9:20:20:20
```

`hbacmd` can be run in out-of-band mode by making the first argument `h=<host>`. For example:

```
/usr/sbin/hbanyware/hbacmd h=cp-hp5670 listhbas  
/usr/sbin/hbanyware/hbacmd h=138.239.91.121 listhbas
```

Syntax Rules

The syntax rules for the HBAnyware utility Command-Line Interface (`hbacmd`) are as follows:

- All commands and their arguments are NOT case sensitive.
- The requested operation must contain at least three characters, or as many as needed to distinguish it from any other operation.
- Whenever a WWPN is specified, individual fields are separated by colons (:) or spaces (). When using space separators, the entire WWPN must be enclosed in quotes ("").
- All `hbacmd` inputs must be in hexadecimal format. The only exceptions are the cycle-counts used in some of the diagnostic commands.

Out-of-Band Access

Out-of-band (OOB) access enables you to access HBAs via their IP-address or by the name of the host on which they reside. Since HBAs may exist on a host but not be a part of a FC network, they will not appear during normal in-band discovery. Thus, OOB access enlarges the number of HBAs that can be queried or modified.

Note: A local host cannot be accessed out-of-band.

OOB access via `hbacmd` uses an additional parameter on the command line. The parameter must be the first parameter in the list, coming immediately after `hbacmd`. The remaining parameters are those documented for each operation.

Note: You can also access an in-band HBA via its OOB address.

The format of the OOB parameter is:

```
h={<IPAddress> | <host-name>}
```

Some examples are:

```
h=128.239.91.88  
h=cp-compaq8000
```

The following lists all HBAs running on the host with a specified IP address:

```
hbacmd h=128.239.91.88 listHBAs
```

If you don't know the IP address, but you know the host name, type:

```
hbacmd h=cp-compaq8000 listHBAs
```

If the host is unreachable, the command will return an error.

CLI Client Command Reference

Version

Syntax: HBACMD Version

Description: Shows the current version of the HBAnyware CLI client application. To view the version, type:

```
hbacmd version
```

Sample response:

```
HBAnyware Command Line Interface: Version 3.0
```

Parameters: None.

ListHBAs

Syntax: HBACMD ListHBAs

Description: Shows a list of the discovered manageable Emulex HBAs and some of their attributes. The list will contain one 6-attribute group for each discovered HBA. Example of an attribute group list:

```
Manageable HBA List
Port WWN: 10:00:00:00:c9:20:08:cc
Node WWN: 20:00:00:00:c9:20:08:cc
Fabric Name:10:00:00:60:69:90:0b:f6
Flags: 0000f900
Host Name: CP-EMULEX-DECPC
Mfg: Emulex Corporation
```

Parameters: None.

SaveConfig

Syntax: HBACMD SaveConfig <wwpn> <filename> <ctrlword>

Description: Saves the contents of the driver parameter list to a file for the specified HBA. The ASCII file lists parameter definitions, delimited by a comma. Each definition is of the form:

```
<parameter-name>=<parameter-value>
```

Save either the values of the global set or those specific to the referenced HBA. The file created by this command stores itself in the Emulex Repository directory.

Example:

```
hbacmd SaveConfig elxstor-5-1.20A0.dpv 10:00:00:00:c9:2e:51:2e N
```

Sample response:

```
HBACMD_SaveConfig: Success writing driver parameters to file
C:\Program Files\HBAnyware\Emulex Repository\elxstor-5-1.20A.dpv
```

Parameters:

WWPN - The World Wide Port Name of the HBA. This HBA can be either local or remote.

filename - The file name that will contain the driver parameter list upon successful completion of this command.

ctrlword - G = save the global parameter set. N = save the local (HBA-specific) parameter set.

HBAAttrib

Syntax: HBACMD HBAAttrib <wwpn>

Description: Shows a list of all attributes for the HBA with the specified WWPN. To view attributes, type:

```
hbacmd hbaattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
HBA Attributes for 10:00:00:00:c9:4a:c5:90

Host Name       : localhost.localdomain
Manufacturer    : Emulex Corporation
Serial Number   : BG53059073
Model           : LP1150-F4
Model Desc      : Emulex LP1150-F4 4Gb 1port FC: PCI-X2 SFF HBA
Node WWN        : 20 00 00 00 c9 4a c5 90
Node Symname    : Emulex LP1150-F4 FV2.10A5 DV8.0.16.25
HW Version      : 1036406d
Opt ROM Version :
FW Version      : 2.10A5 (J2F2.10A5)
Vender Spec ID  : 10DF
Number of Ports : 1
Driver Name     : lpfc
Device ID       : F0D5
HBA Type        : LP1150-F4
Operational FW  : SLI-2 Overlay
SLI1 FW         : SLI-1 Overlay 2.10a5
SLI2 FW         : SLI-2 Overlay 2.10a5
IEEE Address    : 00 00 c9 4a c5 90
Boot BIOS       : Disabled
Driver Version  : 8.0.16.25; HBAAPI(I) v2.1.c, 02-02-06
Kernel Version  : 1.11a5
```

Parameters:

WWPN - The World Wide Port Name of the HBA. This HBA can be either local or remote.

PortAttrib

Syntax: HBACMD PortAttrib <wwpn>

Description: Shows a list of all attributes for the port with the specified WWPN. To view attributes, type:

```
hbacmd portattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

```
Port Attributes for 10:00:00:00:c9:4a:c5:90

Node WWN        : 20 00 00 00 c9 4a c5 90
Port WWN        : 10 00 00 00 c9 4a c5 90
Port Symname     :
Port FCID       : 11400
Port Type       : Fabric
Port State      : Operational
Port Service Type : 12
Port Supported FC4 : 00 00 01 20 00 00 00 01
                  : 00 00 00 00 00 00 00 00
                  : 00 00 00 00 00 00 00 00
                  : 00 00 00 00 00 00 00 00
Port Active FC4  : 00 00 01 00 00 00 00 01
                  : 00 00 00 00 00 00 00 00
                  : 00 00 00 00 00 00 00 00
                  : 00 00 00 00 00 00 00 00
Port Supported Speed: Unknown
Port Speed       : 2 GBit/sec.
Max Frame Size   : 2048
OS Device Name   : /sys/class/scsi_host/host10
Num Discovered Ports: 3
```


Fabric Name : 10 00 00 60 69 50 15 25

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

PortStat

Syntax: HBACMD PortStat <wwpn>

Description: Shows all port statistics for the HBA with the specified WWPN. To view port statistics for the HBA, type:

```
hbacmd portstat 10:00:00:00:c9:20:08:cc
```

Sample response:

Port Statistics for 10:00:00:00:c9:20:08:cc

Exchange Count	:	1496534
Responder Exchange Count	:	37505
TX Seq Count	:	1588007
RX Seq Count	:	1561255
TX Frame Count	:	1588695
RX Frame Count	:	1561892
TX Word Count	:	19821312
RX Word Count	:	66368000
TX KB Count	:	77427
RX KB Count	:	259250
LIP Count	:	1
NOS Count	:	n/a
Error Frame Count	:	0
Dumped Frame Count	:	n/a
Link Failure Count	:	0
Loss of Sync Count	:	9
Loss of Signal Count	:	0
Prim Seq Prot Err Count	:	0
Invalid TX Word Count	:	0
nvalid RX Frame CRC Cnt	:	0
Link Transition Count	:	0
Active RPI Count	:	0
Active XRI Count	:	0
Rx Port Busy Count	:	0
Rx Fabric Busy Count	:	0
Primary Sequence Timeout	:	0
Elastic Buffer Overrun	:	0
Arbitration Timeout	:	0

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

ServerAttrib

Syntax: HBACMD ServerAttrib <WWPN>

Description: Shows a list of attributes of the server running locally to the specified HBA. To view the server attributes for the HBA, type:

```
hbacmd serverattrib 10:00:00:00:c9:20:08:cc
```

Sample response:

Server Attributes for 10:00:00:00:c9:4a:c5:90

Host Name	:	localhost.localdomain
FW Resource Path	:	/usr/sbin/hbanyware/RMRepository/
DR Resource Path	:	/usr/sbin/hbanyware/RMRepository/
HBAnyware Server Version	:	3.0

Parameters:

WWPN - The World Wide Port Name of any HBA local to the designated server. The HBA itself can be either local or remote.

TargetMapping

Syntax: HBACMD TargetMapping <wwpn>

Description: Shows a list of mapped targets and the LUNs attached to each for the port with the specified WWPN. To view the target mapping for 10:00:00:00:c9:20:08:0c, type:

```
hbacmd targetmapping 10:00:00:00:c9:20:08:0c
```

Sample response:

Target Mapping for 10:00:00:00:c9:4a:c5:90

```
FCP ID          : 115E2
SCSI Bus Number: 0
SCSI Target Num: 0
Node WWN        : 50:00:60:E8:02:78:6E:03
Port WWN        : 50:00:60:E8:02:78:6E:03
Tgt Device Name: /dev/sdb
```

```
FCP LUN 00      : 0000 0000 0000 0000
SCSI OS Lun     : 0
Lun Device Name: /dev/sdb
Vendor ID       : HITACHI
Product ID      : OPEN-3
Product Version: 0118
SCSI Capacity   : 2347 MB
Block Size      : 512 Bytes
```

```
FCP LUN 01      : 0001 0000 0000 0000
SCSI OS Lun     : 1
Lun Device Name: /dev/sdb
Vendor ID       : HITACHI
Product ID      : OPEN-3
Product Version: 0118
SCSI Capacity   : 2347 MB
Block Size      : 512 Bytes
```

```
FCP LUN 02      : 0002 0000 0000 0000
SCSI OS Lun     : 2
Lun Device Name: /dev/sdb
Vendor ID       : HITACHI
Product ID      : OPEN-3
Product Version: 0118
SCSI Capacity   : 2347 MB
Block Size      : 512 Bytes
```

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

Reset

Syntax: HBACMD Reset <wwpn>

Description: Resets the HBA with the specified WWPN. Resetting an HBA may require several seconds to complete, especially for remote devices. This command will return for additional input only after the reset has finished. To reset an HBA whose WWPN is 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd reset 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Reset HBA 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - The World Wide Port Name of the port. This port can be either local or remote.

Download

Syntax: HBACMD Download <wwpn> <filename>

Description: Loads the specified firmware image to the HBA with the specified WWPN. To load the firmware image located in hdc190a4.dwc to an HBA with WWPN 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd download 10:00:00:00:c9:2e:51:2e hdc190a4.dwc
```

Sample response for a successful download:

```
Downloading hdc190a4.dwc to hba 10:00:00:00:c9:2e:51:2e
Download Complete.
```

Parameters:

WWPN - The World Wide Port Name of the HBA that is the target of the firmware download. This HBA can be either local or remote.

FileName - The file name of the firmware image you want to load. This can be any file accessible to the CLI client application.

AllNodeInfo

Syntax: HBACMD AllNodeInfo <wwpn>

Description: Shows target node information for each target accessible from the specified HBA. To view the target node data for 10:00:00:00:c9:20:0d:36, type:

```
Hbacmd allnodeinfo 10:00:00:00:c9:20:0d:36
```

Sample response:

```
All Node Info for 10:00:00:00:c9:4a:c5:90

Node Type      : EXIST
FCP ID         : 115E2
SCSI Bus Number: 0
SCSI Target Num: 0
Node WWN       : 50:00:60:E8:02:78:6E:03
Port WWN       : 50:00:60:E8:02:78:6E:03
OS Device Name : /sys/class/scsi_host/host10/device/target10:0:0
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose target node information you want to query. This HBA can be either local or remote.

DriverConfig

Syntax: HBACMD driverconfig <wwpn> elxconfig.dpv <ctrlword>

Description: Sets all driver parameters for the HBA specified by WWPN to the driver parameter values contained in the driver parameter file (elxconfig.dpv in the above example). These files can be easily generated via the HBAware Driver Parameter tab. Driver types must match between .dpv file type and host platform HBA.

For example, type:

```
hbacmd driverconfig 10:00:00:00:c9:2e:51:2e elxconfig G
```

Below is a sample response:

```
hbacmd: Success setting driver configuration parameters to values in .dpv file.
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to set driver parameters.

ctrlword - G = save the global parameter set.

DriverParams

Syntax: HBACMD DriverParams <wwpn>

Description: Shows the name and values of each driver parameter for the selected HBA. To view the driver parameters for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd driverparams 10:00:00:00:c9:2e:51:2e
```

Sample (abbreviated) response:

Driver Params for 10:00:00:00:c9:4a:c5:90. Values in HEX format.

DX	string	Low	High	Def	Cur	Exp	Dyn
00	log-verbose	0	ffff	0	20	1	1
01	lun-queue-depth	1	80	1e	1e	1	4
02	scan-down	0	1	1	1	1	4
03	nodev-tmo	0	ff	1e	3c	1	1
04	topology	0	6	0	0	1	4
05	link-speed	0	4	0	0	1	4
06	fcg-class	2	3	3	3	1	4
07	use-adisc	0	1	0	1	1	1
08	ack0	0	1	0	0	1	4
09	fcg-bind-method	1	4	2	2	1	4
0a	cr-delay	0	3f	0	0	1	4
0b	cr-count	1	ff	1	1	1	4
0c	fdmi-on	0	2	0	0	1	4
0d	discovery-threads	1	40	20	20	1	4
0e	max-luns	1	8000	100	100	1	4

Parameters:

WWPN - The World Wide Port Name of the HBA whose driver parameters you want to view. This HBA can be either local or remote.

DriverParamsGlobal

Syntax: HBACMD DriverParamsGlobal <wwpn>

Description: Shows the name and the global value of each driver parameter for the selected HBA. To view the global driver parameters for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd driverparamsglobal 10:00:00:00:c9:2e:51:2e
```

Sample (abbreviated) response:

Driver Params (Global) for 10:00:00:00:c9:2e:51:2e. Values in HEX.

DX	string	Low	High	Def	Cur	Exp	Dyn
00	AbortStatus	0	ff	e	e	1	1
01	ARBTOV	1f4	4e20	5dc	5dc	1	5
02	BlinkTimeOut	1	1E	8	8	1	0
03	Class	1	2	2	2	1	1

04	CrflIntrpt	0	1	0	0	1	5
05	CrfMsCnt	0	3f	0	0	1	5
06	CrfRspCnt	0	ff	0	0	1	5
07	DebugMask	0	efffffff	0	0	0	5
08	DisableAck0	0	1	0	0	1	5
09	DiscMethod	0	1	1	0	1	1
0a	DiscoveryDelay	0	7	0	0	1	1
0b	ElsRetryCount	1	ff	1	1	1	1
0c	ElsRjtCount	0	ff	2d	2d	1	1
0d	ElsTimeOut	0	1	0	0	1	1
0e	EmulexOption	0	7ffffff	d200	da00	1	0
0f	EnableDPC	0	1	0	1	1	1
10	ErrRetryMax	0	fffffffe	1	1	1	1
11	FrameSizeMSB	0	8	0	0	1	5
12	HardAddress	0	1	0	0	1	0
13	HlinkTimeOut	0	ff	1e	1e	1	1
14	InitialDelay	0	1	1	1	1	0
15	LinkSpeed	0	10	0	0	1	1
16	LinkTimeOut		1f4	3c	3c	1	1
17	LipFFrecovery	0	1	0	0	1	1
18	LogErrors	0	1	0	0	1	1
19	MapNodeName	0	1	0	0	1	0
1a	NodeTimeOut	0	ff	14	14	1	1
1b	QueueAction	0	2	0	0	1	1
1c	QueueDepth	1	ff	20	20	1	1
1d	QueueTarget	0	1	0	0	1	5
1e	QueueIncStep	0	100	2	2	1	1
1f	RegFcpType	0	1	1	1	1	1
20	ResetFF	0	1	0	0	1	1
21	ResetTPRLO	0	2	0	0	1	1
22	RetryNodePurge	0	1	1	1	1	1
23	RTTOV	a	ff	64	64	1	5

Parameters:

WWPN - The World Wide Port Name of the HBA whose driver parameters you want to view. This HBA can be either local or remote.

SetDriverParam

Note: This command may only be used with the `lpfc_log_verbose`, `lpfc_use_adisc` and `lpfc_nodev_tmo` parameters.

Syntax: HBACMD SetDriverParam <wwpn> <ctrlword> <param> <value>

Description: Changes the value of the specified driver parameter that is operating the referenced HBA, and designates the scope of that change. For example, to change the value of the `log_verbose` parameter for 10:00:00:00:c9:2e:51:2e and make it global, type:

```
hbacmd SetDriverParam 10:00:00:00:c9:2e:51:2e g log_verbose 3
```

Sample response:

```
Set Driver Parameter log_verbose=3(g) for 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose Boot BIOS you want to modify. This HBA can be either local or remote.

ctrlword - G = make change global, B = make change both permanent and global, N = make change neither permanent nor global

param - The name of the parameter whose value you want to modify. You can only use the log_verbose, use_adisc and _nodev_tmo parameters. Do not precede these commands with lpfc_. For example use log_verbose not lpfc_log_verbose.

Value - The new value you want to assign to the parameter.

SetBootBios

Syntax: HBACMD SetBootBios <wwpn> <ctrlword>

Description: Enables or disables the Boot BIOS on the referenced HBA. To enable the Boot BIOS for 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd setbootbios 10:00:00:00:c9:2e:51:2e E
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose Boot BIOS you want to modify. This HBA can be either local or remote.

ctrlword - E = enable the Boot BIOS, D = disable the Boot BIOS.

PciData

Syntax: HBACMD PciData <wwpn>

Description: Shows PCI configuration data for the HBA specified by the WWPN. To show PCI configuration data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd pcidata 10:00:00:00:c9:2e:51:2e
```

Sample response:

Vendor ID:	0x10DF	Device ID:	0xF0D5
Command:	0x0157	Status:	0x0230
Revision ID:	0x01	Prog If:	0x00
Subclass:	0x04	Base Class:	0x0C
Cache Line Size:	0x20	Latency Timer:	0xF8
Header Type:	0x00	Built In Self Test:	0x00
Base Address 0:	0xE0001004	Base Address 1:	0x00000000
Base Address 2:	0xE0000004	Base Address 3:	0x00000000
Base Address 4:	0x0000C001	Base Address 5:	0x00000000
CIS:	0x00000000	SubVendor ID:	0x10DF
SubSystem ID:	0xF0D5	ROM Base Address:	0x00000000
Interrupt Line:	0xFF	Interrupt Pin:	0x01
Minimum Grant:	0xFF	Maximum Latency:	0x00
Capabilities Ptr:	0x5C		

Parameters:

WWPN - The World Wide Port Name of the HBA whose PCI configuration data you want to show.

Wakeup

Syntax: HBACMD wakeup <wwpn>

Description: Shows wakeup parameter data for the HBA specified by the WWPN. To show wakeup parameter data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd wakeup 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Wakeup Parameters:
Initial Load:      0x02C03992      0x00103411
Flags:             0x00000000
Boot BIOS          0x03433290      0x00101303
SLI-1:             0x06433992      0x00103411
SLI-2:             0x07433992      0x00103411
Has Expansion ROM   0
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose wakeup parameter data you want to show.

LoopMap

Syntax: HBACMD loopmap <wwpn>

Description: Shows the arbitrated loop map data for the HBA specified by the WWPN. To show the arbitrated loop map data for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd loopmap 10:00:00:00:c9:2e:51:2e
```

Below is a sample response:

```
AL_PA:
01 Local Adapter
E8 SCSI Device
E4 SCSI Device
CA SCSI Device
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose loopmap you want to show.

GetBeacon

Syntax: HBACMD getbeacon <wwpn>

Description: Shows the current beacon status for the HBA specified by the WWPN. To show the current beacon status for HBA 10:00:00:00:c9:2e:51:2e, type:

For example, type:

```
hbacmd getbeacon 10:00:00:00:c9:2e:51:2e
```

Possible responses are:

```
Beacon State = On
Beacon State = Off
Unable to get Beacon state, error 1
Beaconing not supported on host or adapter
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose beacon status you want to show.

SetBeacon

Syntax: HBACMD setbeacon <wwpn> <state>

Description: Sets the current beacon status for the HBA specified by the WWP. To set the current beacon status for HBA 10:00:00:00:c9:2e:51:2e to off, type:

```
hbacmd setbeacon 10:00:00:00:c9:2e:51:2e 0
```

To set the current beacon status for HBA 10:00:00:00:c9:2e:51:2e to on, type:

```
hbacmd setbeacon 10:00:00:00:c9:2e:51:2e 1
```

Possible responses are:

```
Beacon State successfully set to On
Beacons State successfully set to Off
Unable to get Beacon state, error 1
Beaconing not supported on host or adapter
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose beacon status you want to set. This HBA can be either local or remote.

State - The new state of the beacon: 0 = beacon OFF, 1= beacon ON

PostTest

Syntax: HBACMD posttest <wwpn>

Description: Runs the POST test on the HBA specified by the WWP. Support for remote HBA is out-of-band (Ethernet) only. To run the POST test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd posttest 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
Running POST, polling for results.....
Power On Self Test Succeeded;time to execute = 8928 ms
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to run the POST test.

EchoTest

Syntax: HBACMD echotest <wwpn1> <wwpn2> <count> <StopOnError>

Description: Runs the echo test on the HBAs specified by the WWP1 and WWP2.

Note: Support for remote HBA is out-of-band (Ethernet) only. The EchoTest command will fail if the target WWP does not support the ECHO ELS command.

To run the echo test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd echotest 10:00:00:00:c9:2e:51:2e
10:00:00:00:c9:2e:51:45 10 1
```

Sample response:

```
Echo test: polling for results.....
Echo test succeeded; time to execute = 53 ms.
```

Parameters:

WWPN1 - The World Wide Port Name of the originating HBA.

WWPN2 - The World Wide Port Name of the destination (echoing) HBA.

Count - The number of times to run the test.

StopOnError - Should the test be halted on Error? 0 = no halt, 1 = halt

Loopback

Syntax: HBACMD loopback <wwpn> <type> <count> <StopOnError>

Description: Runs the loop test on the HBA specified by the WWPN.

Note: Only external Loopback tests must be run out-of-band.

To run the loop test for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd loopback 10:00:00:00:c9:2e:51:2e 1 10 0
```

Sample response:

```
Running Loopback: polling for results.....  
Loopback Test Failed; xmit errors = 3; rcv errors = 2; time to execute = 1015 ms.
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to run the loopback test(s).

Type -Type of loopback test where: 0 = PCI LoopBack Test, 1 = Internal LoopBack Test, 2 = External LoopBack Test

Count - The number of times to run the test (Range = 1,...10000)

StopOnError - Should the test be halted on Error? 0 = no halt, 1 = halt

Dump

Syntax: HBACMD dump <wwpn>

Description: Runs the dump diagnostic retrieval command on the HBA specified by the WWPN. This command is supported for local HBAs only. The file by default is located in:
/usr/sbin/hbanyware/Dump

To run the dump diagnostic retrieval command for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd dump 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - The World Wide Port Name of the HBA on which to you want to run the dump.

DeleteDumpFiles

Syntax: HBACMD deletedumpfiles <wwpn>

Description: Deletes all dump files associated with the HBA specified by the WWPN. To delete all dump files for HBA 10:00:00:00:c9:2e:51:2e, type:

```
hbacmd deletedumpfiles 10:00:00:00:c9:2e:51:2e
```

Sample response:

```
HBACMD: Dump file deletion complete.
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose dump files you want to delete.

PersistentBinding

Syntax: HBACMD PersistentBinding <wwpn> <source>

Description: Queries the presence of any persistent binding that may exist for the specified WWPN. The <source> is used to query either the configured or live state of any binding that may be present. To view the configured persistent binding for an adapter whose WWPN is 10:00:00:00:c9:20:0d:36, enter:

```
hbacmd persistentbinding 10:00:00:00:c9:20:0d:36 C
```

Sample response:

```
Persistent Binding for 10:00:00:00:c9:20:0d:36
Bind Type      : WWPN
FCP ID         : 10101SCSI
Bus Number: 0SCSI
Target Num: 0Node
WWN            : 20:00:00:D0:B2:00:30:40
Port WWN       : 20:00:00:D0:B2:00:30:40
OS Device Name : \\.\Scsi:4:0
```

```
Bind Type      : WWPN
FCP ID         : 10FEFSCSI
Bus Number: 0SCSI
Target Num: 1Node
WWN            : 50:06:04:8A:CC:C8:99:00
Port WWN       : 50:06:04:8A:CC:C8:99:00
OS Device Name : \\.\Scsi:4:1
```

If the binding does not exist, only the first line is returned.

Parameters:

WWPN - The World Wide Port Name of the HBA whose dump files you want to delete.

source - C if the configured state is being queried. L if the live state is being queried.

SetPersistentBinding

Syntax: HBACMD SetPersistentBinding <wwpn> <scope> <bindtype> <ID> \
<scsibus> <scsitarget>

Description: Sets a persistent binding between a Fibre Channel target and a Scsi bus and target. The binding can be to a target WWPN, target WWNN, or target D_ID. To bind permanently, on behalf of HBA 10:00:00:00:c9:2e:51:2e, target WWPN 20:00:00:d0:b2:00:30:40 to Scsi bus 1, target 3, enter:

```
hbacmd setpersistentbinding 10:00:00:00:c9:2e:51:2e P P \<br>20:00:00:d0:b2:00:30:40 1 3
```

To bind immediately, on behalf of HBA 10:00:00:00:c9:2e:51:2e, target D_ID 10101 to Scsi bus 1, target 3, enter:

```
hbacmd setpersistentbinding 10:00:00:00:c9:2e:51:2e I D \<br>10101 1 3
```

If there are no errors, a response to the last example would be:

```
Set Persistent Binding for 10:00:00:00:c9:2e:51:2e I D \<br>10101 1 3
```

Parameters:

WWPN - The World Wide Port Name of the HBA for which a persistent binding is to be set. This HBA can be either local or remote.

scope - P = binding is permanent (survives across reboot). I = binding is immediate. B = binding is both permanent and immediate.

bindtype - P = enable binding by WWPN. N = enable binding by WWNN. D = enable binding by D_ID.

ID - Target WWPN if bindtype = P. Target WWNN if bindtype = N. Target D_ID if bindtype = D

scsibus - Bus number of SCSI device.

scsitarget - Target number of SCSI device.

RemoveAllPersistentBinding

Syntax: HBACMD RemoveAllPersistentBinding <wwpn>

Description: Removes all persisting bindings associated with the referenced HBA. To remove all persistent bindings for 10:00:00:00:c9:21:5e:21, enter:

```
hbacmd removeallpersistentbinding 10:00:00:00:c9:21:5e:21
```

A sample response would be:

```
Remove All Persistent Binding for 10:00:00:00:c9:2e:51:2e
```

Parameters:

WWPN - The World Wide Port Name of the HBA for which all persistent bindings are to be removed. This HBA can be either local or remote.

RemovePersistentBinding

Syntax: HBACMD RemovePersistentBinding <wwpn> <bindtype> <ID> \
<scsibus> <scsitarget>

Description: Removes a persistent binding between a Fibre Channel target and a SCSI bus and target. The binding to be removed can be to a target WWPN, target WWNN, or target D_ID. To remove, on behalf of HBA 10:00:00:00:c9:2e:51:2e, the binding between target WWPN=20:00:00:d0:b2:00:30:40 and SCSI bus 1, target 3, enter:

```
hbacmd removepersistentbinding 10:00:00:00:c9:2e:51:2e P \  
20:00:00:d0:b2:00:30:40 1 3
```

To remove, on behalf of HBA 10:00:00:00:c9:2e:51:2e, the binding between target D_ID=10101 and SCSI bus 1, target 3, enter:

```
hbacmd removepersistentbinding 10:00:00:00:c9:2e:51:2e D \  
10101 1 3
```

If there are no errors a response to the last example would be:

```
Remove Persistent Binding for 10:00:00:00:c9:2e:51:2e D \  
10101 1 3
```

Parameters:

WWPN - The World Wide Port Name of the HBA for which a persistent binding is to be removed. This HBA can be either local or remote.

bindtype - P = enable binding by WWPN. N = enable binding by WWNN. D = enable binding by D_ID.

ID - Target WWPN if bindtype = P. Target WWNN if bindtype = N. Target D_ID if bindtype = D.

scsibus - Bus number of SCSI device.

scsitarget - Target number of SCSI device.

BindingCapabilities

Syntax: HBACMD BindingCapabilities <wwpn>

Description: Displays the binding capabilities present at the referenced HBA. To view the binding capabilities at 10:00:00:00:c9:21:5e:21, enter:

```
hbacmd bindingcapabilities 10:00:00:00:c9:21:5e:21
```

Sample response:

```
Binding Capability for 10:00:00:00:c9:2e:51:2e
Can bind to D_IDCan bind to WWP
Can bind to WWNN
Can bind AUTOMAP
Can bind CONFIGURED
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose binding capabilities are being queried. This HBA can be either local or remote.

BindingSupport

Syntax: HBACMD BindingSupport <wwpn> <source>

Description: Displays the binding support available at the reference HBA. To view the configured binding support for 10:00:00:00:c9:21:5e:21, enter:

```
hbacmd bindingsupport 10:00:00:00:c9:21:5e:21 C
```

Sample response:

```
Binding Support for 10:00:00:00:c9:2e:51:2e
Can bind to WWP
Can bind AUTOMAP
```

Parameters:

WWPN - The World Wide Port Name of the HBA whose binding support is being queried. This HBA can be either local or remote.

source - C if the configured support is being queried. L if the live support is being queried.

SetBindingSupport

Syntax: HBACMD SetBindingSupport <wwpn> <bindflag>

Description: Sets the binding support(s) for the reference HBA. To enable binding support for WWP and Automap on HBA 10:00:00:00:c9:21:5e:21, enter:

```
hbacmd setbindingsupport 10:00:00:00:c9:21:5e:21 P1
```

Sample response:

```
Set Binding Support for 10:00:00:00:c9:21:5e:21 P1
```

Parameters:

WWPN - The World Wide Port Name of the HBA for which binding support is being set. This HBA can be either local or remote.

bindflag - 1 = enable support for Automap binding. 0 = disable support for Automap binding. P1 = enable support for WWP binding and Automap. N1 = enable support for WWNN binding and Automap. D1 = enable support for D_ID binding and Automap. P0 = enable support for P, disable Automap. N0 = enable support for N, disable Automap. D0 = enable support for D, disable Automap.

Discovering HBAs

Local and remote HBAs are discovered automatically when you launch the HBAnyware utility. Initially, both local and remote HBAs are displayed.

You can also discover HBAs on out-of-band (OOB) hosts. For more information, see *Out-of-Band Access* on page 23.

Note: The HBAnyware utility must be installed and the elxhbamgr process(es) must be running on all remote hosts that you want to discover and manage.

Remote in-band capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts you want to discover and manage using the HBAnyware utility must be in the same zone or discovered and managed out-of-band through an Ethernet connection.

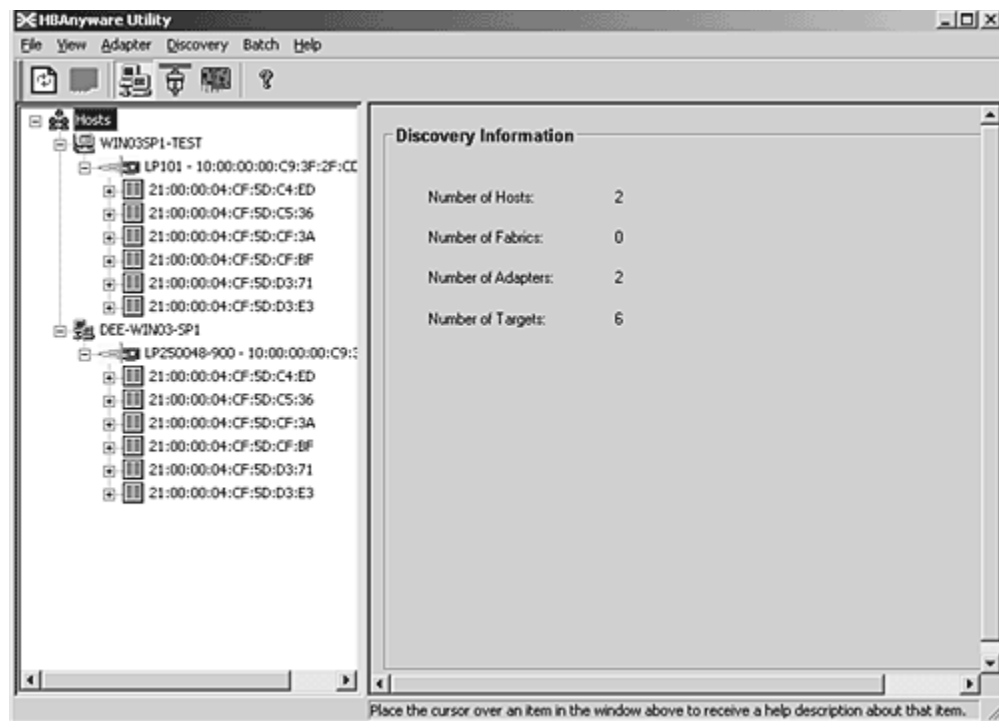


Figure 4: HBAnyware Utility, Discovery Information

Note: Emulex recommends setting the monitor display resolution to 1024x768 as a minimum to properly view the HBAnyware utility.

Configuring Discovery Settings

Use the HBAnyware Discovery Settings dialog box to configure several discovery server parameters. You can define when to start the discovery server, when to refresh in-band and out-of-band discoveries and when to remove previously discovered HBAs that are no longer being discovered.

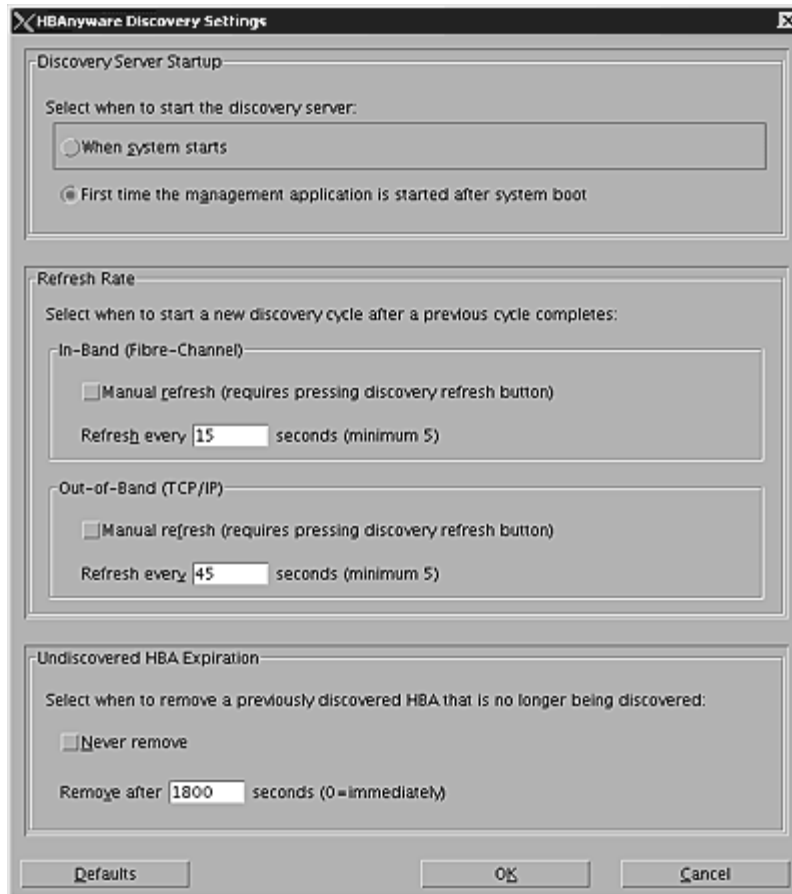


Figure 5: HBAnyware Utility, HBA Discovery Settings Dialog Box

To configure discovery settings:

1. Start the HBAnyware utility.
2. From the menu bar, select Discovery/Modify Settings. The Discovery Settings dialog box appears.
3. Define the discovery properties you wish and click **OK**. Click **Defaults** to return the discovery properties to their default settings.

Sorting HBAs

Sort discovered HBAs by host name, fabric name, HBA name, target name and LUN number. You can also choose to view local HBAs or remote HBAs. By default, both local and remote HBAs are sorted by host name/fabric name.

To sort HBAs:

1. Start the HBAnyware utility.
2. Switch between host name or fabric ID in one of two ways:
 - From the menu bar: click **View**, then click **Sort by Host Name** or **Sort by Fabric ID**. The current adapter display mode is checked.
 - From the toolbar, click one of the following buttons:

Sort HBAs by Host Name (default).



Sort HBAs by Fabric ID.



3. The HBAnyware utility sorts in ascending order. The sort recognizes letters, numbers, spaces and punctuation marks.

Sorting by Host Name

- Initially sorts by host name. You cannot change host names using the HBAnyware utility; names must be changed locally on that system.
- Within each host system, sorts by HBA model.
- If multiple HBAs have the same model number, sorts models by World Wide Node Name (WWNN).
- If targets are present, sorts by World Wide Port Name (WWPN). Multiple HBAs may refer to the same target.
- If LUNs are present, sorts by LUN number.


Sorting by Fabric Address

- Initially sorts by fabric ID.
- Within each fabric ID, sorts by HBA model.
- If multiple HBAs have the same model number, sorts models by WWNN.
- If targets are present, sorts by WWPN. Multiple HBAs may refer to the same target.
- If LUNs are present, sorts by LUN number.
- If the fabric ID is all zeros, no fabric is attached.

Sorting Local HBAs Only

Displays local HBA's only. Works in conjunction with the Sort by Host Name and Sort by Fabric ID buttons.

To display local HBAs only, do one of the following:

- From the menu bar: click **View**, then click **Local HBAs Only**. The current adapter display mode is checked.
- From the toolbar, click the **Local HBAs Only**  button.

Viewing HBA Information

Viewing Discovery Information

The Discovery Information area contains a general summary of the discovered elements. The Host or Fabric icon, depending upon which view you select, is the root of the discovery-tree, but it does not represent a specific network element. Expanding it will reveal all hosts, LUNs, targets and HBAs that are visible on the storage area network (SAN).

To view the discovery information:

1. Start the HBAnyware utility.
2. Click the **Host** or **Fabric** icon at the root of the discovery-tree. Discovered SAN elements appear in the discovery-tree. Select an element from the discovery-tree to learn more about it.

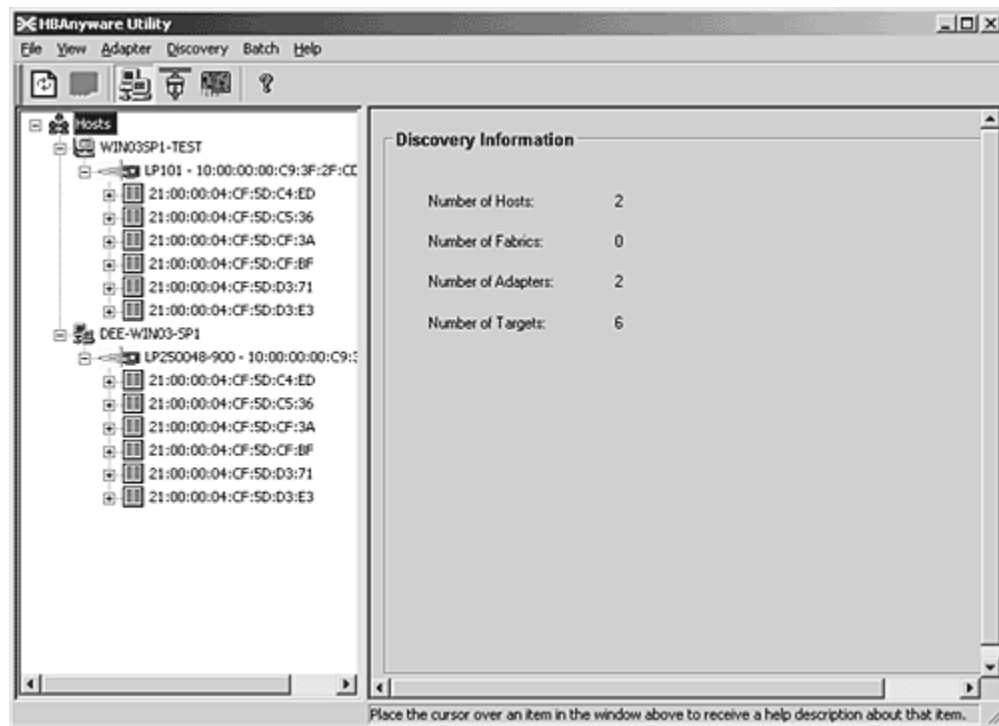


Figure 6: HBAnyware Utility, Discovery Information


Discovery Information Field Definitions

- Number of Hosts - The total number of discovered host computers. This includes servers, workstations, personal computers, multiprocessors and clustered computer complexes.
- Number of Fabrics - The total number of discovered fabrics.
- Number of Adapters - The total number of discovered HBAs.
- Number of Targets - The total number of unique discovered targets on the SAN. In the discovery-tree, the same target can appear under more than one HBA.

Viewing Host Information

There are two tabs that show host information: the Host Information tab and the host Driver Parameters tab. The Host Information tab is read-only. The host Driver Parameters tab enables you to view and define HBA driver settings for a specific host.

To view the Host Information and Driver Parameters tabs:

1. Start the HBAnyware utility.
2. Do one of the following:
 - From the menu bar, click **View**, then click **Sort by Host Name**.
 - From the toolbar, click the **Sort by Host Name**  button.
3. Select a host in the discovery-tree.
4. Select the Host Information tab (see Figure 7) or the Host Driver Parameters tab (Figure 8).

The Host Information Tab

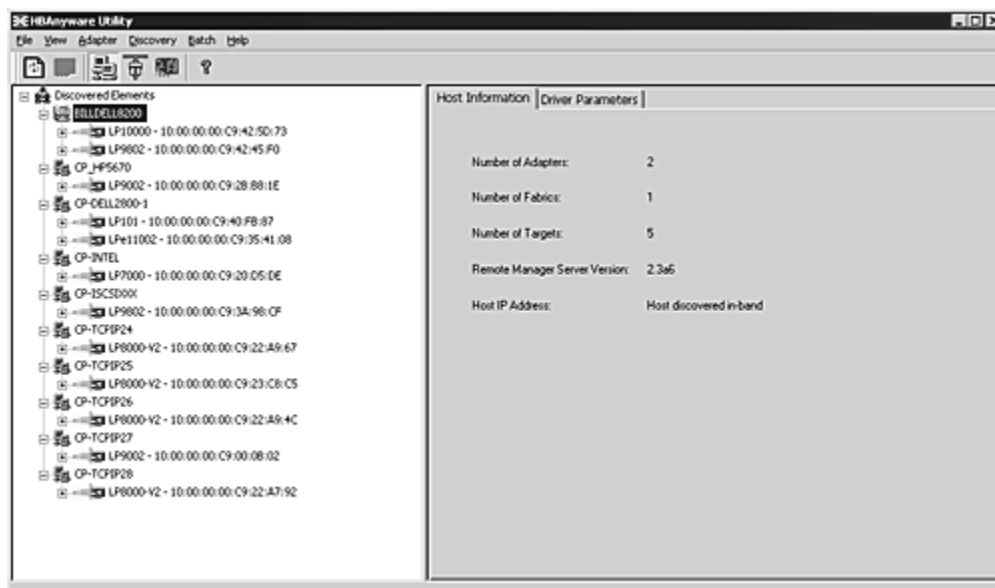


Figure 7: HBAnyware Utility, Host Information Tab

Host Information Field Definitions

- Number of Adapters - The number of HBAs installed in the host.
- Number of Fabrics - The number of fabrics to which this host is attached.
- Number of Targets - The number of storage devices seen by the host.
- Remote Manager Server Version - The version of the HBAnyware utility server that is running on the host. If different versions of the HBAnyware utility are installed on different hosts in the SAN, those differences appear in this field.
- Host IP Address - If the host is discovered in-band, the dialog box displays "Host discovered in-band." If the host is discovered out-of-band, the dialog box displays the host's IP address, e.g., 138.239.82.131.

The Host Driver Parameters Tab

The Host Driver Parameters tab (Figure 8) enables you to view and edit the HBA driver settings contained in a specific host. The host driver parameters are global values and apply to all HBAs in that host unless they are overridden by parameters assigned to a specific HBA using the HBA Driver Parameters tab. For each parameter, the tab shows the current value, the range of acceptable values, the default value, and whether the parameter is dynamic (a dynamic parameter allows the change to take effect without resetting the HBA or rebooting the system).

For more information on changing the parameters for a single HBA, see *Setting Driver Parameters for an HBA* on page 61. For more information changing the parameters for the host, see *Setting Driver Parameters for a Host* on page 62.

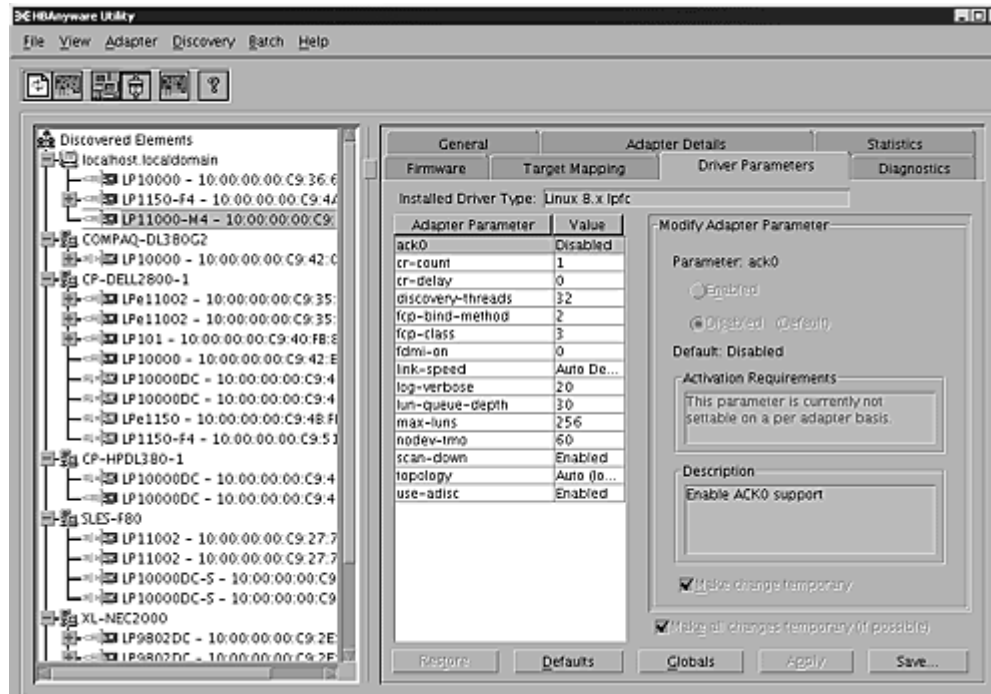


Figure 8: HBAnyware Utility, Driver Parameters Tab - Host Selected

Note: If there is more than one driver type installed, the Installed Driver Types menu shows a list of all driver types and driver versions that are installed on the HBAs in the host.

Driver Parameter Tab Field Definitions

- **Installed Driver Type** - The current driver and version installed.
- **Adapter Parameter table** - A list of HBA driver parameters and their current values.
- **Parameter-specific information** - The details about the parameter appears on the right side of the tab.

Driver Parameter Tab Buttons

- **Restore** - Click to save and restore parameters to this last saved value, if you have made changes to parameters and have not saved them by clicking **Apply**.
- **Defaults** - Click to reset all parameter values to their default (out-of-box) values.
- **Apply** - Click to apply any driver parameter changes. If you changed a parameter that is not dynamic, you must unload the driver and reload it.

Viewing General HBA Attributes

The General tab contains general attributes associated with the selected HBA.

To view general attributes:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Click an HBA in the discovery-tree.

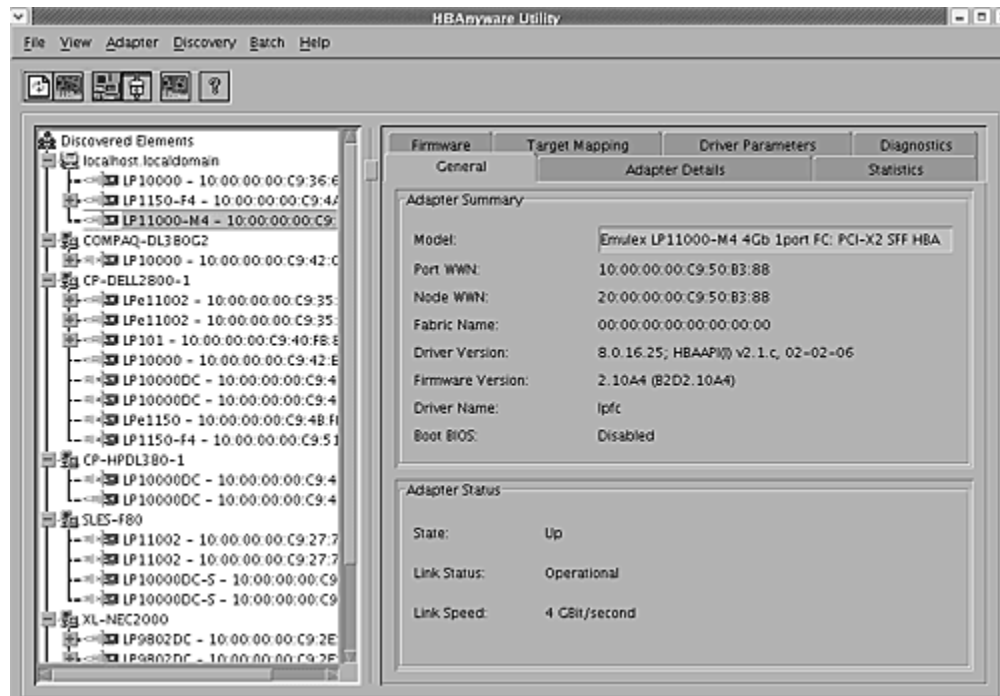


Figure 9: HBAnyware Utility, General Tab

Adapter Summary Field Definitions

- Model - The complete model name of the HBA.
- Port WWN - The Port World Wide Name of the HBA.
- Node WWN - the Node World Wide Name of the selected HBA.
- Fabric Name or Host Name - The Fabric Name field shows if you selected, "Sort by Host Name". The fabric name is a 64-bit worldwide unique identifier assigned to the fabric. The Host Name field shows if you selected "Sort by Fabric ID". The host name is the name of the host containing the HBA.
- Driver Version - The version of the driver installed for the HBA.
- Firmware Version - The version of Emulex firmware currently active on the HBA.
- Driver Name - The executable file image name for the driver as it appears in the Emulex driver download package.
- Boot Bios - Indicates if the boot code is enabled or disabled.

Adapter Status Area Field Definitions

State - The current operational state of the HBA: “Up” or “Down”.

Link Status - The current link status between the HBA and the fabric. There are several possible states:

- The “Operational” state indicates that the HBA is connected to the network and operating normally.
- All other states indicate that the HBA is not connected to the network. Green HBA icons with red descriptive text indicate that the HBA is offline. These offline states are:
 - “User offline” - The HBA is down or not connected to the network.
 - “Bypassed” - the HBA is in Fibre Channel discovery mode.
 - “Diagnostic Mode” - The HBA is controlled by a diagnostic program.
 - “Link Down” - There is no access to the network.
 - “Port Error” - The HBA is in an unknown state; try resetting it.
 - “Loopback” -an FC-1 mode in which information passed to the FC-1 transmitter is shunted directly to the FC-1 Receiver. When a FC interface is in loopback mode, the loopback signal overrides any external signal detected by the receiver.
 - “Unknown” -The HBA is offline for an unknown reason.
- Link Speed - The link speed of the HBA in gigabits per second.

Viewing Detailed HBA Information

The Adapter Details tab in the HBAnyware utility contains detailed information associated with the selected HBA.

To view the detailed attributes:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Select an HBA in the discovery-tree.
4. Select the Adapter Details tab.

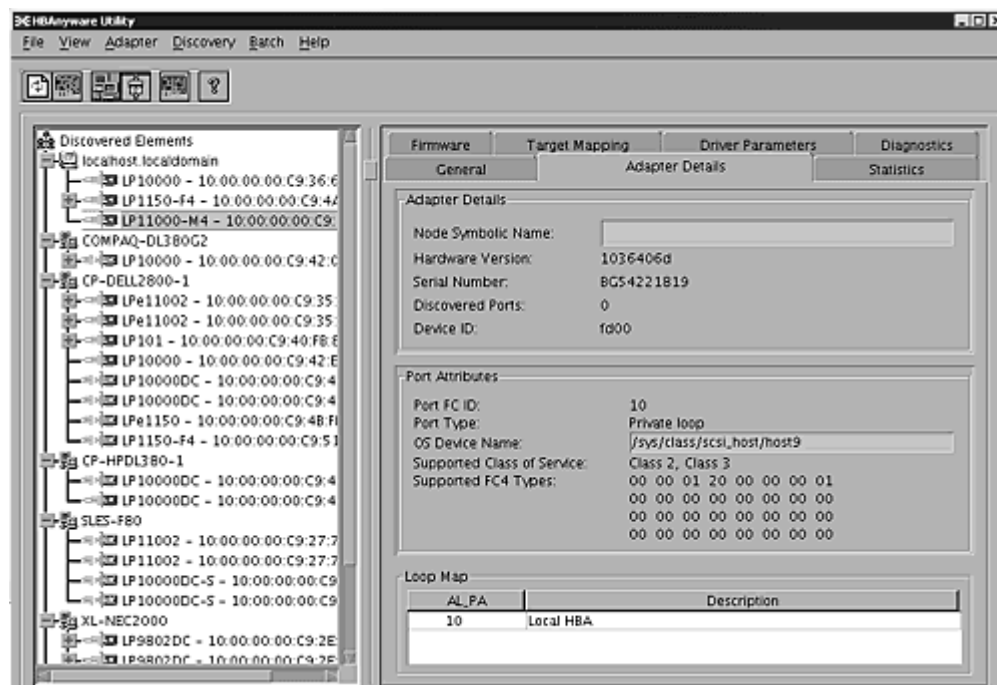


Figure 10: HBAnyware Utility, Adapter Details Tab

Adapter Details Field Definitions

- Node Symbolic Name - The Fibre Channel name used to register the driver with the name server.
- Hardware Version - The JEDEC ID board version of the selected HBA.
- Serial Number - The manufacturer assigned serial number of the selected HBA.
- Discovered Ports - The number of other HBAs visible to the selected HBA.
- Device ID - The HBA's default device ID.

Port Attributes Field Definitions

- Port FC ID - The Fibre Channel ID for the port of the selected HBA.
- Port Type - The current operational mode of the selected HBA's port.
- OS Device Name - The platform-specific name by which the selected HBA is known to the operating system.
- Supported Class of Service - A frame delivery scheme exhibiting a set of delivery characteristics and attributes. There are three classes of service.

- Class-1 provides a dedicated connection between a pair of ports confirmed with delivery or notification of nondelivery.
- Class-2 provides a frame switched service with confirmed delivery or notification of non-delivery.
- Class-3 provides a frame switched service similar to Class-2 but without notification of frame delivery or non-delivery.
- Supported FC4 Types - a 256-bit (8-word) map of the FC-4 protocol types supported by the port containing the selected HBA.

Loop Map Table Definitions

- The loop map shows the different ports present in the loop, and is present only if the port (HBA) is operating in loop mode. The simplest example would be to connect a JBOD directly to an HBA. When this is done, the port type will be a private loop, and the loop map will have an entry for the HBA, and one entry for each of the disks in the JBOD.

Viewing Fabric Information

The Discovery Information area contains information about the selected fabric.

To view the fabric information:

1. Start the HBAnyware utility.
2. Do one of the following:
 - From the menu bar, click **View**, then click **Sort by Fabric ID**.
 - From the toolbar, click the **Sort by Fabric ID**  button.
3. Click on a fabric address in the discovery-tree. The Discovery Information tab shows information about the selected fabric.

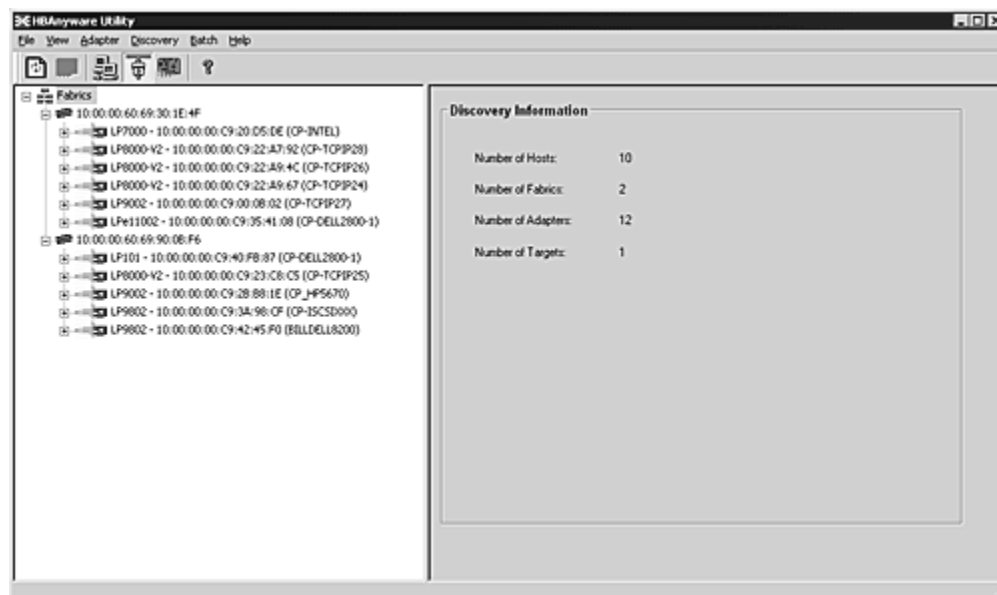


Figure 11: HBAnyware Utility, Discovery Information


Discovery Information Field Definitions

- Number of Hosts - The number of hosts discovered or seen by this host on the selected fabric.
- Number of Fabrics - The number fabrics identified during discovery.
- Number of Adapters - The number of HBAs discovered by this host on the selected fabric.
- Number of Targets - The number of storage devices seen by this host on the selected fabric.

Viewing Target Information

The Target Information area contains information specific to the selected storage device.

To view target information:

1. Start the HBAnyware utility.
2. Do one of the following:
 - From the menu bar, click **View**, then click **Sort by Host Name**.
 - From the toolbar, click the **Sort by Host Name**  button.
3. Click a target in the discovery-tree. The Target Information tab appears.

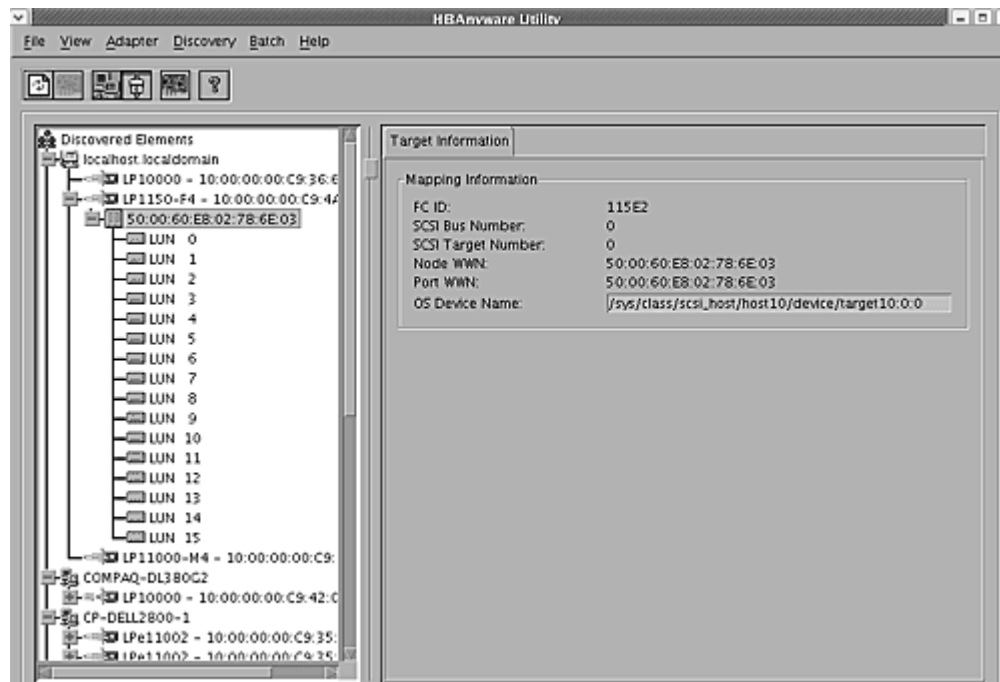


Figure 12: HBAnyware Utility, Target Information

Target Information Field Definitions


- Mapping Information Area
 - FC ID - The Fibre Channel ID for the target; assigned automatically in the firmware.
 - SCSI Bus Number - Defines the SCSI bus to which the target is mapped.
 - SCSI Target Number - The target's identifier on the SCSI bus.

- Node WWN - A unique 64-bit number, in hexadecimal, for the target (N_PORT or NL_PORT).
- Port WWN - A unique 64-bit number, in hexadecimal, for the fabric (F_PORT or FL_PORT).
- OS Device Name - The operating system device name.

Viewing LUN Information

The LUN Information area contains information about the selected logical unit number (LUN).

To view the LUN information:

1. Start the HBAnyware utility.
2. Do one of the following:
 - From the menu bar, click **View**, then click **Sort by Host Name**.
 - From the toolbar, click the **Sort by Host Name**  button.
3. Click on a LUN in the discovery-tree.

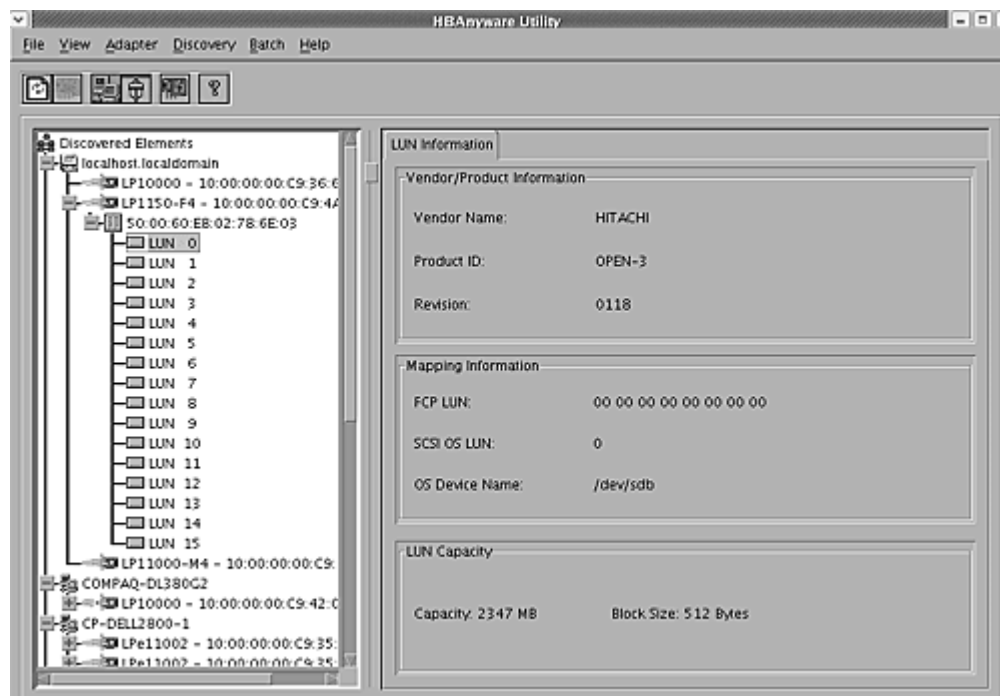


Figure 13: HBAnyware Utility, LUN Information

LUN Information Field Definitions

- Vendor Product Information Area
 - Vendor ID - The name of the vendor of the LUN.
 - Product ID - The vendor-specific ID for the LUN.
 - Revision - The vendor-specific revision number for the LUN.
- Mapping Information Area
 - FCP LUN - The Fibre Channel identifier used by the HBA to map to the SCSI OS LUN.

- SCSI OS LUN - The SCSI identifier used by the operating system to map to the specific LUN.
- OS Device Name - The name assigned by the operating system to the selected LUN.
- LUN Capacity

Note: LUN capacity information is only provided when the LUN is a mass-storage (disk) device. Other devices like tapes and scanners, etc. do not display capacity.

- Capacity - The capacity of the LUN, in megabytes.
- Block Length - The length of a logical unit block in bytes. Capacity - the capacity of the logical unit, in megabytes.
- Block Length - the length of a logical unit block in bytes.

Viewing Port Statistics

The Statistics tab provides cumulative totals for various error events and statistics on the port. Some statistics are cleared when the HBA is reset.

To view port statistics:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Click an HBA in the discovery-tree.
4. Click the Statistics tab.

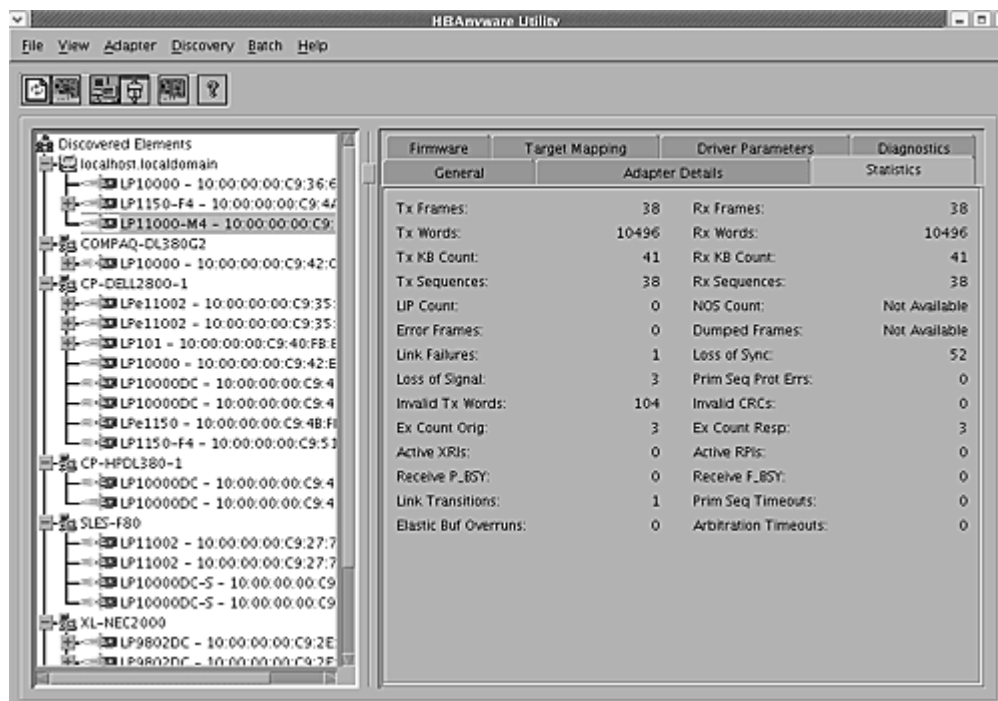


Figure 14: HBAnyware Utility, Statistics Tab

Port Statistics Field Definitions

- Tx Frames - Fibre Channel frames transmitted by this HBA port.
- Tx Words - Fibre Channel words transmitted by this HBA port.
- Tx KB Count - Fibre Channel kilobytes transmitted by this HBA port.
- Tx Sequences - Fibre Channel sequences transmitted by this HBA port.
- LIP count - The number of loop initialization primitive (LIP) events that have occurred for the port. This field is not supported if the topology is not arbitrated loop. Loop initialization consists of the following:
 - Temporarily suspend loop operations.
 - Determine whether loop capable ports are connected to the loop.
 - Assign AL_PA IDs.
 - Provide notification of configuration changes and loop failures.
 - Place loop ports in the "monitoring" state.
- Error Frames - The number of frames received with cyclic redundancy check (CRC) errors.
- Link Failures - The number of times the link failed. A link failure is a possible cause of a time-out.
- Loss of Signal - The number of times the signal was lost.
- Invalid Tx Words - The total number of invalid words transmitted by this HBA port.
- Ex Count Orig - The number of Fibre Channel exchanges originating on this port.
- Active XRIs - The number of active exchange resource indicators.
- Received P_BSY - The number of FC port-busy link response frames received.
- Link Transitions - The number of times the SLI port sent a link attention condition.
- Elastic Buf Overruns - The number of times the link interface has had its elastic buffer overrun.
- Rx Frames - The number of Fibre Channel frames received by this HBA port.
- Rx Words - The number of Fibre Channel words received by this HBA port.
- Rx KB Count - The received kilobyte count by this HBA port.
- Rx Sequences - The number of Fibre Channel sequences received by this HBA port.
- NOS count - This statistic is currently not supported for the SCSIport Miniport and Storport Miniport drivers, nor is it supported for arbitrated loop.
- Dumped Frames - This statistic is not currently supported for the SCSIport Miniport driver, the Storport Miniport driver or the driver for Solaris.
- Loss of Sync - The number of times loss of synchronization has occurred.
- Prim Seq Prot Errs - The primitive sequence protocol error count. This counter increments whenever there is any type of protocol error.
- Invalid CRCs - The number of frames received that contain CRC failures.
- Ex Count Resp - The number of Fibre Channel exchange responses made by this port.
- Active RPIs - The number of remote port indicators.
- Receive F_BSY - The number of Fibre Channel port-busy link response frames received.
- Primitive Seq Timeouts - The number of times a primitive sequence event timed out.
- Arbitration Timeouts - The number of times the arbitration loop has timed out. Large counts could indicate a malfunction somewhere in the loop or heavy usage of the loop.

Viewing Firmware Information

Use the Firmware tab to view current firmware versions, enable system BIOS and update firmware on remote and local HBAs. The update procedure is on page 55.

To view the firmware information:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Select an HBA in the discovery-tree.
4. Select the Firmware tab.

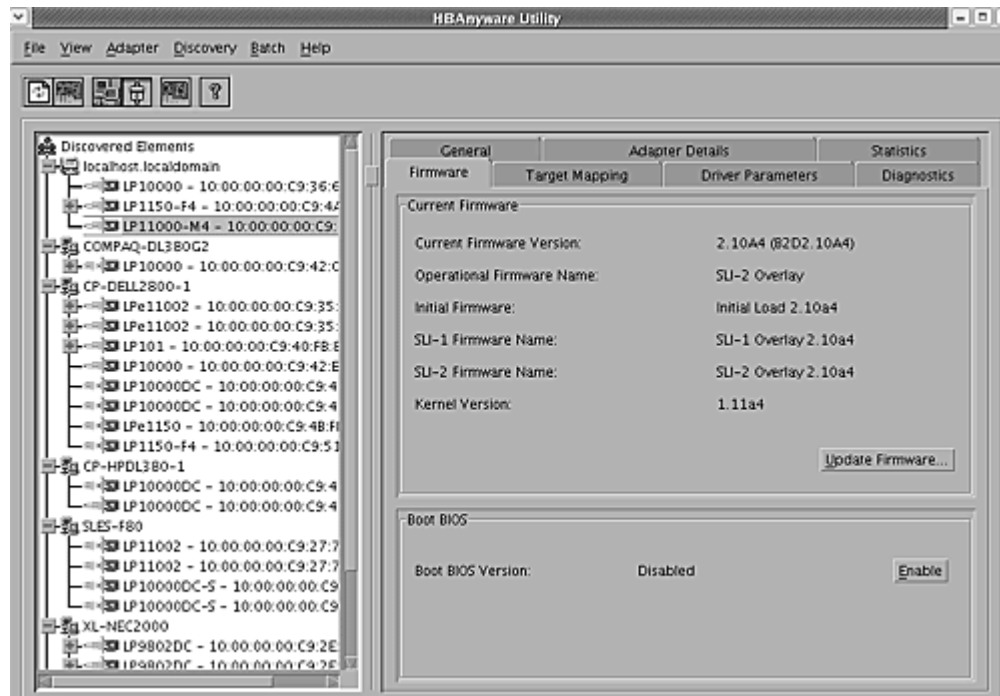


Figure 15: HBAnyware Utility, Firmware Tab

Firmware Field Definitions

Firmware Area

- **Firmware Version** - The Emulex firmware version number for this model of HBA.
- **Operational Firmware Name** - If visible, the name of the firmware that is operational.
- **Initial Firmware** - The firmware version stub responsible for installing the SLI code into its proper slot.
- **SLI-1 Firmware Name** - The name of the SLI-1 firmware overlay.
- **SLI-2 Firmware Name** - The name of the SLI-2 firmware overlay.
- **Kernel Version** - The version of the firmware responsible for starting the driver.

Firmware Tab Buttons

- **Enable/Disable** - Click to enable or disable the boot code.

- **Update Firmware** - Click to this button to display the HBAnyware Firmware Download dialog box. Using the HBAnyware Firmware Download dialog box, browse to the file you wish to download and download the file. See the “Update Firmware” topic on page 55 for more information.

Viewing Target Mapping

The Target Mapping tab in the HBAnyware utility enables you to view current target mapping and to set up persistent binding. You can also set up persistent binding using lputil.

To view target mapping:

1. Start the HBAnyware utility.
2. Select Host or Fabric sort.
3. Select an HBA in the discovery-tree.
4. Select the Target Mapping tab.

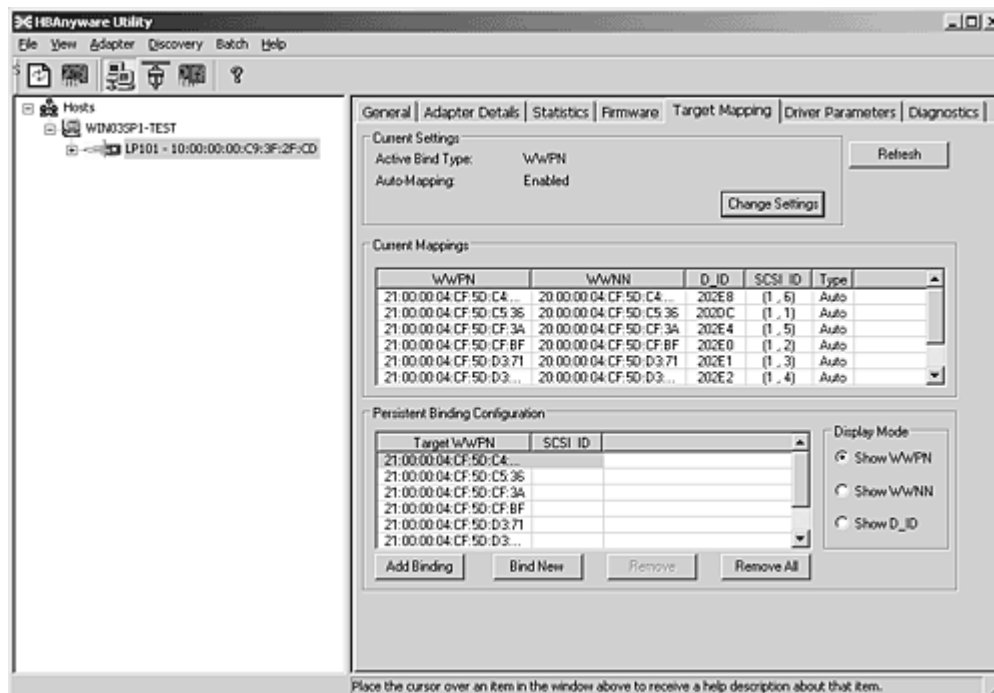


Figure 16: HBAnyware Utility, Target Mapping Tab

Target Mapping Field Definitions

Current Settings Area

- Active Bind Type -N/A
- Automapping - N/A

Current Mappings Table

- This table lists all currently mapped targets for the selected HBA.

Persistent Binding Configuration Table

- This table lists persistent binding information for the selected HBA.

Display Mode Radio Buttons

- Show WWPN
- Show WWNN
- Show D_ID

Target Mapping Buttons


- **Change Settings** - Click to change the Bind Type, the mode used to persistently bind target mappings. The Mapped Target Settings window is displayed. Select the Bind Type (WWPN, WWNN, or D_ID) or set Automapping to Enabled to Disabled.
- **Add Binding** - Click to add a persistent binding.
- **Bind New Target** - Click to add a target that does not appear in the Persistent Binding table.
- **Remove** - Click to remove the selected binding.
- **Remove All Bindings** - Click to remove all persistent bindings that are currently defined for the selected HBA.
- **PCI Configuration Parameters** - Parameters from the PCI configuration space on the HBA. Information includes vendor ID, device ID, base addresses, ROM address, header type, subclass and base class.
- **Adapter Revision Levels** - Firmware revision levels, including kernel and overlay version information.
- **Wakeup Parameters** - BIOS status and version, as well as SLI (service level interface).
- **IEEE Address** - The HBA board address.
- **Loop Map** - If you are using arbitrated loop topology, this option shows information about your connected devices, such as AL_PA and D_ID.
- **Status and Counters** - Byte, frame, sequence and busy counts.
- **Link Status** - Tracks activities such as link failure, loss of sync, and elastic overlay.
- **Configuration Parameters** - D_ID topology, and time-out values for link failures and loss of sync.

Resetting HBAs

The HBAnyware utility allows you to reset remote and local HBAs.

Caution: Do not reset an HBA while copying or writing files. This could result in data loss or corruption.

To reset the HBA using the HBAnyware utility:

1. Start the HBAnyware utility.
2. In the discovery-tree, select the HBA you want to reset.
3. Do one of the following:
 - From the menu bar, click **Adapter**, and then click **Reset HBA**.
 - Click the **Reset HBA**  button.

4. The following warning screen appears:

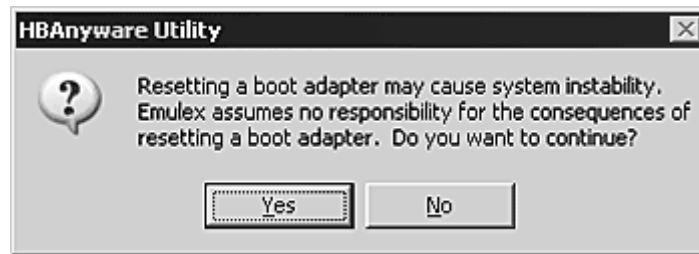


Figure 17: HBAnyware Utility, Reset Warning Screen

5. Click **Yes**. The HBA resets.

The reset may require several seconds to complete. While the HBA is resetting, the status bar shows "Reset in progress." When the reset is finished, the status bar shows "Ready".

Updating Firmware

The HBAnyware utility allows you to update firmware on remote and local HBAs.

Prerequisites

- The Solaris SFS driver is installed properly.
- The HBAnyware utility is installed properly.
- The firmware file has been downloaded from the Emulex Web site and extracted.

Note: The HBAnyware utility will update firmware on all HBAs including Sun-branded HBAs, but the Solaris SFS driver will immediately perform a firmware check and download afterwards on the Sun-branded HBAs only, cancelling the HBAnyware-generated update for these Sun-branded HBAs. See the Sun Web site or contact the OEM's customer service department or technical support department for the firmware files.

Procedure

To update firmware using the HBAnyware utility:

1. Start the HBAnyware utility.
2. In the discovery-tree, select the HBA onto which you want to update firmware.

3. Select the Firmware tab.

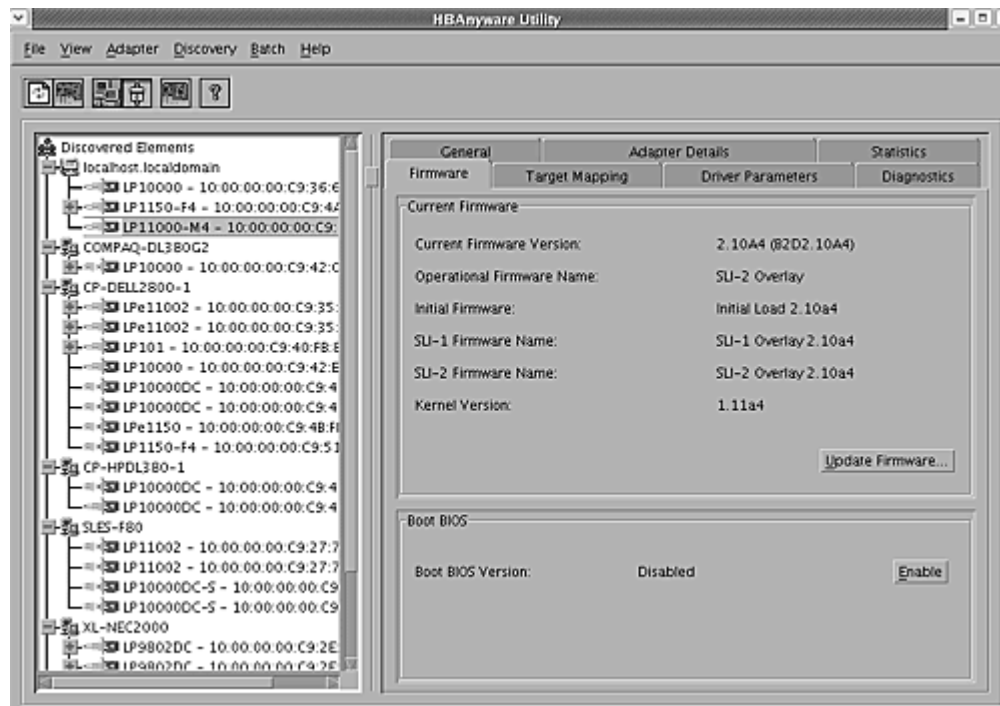


Figure 18: HBAnyware Utility, Firmware Tab

4. Click **Update Firmware**. The Firmware Download dialog box appears.

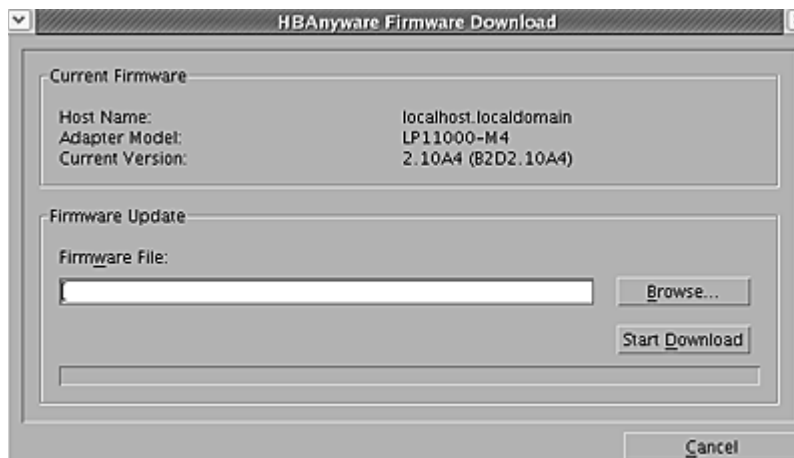


Figure 19: HBAnyware Utility, Firmware Download Dialog Box

5. Click **Browse**. The Firmware File Selection dialog box appears.



Figure 20: HBAnyware Utility, Firmware File Selection Dialog Box

6. Navigate to the extracted firmware file you wish to download. Select the file and click **OK**. A status bar shows the progress of the download and indicates when the download is complete.
7. Click **Start Download**.

If you are updating the firmware on a dual-channel HBA, repeat steps 2 through 7 to update the firmware on the second port or see *Updating Firmware (Batch Mode)* on page 58.

Updating Firmware (Batch Mode)

Loading firmware in batch mode differs from its non-batch counterpart in that it enables you to install firmware on multiple HBAs in a single step. Batch firmware loading is restricted to a single firmware file and to all accessible HBAs for which that file is compatible.

Note: Stop other HBAnyware utility functions while batch loading is in progress.

Prerequisites

- The firmware file has been downloaded from the Emulex Web site and extracted to the Emulex Repository folder (RMRepository). This folder is in /usr/sbin/HBAnyware/RMRepository.

Procedure

To batch load firmware using the HBAnyware utility:

- Start the HBAnyware utility.
- From the menu bar, select **Batch** and click **Download Firmware**.

Note: You do not need to select a particular tree element for this operation.

- When the Batch Firmware File dialog box appears, browse to locate and select the firmware file to download. Click **Open**.

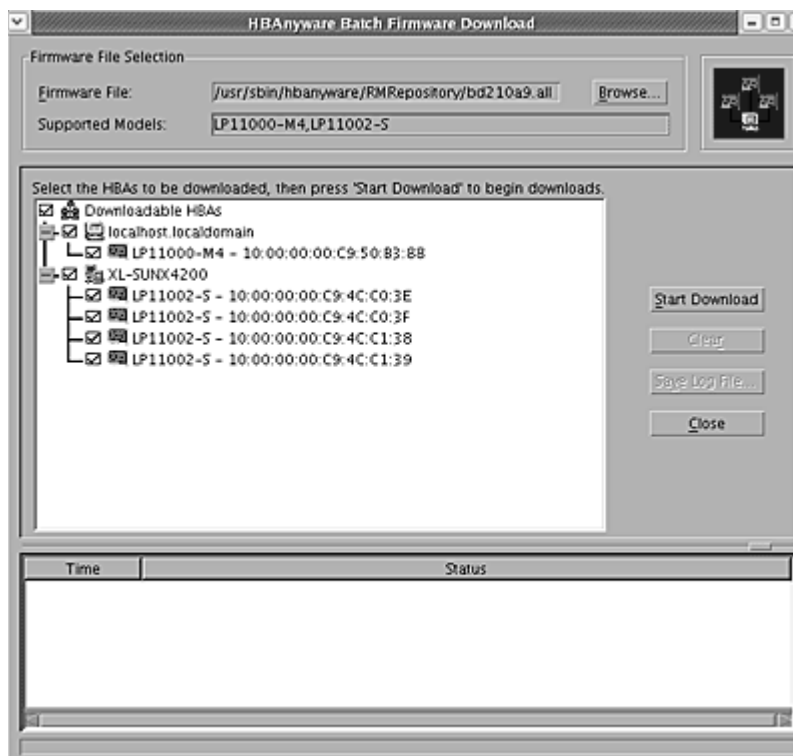


Figure 21: HBAnyware Utility, Batch Firmware Download Dialog Box

- A tree-view appears showing all HBAs and their corresponding hosts for which the selected firmware file is compatible.
- Check boxes next to the host and HBA entries are used to select or deselect an entry. Checking an HBA selects or removes that HBA; checking a host removes or selects all eligible HBAs for that host.

6. When selection/deselection is complete, click **Start Download**.
7. Once downloading begins, the tree-view displays the progress. As firmware for a selected HBA is being downloaded, it appears orange in the tree-view. Once successful downloading is complete, the entry changes to green. If the download failed, the entry is changed to red.

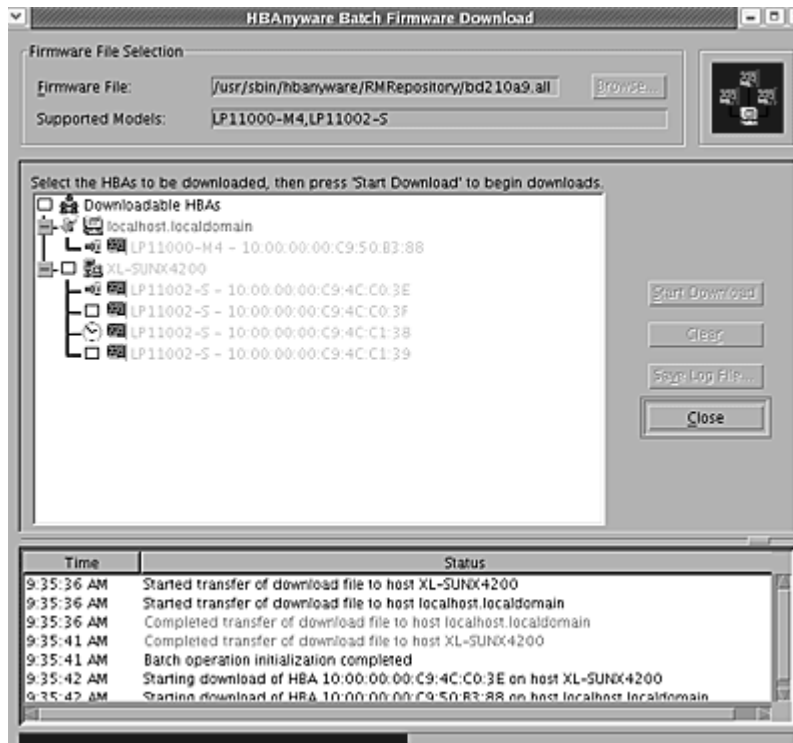


Figure 22: HBAnyware Utility, Firmware Download Dialog Box with Completed Download

8. When downloading is complete, you can click **Print Log** to get a hard copy of the activity log.
9. Click **Close** to exit the batch procedure.

Enabling or Disabling the BIOS

Enabling the BIOS is a two-step process:

1. Enable the system BIOS (x86 BootBIOS, FCode or EFIBoot) to read the Emulex boot code on the HBA (using the HBAnyware utility).
2. Enable the HBA to boot from SAN (using the BIOS utility).see the documentation that accompanies the boot code for more information.

Prerequisites

- The Solaris SFS driver is installed properly.

Procedure

To enable or disable the HBA BIOS:

1. Start the HBAnyware utility.
2. In the discovery-tree, select the HBA whose BIOS you wish to enable/disable.

3. Select the Firmware tab.

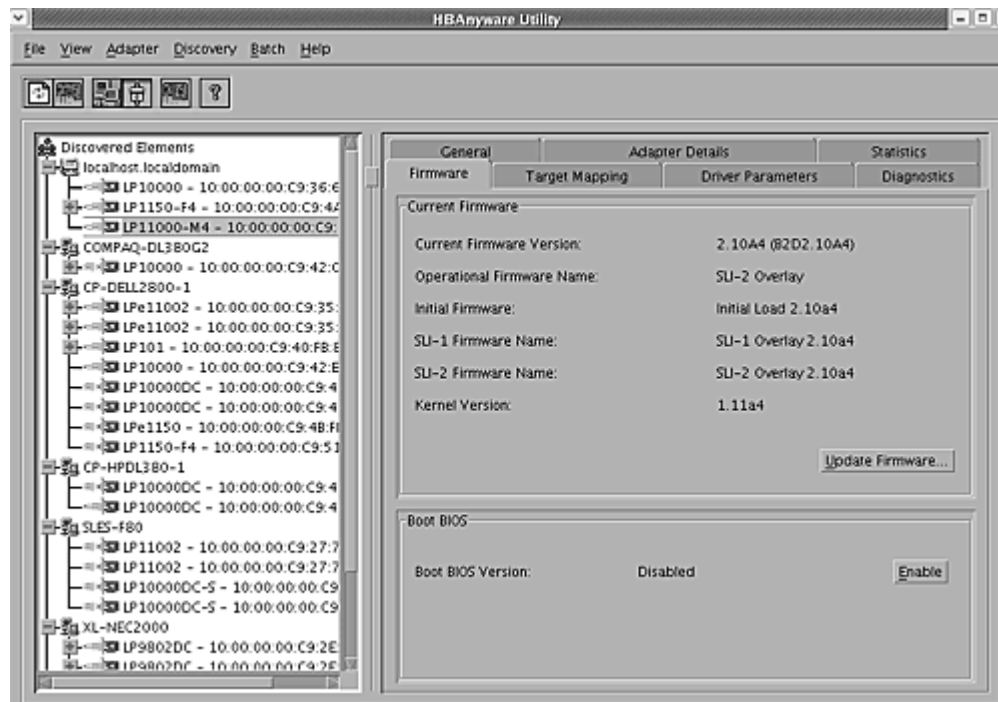


Figure 23: HBAnyware Utility, Firmware Tab with BIOS Disabled

4. To enable or disable the BIOS, click **Enable**. The button title changes from **Enable** to **Disable**.

If you are updating x86 BootBIOS, you must also enable the HBA to boot from SAN using the BIOS utility; see the documentation that accompanies the boot code for more information.

Setting Driver Parameters

The Driver Parameters tab and Host Driver Parameter tab enable you to modify driver parameters for a specific HBA or all HBAs in a host.

For example, if you select a host in the discovery-tree, you can globally change the parameters for all HBAs in that host. If you select an HBA in the discovery-tree, you can change the `lpfc_use_adisc`, `lpfc_log_verbose` and the `lpfc_nodet_tmo` parameters for only that HBA.


For each parameter, the Driver Parameters tab and Host Driver Parameters tab shows the current value, the range of acceptable values, the default value, and whether the parameter is dynamic (a dynamic parameter allows the change to take effect without restarting the HBA or rebooting the system). You can make parameter changes persistent after a reboot of the system. You can also restore parameters to their default settings.

You can also apply driver parameters for one HBA to other HBAs in the system using the Driver Parameters tab. When you define parameters for an HBA, you create a .dpv file. The .dpv file contains the parameters for that HBA. After you create the .dpv file, the HBAnyware utility enables you to apply the .dpv file parameters to multiple HBAs in the system, thereby simplifying multiple HBA configuration. See *Creating the Batch Mode Driver Parameters File* on page 64 for more information.

Note: The HBAnyware utility enables you to make dynamic parameter changes with any version of Solaris. However, changes made by editing the `lpfc.conf` file and issuing an `update_drv` command are only dynamic for Solaris 9 and later.

Setting Driver Parameters for an HBA

To change the driver parameters for an HBA:

1. Start the HBAnyware utility.
2. Do one of the following:
 - From the menu bar, click **View**, then click **Sort by Host Name**.
 - From the toolbar, click the **Sort by Host Name**  button.
3. In the discovery-tree, select the HBA whose parameters you wish to change.
4. Select the Driver Parameters tab (see Figure 24). The parameter values for the selected HBA are displayed.

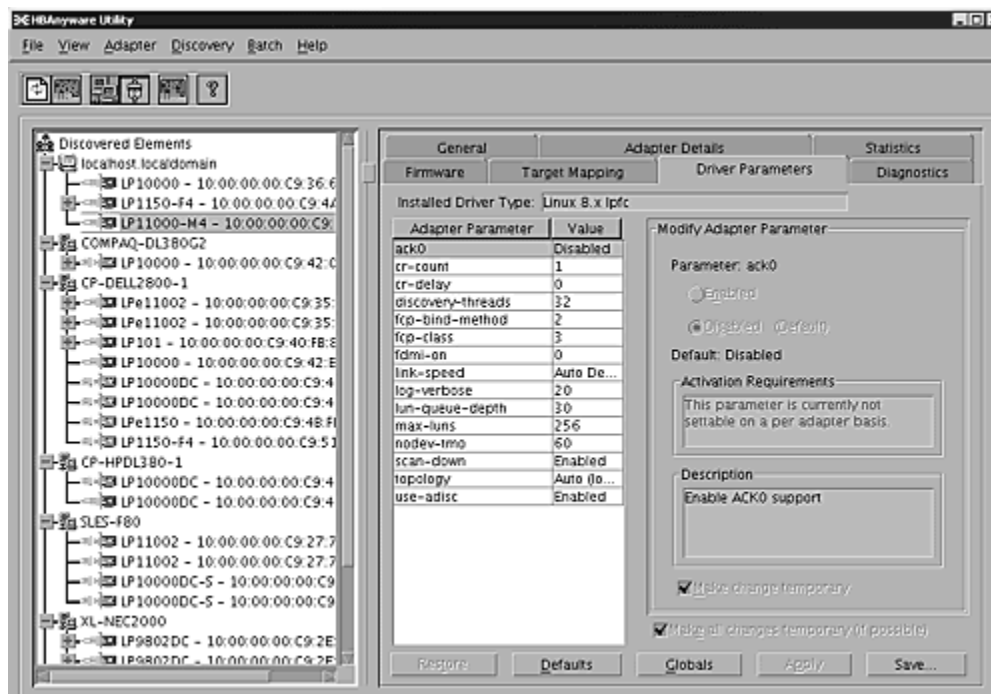


Figure 24: HBAnyware Utility, HBA Selected - Driver Parameters Tab

5. In the Driver Parameters tab, click the parameter that you want to change. A description of the parameter appears on the right side of the dialog box.
6. Enter a new value in the Value field in the same hexadecimal or decimal format as the current value. If the current value is in hexadecimal format, it is prefaced by "0x" (for example, 0x2d). You may enter a new hexadecimal value without the "0x". For example, if you enter ff10, this value is interpreted and displayed as "0xff10".
7. If you want the change to be temporary (causing the parameter to revert to its last permanent setting when the system is rebooted), check the "Make change temporary" box. This option is available only for dynamic parameters.
8. If you are making changes to multiple parameters, and you want all the changes to be temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
9. Click **Apply**.

Restoring All Parameters to Their Earlier Values


If you changed parameters, but did not click **Apply** and you want to restore the parameters to their last saved values, click **Restore**.

Resetting All Default Values

If you want to reset all parameter values to their default (factory) values, click **Defaults**.

Setting Driver Parameters for a Host

To change the driver parameters for HBAs installed in a host:

1. Start the HBAnyware utility.
2. Do one of the following:
 - From the menu bar, click **View**, then click **Sort by Host Name**.
 - From the toolbar, click the **Sort by Host Name**  button.
3. In the discovery-tree, click the host whose HBA driver parameters you wish to change.
4. Click the Host Driver Parameters tab. If there are HBAs with different driver types installed, the installed Driver Types menu shows a list of all driver types and driver versions that are installed on the HBAs in the host. Select the driver whose parameters you wish to change. This menu does not appear if all the HBAs are using the same driver.
5. In the Host Driver Parameters tab, click the parameter that you want to change. A description of the parameter appears on the right side of the dialog box.

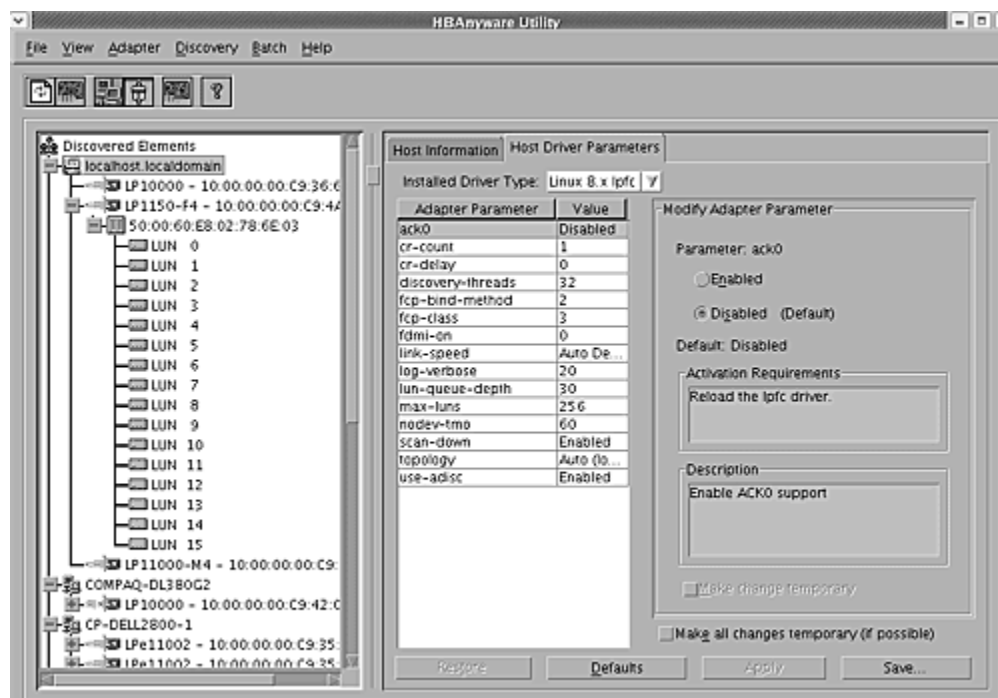


Figure 25: HBAnyware Utility, Host Selected - Driver Parameters Tab

6. Enter a new value in the Value field. You must enter values in decimal or hexadecimal format, depending on how the current value is presented. If the value is in hexadecimal format, it is prefaced by "0x" (for example 0x2d).

7. If you want the change to be temporary (causing the parameter to revert to its last permanent setting when the system is rebooted), check the "Make change temporary" box. This option is available only for dynamic parameters.
8. If you are making changes to multiple parameters, and you want all the changes to be temporary, check the "Make all changes temporary" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be made temporary.
9. Click **Apply**.

Restoring All Parameters to Their Earlier Values

If you changed parameters, but not click **Apply** and you want to restore the parameters to their last saved values, click **Restore**.

Resetting All Default Values

If you want to reset all parameter values to their default (factory) values, click **Defaults**.

Creating the Batch Mode Driver Parameters File

You can apply driver parameters for one HBA to other HBAs in the system using the Driver Parameters tab. When you define parameters for an HBA, you create a .dpv file. The .dpv file contains the parameters for that HBA. After you create the .dpv file, the HBAnyware utility enables you to apply the .dpv file parameters to multiple HBAs in the system, thereby simplifying multiple HBA configuration.

To create the .dpv file:

1. Start the HBAnyware utility.
2. Select the HBA whose parameters you want to apply to other HBAs from the discovery-tree.
3. Select the Driver Parameters tab. Set driver parameters (see Figure 24 on page 61).
4. After you define the parameters for the selected HBA, click **Save Settings**. The Select Driver Parameter File dialog box appears. Use the dialog box to select where to save the file or to rename the file. Click **Save**. The Save Driver Parameters dialog box appears.

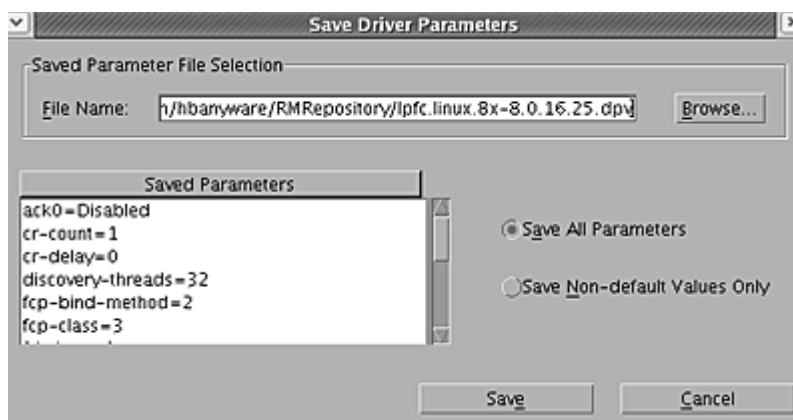


Figure 26: HBAnyware Utility, Save Driver Parameters Dialog Box

5. The two radio buttons allow you to choose the type of parameters to save. You can save all parameters or only those parameters whose current values differ from their corresponding default values.
6. A list of the saved parameters and their current values show in the Saved Parameters box.
7. Click **Save**.

Assigning Batch Mode Parameters to HBAs

After you create the batch mode parameters (.dpv) file, you can assign its parameters to multiple HBAs. Assigning batch mode parameters make it easy to configure multiple HBAs. See *Creating the Batch Mode Driver Parameters File* on page 64 to learn how to create the .dpv file.

To assign batch mode parameters to HBAs:

1. Start the HBAnyware utility.
2. From the HBAnyware utility menu, click **Batch** and select Update Driver Parameters. (You do not need to select any discovery-tree elements at this time.) The Select Driver Parameter File dialog box appears.

3. Select the file whose parameters you wish to apply and click **Open**. The Batch Driver Parameter Update dialog box shows all the batch file compatible HBAs with a check mark beside them.

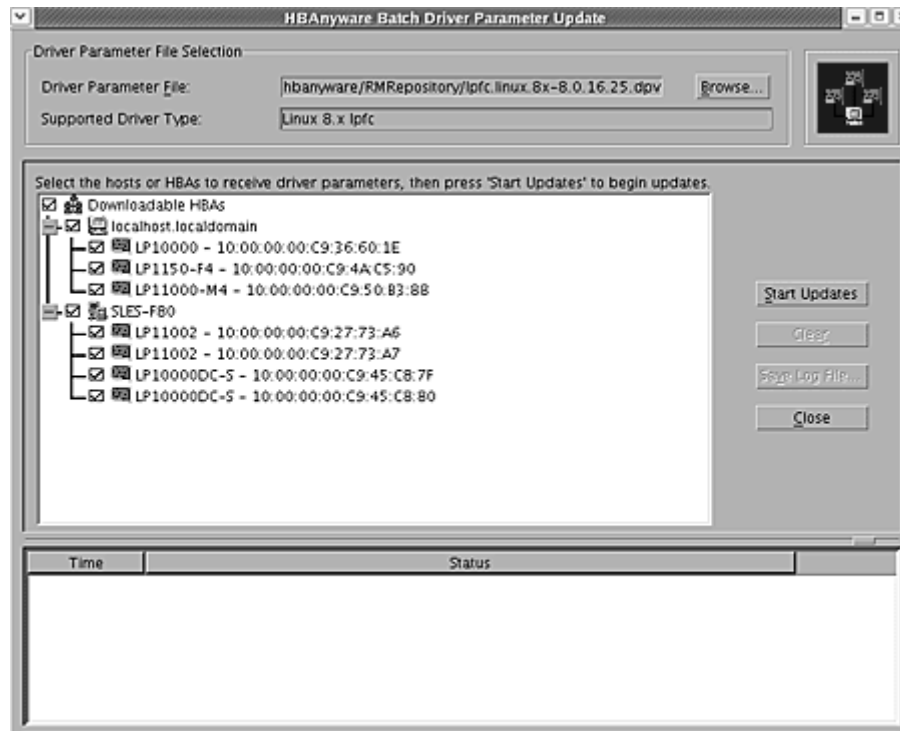


Figure 27: HBAAnyware Utility, Batch Driver Parameters Update Dialog Box

4. Click **Start Updates**. The HBAAnyware utility Batch Driver Update dialog box shows the current status of the update. When the update completes, a final summary shows the number of HBAs that were successfully processed, and the number of HBAs for which one or more parameter updates failed.

If you wish, click **Print Log** to print a report of the update.

Setting Up Persistent Binding

When you create a persistent binding, the HBAAnyware utility tries to make that binding dynamic. However, the binding must meet all of the following criteria to be dynamic:

- The SCSI ID (target/bus combination) specified in the binding request must not be mapped to another target. For example, the SCSI ID must not already appear in the 'Current Mappings' table under 'SCSI ID'. If the SCSI ID is already in use, then the binding cannot be made dynamic, and a reboot is required.
- The target (WWPN, WWNN or DID) specified in the binding request must not be mapped to a SCSI ID. If the desired target is already mapped, then a reboot is required.
- The 'Bind Type Selection' (WWPN, WWNN or DID) specified in the binding request must match the currently active bind type shown under "Current Settings" section of the Target Mapping tab. If they do not match, then the binding cannot be made active.

To set up persistent binding using the HBAAnyware utility:

1. Start the HBAAnyware utility.
2. In the directory tree, click the HBA for which you want to set up persistent binding.

- Click the Target Mapping tab. All targets are displayed.

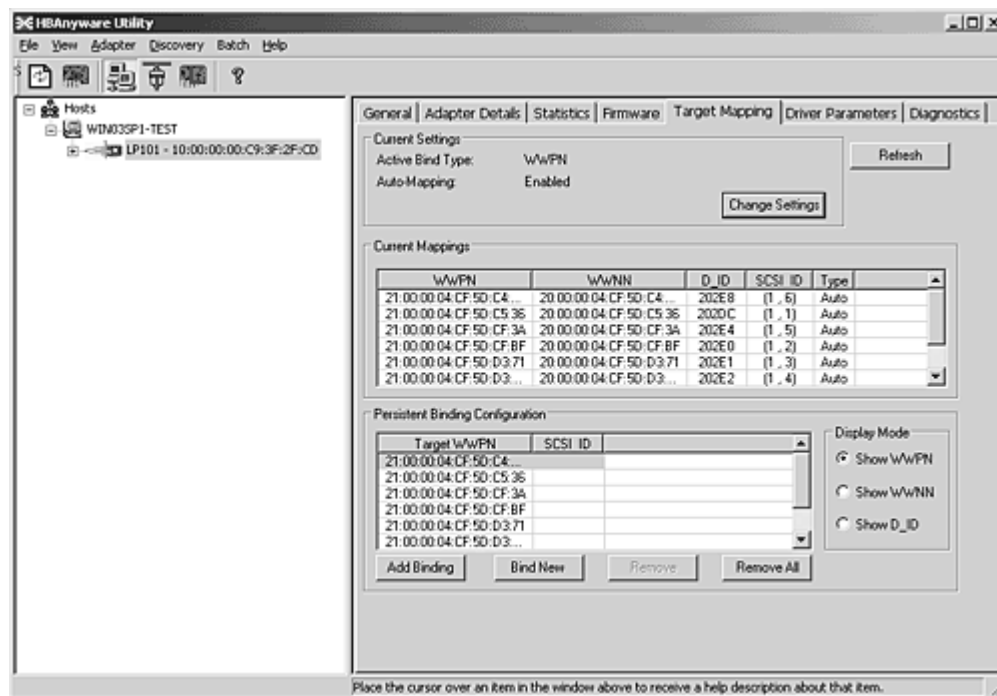


Figure 28: HBAnyware Utility, Target Mapping Tab

- The information for each currently defined mapping includes the world wide port name (WWPN), world wide node name (WWNN), device ID (D_ID), SCSI ID, or Bind Type. The type can be either 'PB', indicating that the mapping was the result of a persistent binding, or 'Auto', indicating that the target was automapped. In the Display Mode section, choose the display mode you want to use.
- If you want to change the Active Bind Type (the mode used to persistently bind target mappings) or Automapping setting, click **Change Settings**. Select the Bind Type (WWPN, WWNN or D_ID), and set Automapping to Enabled or Disabled.

Note: All mapped targets, whether automapped or resulting from a persistent binding configuration, will have entries in the “Current Mappings” table on the Target Mapping dialog box.

If the binding that you defined has been successfully activated, you will see the following message:

“The new binding has been created and is currently active.”

If, however, the binding was successfully created, but could not be made active, you will see the following message:

“The new binding has been created. Note that this binding will not become active until after you have rebooted the system.” Generally, you should ensure that the bind type in the Current Settings section of the Target Mapping dialog box is the same as the type of binding selected in the Persistent Binding Configuration section of the dialog box.

To add a persistent binding:

1. In the Targets Table, click the target that you want to bind.
2. Click **Add Binding**. The Add Persistent Binding dialog box is displayed.

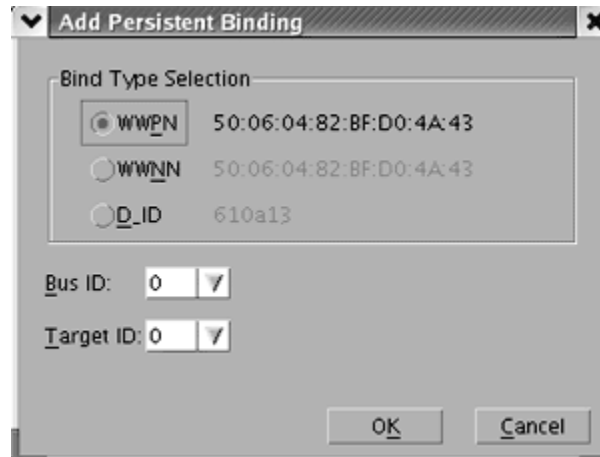


Figure 29: HBAnyware Utility, Add Persistent Binding Dialog Box

3. Select the Bind Type that you want to use (WWPN, WWNN or D_ID).
4. Select the Bus ID and Target ID that you want to bind, and click **OK**.

Note: All mapped targets, whether automapped or resulting from a persistent binding configuration, will have entries in the “Current Mappings” table on the Target Mapping dialog box.

If the binding that you defined has been successfully activated, you will see the following message:

“The new binding has been created and is currently active.”

If, however, the binding was successfully created, but could not be made active, you will see the following message:

“The new binding has been created. Note that this binding will not become active until after you have rebooted the system.” Generally, you should ensure that the bind type in the Current Settings section of the Target Mapping dialog box is the same as the type of binding selected in the Persistent Binding Configuration section of the dialog box.

To bind a target that does not appear in the Persistent Binding Table:

1. Click **Bind New Target**. The Bind New Target dialog box is displayed.

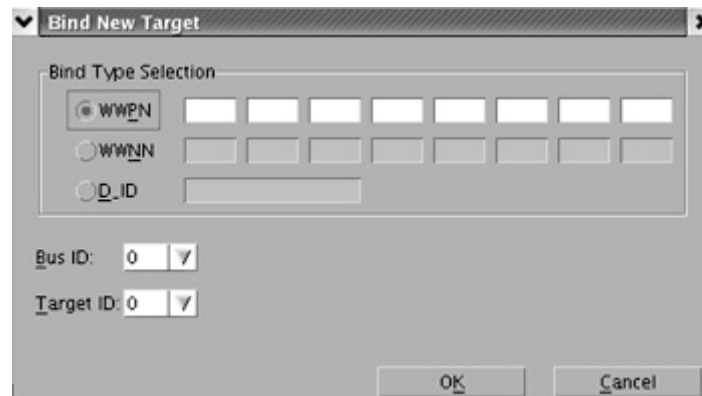


Figure 30: HBAnyware Utility, Bind New Target Dialog Box

2. Click the type of binding you want to use, and type the WWPN, WWNN or D_ID you want to bind to the target.
3. Select the Bus ID and Target ID that you want to bind, and click **OK**.

Note: A target will not appear on the target list if automapping has been disabled and the target is not already persistently bound.

Adding New Targets Using sd.conf for Solaris 8, 9 and 10

You can perform on-the-fly configuration changes, without rebooting, using the HBAnyware utility. For Solaris 8, you must first add the new targets to the sd.conf file.

To add new targets using sd.conf (Solaris 8):

1. Edit the Solaris SCSI configuration file (sd.conf):

```
#vi /kernel/drv/sd.conf
.
.
.
name="sd" parent="lpfc" target=17 lun=1;
name="sd" parent="lpfc" target=18 lun=10;
name="sd" parent="lpfc" target=19 lun=15;
.
.
.
```

2. Save the file and exit vi.

Changing Parameters or Bindings for Solaris 8, 9 and 10

To change parameters or bindings in Solaris 9 and 10, edit the sd.conf file as shown above and force a reread of the file with the `update_drv -f sd` command.

To change parameters or bindings in Solaris 8:

1. Stop all I/O on the device.
2. Unconfigure all ports with open instances to the driver.
3. Unload the driver using the `modunload` command. (See "Loading or Unloading the Driver without Rebooting" on page 69 for more information.)
4. Reload the driver using the `modload` command. (See "Loading or Unloading the Driver without Rebooting" on page 69 for more information.)

Setting Up Target/LUN Blocking Using sd.conf

The class keyword ("scsi") ensures that Solaris specifically probes all adapters controlled by all driver that register themselves as class="scsi". The parent keyword ("lpfc") ensures that Solaris specifically probes all adapters controlled by the lpfc driver for the specified targets and LUNS. The class and parent keywords cause the SCSI layer to probe multiple adapters, even multiple adapters across multiple drivers. This method limits the SCSI layer probing of targets and LUNs on an adapter-by-adapter basis. This gives you control over which targets and LUNs are seen by each initiator (target/LUN blocking).

To set up target/LUN blocking using sd.conf:

1. Reboot the system with the adapter installed.
2. Check the output of `dmesg(1M)`. This message displays in the following format:

```
NOTICE: Device Path for interface lpfcX:/pci@1f.0/pci@1/fibre-channel@3
```

Note: Where lpfcX is the interface for a specific adapter and /pci@1f.0/pci@1/fibre-channel@3 is the device path for the specific adapter.

3. Add entries to the sd.conf file in the following format:

```
name="sd" parent="lpfc" target=16 lun=0 hba="lpfcX";
```

Note: This entry does not cancel the effect of any other parent="lpfc" or class="scsi" entries for target=16 lun=0. If you want the SCSI layer to probe only for target=16 lun=0 on device lpfcX, the parent="lpfc" or class="scsi" entries for target=16 lun=0 need to be deleted. You can cause system problems if certain class="scsi" entries are deleted. These entries are used by the SCSI adapter, so if there is a SCSI boot disk at target=0 lun=0 whose probe entry has been deleted, the system won't boot. Similarly, if any SCSI target's probe entry is deleted, that device won't operate. To guarantee that the Fibre Channel and SCSI probing won't conflict, use persistent binding to assign FC devices target numbers greater than 15. Persistent binding can be used to perform target blocking but not LUN blocking.

No-Reboot Firmware Updates

Emulex is the only vendor providing dynamic adapter firmware updates during operation without stopping I/O traffic. You can dynamically update host bus adapter firmware using the HBAnyware utility. Refer to *Updating Firmware* on page 55 for more information.

Loading or Unloading the Driver Without Rebooting

Note: When the Solaris operating system is installed on a Fibre Channel drive, you must reboot the system because you cannot quiesce all I/O on the OS drive.

Systems must support dynamic reconfiguration.

To load the driver without rebooting:

1. Load the driver using the `modload` command.
2. Use the `cfgadm` command to configure Emulex HBAs.
3. Restart I/O.

To unload the driver without rebooting:

1. Stop all I/O on the device.
2. Use the `cfgadm` command to disconnect Emulex HBAs.
3. Unload the driver using the `modunload` command.

Performing Diagnostic Tests

Use the Diagnostics tab to do the following:

- Run these tests on Emulex HBA's installed in the system:
 - PCI Loopback (see page 74)
 - Internal Loopback (see page 74)
 - External Loopback (see page 74)
 - Power-On Self Test (POST) (see page 71)
 - Echo (End-to-End) (see page 75)
 - Quick Test (see page 70)
- Perform a diagnostic dump (see page 72).
- View PCI registers and wakeup parameter (see page 72).
- Control HBA beaconing (see page 71).

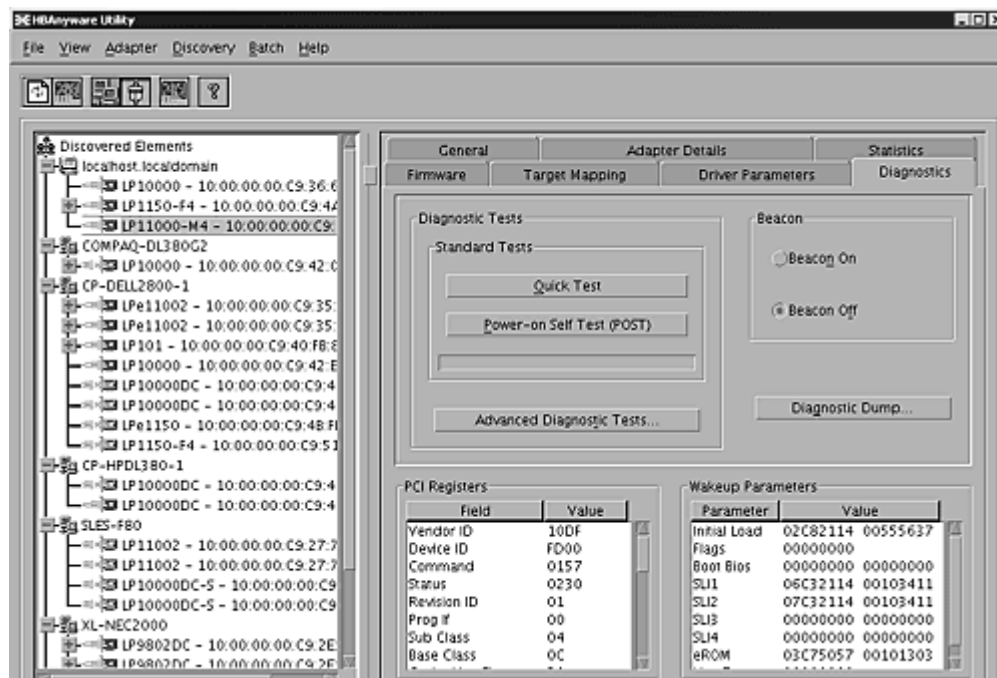


Figure 31: HBAAnyware Utility, Diagnostics Tab

All functions are supported locally and remotely, except for the dump feature which is only supported locally.

Running a Quick Test

The Diagnostics tab enables you to run a "quick" diagnostics test on a selected HBA. The Quick Test consists of 50 PCI Loopback test cycles and 50 Internal Loopback test cycles.

To run a quick test:

1. Start the HBAAnyware utility.
2. From the discovery-tree, select the HBA on which you wish to run the Quick Test.

3. Select the Diagnostics tab and click **Quick Test**. The following message appears:

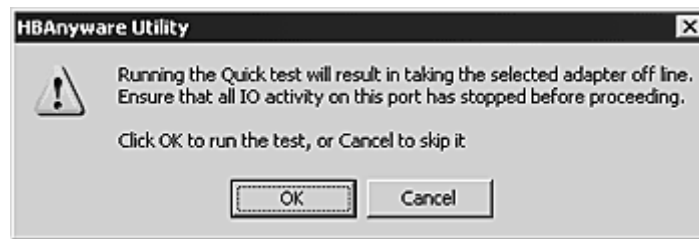


Figure 32: HBAnyware Utility, Quick Test Message

4. Click **OK** to run the test. The Quick Diagnostics Test message shows the PCI Loopback and Internal Loopback test results.

Running a POST Test

The POST (Power On Self Test) is a firmware test normally performed on an HBA after a reset or restart. The POST does not require any configuration to run.

To run the POST Test:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA on which you wish to run the POST Test.
3. Select the Diagnostics tab and click **Power-on Self Test (POST)**. A warning dialog box appears.

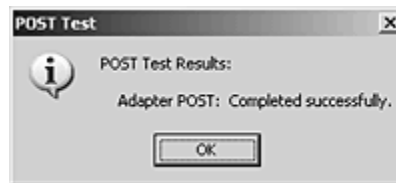


Figure 33: HBAnyware Utility, POST Test Warning Window

4. Click **OK**. A POST Test window shows POST test information.

Using Beaconing

The beaoning feature enables you to force a specific HBA's LEDs to blink in a particular sequence. The blinking pattern acts as a beacon, making it easier to locate a specific HBA among racks of other HBAs.

When you enable beaoning, the two LEDs blink rapidly in unison for 24 seconds, after which the LEDs report the HBA health status for 8 seconds. When the 8 seconds are up, the HBA returns to beaoning mode. This cycle repeats indefinitely until you disable this feature or you reset the HBA.

Note: The beaoning buttons are disabled if the selected HBA does not support beaoning.

To enable or disable beaoning:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA whose LEDs you wish to set.
3. Select the Diagnostics tab and click **Beacon On** or **Beacon Off**.

Creating Diagnostic Dumps

The diagnostic dump feature enables you to create a “dump” file for a selected HBA. Dump files contain various information such as firmware version, driver version and so on, that is particularly useful when troubleshooting an HBA.

Note: The Diagnostic Dump feature is only supported for local HBAs. If a remote HBA is selected from the tree-view, the Initiate Diagnostic Dump is disabled.

To start a diagnostic dump:

1. Start the HBAnyware utility.
2. From the discovery-tree, select a local HBA whose diagnostic information you wish to dump.
3. Select the Diagnostics tab and click **Diagnostic Dump**. The Diagnostic Dump dialog box appears. You can specify how many files you want to save using the Files Retained counter. Click **Delete Existing Dump Files** if you wish to remove existing dump files from your system.

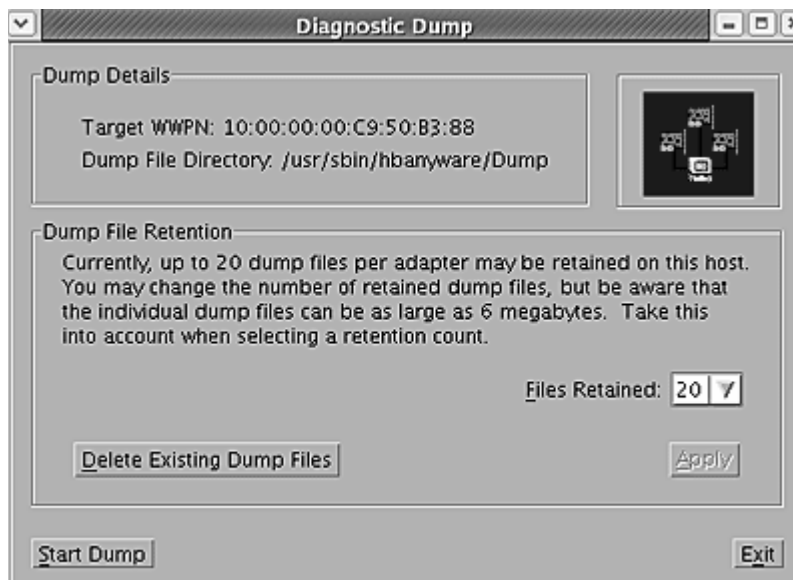


Figure 34: HBAnyware Utility, Diagnostic Dump Dialog Box

4. Click **Start Dump**.

Displaying PCI Registers and Wakeup Information

A PCI Register dump for the selected HBA appears in the lower left panel of the Diagnostics tab. Wakeup information for the selected HBA appears in the lower right panel of the Diagnostics tab. The information is read-only and is depicted below:

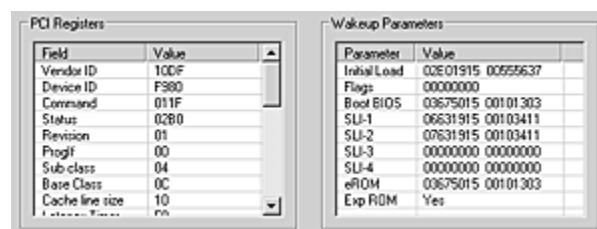


Figure 35: HBAnyware Utility, PCI Registers and Wakeup Parameters Area of the Diagnostics Tab

Running Advanced Diagnostic Tests

The Advanced Diagnostics feature gives you greater control than the Quick Test over the type of diagnostics tests that run. Through Advanced Diagnostics, you can specify which tests to run, the number of cycles to run, and what to do in the event of a test failure.

To run advanced diagnostics tests:

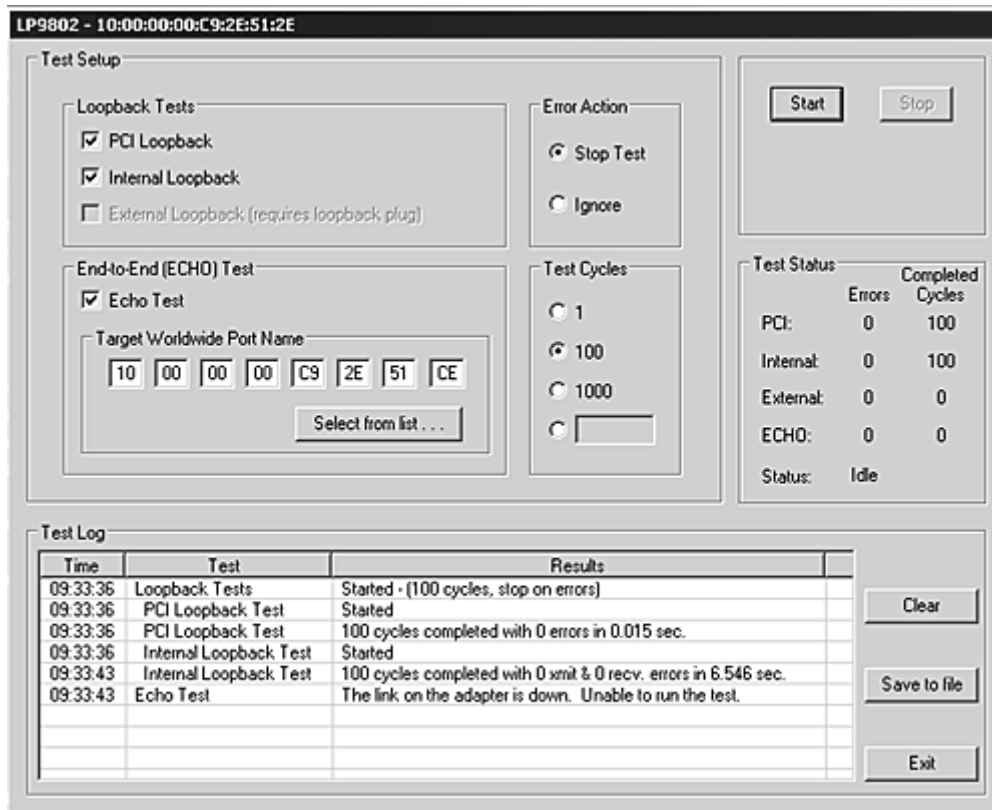
1. Start the HBAnyware utility.
2. Click **Advanced Diagnostics Test** on the Diagnostics tab to view the Advanced Diagnostics dialog box.

You can run four types of tests:

- PCI Loopback
- Internal Loopback
- External Loopback
- End-to-End (ECHO)

Note: You cannot run the External Loopback test and ECHO test concurrently. If you select External Loopback the ECHO test section is disabled and vice versa.

All test results, plus the status of running tests, are time stamped and appear in the log at bottom of the dialog box.



Test Setup

Loopback Tests

- ☒ PCI Loopback
- ☒ Internal Loopback
- ☐ External Loopback (requires loopback plug)

End-to-End (ECHO) Test

- ☒ Echo Test

Target Worldwide Port Name

10 00 00 00 C9 2E 51 CE

Select from list . . .

Error Action

- ☒ Stop Test
- ☐ Ignore

Test Cycles

- ☐ 1
- ☒ 100
- ☐ 1000
- ☐ []

Test Status

	Errors	Completed Cycles
PCI:	0	100
Internal:	0	100
External:	0	0
ECHO:	0	0
Status:	Idle	

Test Log

Time	Test	Results
09:33:36	Loopback Tests	Started - (100 cycles, stop on errors)
09:33:36	PCI Loopback Test	Started
09:33:36	PCI Loopback Test	100 cycles completed with 0 errors in 0.015 sec.
09:33:36	Internal Loopback Test	Started
09:33:43	Internal Loopback Test	100 cycles completed with 0 xmit & 0 recv. errors in 6.546 sec.
09:33:43	Echo Test	The link on the adapter is down. Unable to run the test.

Buttons: Start, Stop, Clear, Save to file, Exit

Figure 36: HBAnyware Utility, Advanced Diagnostics Dialog Box

Running Loopback Tests

To run a loopback test, use the "Loopback Test" section of the Advanced Diagnostics dialog box.

You can run the following loopback test combinations using the appropriate check boxes:

- **PCI Loopback Test** - A firmware controlled diagnostic test in which a random data pattern is routed through the PCI bus without being sent to an adapter link port. The returned data is subsequently validated for integrity.
- **Internal Loopback Test** - A diagnostic test in which a random data pattern is sent down to an adapter link port, then is immediately returned without actually going out on the port. The returned data is subsequently validated for integrity.
- **External Loopback Test** - A diagnostic test in which a random data pattern is sent down to an adapter link port. The data goes out the port and immediately returns via a loopback connector. The returned data is subsequently validated for integrity.

Note: You cannot run the External Loopback test and ECHO test concurrently. If you select External Loopback the ECHO test section is disabled and vice versa.

You can specify the number of test cycles by clicking one of the cycle counts values in the "Test Cycles" section of the dialog box or enter a custom cycle count if you wish. The Test Status section displays how many cycles of each test ran. The "Error Action" section of the dialog box enables you to define what should be done in the event of a test failure.

There are two error action options:

- **Stop Test** - The error will be logged and the test aborted. No further tests will run.
- **Ignore** - Log the error and proceed with the next test cycle.

To run loopback tests:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA on which you wish to run the Loopback Test.
3. Select the Diagnostics tab and click **Advanced Diagnostics Tests**. From the "Loopback Test" section of the dialog box, choose the type of Loopback test you wish to run and define the loopback test parameters.

Note: You must insert a loopback plug in the selected HBA before running an External Loopback test.

4. Click **Start**. The following warning appears:

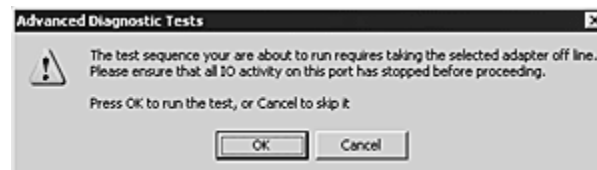


Figure 37: HBAnyware Utility, Advanced Diagnostic Tests Warning

5. Click **OK**. If you choose to run an External Loopback test the following window appears:



Figure 38: HBAnyware Utility, Advanced Diagnostic Tests Warning for External Loopback

6. Click **OK**. The progress bar indicates that the test is running.

Periodic test feedback, consisting of the current loopback test/cycle plus the completion status of each type of test, is displayed in the "Test Log" section of the dialog box. Click **Clear** to erase the contents of the log display or click **Save to File** to save the log file.

Running End-to-End (ECHO) Tests

Run echo tests using the "End-to-End (ECHO) Test" section of the Diagnostics tab. The end-to-end test enables you send an ECHO command/response sequence between an HBA port and a target port.

Note: Not all remote devices respond to an echo command.

You cannot run the ECHO test and the External Loopback test concurrently. If you select the ECHO Test the External Loopback test is disabled.

To run end-to-end echo tests:

1. Start the HBAnyware utility.
2. From the discovery-tree, select the HBA from which you wish to initiate the End-to-End (ECHO) Test.
3. Select the Diagnostics tab. Click **Advanced Diagnostics Test**.
4. Check **Echo Test**. Enter the World Wide Port Name (WWPN) for the target.

or

Click **Select From List** if you do not know the actual WWPN of the test target. The Select Echo Test Target dialog box appears. Select the port you wish to test from the tree-view and click **Select**.

All relevant information for the selected port is automatically added to the Target Identifier section of the Diagnostics dialog box.

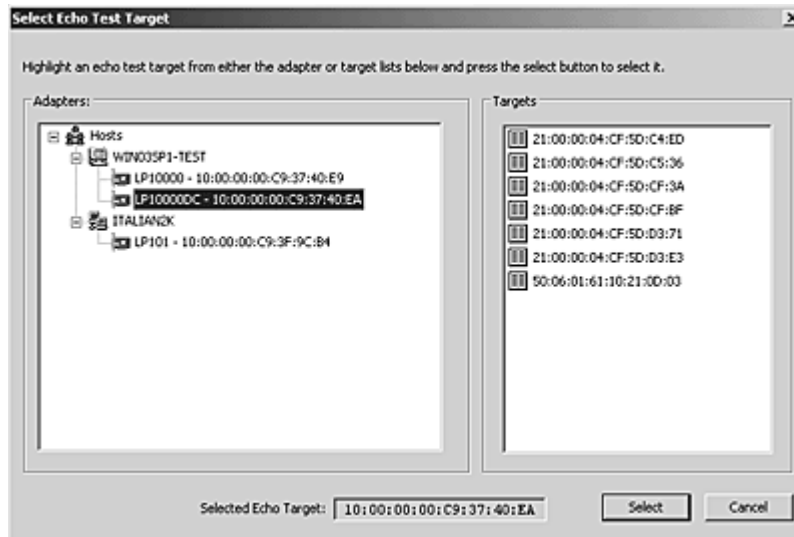


Figure 39: HBAnyware Utility, Select Echo Test Target Window

5. Click **Start**. The following warning window appears:

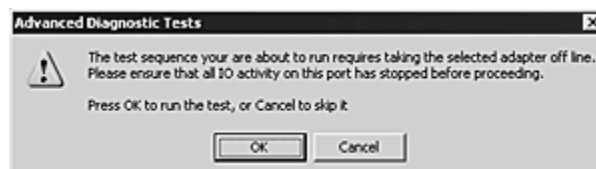


Figure 40: HBAnyware Utility, Advanced Diagnostic Tests Warning

6. Click **OK**. A result screen appears and the test results appear in the Test Log. Click **Clear** to erase the contents of the log display or click **Save to File** to save the log file.

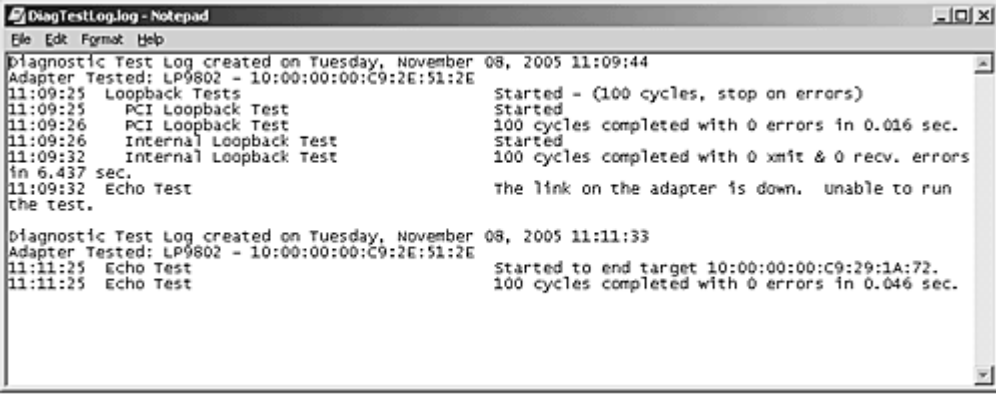
Saving the Log File

You can save the test log to a log file for later viewing or printing. When new data is written to a saved file, the data is appended to the end of the file. Each entry has a two-line header that contains the identifier of the HBA being tested and the date and time of the test. Over time, the data accumulates to form a chronological history of the diagnostics performed on the HBA.

After writing an entry into the log, you are prompted to clear the display.

The default name of the saved file is DiagTestLog.log and by default is located in:
/usr/sbin/hbanyware/Dump

An example of a saved log file appears below:



```

DiagTestLog.log - Notepad
File Edit Format Help
Diagnostic Test Log created on Tuesday, November 08, 2005 11:09:44
Adapter Tested: LP9802 - 10:00:00:00:C9:2E:51:2E
11:09:25 Loopback Tests Started - (100 cycles, stop on errors)
11:09:25 PCI Loopback Test Started
11:09:26 PCI Loopback Test 100 cycles completed with 0 errors in 0.016 sec.
11:09:26 Internal Loopback Test Started
11:09:32 Internal Loopback Test 100 cycles completed with 0 xmit & 0 recv. errors
in 6.437 sec.
11:09:32 Echo Test the link on the adapter is down. unable to run
the test.

Diagnostic Test Log created on Tuesday, November 08, 2005 11:11:33
Adapter Tested: LP9802 - 10:00:00:00:C9:2E:51:2E
11:11:25 Echo Test Started to end target 10:00:00:00:C9:29:1A:72.
11:11:25 Echo Test 100 cycles completed with 0 errors in 0.046 sec.

```

Figure 41: DiagTestLog Window

To save the log file:

1. After running a test from the Diagnostic Test Setup dialog box, Click **Save to File**. The Select Diagnostic Log file Name dialog box appears. The default name of a saved file is DiagTestLog.log.
2. Browse to the desired directory, change the log file name if you wish and click **Save**.

Out-of-Band SAN Management

Out-of-Band (OOB) remote SAN management is achieved by sending the remote management requests over a LAN using the Ethernet TCP/IP protocol to remote hosts.

In-band management is achieved by sending the remote management requests over a SAN to remote hosts.

The principle differences between in-band and out-of-band SAN Management are:

- A management host with an HBA installed does not need to connect to a fabric to manage other hosts.
- An OOB management host can manage all of the HBAs in a remote host, not just the ones connected to the same fabric. In-band can only manage HBAs connected to the same fabric.
- You can manage many more hosts since OOB is not constrained by the boundaries of a fabric or zoning.
- True board status (e.g. link down) is available since the in-band path is not necessary to send a status request to the remote host.
- HBA security in an OOB environment is much more important since many more hosts are available for management and OOB access is not affected by fabrics or zoning.
- Discovery of hosts in an OOB environment is much more difficult than in-band discovery.

Adding a Single Host

The HBAnyware utility enables you to specify a single OOB host to manage. If the host is successfully discovered as a manageable host, it is added to the static list of hosts and if it has not been discovered in-band, the host and its HBAs are added to the discovery tree.

To add a single host:

1. Start the HBAnyware utility.
2. From the Discovery menu, select **Out-of-Band/Add Host**. The Add Remote Host dialog box appears.



Figure 42: HBAnyware Utility, Add Remote Host Dialog Box

3. Enter the name or the IP address of the host to be added. Entering the IP address is the best way to add a new host.

Note: Using the IP address to identify the host avoids name resolution issues.

4. Click **OK**. You will receive a message indicating whether or not the new host was successfully added.

Adding a Range of Hosts

You can find the OOB manageable hosts by searching a range of IP addresses using the Add Range of IP Hosts dialog box.

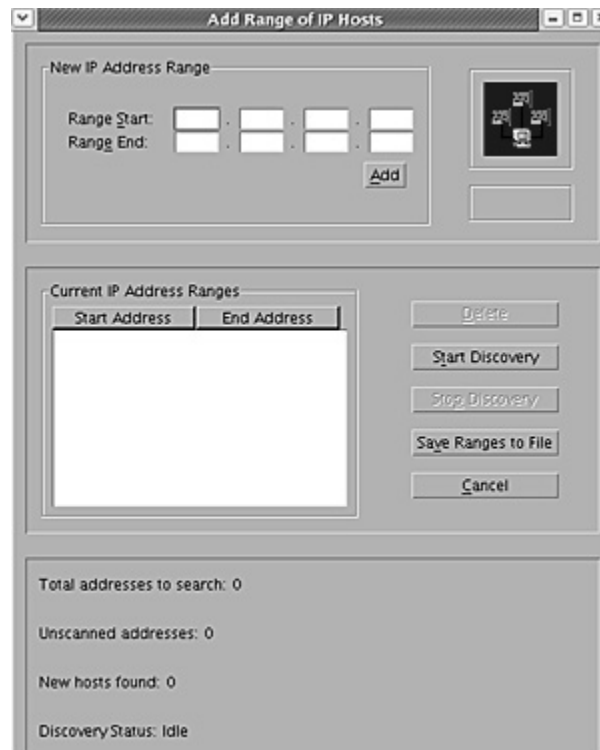


Figure 43: HBAAnyware Utility, Add Remote Hosts Window

The Add Range of IP Hosts dialog box enables you to build the initial list of OOB manageable hosts.

To add a range of hosts:

1. Start the HBAAnyware utility.
2. From the Discovery menu, select **Out-of-Band/Add Range of Hosts**. The Add Range of IP Hosts dialog box appears.
3. Enter the complete start and end address range and click **Add**. The added address range appears in the dialog box. Add any additional ranges you wish to search.
4. Click **Start Discovery**. HBAAnyware checks each address in the range to determine if the host is available and remotely manageable. The number of addresses discovered (of manageable hosts) is periodically updated on the dialog box.

Note: The number of addresses does not correspond directly to the number of hosts added to the discovery-tree.

For example, some of the addresses discovered may be for hosts that have already been discovered in-band. However, new HBAs may be discovered on those hosts that were not discovered in-band.

Also, a host may have more than one HBA installed and both IP addresses for that host are discovered during the search, but only one host will possibly be added to the discovery-tree.

5. When the search is complete, click **Cancel**.

6. A dialog box appears asking to save the IP ranges you searched. Click **Yes** to save the address ranges. If you save the address ranges, these address ranges will appear the next time you use the Add Range of IP Hosts dialog box. Click **No** if you do not want to save the address ranges.

The **Save Ranges to A File** button saves the specified range(s) to a file so that the same ranges can be automatically invoked when the HBAnyware utility is started again.

Removing Hosts

Periodically you may want to remove hosts that are no longer part of the network. You may want to remove a host when it is removed from the network or to detect hosts that are no longer being discovered. Removing hosts that can no longer be discovered improves the operation of the discovery server.

To remove hosts:

1. Start the HBAnyware utility.
2. From the Discovery menu, select Out-of-Band/Remove Host. The Remove Remote Hosts dialog box shows a list of discovered OOB hosts. Any host not currently discovered appears in red. Click **Show Undiscovered Hosts Only** to only display currently undiscovered hosts.
3. From the Remove Remote Hosts dialog box, select the hosts you wish to remove. You can select all the displayed hosts by clicking **Select All**.
4. Click **OK** to remove the selected hosts.

HBAnyware Security

Introduction

Initially, only the HBAnyware software package has been installed on all of the systems of a Fibre Channel network. Any of those systems can remotely access and manage the HBAs on any systems in the group. This may not be a desirable situation, because any system can perform actions such as resetting boards or downloading firmware. Figure 44 illustrates a system with no security.

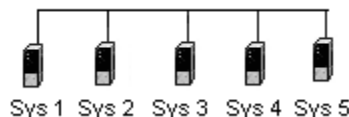


Figure 44: Initial State - No Security

The HBAnyware security software consists of an application programming interface (API) containing a set of security management functions and a user interface (UI). Together these allow you to administer a security system configuration (SSC). HBAnyware security is system-based, not user-based.

SSC provides two main security features:

1. Prevents remote HBA management from systems that you do not want to have this capability.
2. Prevents an accidental operation (such as firmware download) on a remote HBA. In this case, you do not want to have access to HBAs in systems you are not responsible for maintaining.

SSC has several components that enable you to setup your environment in a secure way:

- Security association (SA) - A record consisting of a key and an access control record. Related components are the SA table, SA File and SA Identifier (SA_ID).
 - SA table - a group of 256 Security Associations and a flag to enable/disable security.
 - SA file - A locally encrypted file on each system that is part of the HBAnyware security environment that stores the SA table.

- SA_ID - An index (into the SA table) that is passed in the CT command descriptor to indicate which Access Control Record (containing the key is being used to encrypt/decrypt the command data) to use in the SA table.
- Master Security Client (MSC) - Upon first discovery, an MSC will configure the first ACG, granting itself client access and all of the systems it wants to manage server access. Once security is enabled on a server system, that server cannot grant itself client access. Only an MSC can grant this access to a server by creating an Access Sub Group (ASG) and making a server the client to the ASG.
- ACG - An ACG consists of a client system and the servers it is allowed access to manage. An MSC creates an initial ACG. All additional ACGs are defined out of this initial ACG.
- ASG - A sub-group of systems created from the systems of a client's ACG. One system is the designated client and the others are made servers. The updates to the SA files are sent from the client to the appropriate systems to create an ASG. The new client system not only has access to remotely manage the servers in its new ACG, but and can also create additional ASGs from its own systems in its ACG. This gives the ASG a hierarchical nature:
- Backup Master - The system designated by an MSC as the backup MSC. It can take over the MSC if the MSC becomes permanently disabled and can no longer be the MSC.

Starting the Security Configurator for the First Time: Creating the First ACG, Designating the MSC and Selecting Systems in the FC Network

Prerequisites

- The Solaris SFS Driver is installed.
- The HBAnyware and lputil utilities are installed.
- The HBAnyware Security Configurator is installed.
- All of the systems that are part of, or will be part of, the security configuration are online on the Fibre Channel network. This enables the systems to receive updates and changes made to the security configuration.

Caution: Any system that is part of the security installation, but offline when the Security Configurator starts for the first time will not be available for security configuration changes even if it is brought online while the Configurator is running. Any system that is already part of the security installation might not run with the proper security attributes if updates to the security configuration are made while it is offline.

Procedure

Start the HBAnyware Security Configurator for the first time in an unsecure environment. The computer from which you run the Security Configurator will become an MSC.

1. Run the `/usr/sbin/hbanyware/ssc` script. Type:

```
/usr/sbin/hbanyware/ssc
```

The "Unsecure System" message is displayed.:

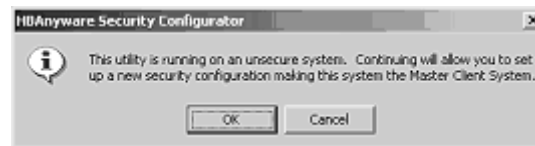


Figure 45: Security Configurator, "Unsecure System" Message

2. Click **OK** on the Unsecure System message to have the systems with HBAs discovered. The Discovery Window is displayed:



Figure 46: Discovery Window

All of the available servers are discovered and available to become part of the system Access Control Group (ACG).

3. Select the unsecured servers to be added to the ACG from the Available Servers list.

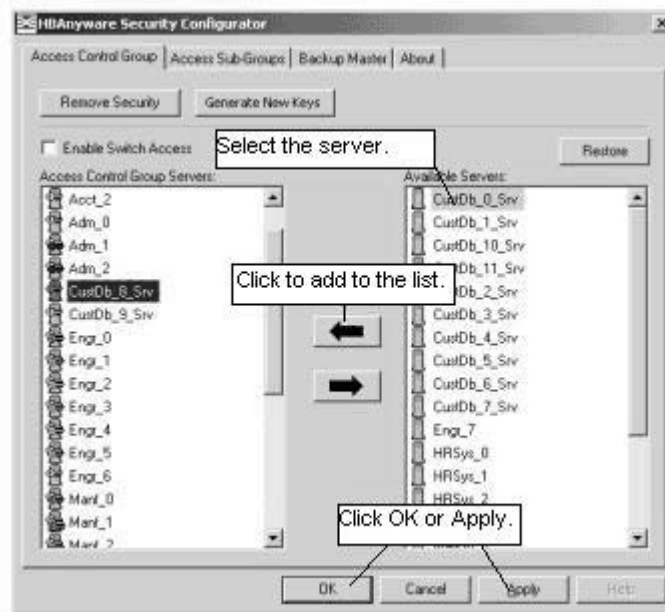


Figure 47: Security Configurator, Access Group Control Tab with Call Outs

4. Click the left arrow to add the servers to the Access Control Group Servers list.

Note: There can be only one MSC per access control group (ACG). There can be multiple MSCs (thus multiple ACGs) in a SAN, however the set of ACG servers controlled by each MSC must not overlap (i.e. ACG servers controlled by one MSC cannot be added to another MSC's ACG). For example, if you designate a host in a SAN as an MSC, and assign some, but not all, of the servers in the SAN to that MSC (i.e. move some of the hosts in the 'Available Servers' list on the 'Access Control Group' tab to the 'Access Control Group Servers' list), then any of the servers that still remain in the 'Available Servers' list can be designated as a separate MSC. The servers that appear in the 'Available Servers' list have yet to be claimed by an MSC and are thus in an unsecured state. Any leftover servers that still remain in the 'Available Servers' list can subsequently be added to the ASG controlled by the new MSC.

5. Click **OK** or **Apply**. The security configuration is updated on all of the selected servers as well as on the initial system. The following process sets up an MSC (see Figure 48).

- a. The SSC utility runs.
- b. SA_ID is selected.
- c. SA files are created for systems 2 through 5.
- d. SA files are sent to each system and system 1 becomes an ACG and an MSC, the only system which can run the HBAnyware client to remotely access all other system.

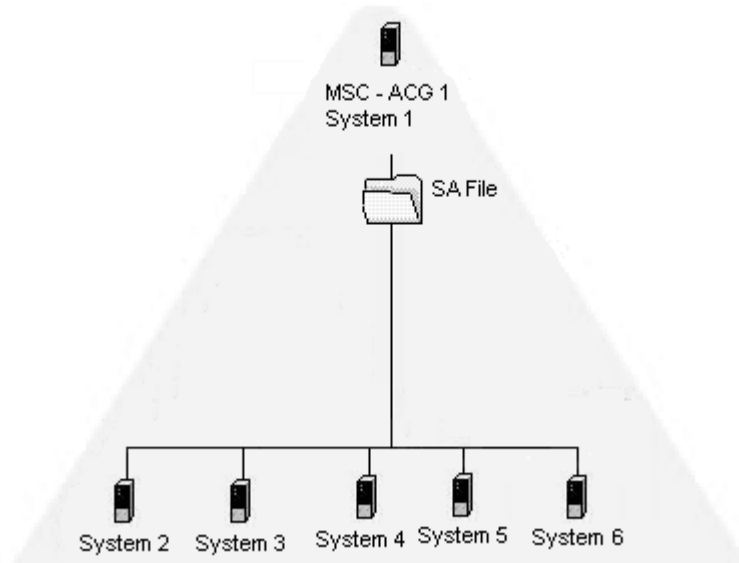


Figure 48: Systems 2 through 6 can access and control their local HBAs

Access Control Groups

Introduction

The Access Control Group tab shows the systems that are part of a client's Access Control Group (ACG) and, from an MSC, allows you to select the systems that belong to the ACG.

Access Control Group Tab on the MSC

On an MSC, you select or deselect the systems that are to be part of the security installation in the Access Control Group tab. When you select unsecure systems and move them to the Access Control Group Servers list, these systems are updated to secure them and bring them into the MSC's ACG.

When you select systems in the ACG and move them to the Available Servers list, the security configuration for those systems is updated to make them unsecure. After you have configured security from the MSC for the first time, the Access Control Group tab looks similar to the following:

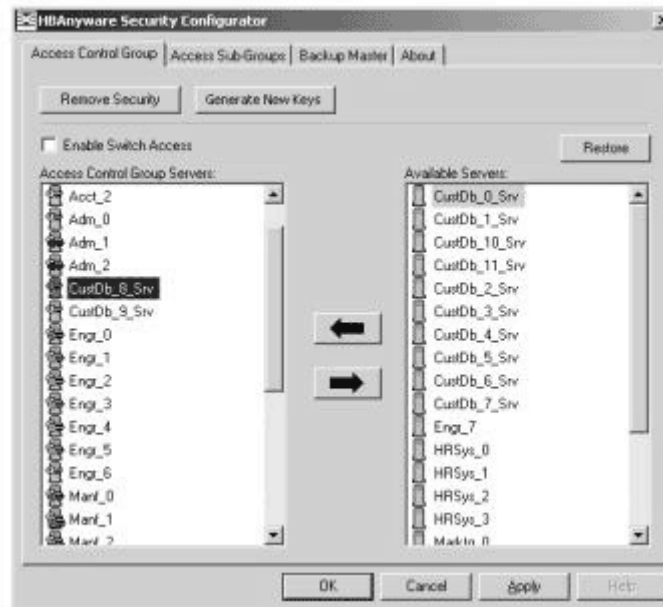


Figure 49: Security Configurator, Access Control Group Tab on a non-MSC system

Access Control Group Tab on a Non-MSC

On a non-MSC system, the Access Control Group tab shows the systems that are part of the client's ACG. You cannot modify the ACG on a non-MSC. (You can modify the ACG only on the MSC or a client higher in the security topology's hierarchy.) The ACG tab on a non-MSC system looks similar to the following:

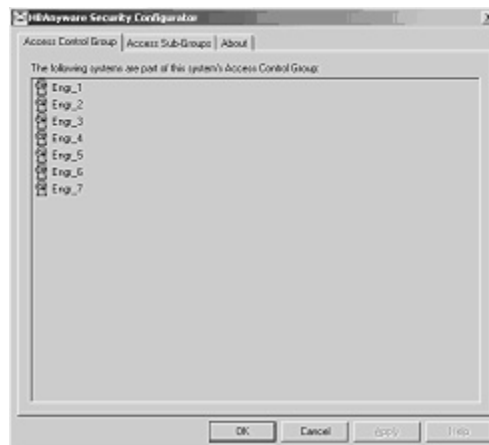







Figure 50: Security Configurator, Access Control Group Tab after MSC security is configured

ACG Icons

Depending on the configured security topology, a system can be a server in one or more ACGs. It can also be a client to an ACG. The following icons indicate the state of each of the systems in the Access Control Group Servers list.

-  The system is a secure server in the ACG. It does not belong to an Access Sub-Group (ASG). You can remove this system from the ACG.
-  The system is a secure server in the ACG and belongs to one or more ASGs. You can remove this system from the ACG.
-  The system is a secure server in the ACG and a client to an ASG. You cannot remove this system from the ACG until you remove it as a client from the ASG.
-  The system is a secure server in the ACG, a secure server in one or more ASGs and a client to an ASG. You cannot remove this system from the ACG until you remove it as a client from the ASGs.
-  The system is a Backup Master. You cannot remove this system from the ACG until you remove it as a Backup Master.

Adding a Server to the ACG

After you create the initial Access Control Group (ACG) on the Master Security Client (MSC), you may want to add unsecured servers to the ACG.

To add servers to the ACG:

1. Start the HBAnyware Security Configurator.
2. On the Access Control Group tab, from the Available Servers list, select the unsecured servers that you want to add to the ACG.

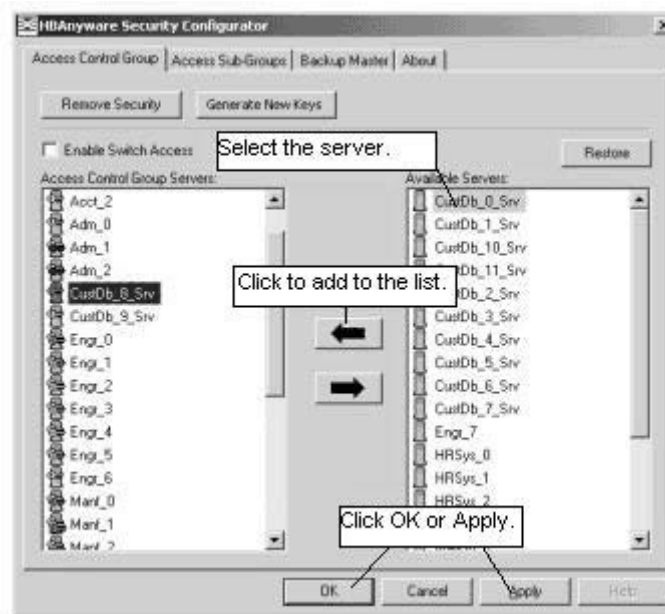


Figure 51: Security Configurator, The Access Group Control Tab with Call Outs

3. Click the **left arrow** to add the server to the Access Control Group Servers list.
4. Click **OK** or **Apply**.

Deleting a Server from the ACG

To delete a server from the Access Control Group (ACG):

1. Start the HBAware Security Configurator.
2. On the Access Control Group tab, from the Access Control Group Servers list, select the secured systems that you want to delete from the ACG.

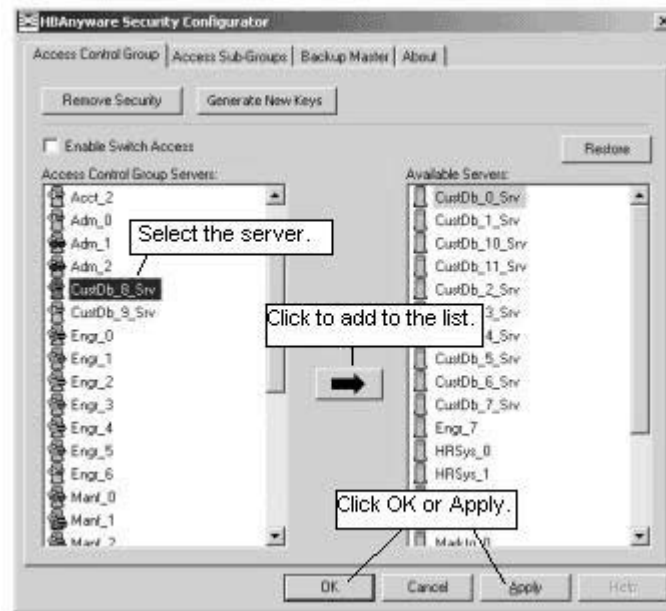


Figure 52: Security Configurator, The Access Group Control Tab with Call Outs

3. Click the **right arrow** to remove the servers from the Access Control Group Servers list.
4. Click **OK** or **Apply**.

Removing Security from all Servers in the ACG

You can remove security from all systems only from the Master Security Client (MSC). Removing the entire security topology on all of the servers in the MSC's ACG puts the servers in an unsecure state. The MSC is also put in an unsecure state; consequently, it is no longer the MSC. Any participating systems that are not online will not receive the 'remove security' configuration update, and as a result will no longer be accessible remotely.

To remove security from all servers in the ACG:

1. Start the HBAnyware Security Configurator. The Access Control Group tab is displayed.

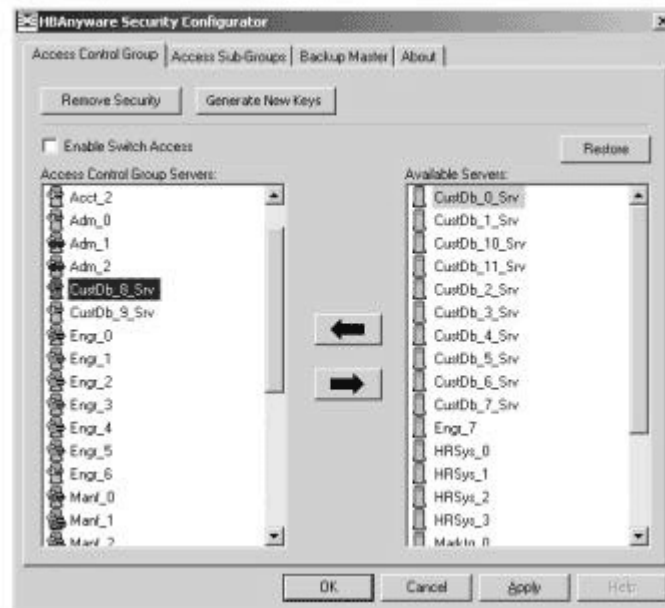


Figure 53: Security Configurator, Access Control Group Tab

2. On the Access Control Group tab, click the **Remove Security** button. The following message is displayed:



Figure 54: The HBAnyware Security Configurator "Warning" Dialog Box

3. Click **Yes**. Security is removed from all servers in the ACG.

Generating New Security Keys

You can generate new security keys only from a Master Security Client (MSC). After the new security keys are generated, they are automatically sent to all of the remote servers in the Access Control Group (ACG).

Note: All the servers that are part of the ACG must be online when this procedure is performed so that they may receive the new keys. Any servers that do not receive the new keys will no longer be accessible remotely.

To generate new security keys for all servers in the ACG:

1. From the MSC, start the HBAnyware Security Configurator. The Access Control Group tab is displayed.

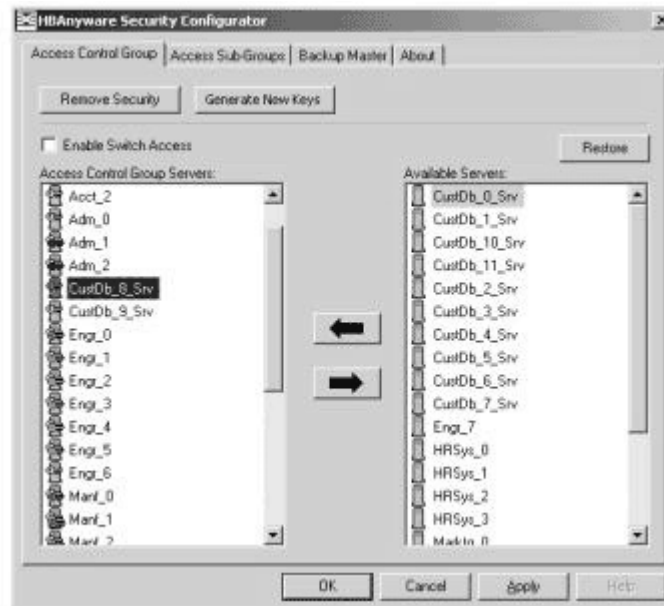


Figure 55: Security Configurator, Access Control Group Tab

2. On the Access Control Group tab, click the **Generate New Keys** button. A dialog box warns you that you are about to generate new security keys for all systems.
3. Click **Yes**. The new keys are generated and sent to all of the remote servers in the ACG.

Restoring the ACG to Its Last Saved Configuration

You can restore the ACG to its last saved configuration, if there are unsaved changes to the ACG, only from the Master Security Client (MSC).

To restore the ACG to its last saved configuration:

1. From the Access Control Group tab on the MSC, click the **Restore** button.

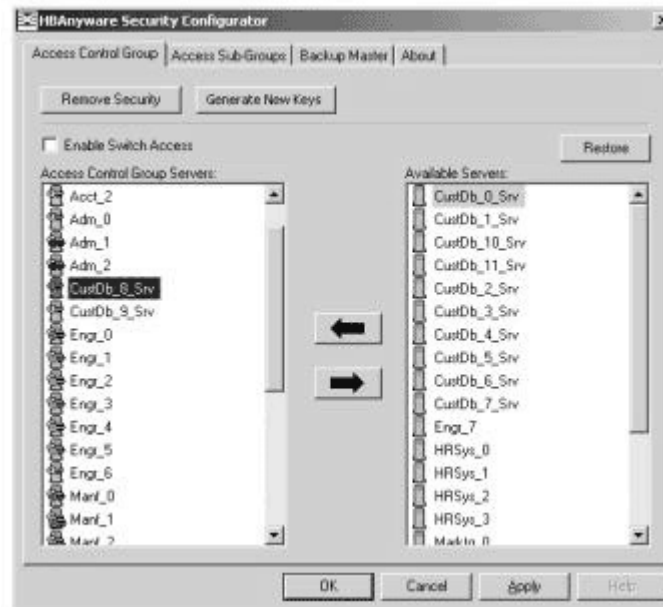


Figure 56: Security Configurator, Access Control Group Tab

Accessing a Switch

You can enable switch access only on a Master Security Client (MSC). Switch access grants the client access rights to a switch to remotely access HBAs on servers in the Access Control Group (ACG).

To enable switch access:

1. Start the HBAnyware Security Configurator.
2. From the Access Control Group tab, check **Enable Switch Access**.

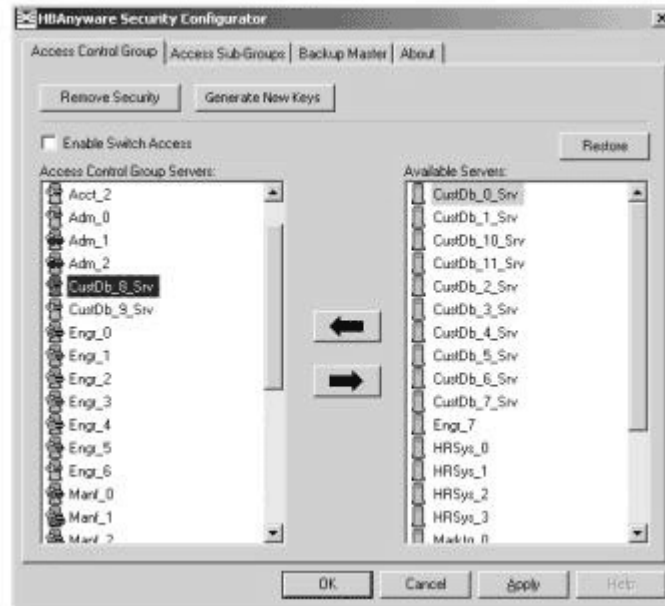


Figure 57: Security Configurator, Access Control Group Tab

Access Sub-Groups

Introduction

The Access Sub-Group tab allows you to create multiple Access Sub-Groups (ASGs) and multiple levels (tiers) in the security topology hierarchy. The hierarchy can be as many levels deep as desired. However, it is recommended the hierarchy extend no more than three levels deep, as it becomes increasingly difficult to keep track of the topology the deeper it goes. The hierarchy of ASGs is displayed in the Access Sub-Groups tab as a tree. You can create, modify and delete ASGs at each level in this tree

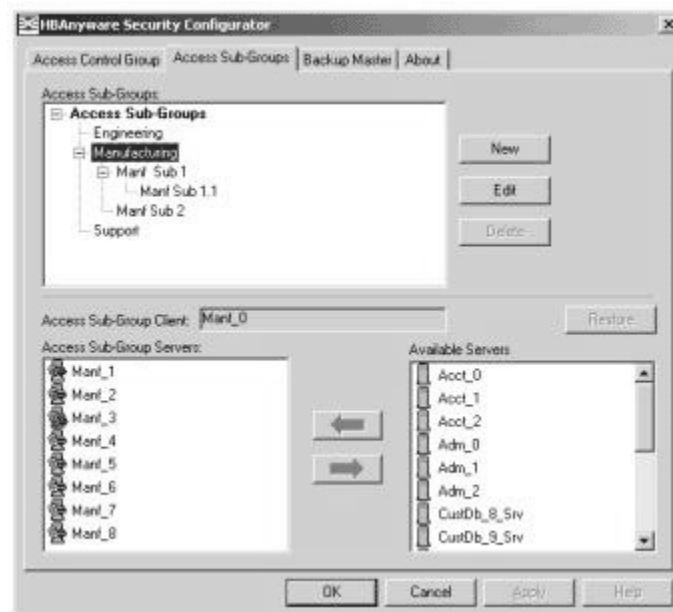


Figure 58: Security Configurator, Access Sub-Groups Tab with Servers

ASG Icons

The following icons indicate the state of each of the servers in the Access Sub-Group Servers list.



The system is a server in the ASG but not in any child ASGs. You can remove it from the ASG.



The system is a server in the ASG and at least one child ASG. You cannot remove it from the ASG until you remove it from the child ASGs.



The system is a server in the ASG and a client to a child ASG. You cannot remove it from the ASG until you remove it as a client from the child ASG (by either deleting or editing the child ASG).



The system is a server in the ASG, a server in at least one other child ASG and a client to a child ASG. You cannot remove it from the ASG until you remove it from the child ASGs and as a client from the child ASG (by either deleting or editing the child ASG).



The system is a server in the ASG and a client to a non-child ASG. You can remove it from the ASG.



The system is a server in the ASG, a server in at least one child ASG, and a client to a non-child ASG. You cannot remove it from the ASG until you remove it from the child ASGs.

Creating an ASG

You create a new Access Sub-Group (ASG) by selecting one system from the Access Control Group (ACG) to be the client, and some or all of the other systems to be servers to this client, thus defining the new client's ACG. When the HBAAnyware Security Configurator is run on the new client, the displayed ACG shows the servers that were configured in the ASG by its parent client.

To create an ASG:

1. Start the HBAAnyware Security Configurator.
2. Click the Access Sub-Groups tab.

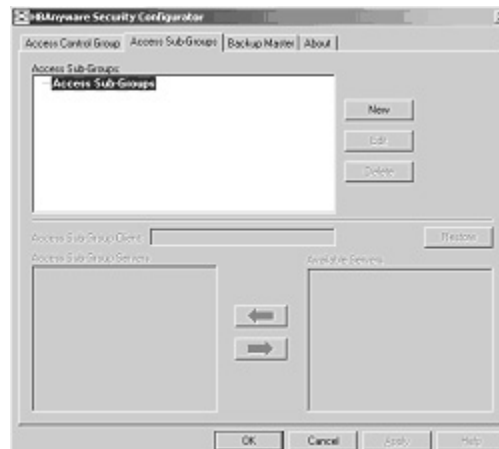


Figure 59: Security Configurator, Access Control Group Tab (new)

3. Click **New**. The New Access Sub-Group dialog box is displayed.

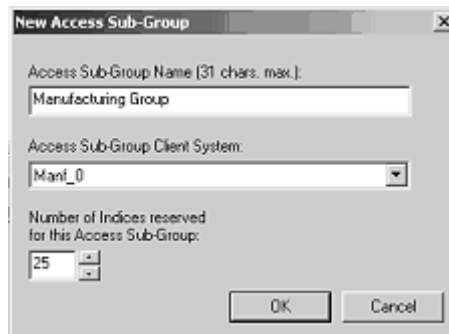


Figure 60: Security Configurator, New Access Sub-Group Window

4. Enter the ASG information:
 - Access Sub-Group Name: Enter the name of the ASG. The ASG name is for identification purposes only. It does not provide any security function. Provide a name that will make it easy to remember the systems that are part of the ASG. The name can contain any alphanumeric characters, symbols or spaces (up to 31). At each level of the security topology, each ASG name must be unique. If the name is not unique at its level, an error message informs you of this when you click **OK**.
 - Access Sub-Group Client System: Select the system that is to be the client.
 - Number of indices reserved for this Access Sub-Group: Select the number of 'indices' you want to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that can subsequently be created on the new client's system. See the Reserved Indices topic (under Access Sub-Groups in this manual) for examples.

5. Click **OK** in the New Access Sub-Group dialog box. The ASG is created. The following process sets up the ASG (see Figure 61)
 - a. The SSC utility runs.
 - b. A new ASG is created with Systems 2 and 15 as clients.
 - c. A new SA_ID is selected for System 2, and a new SA_ID is selected for System 15.
 - d. SA file updates are sent to each system in the ASGs. In Figure 61, System 2 has remote access to systems 3 through 9. System 15 has remote access to systems 8 through 15. System 2 and System 15 have remote access to systems 8 and 9.

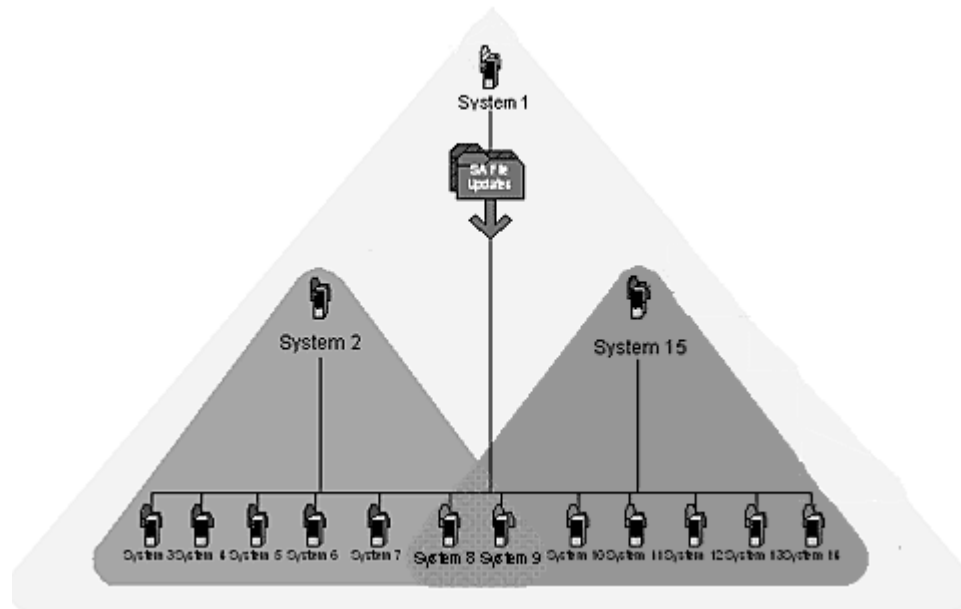


Figure 61: ASG Creation Example

Reserved Indices - Examples

A particular security installation can support the creation of several hundred access groups (ACGs and ASGs). When you create each new access group, you allocate some number of 'indices' to the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that can subsequently be created at the new client's system.

- If zero indices are reserved, you cannot create any lower-level ASG under the client of the new ASG. Thus, for example, if you want to implement a multi-tiered security architecture consisting of many ASGs, and you wanted to create them all from the Master Security Client (MSC), zero indices would be allocated to each of the new ASGs client platforms when they are created.
- If you create an ASG, and you reserve 25 indices for the new ASG client platform, a child ASG created by this platform will have a maximum of only 24 indices available to be reserved (one is taken by the creation of the child ASG itself). This continues down the ASG hierarchy as each lower level ASG is created.
- When you create an ASG from the MSC, a maximum of 50 indices (or less if fewer are available) can be reserved. For all other clients, the maximum depends on how many indices were reserved to that client when its ASG was created, and on how many it has subsequently allocated to its ASGs.

Adding a Server to an ASG

To add a server to an ASG:

1. Start the HBAnyware Security Configurator.
2. Click the Access Sub-Group tab.

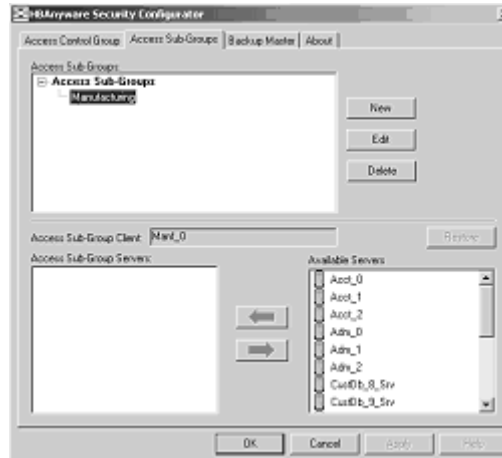


Figure 62: Security Configurator, Access Sub-Groups Tab with Available Servers

3. The name of the ASG is displayed in the Access Sub-Groups tree. From the Available Servers list, select the servers to be added to the ASG.
4. Click the **left arrow** to move the servers to the Access Sub-Group Servers list.
5. Click **OK** or **Apply** to update servers, adding them to the ASG. The new client can remotely manage the HBAs on those servers using the HBAnyware utility.

Deleting an ASG

Only a leaf node ASG may be deleted (i.e. not ASGs underneath it in the tree). If an ASG has at least one child ASG, those child ASGs must be deleted first.

To delete an ASG:

1. From the Access Sub-Group tree, select the leaf node ASG you wish to delete.
2. Click the **Delete** button. A dialog box appears warning you that if you continue the access sub-group will be deleted.
3. Click **Yes**. This operation is immediate. There is no need to click the **OK** or **Apply** button under the tab.

Restoring an ASG to Its Last Saved Configuration

You can restore an ASG to its last saved configuration if there are unsaved changes to it.

To restore an ASG to its last saved configuration:

1. Click the Access Sub-Group tab.

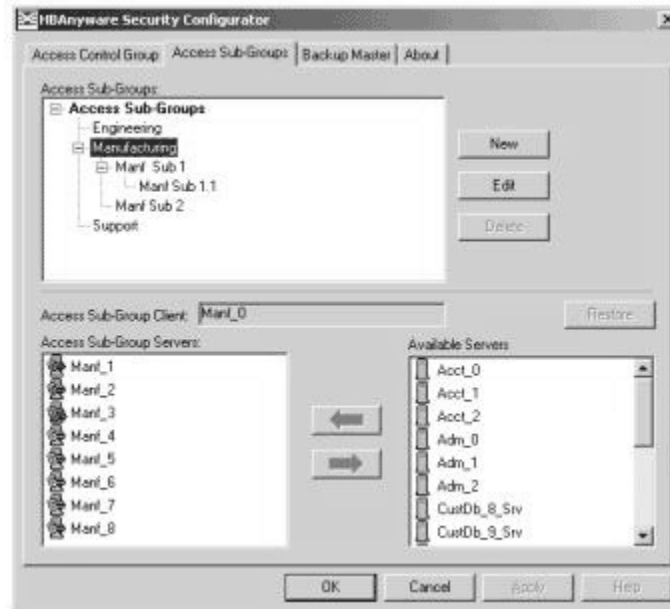


Figure 63: Security Configurator, Access Sub-Groups Tab with Available Servers

2. Select the ASG whose configuration you want to restore.
3. Click **Restore**.
4. Click **OK** or **Apply** to save your changes.

Editing an ASG

You can change the name, client system or reserved indices of an Access Sub-Group (ASG).

To edit an ASG:

1. Start the HBAware Security Configurator.
2. Click the Access Sub-Group tab.



Figure 64: Security Configurator, Access Sub-Groups Tab with Available Servers

3. Select the ASG you want to edit.
4. Click **Edit**. The Edit Access Sub-Group dialog box is displayed.

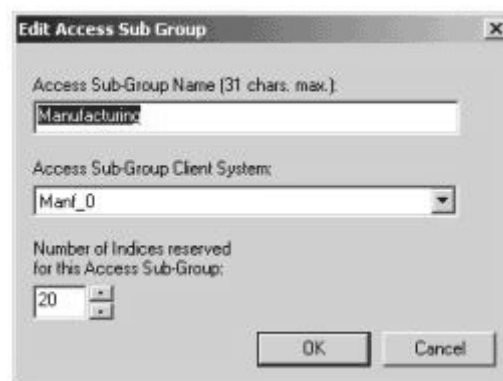


Figure 65: Security Configurator, Edit Access Sub Group Dialog Box

5. Change the ASG information:
 - Access Sub-Group Name: Change the name of the ASG. The ASG name is for identification purposes only. It does not provide any security function. Provide a name that will make it easy to remember the systems that are part of the ASG. The name can contain any alphanumeric characters, symbols or spaces (up to 31). At each level of the security topology, each ASG name must be unique. If the name is not unique at its level, an error message informs you of this when you click **OK**.
 - Access Sub-Group Client System: Select the new system that is to be the client. If the Configurator is running on a system connected to more than one fabric, the client list contains only those systems that can be accessed by the original client of the ASG.
 - Number of indices reserved for this Access Sub-Group: Select the new number of 'indices' you want to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that can subsequently be created on the new client's

system. See the Reserved Indices topic (under Access Sub-Groups in this manual) for examples.

6. Click **OK** in the Edit Access Sub-Group dialog box to save your changes.

About Offline ASGs

Sometimes a client system may not be online when the HBAAnyware Security Configurator is running. In this case, the Access Sub-Group (ASG) for the client appears offline in the ASG tree, much like the following:

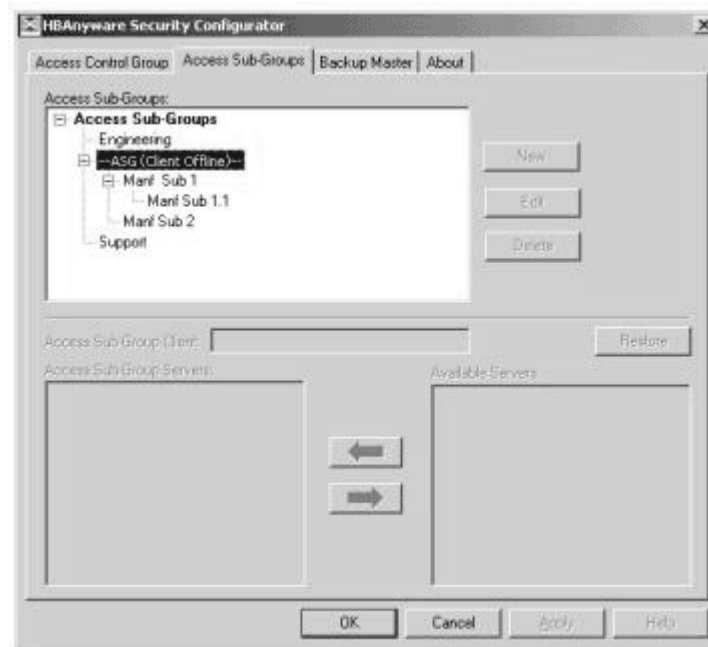


Figure 66: Security Configurator, Access Sub-Groups Tab with Offline Client

The offline ASG entry serves as a placeholder for where the real ASG would be in the tree. You cannot modify or delete the entry (although it is removed from the display if all of its child ASGs are deleted).

It is possible to delete the child ASGs of an offline ASG. However, it is recommended that you delete them only if the client for the offline ASG will never be put online again. It is best to delete child ASGs when the parent ASG is online.

If you choose to delete a child ASG, the operation is immediate. There is no need to click **OK** or **Apply**.

Backup Masters

Introduction

A Backup Master mirrors the security data of the Master Security Client (MSC) in case it has to take over as the MSC if the MSC becomes unable to operate or is removed from the security configuration. A Backup master system receives all the updates to the security configuration on the MSC. However, you cannot make modifications to the security configuration on a Backup Master.

When the Configurator runs on a Backup Master, the Access Control Group tab looks like the tab on a non-MSC system. The Access Sub-Group tab displays the ASGs, but you cannot change the ASGs.

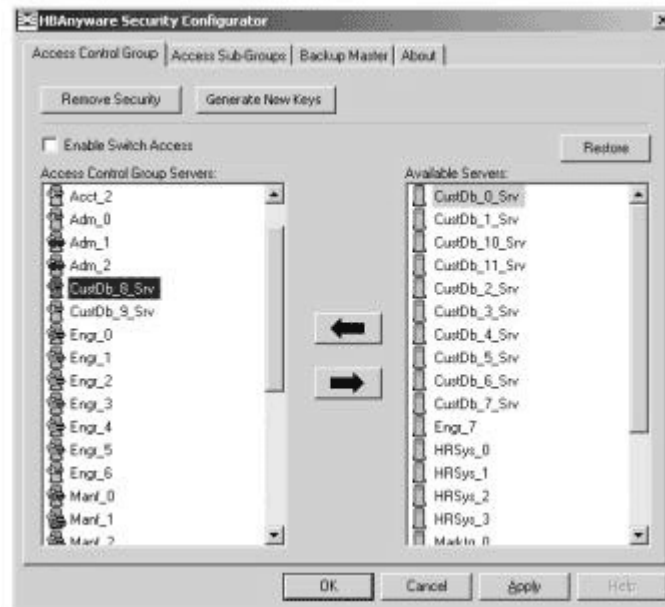


Figure 67: Security Configurator, Access Control Group Tab

The Backup Master tab is available only when the HBAAnyware Security Configurator is running on the MSC or a Backup Master. Use this tab to set up a system as a Backup Master to the MSC and to replace the MSC with a Backup Master.

Each time the HBAAnyware Security Configurator is started on the MSC and no Backup Master is assigned, a message warns you that no Backup Master Client is assigned to the security configuration.

If you run the HBAAnyware Security Configurator on a Backup Master, a message warns you that you can only view security information on a Backup Master. Security changes must be made to the MSC.

Because a Backup Master system receives all the updates that the MSC makes to the security configuration, it is very important that the Backup Master is online when the HBAAnyware Security Configurator is running on the MSC. Otherwise, updates to the security configuration are not reflected to the Backup Master. If the Backup Master then becomes the MSC, the security configuration may be corrupted.

Backup Master Eligible Systems

In order to be eligible to become a Backup Master, a system must not be a client or server in any ASG. In other words, it must be either a server in the MSC's Access Control Group (ACG) or an unsecure system. If it is an unsecure system, it will be secure when it becomes a Backup Master.

Backup Master Tab and Controls

The first time the Backup Master tab is selected on the MSC, it looks similar to the following:

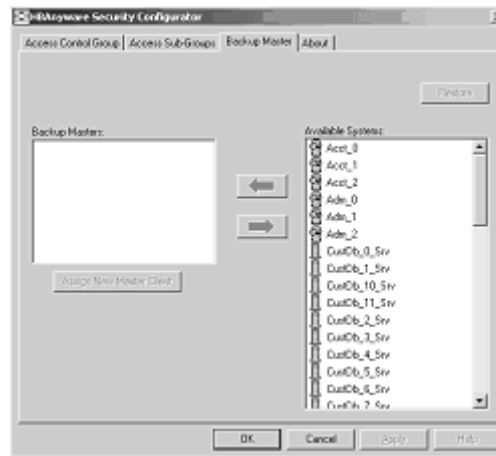


Figure 68: Security Configurator, Backup Master Tab (initial view)

Creating a Backup Master

To create a Backup Master:

1. On the Master Security Client (MSC), start the HBAware Security Configurator.
2. Click the Backup Master tab.

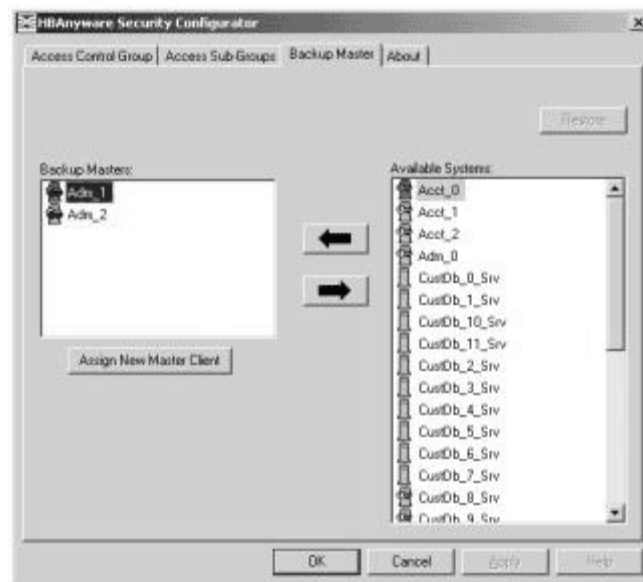


Figure 69: Security Configurator, Backup Master Tab with Backup Master Selected

3. Select a system from the Available Systems list.
4. Click the **left arrow** to move the system to the Backup Masters list.
5. Click **OK** or **Apply** to save your changes. The backup master is created. The following process sets up the backup master (see Figure 70)

- a. The SSC utility runs.
- b. Discovery finds System 16.
- c. The SA File is sent to System 16 with the correct SA_ID set for server access.

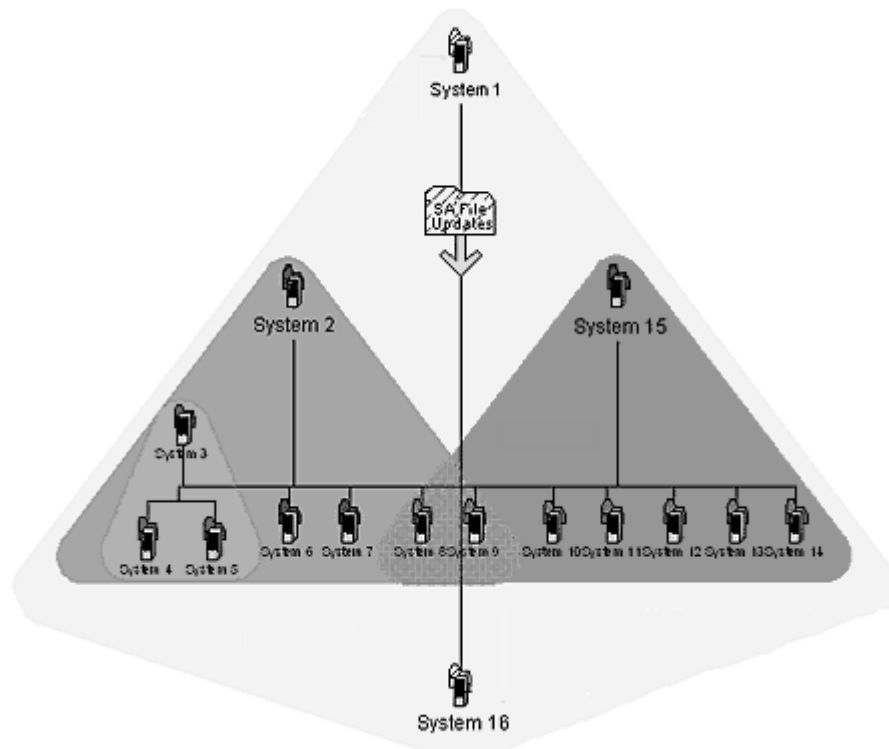


Figure 70: System16 as Backup Master

Reassigning a Backup Master as the New MSC from the Old MSC

Because a Backup Master may have to take over as the Master Security Client (MSC), it should be able to physically access all of the HBAs that the MSC can access. If the MSC is connected to multiple fabrics, its Backup Master should be selected from the Available Systems list that is connected to the same fabrics as the MSC.

To reassign a Backup Master as the new MSC from the old MSC:

1. On the MSC, start the HBAnyware Security Configurator.

2. Click the Backup Master tab.

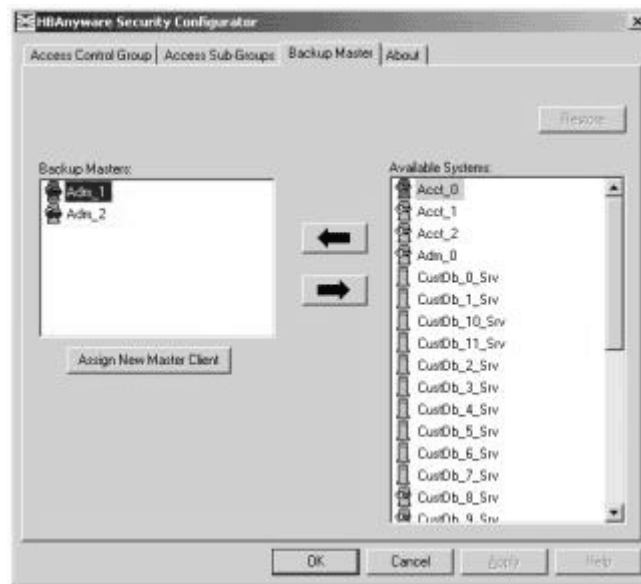


Figure 71: Security Configurator, Backup Master Tab with Backup Master Selected

3. In the Backup Masters list, select the Backup Master system that you want to reassign as the MSC.
4. Click **Assign New Master Client**. You will be asked if you wish to proceed.
5. Click **Yes**. The selected Backup Master becomes the new MSC. The current MSC becomes a server in the new MSC's ACG. After the changes are made, a message indicates that the reassignment is complete.
6. Click **OK**. The Configurator closes because the system is no longer the MSC.

Reassigning a Backup Master as the New MSC from the Backup Master

WARNING: Use this method only if the MSC cannot relinquish control to a Backup Master. For example, if the MSC is no longer bootable or able to connect to the Fibre Channel network. Under any other circumstances, if the Backup Master takes over as the MSC, and the MSC is still running or comes back online later, there will be two MSCs for the same security configuration. This will eventually lead to corruption of the security configuration.

To reassign a Backup Master as the new MSC from the Backup Master:

1. On the Backup Master system that you want to reassign as the MSC, start the HBAnyware Security Configurator.
2. Click the Backup Master tab.



Figure 72: Security Configurator, Backup Master "Warning" Dialog Box

3. Click **Assign This System As The Master Client**. A prompt asks if you want to continue.
4. Click **Yes**. A prompt notifies you that this system is now the new MSC.
5. Click **OK**. The Configurator closes. Restart the HBAnyware Security Configurator to run the former Backup Master as the MSC.

Using the emlxadm Utility

The emlxadm utility is a direct user interface to the FCIO interface provided by the Sun StorEdge Solaris SFS. The FCIO interface provides a Sun common ioctl interface to the FCTL, which manages the FCA drivers for each FC HBA attached to the host system.

Modes of Operation (emlxadm)

The emlxadm utility program can be run in two modes:

- Interactive
- Command line interface (CLI)

Interactive Mode (emlxadm)

The emlxadm utility program can be run in an interactive command mode by typing the name of the program without any command line arguments. For example:

```
# emlxadm
```

After it is started, the emlxadm program scans the host system and prepares a list of qualified HBA ports to choose from. Qualified HBA ports are devices that attach to the SUN StorEdge Solaris SFS through the FP driver. After the list is prepared, the utility displays the following information:

```
EMLXADM Device Management Utility, Version 1.00r
COPYRIGHT © 2004-2006 Emulex. All rights reserved.
```

```
Available HBA's:
```

1. /devices/pci@1e,600000/SUNW,qlc@3/fp@0,0:devctl (CONNECTED)
2. /devices/pci@1e,600000/SUNW,qlc@3,1/fp@0,0:devctl (NOT CONNECTED)
3. /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl (CONNECTED)
4. /devices/pci@1e,600000/SUNW,emlxs@2,1/fp@0,0:devctl (NOT CONNECTED)

```
Enter an HBA number or zero to exit:
```

You must choose from one of the available HBAs in the list by entering the appropriate number. In this example, if you enter 3, the utility displays the HBA device name selected and presents a list of command options:

```
HBA: /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl
```

```
Available commands:
```

```
[rev 2]
```

```
get_num_devs - Returns the number of FC devices seen by this HBA.
get_dev_list - Returns a list of FC devices seen by this HBA.
get_logi_params <wwpn> - Returns the login parameters for a specified FC device.
get_host_params - Return the host parameters.
get_sym_pname - Returns the symbolic port name of a device.
set_sym_pname <string> - Sets the symbolic port name for a device.
get_sym_nname - Returns the symbolic node name of a device.
set_sym_nname <string> - Sets the symbolic node name for a device.
dev_login <wwpn> - Performs an FC login to a device.
dev_logout <wwpn> - Performs an FC logout to a device.
get_state <wwpn> - Returns current Leadville state of a specified device.
dev_remove <wwpn> - Remove the FC device from Leadville management.
link_status <d id> - Request link error status from a specified D_ID.
get_fcode_rev - Returns the current Fcode revision of the HBA.
download_fcode [filename] - Download the HBA fcode.
get_fw_rev - Returns the current firmware revision of the HBA.
download_fw [filename] - Download the HBA firmware.
get_boot_rev *Returns the current boot revision of the HBA.
download_boot [filename] *Download the HBA boot image.
get_dump_size - Returns the HBA's firmware core dump size.
force_dump - Force a firmware core dump on this HBA.
get_dump <-t,-b> <file> - Saves firmware core dump to a file.
get_topology - Returns the current FC network topology.
```

```
reset_link <wwpn,0> - Resets the link of a specified FC device.
reset_hard - Reset the HBA.
reset_hard_core - Reset the HBA firmware core.
diag <test> - Perform a diagnostic test on the HBA.
ns - Performs a complete query of the fabric name server.
parm_get_num - *Returns the total number of configurable parameters.
parm_get_list - *Returns a list of configurable parameters.
parm_get <label> - *Gets the value of a specified parameter in the driver.
parm_set <label> <val> - *Sets the value of a specified parameter in the driver.
msgbuf all or <number> [-i interval] - *Returns the driver's internal message
log.
get_host_attrs - Returns the host adapter and port attributes.
get_port_attrs <index>, <wwn> or all - Returns the port attributes.
get_path <index> - Returns the adapter path.
get_vpd - *Returns the adapter's Vital Product Data (VPD).
boot_code [enable or disable] - *Sets or shows the boot code state in this HBA.
q - Exits this program.
h - Returns this help screen.
hba - Select another hba.
p - Repeat previous command.
```

*Emulex adapters only

emlxadm>

At the bottom of the command list is an emlxadm> prompt. From this point, the utility is prompt driven. When the prompt is displayed, you must enter one of the commands in the list. The list is displayed automatically only once, but you can display it again by entering <h> at the prompt. To exit the program, enter <q>.

Some commands require additional arguments, such as a FC World Wide Port Name (WWPN) or a FC port address (D_ID). To display the available arguments for a command, enter the command without any arguments.

For example, the command get_state requires a WWPN for the target device. If only the command without the argument is entered, the following statement appears to indicate that the command requires an argument to be executed. For example:

```
emlxadm> get_state
Usage: get_state <wwpn>
emlxadm> get_state 21000020371938fa
State: PORT_DEVICE_LOGGED_IN
```

For a detailed explanation of each command and its arguments, see *Command Descriptions (emlxadm)* on page 107.

CLI Mode (emlxadm)

You can run the emlxadm utility program in CLI mode by typing the name of the program, followed by the full device name of the desired HBA (or a pattern string for multiple HBAs), followed by a valid command and any required command arguments. In the following example, the emlxadm utility pauses to ask if you want to continue before executing the command. To specify a full device name, type:

```
# emlxadm /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl get_state
21000020371938fa
```

Information similar to the following is displayed:

```
Found path to 1 HBA port(s).
HBA port: /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl
>Do you wish to continue with this device [y,n,q] ? y <---Response required
State: PORT_DEVICE_LOGGED_IN
```


#

If you do not want the utility to pause for verification, add a "-y" option just after the device path, and the emlxadm utility will skip the verification. For example:

```
# emlxadm /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl -y get_state
21000020371938fa
```

Information similar to the following is displayed:

```
Found path to 1 HBA port(s).
HBA port: /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl
State: PORT_DEVICE_LOGGED_IN
```

#

If you want to run a command on multiple HBAs at once, you can use a pattern string instead of a full device path. If the entire pattern string matches any part of an HBA device path, the command will execute against that HBA. Again, in this example the emlxadm utility pauses to ask if you want to continue before executing the command. For example:

```
# emlxadm "SUNW,emlxs@2" get_num_devs
```

Information similar to the following is displayed:

```
Found path to 2 HBA port(s).
HBA port: /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl
> Do you wish to continue with this device [y,n,q] ? y <--- Response
required
```

There are 5 devices reported on this port.

```
HBA port: /devices/pci@1e,600000/SUNW,emlxs@2,1/fp@0,0:devctl
> Do you wish to continue with this device [y,n,q] ? y <--- Response
required
```

There are 0 devices reported on this port.

#

If you do not want the utility to pause for verification, add a "-y" option just after the pattern string, and the emlxadm utility will skip the verification. For example:

```
# emlxadm "SUNW,emlxs@2" -y get_num_devs
```

Information similar to the following is displayed:

```
Found path to 2 HBA port(s).
HBA port: /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl
```

There are 5 devices reported on this port.

```
HBA port: /devices/pci@1e,600000/SUNW,emlxs@2,1/fp@0,0:devctl
```

There are 0 devices reported on this port.

#

This mode of operation enables you to use the emlxadm utility as part of a script or another program capable of executing system level calls.

Command Descriptions (emlxadm)

This section provides a list of commands and descriptions that can be issued with the emlxadm utility.

get_num_devs

Returns the number of FC devices currently seen by this HBA port.

Example:

```
emlxadm> get_num_devs

There are 4 devices reported on this port.
```

get_dev_list

Returns a list of FC devices currently seen by this HBA port.

Example:

```
emlxadm> get_dev_list

-----
Device 0:
  Dtype: 0
  FC4_type[proto]: 0x00000100, 0x00000000, 0x00000000, 0x00000000, 0x00000000,
  0x00000000, 0x00000000, 0x00000000
  State: Logged_In
  D_id: 113e1
  LILP: 0
  Hard Addr: e1
  WWPN: 21000020371938fa
  WWNN: 20000020371938fa

-----
Device 1:
  Dtype: 0
  FC4_type[proto]: 0x00000100, 0x00000000, 0x00000000, 0x00000000, 0x00000000,
  0x00000000, 0x00000000, 0x00000000
  State: Logged_In
  D_id: 113e2
  LILP: 0
  Hard Addr: e2
  WWPN: 21000020371939a2
  WWNN: 20000020371939a2

-----
Device 2:
  Dtype: 0
  FC4_type[proto]: 0x00000100, 0x00000000, 0x00000000, 0x00000000, 0x00000000,
  0x00000000, 0x00000000, 0x00000000
  State: Logged_In
  D_id: 113e4
  LILP: 0
  Hard Addr: e4
  WWPN: 21000020371938a3
  WWNN: 20000020371938a3

-----
Device 3:
  Dtype: 0
  FC4_type[proto]: 0x00000100, 0x00000000, 0x00000000, 0x00000000, 0x00000000,
  0x00000000, 0x00000000, 0x00000000
  State: Logged_In
  D_id: 113e8
  LILP: 0
  Hard Addr: e8
  WWPN: 2100002037193670
  WWNN: 2000002037193670
```

get_logi_params <wwpn>

Returns the FC login common service parameters for a specified FC device on the network.

Example:

```
emlxadm> get_logi_params 21000020371938fa
```

Login Parameters:

```
00 00 00 00
20 20 00 00
88 00 08 00
00 ff 00 02
00 00 01 f4
21 00 00 20
37 19 38 fa
20 00 00 20
37 19 38 fa
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
80 00 00 00
00 00 08 00
00 ff 00 00
00 01 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
00 00 00 00
```

get_host_params

Returns the FC login parameters of this HBA port.

Example:

```
emlxadm> get_host_params
```

Host:

```
      Dtype: 0
FC4_type[proto]: 0x00000120, 0x00000000, 0x00000000, 0x00000000, 0x00000000,
0x00000000, 0x00000000, 0x00000000
      State: Online
      Linkspeed: 1Gb
      D_id: 11700
      LILP: 5
Hard Addr: 0
      WWPN: 10000000c942097e
      WWNN: 20000000c942097e
```

get_sym_pname

Returns the symbolic FC port name of the HBA port.

Note: This operation is currently not supported by the Solaris Leadville stack.

Example:

```
emlxadm> get_sym_pname
ioctl: FCIO_GET_SYM_PNAME: Operation not supported
```

set_sym_pname <"string">

Sets the symbolic FC port name of the HBA to the string provided.

Note: This operation is currently not supported by the Solaris Leadville stack.

Example:

```
emlxadm> set_sym_pname "Emulex Corporation"
ioctl: FCIO_SET_SYM_PNAME: Operation not supported
```

get_sym_nname

Returns the symbolic FC node name of the HBA port.

Note: This operation is currently not supported by the Solaris Leadville stack.

Example:

```
emlxadm> get_sym_nname
ioctl: FCIO_GET_SYM_NNAME: Operation not supported
```

set_sym_nname <"string">

Sets the symbolic FC node name of the HBA to the string provided.

Note: This operation is currently not supported by the Solaris Leadville stack.

Example:

```
emlxadm> set_sym_nname "Emulex Corporation"
ioctl: FCIO_SET_SYM_NNAME: Operation not supported
```

dev_login <wwpn>

Performs an FC login to an FC device on the network, if not already logged in.

Example:

```
emlxadm> dev_login 21000020371938fa
Done.
```

dev_logout <wwpn>

Performs an FC logout to an FC device on the network, if not already logged in.

Example:

```
emlxadm> dev_logout 21000020371938fa  
Done.
```

get_state <wwpn>

Returns the current Leadville state of the specified FC device on the network.

Example:

```
emlxadm> get_state 21000020371938fa  
State: PORT_DEVICE_LOGGED_IN
```

dev_remove <wwpn>

Removes the specified FC device from Leadville management.

WARNING: This command is currently not properly supported in the Leadville stack and will cause the host operating system to panic.

link_status <d_id>

Requests and returns the current link error status from the FC device specified by the d_id address.

Example:

```
emlxadm> link_status e8  
D_ID: e8  
      Link failures: 3 (0x3)  
      Loss of sync count: 12 (0xc)  
      Loss of signal count: 0 (0x0)  
      Primitive sequence errors: 0 (0x0)  
      Invalid tx words: 17 (0x11)  
      Invalid CRC count: 0 (0x0)
```

get_fcode_rev

Returns the current FCode revision of the HBA.

Example:

```
emlxadm> get_fcode_rev  
FCODE revision: LP10000-S 1.41a3
```

download_fcode <filename>

Downloads the specified FCode image file to the HBA.

Example:

```
emlxadm> download_fcode LP10000DC-S.fcode

Image Components: REL type    size=33848
                  DWC file:    BOOT: version=03841512, 1.50a2

Current: Fcode: 1.50a1
New:      Fcode: 1.50a2    33848 (0x8438) bytes

Are you sure you want to download this image? (y or n): y

Downloading...

Result: Operation successful.
Done.
```

Note: If the file name is not provided, the program attempts to identify the adapter model, then downloads a default FCode image file, if one is available.

get_fw_rev

Returns the current firmware revision of the HBA.

Example:

```
emlxadm> get_fw_rev

Firmware revision: LP10000DC-S 1.90a3
```

download_fw <filename>

Downloads the specified firmware image file to the HBA.

Example:

```
emlxadm> download_fw LP10000DC-S.fw

Image Components: NOP type
  AWC file:      KERN: version=ff801315, 1.30a5
  DWC file:      SLI2: version=07831914, 1.90a4
  DWC prog:      TEST: version=00f51010, 1.00a0
  DWC prog:      STUB: version=02881914, 1.90a4
  DWC prog:      SLI1: version=06831914, 1.90a4
  DWC prog:      SLI2: version=07831914, 1.90a4

Current: Firmware: 1.90a3
New:      Firmware: 1.90a4  366712 (0x59878) bytes

Are you sure you want to download this image? (y or n): y

Downloading...

Done.
```

Note: If the file name is not provided, the program attempts to identify the adapter model, then downloads a default firmware image file, if one is available.

get_boot_rev

Returns the current boot revision of the HBA.

Example:

```
emlxadm> get_boot_rev  
  
Firmware revision: LP10000DC-S 1.90a3
```

download_boot <filename>

Downloads the specified boot image file to the HBA.

Example:

```
emlxadm> download_boot TD190A4.PRG  
  
Image Components: REL type    size=143416  
DWC file:        BOOT: version=03845054, 1.90a4  
  
Current: Boot: 1.90a3  
New:      Boot: 1.90a4    143416 (0x23038) bytes  
  
Are you sure you want to download this image? (y or n): y  
  
Downloading...  
  
Done.
```

Note: If the file name is not provided, the program attempts to identify the adapter model, then downloads a default boot image file, if one is available.

get_dump_size

Returns the byte size of the HBA's firmware core dump buffer.

Example:

```
emlxadm> get_dump_size  
  
Size: 256 (0x100) bytes
```

force_dump

Forces the HBA to perform a firmware core dump to the core dump buffer.

Example:

```
emlxadm> force_dump  
  
Done.
```

get_dump <-t filename.txt or -b filename.bin>

Returns a copy of the HBA's firmware core dump buffer to the specified file in the specified text (-t) or binary (-b) format.

Example:

```
emlxadm> get_dump -t mydump.txt  
  
Done.
```

The following is an example of the text file created by this operation. The binary version of the file has the binary pattern indicated without the column or row labels and white spaces.

mydump.txt

```

-----
      00 01 02 03    04 05 06 07    08 09 0A 0B    0C 0D 0E 0F
-----
00000000: 00 01 02 03    04 05 06 07    08 09 0a 0b    0c 0d 0e 0f
00000010: 10 11 12 13    14 15 16 17    18 19 1a 1b    1c 1d 1e 1f
00000020: 20 21 22 23    24 25 26 27    28 29 2a 2b    2c 2d 2e 2f
00000030: 30 31 32 33    34 35 36 37    38 39 3a 3b    3c 3d 3e 3f
00000040: 40 41 42 43    44 45 46 47    48 49 4a 4b    4c 4d 4e 4f
00000050: 50 51 52 53    54 55 56 57    58 59 5a 5b    5c 5d 5e 5f
00000060: 60 61 62 63    64 65 66 67    68 69 6a 6b    6c 6d 6e 6f
00000070: 70 71 72 73    74 75 76 77    78 79 7a 7b    7c 7d 7e 7f
00000080: 80 81 82 83    84 85 86 87    88 89 8a 8b    8c 8d 8e 8f
00000090: 90 91 92 93    94 95 96 97    98 99 9a 9b    9c 9d 9e 9f
000000a0: a0 a1 a2 a3    a4 a5 a6 a7    a8 a9 aa ab    ac ad ae af
000000b0: b0 b1 b2 b3    b4 b5 b6 b7    b8 b9 ba bb    bc bd be bf
000000c0: c0 c1 c2 c3    c4 c5 c6 c7    c8 c9 ca cb    cc cd ce cf
000000d0: d0 d1 d2 d3    d4 d5 d6 d7    d8 d9 da db    dc dd de df
000000e0: e0 e1 e2 e3    e4 e5 e6 e7    e8 e9 ea eb    ec ed ee ef
000000f0: f0 f1 f2 f3    f4 f5 f6 f7    f8 f9 fa fb    fc fd fe ff
00000100:

```

get_topology

Returns the FC network topology of the HBA port.

Example:

```

emlxadm> get_topology

Topology: PRIVATE_LOOP

```

reset_link <wwpn or zero for local link>

Resets the local link, if zero is specified, or the link of a specified FC device on the network.

Example:

```

emlxadm> reset_link 0

Done.

```

or

```

emlxadm> reset_link 21000020371938fa

Done.

```

reset_hard

Forces the HBA to perform a hardware reset.

Example:

```

emlxadm> reset_hard

Done.

```


reset_hard_core

Forces the HBA to perform a core firmware reset.

Example:

```
emlxadm> reset_hard_core  
  
Done.
```

diag <test [parameters]> or diag code <cmd_code (hex)>

Performs the specified diagnostics function or command code on the HBA port. This command provides support for the Emulex-specific tests shown below, or generic support to issue an HBA-specific diagnostic code (in hexadecimal) to any third party HBA.

Tests:

```
emlx_biu [pattern]           - Performs the Bus Interface Unit test.  
emlx_echo <did> [pattern]    - Performs the ECHO test to a specified port id.  
emlx_post                    - Performs the Power-On Self Tests.
```

Parameters:

pattern - 4 byte hex pattern to be used for test. (e.g. 0xA5A5A5A5)

Example:

```
emlxadm> diag emlx_biu  
  
Result: EMLX_DIAG_BIU: Operation successful.
```

or

```
emlxadm> diag emlx_echo fffffffc  
  
Result: EMLX_DIAG_ECHO: Operation successful.
```

or

```
emlxadm> diag emlx_post  
  
Result: EMLX_DIAG_POST: Operation successful.
```

Example:

```
emlxadm> diag code 0x4526  
  
Result: CODE(0x4526): 16 (0x10)
```

Note: The return status from the HBA is displayed in decimal and hexadecimal if the diagnostic code is valid for the HBA. No interpretation of the return status is provided.

ns

Performs and returns a complete query of the fabric name server.

Example:

```
emlxadm> ns

Nameserver:
-----
      TYPE: Lport
      PID: 0113E1
      WWPN: 21000020371938fa
PORT_NAME: (SEAGATE ST39103FC      0004)
      WNNN: 20000020371938fa
NODE_NAME: (null)
      IPA: ffffffffffffffff
      IP_ADDR: 0.0.0.0
      CLASS: Class3
FC4_TYPES:
00000100,00000000,00000000,00000000,00000000,00000000,00000000,00000000
-----
      TYPE: Lport
      PID: 0113E2
      WWPN: 21000020371939a2
PORT_NAME: (SEAGATE ST39103FC      0004)
      WNNN: 20000020371939a2
NODE_NAME: (null)
      IPA: ffffffffffffffff
      IP_ADDR: 0.0.0.0
      CLASS: Class3
FC4_TYPES:
00000100,00000000,00000000,00000000,00000000,00000000,00000000,00000000
-----
      TYPE: Lport
      PID: 0113E4
      WWPN: 21000020371938a3
PORT_NAME: (SEAGATE ST39103FC      0004)
      WNNN: 20000020371938a3
NODE_NAME: (null)
      IPA: ffffffffffffffff
      IP_ADDR: 0.0.0.0
      CLASS: Class3
FC4_TYPES:
00000100,00000000,00000000,00000000,00000000,00000000,00000000,00000000
-----
      TYPE: Lport
      PID: 0113E8
      WWPN: 2100002037193670
PORT_NAME: (SEAGATE ST39103FC      0004)
      WNNN: 2000002037193670
NODE_NAME: (null)
      IPA: ffffffffffffffff
      IP_ADDR: 0.0.0.0
      CLASS: Class3
FC4_TYPES:
00000100,00000000,00000000,00000000,00000000,00000000,00000000,00000000
```

parm_get_num

Returns the total number of configurable parameters.

Example:

```
emlxadm> parm_get_num

Result: There are 18 configurable parameters in the driver.
```

parm_get_list

Returns a list of configurable parameters.

Example:

```
emlxadm> parm_get_list

Parameter:
-----
  label: console-notices
    min: 0x0
current: 0x0
    max: 0xffffffff
default: 0x0
dynamic: yes
  desc: Verbose mask for notice messages to the console.
-----
  label: console-warnings
    min: 0x0
current: 0x0
    max: 0xffffffff
default: 0x0
dynamic: yes
  desc: Verbose mask for warning messages to the console.
-----
  label: console-errors
    min: 0x0
current: 0x0
    max: 0xffffffff
default: 0x0
dynamic: yes
  desc: Verbose mask for error messages to the console.
-----
  label: log-notices
    min: 0x0
current: 0xffffffff
    max: 0xffffffff
default: 0xffffffff
dynamic: yes
  desc: Verbose mask for notice messages to the messages file.
-----
  label: log-warnings
    min: 0x0
current: 0xffffffff
    max: 0xffffffff
default: 0xffffffff
dynamic: yes
  desc: Verbose mask for warning messages to the messages file.
-----
  label: log-errors
    min: 0x0
current: 0xffffffff
    max: 0xffffffff
default: 0xffffffff
dynamic: yes
  desc: Verbose mask for error messages to the messages file.
-----
  label: num-iocbs
    min: 128
current: 1024
    max: 10240
default: 1024
dynamic: no
  desc: Number of outstanding IOCBs driver can queue to adapter.
```

```
-----
label: ub-bufs
  min: 40
current: 1000
  max: 16320
default: 1000
dynamic: no
  desc: Number of unsolicited buffers the driver should allocate.
-----

label: network-on
  min: 0
current: 1
  max: 1
default: 1
dynamic: no
  desc: Enable IP processing.
-----

label: ack0
  min: 0
current: 0
  max: 1
default: 0
dynamic: no
  desc: Enable ACK0 support.
-----

label: topology
  min: 0
current: 0
  max: 6
default: 0
dynamic: no
  desc: Select Fibre Channel topology.
-----

label: link-speed
  min: 0
current: 0
  max: 4
default: 0
dynamic: no
  desc: Select link speed.
-----

label: num-nodes
  min: 2
current: 512
  max: 512
default: 512
dynamic: no
  desc: Number of fibre channel nodes (NPorts) the driver will support.
-----

label: cr-delay
  min: 0
current: 0
  max: 63
default: 0
dynamic: no
  desc: A count of milliseconds after which an interrupt response is generated.
-----

label: cr-count
  min: 1
current: 1
  max: 255
default: 1
dynamic: no
  desc: A count of I/O completions after which an interrupt response is
        generated.
```

```

-----
label: assign-alpa
min: 0x0
current: 0x0
max: 0xef
default: 0x0
dynamic: no
desc: Assigns a preferred ALPA to the port. Only used in Loop topology.

-----
label: adisc-support
min: 0
current: 1
max: 2
default: 1
dynamic: yes
desc: Sets the Fibre Channel ADISC login support level.

-----
label: pm-support
min: 0
current: 1
max: 1
default: 1
dynamic: no
desc: Enables power management support.

```

parm_get <label>

Gets the value of a specified parameter in the driver.

Example:

```

emlxadm> parm_get adisc-support

label: adisc-support
min: 0
current: 1
max: 2
default: 1
dynamic: yes
desc: Sets the Fibre Channel ADISC login support level.

```

parm_set <label> <value>

Sets the value of a specified parameter in the driver. Only dynamic parameters can be set.

Example: This example sets a dynamic parameter:

```

emlxadm> parm_set adisc-support 2

label: adisc-support
min: 0
current: 2
max: 2
default: 1
dynamic: yes
desc: Sets the Fibre Channel ADISC login support level.

```

Note: To make this change permanent, you must edit the /kernel/drv/emlxs.conf file.

Example: This example attempts to set a static parameter:

```

emlxadm> parm_set network-on 1

emlxadm: EMLX_PARM_SET: Parameter (network-on) is not dynamic and cannot be
changed here.

** To make this change you must edit the /kernel/drv/emlxs.conf or **
** the /kernel/drv/emlx.conf file(s) and reboot the system.      **

```

msgbuf all or <number> [-i interval]

Displays all or part (the last <number> of lines) of the current driver message log, and can update the screen every <interval> seconds if desired. To stop the program from updating the screen, press **<Ctrl>+<C>**. If no interval is provided, the current message log is displayed with no additional updates, and the emlxadm prompt returns.

Example:

```
emlxadm> msgbuf 10

155130.01: 1002033:[B.1C35]emlxs0:  DEBUG: 800: ELS sent.  (GA_NXT: did=ffffffc
[00011000,00000000])
155130.02: 1002034:[4.00C9]emlxs0:  DEBUG: 801: ELS comp.  (GA_NXT: CT_ACC:
Rsn=0 Exp=0 [020113e1,21000020])
155130.02: 1002035:[B.1C35]emlxs0:  DEBUG: 800: ELS sent.  (GA_NXT: did=ffffffc
[000113e1,00000000])
155130.02: 1002036:[4.00C9]emlxs0:  DEBUG: 801: ELS comp.  (GA_NXT: CT_ACC:
Rsn=0 Exp=0 [020113e2,21000020])
155130.02: 1002037:[B.1C35]emlxs0:  DEBUG: 800: ELS sent.  (GA_NXT: did=ffffffc
[000113e2,00000000])
155130.02: 1002038:[4.00C9]emlxs0:  DEBUG: 801: ELS comp.  (GA_NXT: CT_ACC:
Rsn=0 Exp=0 [020113e4,21000020])
155130.03: 1002039:[B.1C35]emlxs0:  DEBUG: 800: ELS sent.  (GA_NXT: did=ffffffc
[000113e4,00000000])
155130.03: 1002040:[4.00C9]emlxs0:  DEBUG: 801: ELS comp.  (GA_NXT: CT_ACC:
Rsn=0 Exp=0 [020113e8,21000020])
155130.03: 1002041:[B.1C35]emlxs0:  DEBUG: 800: ELS sent.  (GA_NXT: did=ffffffc
[000113e8,00000000])
155130.03: 1002042:[4.00C9]emlxs0:  DEBUG: 801: ELS comp.  (GA_NXT: CT_ACC:
Rsn=0 Exp=0 [01011500,210000e0])
```

get_host_attrs

Displays all of the current host HBA API attributes.

Example:

```
emlxadm> get_host_attrs

Host Attributes:

Manufacturer           = Sun Microsystems, Inc.
Serial Number          = BG43918495
Model                  = LP10000DC-S
Model Description      = EMULEX LIGHTPULSE LP10000DC-S 2GB PCI-X FIBRE
CHANNEL ADAPTER
Node WWN                = 20000000C942097E
Node Symbolic Name     = none
Hardware Version        = 1001206d
Driver Version          = 1.11f.t3 (2006.04.25.11.43)
Optional ROM Version   = 1.50a9test1
Firmware Version       = 1.91b5
Vendor Specific ID     = fc00
Number of HBA ports    = 1
Driver Name            = Emulex-S s9-64 sparv v1.11f.t3
Last Change            = 5
fp Instance            = e
Node WWN                = 20000000C942097E
Port WWN               = 10000000C942097E
Port Fc Id             = 011700
Port Type              = Nport
Port State             = Online
Port Supported COS     = Class3
Port Supported FC4 Types:
00000000, 00000000, 00000000, 00000000,
00000000, 00000000, 00000000, 00000000,
Port Active FC4 Types:
00000120, 00000000, 00000000, 00000000,
```

```

00000000, 00000000, 00000000, 00000000,
Port Symbolic Name      = none
Port Supported Speed    = 1Gb, 2Gb
Port Speed              = 1Gb
Port Max Frame Size     = 0x800 bytes
Fabric Name             = 0000000000000000
Number of Discovered Ports = 4

```

get_port_attrs <index>, <wwn> or all

Displays the current HBA API port attributes. All of the port attributes can be displayed, or a single port can be specified by <index> or <wwn>. The total number of ports available can be seen in the "Number of Discovered Ports" attribute displayed using the get_host_attrs command. The <index> argument is an index into this list.

Example:

```
emlxadm> get_port_attrs all
```

Host Port Attributes:

```

Last Change              = 5
fp Instance              = e
Node WWN                 = 20000000C942097E
Port WWN                  = 10000000C942097E
Port Fc Id               = 011700
Port Type                 = Nport
Port State                = Online
Port Supported COS        = Class3
Port Supported FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Active FC4 Types:
    00000120, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Symbolic Name        = none
Port Supported Speed      = 1Gb, 2Gb
Port Speed                = 1Gb
Port Max Frame Size       = 0x800 bytes
Fabric Name               = 0000000000000000
Number of Discovered Ports = 4

```

Port[0] Attributes:

```

Node WWN                  = 20000020371938FA
Port WWN                  = 21000020371938FA
Port Fc Id                = 0113e1
Port Type                 = Unknown
Port State                = Unknown
Port Supported COS        = Class3
Port Supported FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Active FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Symbolic Name        = SEAGATE ST39103FC      0004
Port Supported Speed      = Unknown
Port Speed                = Unknown
Port Max Frame Size       = 0x0 bytes
Fabric Name               = 0000000000000000

```

Port[1] Attributes:

```

Node WWN                  = 20000020371938A2
Port WWN                  = 21000020371938A2
Port Fc Id                = 0113e2
Port Type                 = Unknown

```

```

Port State                      = Unknown
Port Supported COS              = Class3
Port Supported FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Active FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Symbolic Name              = SEAGATE ST39103FC          0004
Port Supported Speed            = Unknown
Port Speed                     = Unknown
Port Max Frame Size             = 0x0 bytes
Fabric Name                     = 0000000000000000

```

Port[2] Attributes:

```

Node WWN                      = 20000020371939A3
Port WWN                      = 21000020371939A3
Port Fc Id                    = 0113e4
Port Type                     = Unknown
Port State                    = Unknown
Port Supported COS            = Class3
Port Supported FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Active FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Symbolic Name              = SEAGATE ST39103FC          0004
Port Supported Speed            = Unknown
Port Speed                     = Unknown
Port Max Frame Size             = 0x0 bytes
Fabric Name                     = 0000000000000000

```

Port[3] Attributes:

```

Node WWN                      = 2000002037193670
Port WWN                      = 2100002037193670
Port Fc Id                    = 0113e8
Port Type                     = Unknown
Port State                    = Unknown
Port Supported COS            = Class3
Port Supported FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Active FC4 Types:
    00000000, 00000000, 00000000, 00000000,
    00000000, 00000000, 00000000, 00000000,
Port Symbolic Name              = SEAGATE ST39103FC          0004
Port Supported Speed            = Unknown
Port Speed                     = Unknown
Port Max Frame Size             = 0x0 bytes
Fabric Name                     = 0000000000000000

```

get_path <index>

Displays the current Solaris device path for a specified HBA port. The total number of ports available can be seen in the "Number of HBA ports" attribute displayed using the `get_host_attrs` command. The <index> argument is an index into this list.

Example:

```

emlxadm> get_path 0

Adapter: /pci@1e,600000/SUNW,emlxs@2/fp@0,0

emlxadm> get_path 1

Adapter: /pci@1e,600000/SUNW,emlxs@2,1/fp@0,0

```


get_vpd

Displays the current adapter's vital product data (VPD).

Example:

```
emlxadm> get_vpd

Vital Product Data:
  Identifier (ID): FC2G PCI-X LP10000DC - SUN
  Part Number (PN): LP10000DC-S
  Manufacturer (MN): Sun Microsystems, Inc.
  Serial Number (SN): BG43918495
  Description (V1): EMULEX LIGHTPULSE LP10000DC-S 2GB PCI-X FIBRE CHANNEL
ADAPTER
  Model (V2): LP10000DC-S
  Program Types (V3): T2:83,88,T3:84,T6:83,T7:83,TB:83,TFF:80
  Port Number (V4): 0
```

boot_code [enable or disable]

Sets or shows the boot code state of the current adapter.

Example:

```
emlxadm> boot_code

Boot code: Disabled

emlxadm> boot_code enable

Boot code: Enabled

emlxadm> boot_code disable

Boot code: Disabled
```

q

Exits the utility program.

Example:

```
emlxadm> q

Exiting...
```

h

Displays a help menu of utility commands.

Example:

```
emlxadm> h

Available commands: [rev 2]

get_num_devs - Returns the number of FC devices seen by this HBA.
get_dev_list - Returns a list of FC devices seen by this HBA.
get_login_params <wwpn> - Returns the login parameters for a specified FC device.
get_host_params - Return the host parameters.
get_sym_pname - Returns the symbolic port name of a device.
set_sym_pname <string> - Sets the symbolic port name for a device.
get_sym_nname - Returns the symbolic node name of a device.
set_sym_nname <string> - Sets the symbolic node name for a device.
dev_login <wwpn> - Performs an FC login to a device.
dev_logout <wwpn> - Performs an FC logout to a device.
get_state <wwpn> - Returns current Leadville state of a specified device.
```

```
dev_remove <wwpn> - Remove the FC device from Leadville management.
link_status <d_id> - Request link error status from a specified D_ID.
get_fcode_rev - Returns the current Fcode revision of the HBA.
download_fcode [filename] - Download the HBA fcode.
get_fw_rev - Returns the current firmware revision of the HBA.
download_fw [filename] - Download the HBA firmware.
get_boot_rev *Returns the current boot revision of the HBA.
download_boot [filename] *Download the HBA boot image.
get_dump_size - Returns the HBA's firmware core dump size.
force_dump - Force a firmware core dump on this HBA.
get_dump <-t,-b> <file> - Saves firmware core dump to a file.
get_topology - Returns the current FC network topology.
reset_link <wwpn,0> - Resets the link of a specified FC device.
reset_hard - Reset the HBA.
reset_hard_core - Reset the HBA firmware core.
diag <test> - Perform a diagnostic test on the HBA.
ns - Performs a complete query of the fabric name server.
parm_get_num *Returns the total number of configurable parameters.
parm_get_list *Returns a list of configurable parameters.
parm_get <label> *Gets the value of a specified parameter in the driver.
parm_set <label> <val> *Sets the value of a specified parameter in the driver.
msgbuf all or <number> [-i interval] *Returns the driver's internal message log.
get_host_attr - Returns the host adapter and port attributes.
get_port_attr <index>, <wwn> or all - Returns the port attributes.
get_path <index> - Returns the adapter path.
get_vpd *Returns the adapter's Vital Product Data (VPD).
boot_code [enable or disable] - *Sets or shows the boot code state in this HBA
q - Exits this program.
h - Returns this help screen.
hba - Select another hba.
p - Repeat previous command.
```

*Emulex adapters only

hba

Allows you to select another HBA to interface with. This prevents you from having to exit and reenter the program.

Example:

```
emlxadm> hba

Available HBA's:

1.  /devices/pci@1e,600000/SUNW,qlc@3/fp@0,0:devctl (CONNECTED)
2.  /devices/pci@1e,600000/SUNW,qlc@3,1/fp@0,0:devctl (NOT CONNECTED)
3.  /devices/pci@1e,600000/SUNW,emlxs@2/fp@0,0:devctl (CONNECTED)
4.  /devices/pci@1e,600000/SUNW,emlxs@2,1/fp@0,0:devctl (NOT CONNECTED)

Enter an HBA number or zero to exit:
```

p

Repeats the last command.

Example:

```
emlxadm> get_num_devs

There are 4 devices reported on this port.

emlxadm> p
emlxadm> get_num_devs

There are 4 devices reported on this port.
```

Using the emlxdrv Utility

The emlxdrv utility is used for binding (associating) the Emulex emlxs (Leadville FC) driver and the Emulex lpfc (traditional non-Leadville FC) driver to the various models of Emulex FC HBAs. This allows both drivers to coexist in the same host and attach to mutually exclusive Emulex FC HBA models. In other words, the emlxs driver can be configured to attach and operate one set of HBA models, while the lpfc driver can be configured to attach and operate a different set of HBA models. However, Solaris does not allow both drivers to attach and operate the same model of HBA even if there are multiple HBAs of that model present. If the driver binding configuration is changed, the host system must usually be rebooted for the new configuration to take effect.

Modes of Operation (emlxdrv)

The emlxdrv utility program can be run in two modes:

- Interactive
- CLI

Interactive Mode (emlxdrv)

Run the emlxdrv utility program in interactive mode by typing the name of the program without any command line arguments:

```
# emlxdrv
```

After it is started, the emlxdrv program scans the host system and prepares a driver configuration table consisting of bindings (associations) between the emlxs and lpfc drivers and a list of Emulex FC HBA models. After the table is prepared, the utility displays the following:

```
EMLXDRV Driver Management Utility, Version 1.00k
COPYRIGHT © 2004-2006 Emulex. All rights reserved.
```

Driver	Alias	Present	Boot	Sun	Models
-	lpfs	no	no	no	LP8000S and LP9002S (SBUS)
-	f800	no	no	no	LP8000 and LP8000DC
lpfc	f900	yes	no	no	LP9002, LP9002C, LP9002DC, and LP9402DC
lpfc	f980	no	no	no	LP9802 and LP9802DC
emlxs	fa00	yes	no	no	LP10000, LP10000DC and LP10000ExDC
emlxs	fd00	no	no	no	LP11000 and LP11002
emlxs	fe00	no	no	no	LPe11000 and LPe11002
emlxs	f0a5	no	no	no	2G Blade Adapter (emlxs only)
emlxs	fc00	yes	no	yes	LP10000-S and LP10000DC-S (emlxs only)
emlxs	fc10	no	no	yes	LP11000-S and LP11002-S (emlxs only)
emlxs	fc20	no	no	yes	LPe11000-S and LPe11002-S (emlxs only)

```
Available commands:
-----
set_emlxs <Alias> - Sets emlxs driver to bind to the specified device(s)
set_emlxs_sun    - Sets emlxs driver to bind to all Sun devices
set_emlxs_all    - Sets emlxs driver to bind to all devices
set_lpfc <Alias> - Sets lpfc driver to bind to the specified device(s)
set_lpfc_nonsun  - Sets lpfc driver to bind to all non-Sun devices
clear_dev <Alias> - Clears driver binding to the specified device(s)
clear_lpfc       - Clears all lpfc driver bindings
clear_emlxs      - Clears all emlxs driver bindings
clear_sun        - Clears driver bindings to all Sun devices
clear_nonsun     - Clears driver bindings to all non-Sun devices
clear_all        - Clears driver bindings to all devices
q               - Exits this program.
```

```
emlxdrv>
```

The display comprises three parts: the current driver configuration table, a list of available commands and the emlxdrv prompt.

The driver configuration table contains the following columns of data:

- **Driver.** Indicates which driver (emlxs, lpfc or "-" if none) is currently configured to bind or attach to a specific adapter alias.
- **Alias.** Indicates the specific adapter alias associated with a set of Emulex HBA models. Driver bindings can be made only with a specific adapter alias and not with a specific adapter model.
- **Present.** Indicates whether this specific type of adapter is currently present in the host system. Emlxdrv allows you to bind a driver to adapters that are not currently present in the system but that may be present in the future.
- **Boot.** Indicates whether this specific type of HBA currently provides connectivity to the system's boot disk. This is important because the emlxdrv utility does not allow you to change the driver binding to an HBA currently providing connectivity to the boot disk. If the driver binding must be changed to the system boot disk, the system must first be configured to boot through another type of HBA. The procedure to change to another type of HBA that will provide connectivity to the system's boot disk is not in the scope of this document, but is included in the FC Boot User Manual (the FC Boot User Manual for your HBA is available in the support pages of the Emulex Web site).
- **Sun.** Indicates whether this specific type of adapter is branded and sold directly by Sun Microsystems.
- **Models.** Provides a list of Emulex HBA models that are identified by a common adapter alias. Driver bindings can be made only with a specific adapter alias and not with a specific adapter model.

After the driver configuration table is a list of available commands. For a detailed explanation of each command and its arguments, see *Command Descriptions (emlxdrv)* on page 126.

Below the command list is an **emlxdrv>** prompt. From this point, the utility is prompt driven. When the prompt is displayed, you must enter one of the commands in the list. The current driver configuration table and the available command list are displayed automatically after each command is issued.

Some commands require an additional <alias> argument. You must specify one of the valid adapter aliases listed in the current driver configuration table. Each alias is shared by multiple adapter models. Driver bindings can be made only with an adapter alias and not with a specific adapter model.

To exit the program, enter **q**.

CLI Mode (emlxdrv)

The emlxdrv utility program can be run in CLI mode by typing the name of the program followed by a valid command and any required command arguments. For example, you can update the a device binding by entering all the information on one line at the operating system prompt:

```
# emlxdrv set_emlxs f980
```

```
Updating f980 ...
Done.
```

Driver	Alias	Present	Boot	Sun	Models
emlxs	lpfs	no	no	no	LP8000S and LP9002S (SBUS)
-	f800	no	no	no	LP8000 and LP8000DC
lpfc	f900	yes	no	no	LP9002, LP9002C, LP9002DC, and LP9402DC
lpfc	f980	no	no	no	LP9802 and LP9802DC
emlxs	fa00	yes	no	no	LP10000, LP10000DC and LP10000ExDC
emlxs	fd00	no	no	no	LP11000 and LP11002
emlxs	fe00	no	no	no	LPe11000 and LPe11002

emlxs	f0a5	no	no	no	2G Blade Adapter (emlxs only)
emlxs	fc00	yes	no	yes	LP10000-S and LP10000DC-S
emlxs	fc10	no	no	yes	LP11000-S and LP11002-S (emlxs only)
emlxs	fc20	no	no	yes	LPe11000-S and LPe11002-S

#

This mode of operation enables you to use the `emlxdv` utility as part of a script or another program capable of executing system-level calls. For a detailed explanation of each command and its arguments, see *Command Descriptions (emlxdv)* on page 126.

Command Descriptions (emlxdv)

This section provides a list of commands that can be issued with the `emlxdv` utility program. You can view the list of commands at any time by running the `emlxdv` utility in interactive mode (see *Interactive Mode (emlxdv)* on page 124).

set_emlxs <alias>

Sets the `emlxs` driver to bind to the specified devices. You must specify one of the valid adapter aliases listed on the screen. Note that each alias is shared by multiple adapter models. Driver bindings can be made only with an adapter alias and not with a specific adapter model.

You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; `emlxdv` only updates the system configuration for the next boot.

Example:

```
emlxdv> set_emlxs f980

Updating f980 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Done.
```

set_emlxs_sun

Sets the `emlxs` driver to bind to all Sun devices.

Example:

```
emlxdv> set_emlxs_sun

Updating fc00 ...
Updating fc10 ...
Updating fc20 ...
Done.
```

set_emlxs_all

Sets the `emlxs` driver to bind to all devices. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; `emlxdv` only updates the system configuration for the next boot.

Example:

```
emlxdv> set_emlxs_all

Updating lpfs ...
Updating f800 ...
Updating f900 ...
```

```
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating f980 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating fa00 ...
Updating fd00 ...
Updating fe00 ...
Updating fc00 ...
Updating fc10 ...
Updating fc20 ...
Done.
```

set_lpfc <alias>

Sets the lpfc driver to bind to the specified devices. You must specify one of the valid adapter aliases listed on the screen. Each alias is shared by multiple adapter models. Driver bindings can be made only with an adapter alias and not with a specific adapter model.

You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> set_lpfc fa00

Updating fa00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.
Done.
```

set_lpfc_nonsun

Sets the lpfc driver to bind to all non-Sun devices. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> set_lpfc_nonsun

Updating lpfs ...
Updating f800 ...
Updating f900 ...
Updating f980 ...
Updating fa00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fd00 ...
Updating fe00 ...
Done.
```

clear_dev <alias>

Clears driver binding to the specified devices. You must specify one of the adapter aliases listed on the screen. Each alias is shared by multiple adapter models. Driver bindings can be made only with an adapter alias and not with a specific adapter model.

You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> clear_dev fe00

Updating fe00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.
Done.
```

clear_lpfc

Clears all lpfc driver bindings. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> clear_lpfc

Updating f900 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating f980 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Done.
```

clear_emlxs

Clears all emlxs driver bindings. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> clear_emlxs

Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc10 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc20 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Done.
```

clear_sun

Clears driver bindings to all Sun devices. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> clear_sun

Updating fc00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc10 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc20 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Done.
```

clear_nonsun

Clears driver bindings to all non-Sun devices. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxdrv> clear_nonsun

Updating lpfs ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating f800 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating f900 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating f980 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating fa00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fd00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fe00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Done.
```


clear_all

Clears driver bindings to all devices. You may see the message "Cannot unload module". This indicates that you must reboot the system to get a driver to unbind from that adapter alias; emlxdrv only updates the system configuration for the next boot.

Example:

```
emlxadm> clear_all

Updating lpfs ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating f800 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating f900 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating f980 ...
Cannot unload module: lpfc
Will be unloaded upon reboot.

Updating fa00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fd00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fe00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc00 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc10 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Updating fc20 ...
Cannot unload module: emlxs
Will be unloaded upon reboot.

Done.
```

q

Exits the program. If changes were made to the driver bindings, a system reboot is usually required for all the changes to take effect.

Example:

```
emlxdrv> q

Exiting...

NOTE: If changes were made, then a system reboot may be required.

#
```

Troubleshooting

Introduction

This Troubleshooting section contains the following tables with helpful information should your system operate in an unexpected manner. These tables explain many of these circumstances and offers one or more workarounds for each situation.

- General situations that involve HBAnyware (Table 1)
- HBAnyware Security Configurator Situations - Access Control Groups (ACG) (Table 2)
- HBAnyware Security Configuration Situations - Access Sub-Groups (ASG) (Table 3)
- HBAnyware Security Configurator Situations - Backup Masters (Table 4)
- HBAnyware Security Configurator Error Message Situations (Table 5)
- HBAnyware Security Configurator Master Security Client Situations (Table 6)

This Troubleshooting section also contains console and log messages. Types of log messages, security levels and an extensive listing of message IDs and descriptions are also provided. Console and log message information begins on page 139.

Situations That Involve HBAnyware

General Situations

Table 1: General Situations

Situation	Resolution
When attempting to start HBAnyware the Web browser displays “Emulex Corporation HBAnyware Demo of HBAnyware WebStart web n.n.n.n...”	The document caching mechanism sometimes behaves erratically if more than one version of Java Runtime is installed on the browser client. There are two workarounds for this problem: <ul style="list-style-type: none"> • Exit the browser and restart it. HBAnyware with Web launch should start successfully. • Uninstall all non-essential versions of the Java Runtime. HBAnyware Web Launch services require that only a single version of the Java Runtime be installed on the browser client. This single version should be JRE version 1.5 or greater.
Operating Error Occurs When Attempting to Run HBAnyware. When you attempt to run the HBAnyware utility, an operating system error may occur. The computer may freeze.	Reboot the system.
Cannot See Multiple Zones from the Management Server. Cannot see multiple zones on the same screen of my management server running the HBAnyware utility.	Provide a physical FC connection into each of the zones. For each zone you want to see, connect an Emulex HBAnyware utility enabled port into that zone.

Table 1: General Situations (Continued)

Situation	Resolution
<p>Cannot See Other HBAs or Hosts. Although the HBAnyware utility is installed, only local HBAs are visible. The other HBAs and hosts in the SAN cannot be seen.</p>	<p>The HBAnyware utility uses in-band data communication, meaning that the management server running the HBAnyware utility must have a physical FC connection to the SAN. All the HBAs in the SAN will be visible if:</p> <ul style="list-style-type: none"> • The other servers have a FC connection to your zone of the SAN. Check fabric zoning. • Ensure that elxhbamgr processes are running on the remote host: enter <code>ps -ef grep elxhbamgr</code>. • All other HBAs are running the HBAnyware utility and the appropriate driver. • Other HBAs are Sun-branded Emulex HBAs or Emulex HBAs. <p>Note: The HBAnyware utility must be running on all remote hosts that are to be discovered and managed. Remote capabilities of the HBAnyware utility are subject to fabric zoning configuration. Remote hosts to be discovered and managed by the HBAnyware utility must be in the same zone.</p>
<p>SAN Management Workstation Does Not Have a FC Connection. The SAN management workstation does not have a physical FC connection into the SAN because the other management tools are all out-of-band. Can the HBAnyware utility be run on this SAN management workstation?</p>	<p>From the SAN management workstation, run a terminal emulation session into one of the servers that has the HBAnyware utility loaded on it. Open an X-Windows session to run the server's HBAnyware utility GUI remotely.</p>
<p>Cannot See New LUNs. Although new LUNs were created on the storage array, they do not appear in the HBAnyware utility.</p>	<p>Refresh the screen.</p>
<p>The HBAnyware Utility Appears on Remote Servers in the SAN.</p>	<p>To prevent the HBAnyware utility from appearing on remote servers in the SAN, disable the elxhbamgr process:</p> <ol style="list-style-type: none"> 1. Navigate to <code>/usr/sbin/hbanyware</code>. 2. Run <code>./stop_hbanyware</code> to stop both the elxhbamgr and elxdiscovery processes. 3. Run <code>./start_elxhbamgr</code> and <code>./start_elxdiscovery</code> to restart both processes. <p>Disabling this service or process prevents the local servers from being seen remotely.</p>
<p>The HBAnyware Security Configurator (Security Configurator) software package will not install. An error message states that the latest version of the HBAnyware utility must be installed first.</p>	<p>The system either has no HBAnyware software installed or has an older version of the HBAnyware software installed. In either case, obtain the latest version of the HBAnyware software and follow the installation instructions. Remember to install the HBAnyware software before installing the Security Configurator package.</p>
<p>Cannot access formerly accessible servers via the Security Configurator or the HBAnyware utility.</p>	<p>This is actually a symptom of two different problems.</p> <ul style="list-style-type: none"> • New Keys Were Generated While Servers Were Offline • Security Removed While Servers Were Offline <p>See Table 6 on page 137 for details regarding these problems.</p>

Table 1: General Situations (Continued)

Situation	Resolution
Cannot run the Security Configurator on a system that is configured for only secure access. I cannot run the Security Configurator on a system that is configured for only secure server access (it has no client privileges). The following message is displayed when the Security Configurator starts: "This system is not allowed client access to remote servers. This program will exit."	You cannot run the Security Configurator on a system that is configured for only secure server access. Click OK to close the message and the Configurator stops.

Security Configurator Situations - Access Control Groups (ACG)

Table 2: Access Control Groups Situations

Situation	Resolution
All servers are not displayed. When I run the Security Configurator on the Master Security Client (MSC), I do not see all of the systems in available servers or ACG Servers lists. When I run the Security Configurator on a non-MSC, I do not see all of the systems I should see in the ACG Servers list.	Make sure all of the systems are connected to the FC network and are online when you start the Configurator. Discovery of the systems is done only once, at startup. Unlike the HBAnyware utility, there is no Rediscover Devices button. Therefore, the Security Configurator must be restarted to rediscover new systems.
Cannot add or remove a server. The Security Configurator shows only a list of the systems in this system's ACG. I cannot add or remove systems from the ACG.	This is normal. You can modify the ACG for your system only on the MSC or on a parent client system.
HBAnyware utility shows non-ACG Servers. The HBAnyware utility shows servers that are part of the ACG and that are not part of the ACG.	The HBAnyware utility discovers unsecured servers as well as servers that are part of its ACG. The servers that you see that are not part of the ACG are unsecured. They will be discovered by any system running the HBAnyware utility on the same FC fabric.

Security Configuration Situations - Access Sub-Groups (ASG)

Table 3: HBAnyware Security Configurator - Access Sub-Groups Situations

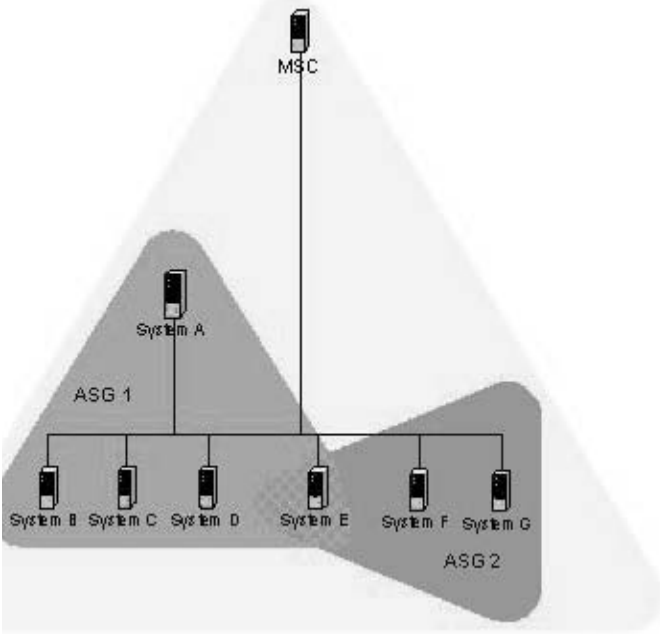
Situation	Resolution
<p>ASG Appears to Be Non-Hierarchical. It is possible from a higher-level client (such as the MSC) to create an ASG 1 with system A as the client and systems B, C, D, and E as servers. Then create an ASG 2 with system E as the client, but with systems F and G as servers even though F and G are not part of ASG 1. This makes the topology non-hierarchical.</p>	<p>Non-Hierarchical and Hierarchical ASG It is possible from a higher-level client (such as the MSC) to create an ASG 1 with system A as the client and systems B, C, D, and E as servers. Then create an ASG 2 with system E as the client, but with systems F and G as servers even though F and G are not part of ASG 1. This makes the topology non-hierarchical:</p> 
<p>Cannot add or remove a server.</p>	<p>When all of the systems in an ACG are running on a single fabric, they are all available to be added to any ASG. However, if the client is connected to more than one fabric, it is possible that not all of the servers in the client's ACG are physically accessible by a chosen client for an ASG. In this case, those servers are not available to be added to that ASG.</p> <p>If you add a system to an ASG as a server, and then make the system a client to a child ASG, you cannot remove it from the ACG it belongs to as a server until you delete the ASG to which it is a client.</p> <p>Before you delete a server from an ASG, you must first remove the server from any lower level ASGs to which it belongs.</p>
<p>In the ASG tree of the Access Sub-Groups tab, one or more of the names of the ASGs is displayed as "- ASG (Client Offline) -".</p>	<p>The client system for the ASG was not discovered when the Configurator was started. This is actually a symptom of two different problems.</p> <ul style="list-style-type: none"> • All Servers Are Not Displayed • New Keys Were Generated While Servers Were Offline <p>See Table 6 on page 137 for details regarding these problems.</p>

Table 3: HBAware Security Configurator - Access Sub-Groups Situations (Continued)

Situation	Resolution
Not All Servers are available to an ASG. When you create a new ASG or modify an existing ASG, not all of the servers in the ACG are available to be added to the ASG.	A client system can be connected to more than one fabric. While the system the Security Configurator is running on may be able to access all of the servers in its ACG, it is not necessarily the case that the selected client for the ASG can access all of the servers. Only those that can be accessed by the selected server will be available.

HBAware Security Configurator Situations - Backup Masters

Table 4: HBAware Security Configurator - Backup Masters Situations

Situation	Resolution
Cannot create a backup master.	Select a system (or group of systems) from the MSC to be the Backup Master. The system must be either an unsecured system (which will be secured by being made a Backup Master), or a system that is not part of any ASG (client or server). These systems will mirror the MSC's security configuration. Because the Backup Master may some day take over as the MSC, the Backup Master must be able to physically access all of the systems that the MSC can access. Therefore, if the MSC is connected to multiple fabrics, the Backup Master also must be connected to those same fabrics. When you select a Backup Master, the HBAware Security Configurator displays a warning if it detects that the system selected to be a Backup Master is not able to physically access the same systems that the MSC can access
Cannot modify the Security Configurator.	Select a system (or group of systems) from the MSC to be the Backup Master. The system must be either an unsecured system (which will be secured by being made a Backup Master), or a system that is not part of any ASG (client or server). These systems will mirror the MSC's security configuration. The Backup Master has client access from the HBAware utility to all of the servers in the MSC's ACG. However, the Backup Master does not have client access to the MSC and it cannot modify the security configuration (create, modify or delete ASGs).
No Backup Master and the MSC Is no longer available. I do not have a Backup Master and the MSC system is no longer available. The servers are still secure. I installed the Security Configurator on another system, but I cannot access those servers to remove the security from them.	The servers are no longer part of a valid security configuration because there is no MSC to provide master control of the configuration. In order to reset the security on the affected servers, you must contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they should be seen by the Security Configurator and the HBAware utility. At this point, you can set up security again through another MSC. At this time, also create a Backup Master.

Table 4: HBAnyware Security Configurator - Backup Masters Situations

Situation	Resolution
The Backup Master tab is not available.	<p>The Backup Master tab is displayed only when the Security Configurator is running on the MSC or a Backup Master. You use this tab to set up a system or systems to be backups to the MSC and to replace the MSC with a Backup Master.</p> <p>Each time you start the Security Configurator on the MSC and there is no Backup Master assigned, a warning message urges you to assign at least one Backup Master to prevent the loss of security information if the MSC were to become disabled.</p>

Error Message Situations

Table 5: Error Message Situations

Situation	Resolution
The following error message is displayed when creating an ASG: "The Access Sub-Group name already exists. Please use a different name."	<p>You entered a duplicate ASG name in the Access Sub-Group Name field. At each level of the security topology, each ASG name must be unique.</p> <p>Click OK on the message and enter a unique ASG name.</p>
The following error message is displayed when deleting an ASG: "The Access Sub-Group parent's ASG is offline. You should delete the ASG when the parent ASG is available. This ASG should only be deleted if the parent ASG will not be available again. Are you sure you want to delete this ASG?"	<p>The offline ASG entry serves as a placeholder for where the real ASG would be in the tree. You can neither modify nor delete it (although it is removed from the display if all of the child ASGs are deleted). It is possible to delete the child ASGs of the offline ASG. However, it is recommended that you delete them only if the client for the offline ASG will never be put online again. It is best to delete child ASGs when the parent ASG is online.</p> <p>Click Yes on the error message to delete the ASG or No to close the message without deleting.</p>
The following error message is displayed when starting the HBAnyware Security Configurator: "This system is not allowed client access to remote servers. This program will exit."	<p>The system you are running the Security Configurator on is already under the security umbrella as a server to one or more clients. To make this server a client (so that it can successfully run the Security Configurator), click OK to close the message and exit the program, then do the following:</p> <ol style="list-style-type: none"> 1. Run the Security Configurator on the MSC or on any client that has this server in its ASG. 2. Make this server a client to a group of servers.
The following error message is displayed when starting the Security Configurator: "There are no Backup Master Client Systems assigned to this security configuration. At least one should be assigned to avoid loss of the security configuration should the Master Client System become disabled."	<p>Use the Backup Master tab to assign a Backup Master for the MSC.</p>

Table 5: Error Message Situations

Situation	Resolution
The first time the Security Configurator is started in an unsecure environment, the following message is displayed: "This utility is running on an unsecure system. Continuing will allow you to set up a new security configuration making this system the Master Client System."	Click OK on the message and complete the ACG setup. The system on which the Security Configurator is running will become the MSC.
When I start the Security Configurator on a Backup Master system, the following message is displayed: "Warning: This system is a backup master client system. Therefore you will only be able to view the security configuration. To make changes, you will need to run this utility on the master client system."	Because each Backup Master system receives all the updates that the MSC makes to the security configuration, the Backup Master systems must be online when the Security Configurator is running on the MSC. Otherwise, updates to the security configuration are not reflected to the Backup Master. If the Backup Master becomes the MSC, corruption of the security configuration may occur. Click OK to close the message.

Master Security Client Situations

Table 6: Master Security Client Situations

Situation	Resolution
The MSC is no longer bootable or able to connect to the FC network.	<p>You must reassign a Backup Master as the new MSC from the Backup Master.</p> <p>Warning: Use this procedure only if the MSC cannot relinquish control to a Backup Master. For example, if the MSC is no longer bootable or able to connect to the FC network. Under any other circumstances, if the Backup Master takes over as the MSC and the MSC is still running or comes back online later, there will be two MSCs for the same security configuration. This will eventually lead to corruption of the security configuration.</p>
New Keys Were Generated While Servers Were Offline. A "Generate New Keys" operation was performed while one or more of the servers were offline. Now those servers can no longer access the HBAnyware Security Configurator or the HBAnyware utility.	<p>The servers are no longer part of the security configuration. In order to reset the security on the affected servers, you must contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they can be added back into the security topology by the MSC.</p> <p>Note: If the server was also a client to an ASG, then when you run the Security Configurator on the MSC or a parent client of this client, its label in the ASG tree of the Access Sub-Group tab will be "- ASG (Offline Client) -". You must delete the ASG (after deleting the child ASGs) and recreate the ASG configuration of this client and its child ASGs.</p>

Table 6: Master Security Client Situations

Situation	Resolution
Security Removed While Servers Were Offline. Security was removed while one or more servers were offline. I can no longer access those servers from the Security Configurator or the HBAnyware utility.	The servers are no longer part of the security configuration. In order to reset the security on the affected servers, contact Emulex Technical Support to receive a special application and instructions on the reset procedure. After the servers have been reset, they should be seen by the Security Configurator or the HBAnyware utility.

Console and Log Messages

Introduction

Log messages are logged to the /var/adm/messages system file.

Table 7: Notice, Warnings and Error Types

Driver Parameter	Default/ Min/Max	Effect of Changing Default	Related lpfc Driver Parameters
console-notices	0	Sets the verbose level for driver notices to the console.	log-only (when set to 0, log messages are logged to the system log file and also printed on the console.) Default = Disabled
console-warnings	0	Sets the verbose level for driver warnings to the console.	
console-errors	0	Sets the verbose level for driver errors to the console.	
log-notices	0xffffffff;	Sets the verbose level for driver notices to the system log file.	log-verbose (when set to non-zero, verbose messages are generated.) Default = Disabled
log-warnings	0xffffffff;	Sets the verbose level for driver warnings to the system log file.	
log-errors	0xffffffff;	Sets the verbose level for driver errors to the system log file.	

Table 8 lists the types of log messages that can be logged to the system file.

Table 8: Log Message Types

LOG Message Verbose Mask	Verbose Bit	Verbose Description
LOG_MISC	0x00000001	Miscellaneous events
LOG_DRIVER	0x00000002	Driver attach and detach events
LOG_INIT	0x00000004	HBA Initialization events
LOG_MEM	0x00000008	Memory management events
LOG_SLI	0x00000010	Service Level Interface (SLI) events
LOG_MBOX	0x00000020	Mailbox events
LOG_NODE	0x00000040	Node events
LOG_LINK	0x00000080	Link events
LOG_ELS	0x00000100	ELS events
LOG_PKT	0x00000200	General I/O packet events

Table 8: Log Message Types (Continued)

LOG Message Verbose Mask	Verbose Bit	Verbose Description
LOG_FCP	0x00000400	FCP traffic events
LOG_TGTM	0x00000800	FCP target mode events
LOG_IP	0x00001000	IP traffic events
LOG_SFS	0x00002000	Solaris SFS events
LOG_IOCTL	0x00004000	IOCTL events
LOG_FIRMWARE	0x00008000	Firmware download events
LOG_CT	0x00010000	FC Common Transport events
LOG_RESERVED	0x01FE0000	Reserved for future use
LOG_NODE_DETAIL	0x02000000	Detailed Node events
LOG_IOCTL_DETAIL	0x04000000	Detailed IOCTL events
LOG_IP_DETAIL	0x08000000	Detailed IP events
LOG_FIRMWARE_DETAIL	0x10000000	Detailed Firmware events
LOG_Solaris SFS_DETAIL	0x20000000	Detailed Solaris SFS events
LOG_MBOX_DETAIL	0x40000000	Detailed Mailbox events
LOG_SLI_DETAIL	0x80000000	Detailed HBA SLI events
LOG_ALL_MSG	0xFFFFFFFF	Detailed Node events

Severity Levels

Table 9: Severity Levels

Level	Message Description
DEBUG (Informational)	Message provides engineering debug information.
NOTICE (Informational)	Message provides a general purpose information.
WARNING	Message provides a general purpose warning.
ERROR	Message indicates that a driver error has occurred.
PANIC (Severe)	Message indicates that the driver has forced a system panic to occur.

Message Log Example

The following is an example of a message on the system console.

```
[5.0336]emlxs0: NOTICE: 720: Link up. (1Gb, fabric)
```

The following is an example of the same message in the system message log (/var/adm/messages) file.

```
Jan 19 14:45:36 sunv240 emlxs: [ID 349649 kern.info] [5.0336]emlxs0: NOTICE: 720: Link up. (1Gb, fabric)
```

In the above system log message:

- Jan 19 14:45:36 unidentified the date and time when the error or event occurred.
- sunv240 identifies the name of the host machine.
- emlxs identifies the message came from the Emulex emlxs driver.
- [ID 349649 kern.info] identifies a Solaris-specific message ID and kernel message level. This will change from one driver message to another.
- [5.0336] identifies the emlxs driver message context tag. This may change from one driver version to another.
- emlxs0 identifies the message is coming from the emlxs driver instance zero. This will change from one driver instance to another.
- NOTICE identifies the emlxs message severity level. This may change from one driver version to another.
- 720 identifies the emlxs drive message id. This will not change from one driver version to another.
- Link up identifies the actual error or event message. This will not change from one driver version to another.
- (1Gb, fabric) identifies additional information specific to the error or event message. This information is normally intended for Technical support / engineering use. This may change from one driver version to another.

Miscellaneous Events

MSG_ID: 0001 Debug

VERBOSE_MASK: LOG_MISC (0x00000001)

DESCRIPTION: This is a general purpose informational message.

SEVERITY LEVEL: Debug

MESSAGE: None

ACTION: No action needed, informational.

MSG_ID: 0002 Notice

VERBOSE_MASK: LOG_MISC (0x00000001)

DESCRIPTION: This is a general purpose informational message.

SEVERITY LEVEL: Notice

MESSAGE: None

ACTION: No action needed, informational.

MSG_ID: 0003 Warning

VERBOSE_MASK: LOG_MISC (0x00000001)

DESCRIPTION: This is a general purpose warning message.

SEVERITY LEVEL: Warning

MESSAGE: None

ACTION: No action needed, informational.

MSG_ID: 0004 Error

VERBOSE_MASK: LOG_MISC (0x00000001)

DESCRIPTION: This is a general purpose error message.

SEVERITY LEVEL: Error

MESSAGE: None

ACTION: No action needed, informational.

MSG_ID: 0005 Panic

VERBOSE_MASK: LOG_MISC (0x00000001)
DESCRIPTION: This is a general purpose panic message.
SEVERITY LEVEL: Panic (Severe)
MESSAGE: None
ACTION: Contact Technical Support.

Driver Events

MSG_ID: 0100 Notice: Driver Attach

VERBOSE_MASK: LOG_DRIVER (0x00000002)
DESCRIPTION: This indicates that the driver is performing an attach operation.
SEVERITY LEVEL: Notice
MESSAGE: None
ACTION: No action needed, informational.

MSG_ID: 0101 Error: Driver Attach Failed

VERBOSE_MASK: LOG_DRIVER (0x00000002)
DESCRIPTION: This indicates that the driver was unable to attach due to some issue.
SEVERITY LEVEL: Error
MESSAGE: Driver attach failed
ACTION: Check your hardware and software configuration. If problems persist, report these errors to Technical Support.

MSG_ID: 0102 Debug: Driver Attach

VERBOSE_MASK: LOG_DRIVER (0x00000002)
DESCRIPTION: This indicates that the driver is performing an attach operation.
SEVERITY LEVEL: Debug
MESSAGE: Driver attach
ACTION: No action needed, informational.

MSG_ID: 0110 Notice: Driver Detach

VERBOSE_MASK: LOG_DRIVER (0x00000002)
DESCRIPTION: This indicates that the driver is performing an detach operation.
SEVERITY LEVEL: Notice
MESSAGE: Driver detach
ACTION: No action needed, informational.

MSG_ID: 0111 Error: Driver Detach Failed

VERBOSE_MASK: LOG_DRIVER (0x00000002)
DESCRIPTION: This indicates that the driver was unable to detach due to some issue.
SEVERITY LEVEL: Error
MESSAGE: Driver detach failed
ACTION: Check your hardware and software configuration. If problems persist, report these errors to Technical Support.

MSG_ID: 0112 Debug: Driver Detach

VERBOSE_MASK: LOG_DRIVER (0x00000002)

DESCRIPTION: This indicates that the driver is performing an detach operation.

SEVERITY LEVEL: Debug

MESSAGE: Driver detach

ACTION: No action needed, informational.

MSG_ID: 0120 Debug: Driver Suspend

VERBOSE_MASK: LOG_DRIVER (0x00000002)

DESCRIPTION: This indicates that the driver is performing a suspend operation.

SEVERITY LEVEL: Debug

MESSAGE: Driver suspend

ACTION: No action needed, informational.

MSG_ID: 0121 Error: Driver Suspend Failed

VERBOSE_MASK: LOG_DRIVER (0x00000002)

DESCRIPTION: This indicates that the driver was unable to suspend due to some issue.

SEVERITY LEVEL: Error

MESSAGE: Driver suspend failed

ACTION: Check your hardware and software configuration. If problems persist, report these errors to Technical Support.

MSG_ID: 0130 Debug: Driver Resume

VERBOSE_MASK: LOG_DRIVER (0x00000002)

DESCRIPTION: This indicates that the driver is performing a resume operation.

SEVERITY LEVEL: Debug

MESSAGE: Driver resume

ACTION: No action needed, informational.

MSG_ID: 0131 Error: Driver Resume Failed

VERBOSE_MASK: LOG_DRIVER (0x00000002)

DESCRIPTION: This indicates that the driver was unable to resume due to some issue.

SEVERITY LEVEL: Error

MESSAGE: Driver resume failed

ACTION: Check your hardware and software configuration. If problems persist, report these errors to Technical Support.

HBA Initialization Events

MSG_ID: 0200 Notice: Adapter Initialization

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that the adapter is initializing.

SEVERITY LEVEL: Notice

MESSAGE: Adapter Initialization

ACTION: No action needed, informational.

MSG_ID: 0201 Error: Adapter Initialization Failed

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that an attempt to initialize the adapter has failed.

SEVERITY LEVEL: Error

MESSAGE: Adapter initialization failed

ACTION: Check your hardware configuration. If problems persist, report these errors to Technical Support.

MSG_ID: 0202 Debug: Adapter Initialization

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that the adapter is initializing.

SEVERITY LEVEL: Debug

MESSAGE: Adapter Initialization

ACTION: No action needed, informational.

MSG_ID: 0210 Debug: Adapter Transition

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that the adapter is changing states.

SEVERITY LEVEL: Debug

MESSAGE: Adapter transition

ACTION: No action needed, informational.

MSG_ID: 0220 Debug: Adapter Online

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that the adapter is online and ready to communicate.

SEVERITY LEVEL: Debug

MESSAGE: Adapter online

ACTION: No action needed, informational.

MSG_ID: 0230 Debug: Adapter Offline

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that the adapter is offline and unable to communicate.

SEVERITY LEVEL: Debug

MESSAGE: Adapter offline

ACTION: No action needed, informational.

MSG_ID: 0230 Warning: Adapter Shutdown

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that the adapter has been shutdown and will require a reboot to reinitialize.

SEVERITY LEVEL: Warning

MESSAGE: Adapter shutdown

ACTION: Contact Technical Support.

MSG_ID: 0240 Error: Adapter Reset Failed

VERBOSE_MASK: LOG_INIT (0x00000004)

DESCRIPTION: This indicates that an attempt to reset the adapter has failed.

SEVERITY LEVEL: Error

MESSAGE: Adapter reset failed

ACTION: Check your hardware configuration. If problems persist, report these errors to Technical Support.

Memory Management Events

MSG_ID: 0300 Debug: Memory Allocated

VERBOSE_MASK: LOG_MEM (0x00000008)

DESCRIPTION: This indicates that the driver allocated system memory.

SEVERITY LEVEL: Debug

MESSAGE: Memory alloc

ACTION: No action needed, informational.

MSG_ID: 0301 Error: Memory Allocation Failed

VERBOSE_MASK: LOG_MEM (0x00000008)

DESCRIPTION: This indicates that the driver was unable to allocate system memory. The system is low on memory resources.

SEVERITY LEVEL: Error

MESSAGE: Memory alloc failed

ACTION: No action needed. If problems persist, report these errors to your system administrator.

MSG_ID: 0310 Error: Memory Pool Error

VERBOSE_MASK: LOG_MEM (0x00000008)

DESCRIPTION: This indicates that a problem has occurred with the memory buffer pool management.

SEVERITY LEVEL: Error

MESSAGE: Memory pool error

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 0311 Debug: Memory Pool Allocation Failed

VERBOSE_MASK: LOG_MEM (0x00000008)

DESCRIPTION: This indicates that the driver was unable to allocate memory from one of its own memory pools.

SEVERITY LEVEL: Debug

MESSAGE: Memory pool alloc failed

ACTION: If the problem occurs frequently you may be able to configure more resources for that pool. If this does not solve the problem, report these errors to Technical Support.

MSG_ID: 0320 Notice: No Unsolicited Buffer Available

VERBOSE_MASK: LOG_MEM (0x00000008)

DESCRIPTION: This indicates that the driver's unsolicited buffer pool is exhausted. The I/O will be dropped and most likely retried by the remote device.

SEVERITY LEVEL: Notice

MESSAGE: No unsolicited buffer available

ACTION: If the problem occurs frequently you may be able to configure more resources for that pool. If this does not solve the problem, report these errors to Technical Support.

Service Level Interface (SLI) Events

MSG_ID: 0400 Debug: Vital Product Data

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This provides vendor-specific information about the adapter.
SEVERITY LEVEL: Debug
MESSAGE: Vital Product Data
ACTION: No action needed, informational.

MSG_ID: 0410 Debug: Link Attention

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that the adapter has triggered a link attention interrupt.
SEVERITY LEVEL: Debug
MESSAGE: Link attn
ACTION: No action needed, informational.

MSG_ID: 0411 Debug: State Change

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that the adapter has changed state.
SEVERITY LEVEL: Debug
MESSAGE: State change
ACTION: No action needed, informational.

MSG_ID: 0420 Error: Adapter Hardware Error

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that an interrupt has occurred and the status register indicates a nonrecoverable hardware error.
SEVERITY LEVEL: Error
MESSAGE: Adapter hardware error
ACTION: This error usually indicates a hardware problem with the adapter. Try running adapter diagnostics. Report these errors to Technical Support.

MSG_ID: 0430 Debug: Ring Event

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that an SLI ring event has occurred.
SEVERITY LEVEL: Debug
MESSAGE: Ring event
ACTION: No action needed, informational.

MSG_ID: 0431 Debug: Ring Error

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that an SLI ring error is being reported by the adapter.
SEVERITY LEVEL: Debug
MESSAGE: Ring error
ACTION: No action needed, informational.

MSG_ID: 0432 Debug: Ring Reset

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates an SLI ring is being reset.
SEVERITY LEVEL: Debug
MESSAGE: Ring reset
ACTION: No action needed, informational.

MSG_ID: 0440 Debug: Adapter Msg

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that a message was sent to the driver from the adapter.
SEVERITY LEVEL: Debug
MESSAGE: Adapter msg
ACTION: No action needed, informational.

MSG_ID: 0450 Error: IOCB Invalid

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that an IOCB was received from the adapter with an illegal value. This error could indicate a driver or firmware problem.
SEVERITY LEVEL: Error
MESSAGE: IOCB invalid
ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 0451 Debug: IOCB Queue Full

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates that the IOCB queue is full. This will occur during normal operation.
SEVERITY LEVEL: Debug
MESSAGE: IOCB queue full
ACTION: No action needed, informational.

MSG_ID: 0452 Debug: IOCB Error

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates an IOCB local error is being reported by the adapter.
SEVERITY LEVEL: Debug
MESSAGE: IOCB error
ACTION: No action needed, informational.

MSG_ID: 0453 Debug: IOCB Stale

VERBOSE_MASK: LOG_SLI (0x00000010)
DESCRIPTION: This indicates an IOCB completed after its associated packet completed.
SEVERITY LEVEL: Debug
MESSAGE: IOCB stale
ACTION: No action needed, informational.

MSG_ID: 0460 Debug: SLI Detail

VERBOSE_MASK: LOG_SLI_DETAIL (0x20000000)
DESCRIPTION: This provides detailed information about an SLI event.
SEVERITY LEVEL: Debug
MESSAGE: SLI detail
ACTION: No action needed, informational.

Mailbox Events

MSG_ID: 0500 Debug: Mailbox Event

VERBOSE_MASK: LOG_MBOX (0x00000020)

DESCRIPTION: This indicates that a mailbox event has occurred.

SEVERITY LEVEL: Debug

MESSAGE: Mailbox event

ACTION: No action needed, informational.

MSG_ID: 0501 Debug: Mailbox Detail

VERBOSE_MASK: LOG_MBOX_DETAIL (0x40000000)

DESCRIPTION: This provides detailed information about a mailbox event.

SEVERITY LEVEL: Debug

MESSAGE: Mailbox detail

ACTION: No action needed, informational.

MSG_ID: 0510 Debug: Stray Mailbox Interrupt

VERBOSE_MASK: LOG_MBOX (0x00000020)

DESCRIPTION: This indicates that a mailbox command completion interrupt was received and the mailbox is not valid. This error could indicate a driver or firmware problem.

SEVERITY LEVEL: Debug

MESSAGE: Stray mailbox interrupt

ACTION: No action needed, informational. If problems persist, report these errors to Technical Support.

MSG_ID: 0520 Error: Mailbox Completion Error

VERBOSE_MASK: LOG_MBOX (0x00000020)

DESCRIPTION: This indicates that an unsupported or illegal mailbox command was completed. This error could indicate a driver or firmware problem.

SEVERITY LEVEL: Error

MESSAGE: Mailbox completion error

ACTION: No action needed. If problems persist, report these errors to Technical Support.

Node Events

MSG_ID: 0600 Debug: Node Create

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that a node has been created for a remote device.

SEVERITY LEVEL: Debug

MESSAGE: Node create

ACTION: No action needed, informational.

MSG_ID: 0601 Debug: Node Opened

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that a node has been opened for I/O transport.

SEVERITY LEVEL: Debug

MESSAGE: Node opened.

ACTION: No action needed, informational.

MSG_ID: 0602 Notice: Node Create Failed

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that a node create request for a remote device has failed.

SEVERITY LEVEL: Notice

MESSAGE: Node create failed

ACTION: No action needed, informational.

MSG_ID: 0603 Debug: Node Updated

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that a node has been updated for a remote device.

SEVERITY LEVEL: Debug

MESSAGE: Node updated

ACTION: No action needed, informational.

MSG_ID: 0610 Debug: Node Destroy

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that a node has been destroyed for a remote device.

SEVERITY LEVEL: Debug

MESSAGE: Node destroyed

ACTION: No action needed, informational.

MSG_ID: 0611 Debug: Node Closed

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that a node has been temporarily closed for I/O transport.

SEVERITY LEVEL: Debug

MESSAGE: Node closed

ACTION: No action needed, informational.

MSG_ID: 0612 Notice: Node Missing

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that an FCP2 device node has been found missing.

SEVERITY LEVEL: Notice

MESSAGE: Node missing

ACTION: No action needed, informational.

MSG_ID: 0620 Debug: Node Not Found

VERBOSE_MASK: LOG_NODE (0x00000040)

DESCRIPTION: This indicates that there was an attempt to send an I/O packet to an unknown device node. The driver maintains a node table entry for every device it needs to communicate with on the FC network.

SEVERITY LEVEL: Debug

MESSAGE: Node not found

ACTION: No action needed, informational. If problems persist, report these errors to Technical Support.

Link Events

MSG_ID: 0700 Debug: Link Event

VERBOSE_MASK: LOG_SLI (0x00000010) or LOG_LINK (0x00000080)

DESCRIPTION: This indicates that a link event has occurred.

SEVERITY LEVEL: Debug

MESSAGE: Link event

ACTION: No action needed, informational.

MSG_ID: 0710 Notice: Link Down

VERBOSE_MASK: LOG_LINK (0x00000080)

DESCRIPTION: This indicates that the FC link is down to the adapter.

SEVERITY LEVEL: Notice

MESSAGE: Link down

ACTION: Check your network connections. If problems persist, report these errors to system administrator.

MSG_ID: 0720 Notice: Link Up

VERBOSE_MASK: LOG_LINK (0x00000080)

DESCRIPTION: This indicates that the FC link is up.

SEVERITY LEVEL: Notice

MESSAGE: Link up

ACTION: No action needed, informational.

MSG_ID: 0721 Notice: NPIV Link Up

VERBOSE_MASK: LOG_LINK (0x00000080)

DESCRIPTION: This indicates that the FC link is up for all virtual ports.

SEVERITY LEVEL: Notice

MESSAGE: NPIV Link up

ACTION: No action needed, informational.

MSG_ID: 0730 Notice: Link Reset

VERBOSE_MASK: LOG_LINK (0x00000080) or LOG_SFS (0x00002000)

DESCRIPTION: This indicates that an issue has forced the FC link to be reset.

SEVERITY LEVEL: Notice

MESSAGE: Link reset

ACTION: No action needed, informational.

MSG_ID: 0731 Error: Link Reset Failed

VERBOSE_MASK: LOG_LINK (0x00000080) or LOG_SFS (0x00002000)

DESCRIPTION: This indicates that an attempt to reset the FC link has failed.

SEVERITY LEVEL: Error

MESSAGE: Link reset failed

ACTION: No action needed. If problems persist, report these errors to Technical Support.

ELS Events

MSG_ID: 0800 Debug: ELS Sent

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an ELS command is being sent.

SEVERITY LEVEL: Debug

MESSAGE: ELS sent

ACTION: No action needed, informational.

MSG_ID: 0801 Debug: ELS Comp

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an ELS command completed normally.

SEVERITY LEVEL: Debug

MESSAGE: ELS comp

ACTION: No action needed, informational.

MSG_ID: 0810 Error: Stray ELS Completion

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an ELS command completion was received without issuing a corresponding ELS command. This error could indicate a driver or firmware problem.

SEVERITY LEVEL: Error

MESSAGE: Stray ELS completion

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 0811 Debug: Abnormal ELS Completion

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an ELS command completion with a status error in the IOCB. It could mean the FC device on the network is not responding or the FC device is not an FCP target. The driver will automatically retry this ELS command if needed.

SEVERITY LEVEL: Debug

MESSAGE: Abnormal ELS completion

ACTION: If the command is a PLOGI or PRLI, and the destination PortID is not an FCP target, no action is needed. Otherwise, check the physical connections to the FC network and the state of the remote PortID.

MSG_ID: 0820 Debug: ELS Rcvd

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an unsolicited ELS command was received.

SEVERITY LEVEL: Debug

MESSAGE: ELS rcvd

ACTION: No action needed, informational.

MSG_ID: 0821 Debug: Unsolicited ELS Dropped

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an unsolicited ELS command was received and then dropped for some reason.

SEVERITY LEVEL: Debug

MESSAGE: Unsolicited ELS dropped

ACTION: No action needed, informational.

MSG_ID: 0822 Debug: ELS Reply

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that a reply is being sent for an unsolicited ELS command.

SEVERITY LEVEL: Debug

MESSAGE: ELS reply

ACTION: No action needed, informational.

MSG_ID: 0830 Error: Invalid ELS Command Found

VERBOSE_MASK: LOG_ELS (0x00000100)

DESCRIPTION: This indicates that an ELS command was found with an invalid command code.

SEVERITY LEVEL: Error

MESSAGE: Invalid ELS command found

ACTION: No action needed. If problems persist, report these errors to Technical Support.

General I/O Packet Events

MSG_ID: 0900 Notice: Packet Abort

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an I/O packet is being aborted.

SEVERITY LEVEL: Notice

MESSAGE: Packet abort

ACTION: No action needed, informational.

MSG_ID: 0901 Warning: Packet Abort Failed

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an attempt to abort an I/O packet has failed.

SEVERITY LEVEL: Warning

MESSAGE: Packet abort failed

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 0910 Debug: Packet Timeout

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an I/O packet has timed out and is being aborted.

SEVERITY LEVEL: Debug

MESSAGE: Packet timeout

ACTION: No action needed, informational.

MSG_ID: 0911 Debug: Ring Watchdog

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that I/O(s) are getting stale waiting on a ring TX queue

SEVERITY LEVEL: Debug

MESSAGE: Ring watchdog

ACTION: No action needed, informational.

MSG_ID: 0911 Debug: TXQ Watchdog

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that I/O(s) was found missing from the transmit queue.

SEVERITY LEVEL: Debug

MESSAGE: TXQ watchdog

ACTION: No action needed, informational.

MSG_ID: 0920 Debug: Packet Flush

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an I/O packet is being flushed.

SEVERITY LEVEL: Debug

MESSAGE: Packet flush

ACTION: No action needed, informational.

MSG_ID: 0921 Debug: Packet Flushed

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an I/O packet has been flushed.

SEVERITY LEVEL: Debug

MESSAGE: Packet flushed

ACTION: No action needed, informational.

MSG_ID: 0922 Notice: Packet Flush Timeout

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an I/O packet flush request has timed out with some I/O packets still not completed. The driver will attempt to recover by itself.

SEVERITY LEVEL: Notice

MESSAGE: Packet flush timeout

ACTION: No action needed, informational. If problems persist, report these errors to Technical Support.

MSG_ID: 0930 Notice: Packet Transport Failed

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an attempt to send an I/O packet failed. The I/O packet will be retried by the upper layer.

SEVERITY LEVEL: Notice

MESSAGE: Packet transport failed

ACTION: No action needed, informational.

MSG_ID: 0931 Error: Packet Transport Error

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an error occurred while attempting to send an I/O packet. The I/O packet will likely be failed back to the user application.

SEVERITY LEVEL: Error

MESSAGE: Packet transport error

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 0932 Debug: Packet Transport

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This provides additional information about a packet being sent.

SEVERITY LEVEL: Debug

MESSAGE: Packet transport

ACTION: No action needed, informational.

MSG_ID: 0940 Debug: Packet Completion Error

VERBOSE_MASK: LOG_PKT (0x00000200)

DESCRIPTION: This indicates that an I/O packet was completed with an error status. This can occur during normal operation.

SEVERITY LEVEL: Debug

MESSAGE: Packet completion error.

ACTION: No action needed, informational. If problems persist, report these errors to Technical Support.

FCP Traffic Events

MSG_ID: 1000 Debug: Stray FCP Completion

VERBOSE_MASK: LOG_FCP (0x00000400)

DESCRIPTION: This indicates that an FCP command completion was received without issuing a corresponding FCP command. This error could indicate a driver or firmware problem.

SEVERITY LEVEL: Debug

MESSAGE: Stray FCP completion

ACTION: No action needed, informational. If problems persist, report these errors to Technical Support.

MSG_ID: 1001 Debug: FCP Completion Error

VERBOSE_MASK: LOG_FCP (0x00000400)

DESCRIPTION: This indicates that an FCP command completed with an error status. These errors can occur during normal operation.

SEVERITY LEVEL: Debug

MESSAGE: FCP completion error

ACTION: No action needed, informational.

IP Traffic Events

MSG_ID: 1200 Debug: IP Detail

VERBOSE_MASK: LOG_IP_DETAIL (0x08000000)

DESCRIPTION: This provides detailed information about the driver's IP interface.

SEVERITY LEVEL: Debug

MESSAGE: IP detail

ACTION: No action needed, informational.

MSG_ID: 1210 Error: Stray IP Completion

VERBOSE_MASK: LOG_IP (0x00001000)

DESCRIPTION: This indicates that an IP sequence completion was received without issuing a corresponding IP sequence. This error could indicate a driver or firmware problem.

SEVERITY LEVEL: Error

MESSAGE: Stray IP completion

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 1211 Debug: Abnormal IP Completion

VERBOSE_MASK: LOG_IP (0x00001000)

DESCRIPTION: This indicates that an IP sequence completed with a status error in the IOCB. It could mean the FC device on the network is not responding.

SEVERITY LEVEL: Debug

MESSAGE: Abnormal IP completion

ACTION: No action needed, informational. If problems persist, report these errors to system administrator.

MSG_ID: 1220 Debug: Unsolicited IP Dropped

VERBOSE_MASK: LOG_IP (0x00001000)

DESCRIPTION: This indicates that an unsolicited IP sequence was received, but was dropped for some reason.

SEVERITY LEVEL: Debug

MESSAGE: Unsolicited IP dropped

ACTION: No action needed, informational.

MSG_ID: 1221 Debug: IP Recvd

VERBOSE_MASK: LOG_IP (0x00001000)

DESCRIPTION: This indicates that an unsolicited IP sequence was received.

SEVERITY LEVEL: Debug

MESSAGE: IP received

ACTION: No action needed, informational.

MSG_ID: 1230 Error: Invalid IP Sequence Found

VERBOSE_MASK: LOG_IP (0x00001000)

DESCRIPTION: This indicates that an IP sequence was found with an invalid code.

SEVERITY LEVEL: Error

MESSAGE: Invalid IP sequence found

ACTION: No action needed. If problems persist, report these errors to Technical Support.

Solaris SFS Events**MSG_ID: 1300 Debug: SFS**

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This provides general information about the driver's Solaris SFS interface.

SEVERITY LEVEL: Debug

MESSAGE: SFS

ACTION: No action needed, informational.

MSG_ID: 1301 Debug: SFS Detail

VERBOSE_MASK: LOG_SFS_DETAIL (0x20000000)

DESCRIPTION: This provides detailed information about the driver's Solaris SFS interface.

SEVERITY LEVEL: Debug

MESSAGE: SFS detail

ACTION: No action needed, informational.

MSG_ID: 1310 Warning: Diagnostic Error

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that a diagnostic request did not complete because of some issue.

SEVERITY LEVEL: Warning

MESSAGE: Diagnostic error

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 1311 Debug: ECHO Diagnostic Completed

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that an ECHO diagnostic has completed.

SEVERITY LEVEL: Debug

MESSAGE: ECHO diagnostic completed

ACTION: No action needed, informational.

MSG_ID: 1312 Warning: ECHO Diagnostic Failed

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that an ECHO diagnostic has failed to return a positive result. This could indicate a connectivity problem with your FC network.

SEVERITY LEVEL: Warning

MESSAGE: ECHO diagnostic failed

ACTION: Check your network connections. If problems persist report these errors to system administrator.

MSG_ID: 1313 Debug: BIU Diagnostic Completed

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that a BIU diagnostic has completed.

SEVERITY LEVEL: Debug

MESSAGE: BIU diagnostic completed

ACTION: No action needed, informational.

MSG_ID: 1314 Error: BIU Diagnostic Failed

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that a BIU diagnostic has failed to return a positive result. This is usually caused by an adapter hardware problem.

SEVERITY LEVEL: Error

MESSAGE: BIU diagnostic failed

ACTION: Report this error to Technical Support.

MSG_ID: 1315 Debug: POST Diagnostic Completed

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that a POST diagnostic has completed.

SEVERITY LEVEL: Debug

MESSAGE: POST diagnostic completed

ACTION: No action needed, informational.

MSG_ID: 1316 Error: POST Diagnostic Failed

VERBOSE_MASK: LOG_SFS (0x00002000)

DESCRIPTION: This indicates that a POST diagnostic has failed to return a positive result. This is usually caused by an adapter hardware problem.

SEVERITY LEVEL: Error

MESSAGE: POST diagnostic failed

ACTION: Report this error to Technical Support.

IOCTL Events

MSG_ID: 1400 Debug: IOCTL

VERBOSE_MASK: LOG_IOCTL (0x00004000)

DESCRIPTION: This provides general information about the driver's IOCTL interface.

SEVERITY LEVEL: Debug

MESSAGE: IOCTL

ACTION: No action needed, informational.

MSG_ID: 1401 Debug: IOCTL Detail

VERBOSE_MASK: LOG_IOCTL_DETAIL (0x04000000)

DESCRIPTION: This provides detailed information about the driver's IOCTL interface.

SEVERITY LEVEL: Debug

MESSAGE: IOCTL detail

ACTION: No action needed, informational.

MSG_ID: 1410 Debug: DFC

VERBOSE_MASK: LOG_IOCTL (0x00004000)

DESCRIPTION: This provides general information about the driver's DFC interface.

SEVERITY LEVEL: Debug

MESSAGE: DFC

ACTION: No action needed, informational.

MSG_ID: 1411 Debug: DFC Detail

VERBOSE_MASK: LOG_IOCTL_DETAIL (0x04000000)

DESCRIPTION: This provides detailed information about the driver's DFC interface.

SEVERITY LEVEL: Debug

MESSAGE: DFC detail

ACTION: No action needed, informational.

MSG_ID: 1420 Debug: DFC Error

VERBOSE_MASK: LOG_IOCTL (0x00004000)

DESCRIPTION: This indicates that an error was found while processing a DFC request.

SEVERITY LEVEL: Debug

MESSAGE: DFC error

ACTION: No action needed, informational.

Firmware Download Events

MSG_ID: 1500 Debug: Firmware Image

VERBOSE_MASK: LOG_FIRMWARE (0x00008000)
DESCRIPTION: This provides information about the firmware interface.
SEVERITY LEVEL: Debug
MESSAGE: Firmware image
ACTION: No action needed, informational.

MSG_ID: 1501 Debug: Firmware Image Detail

VERBOSE_MASK: LOG_FIRMWARE_DETAIL (0x10000000)
DESCRIPTION: This provides detailed information about the firmware interface.
SEVERITY LEVEL: Debug
MESSAGE: Firmware detail
ACTION: No action needed, informational.

MSG_ID: 1510 Error: Bad Firmware Image

VERBOSE_MASK: LOG_FIRMWARE (0x00008000)
DESCRIPTION: This indicates that a bad firmware image was provided to the download function.
SEVERITY LEVEL: Error
MESSAGE: Bad firmware image
ACTION: Obtain the proper image file. If problems persist report these errors to Technical Support.

MSG_ID: 1511 Error: Firmware Image Not Compatible

VERBOSE_MASK: LOG_FIRMWARE (0x00008000)
DESCRIPTION: This indicates that the firmware image provided was not compatible with the existing hardware.
SEVERITY LEVEL: Error
MESSAGE: Firmware image not compatible
ACTION: Obtain the proper image file. If problems persist report these errors to Technical Support.

MSG_ID: 1520 Notice: Firmware Download

VERBOSE_MASK: LOG_FIRMWARE (0x00008000)
DESCRIPTION: This indicates that an attempt to download a firmware image has occurred.
SEVERITY LEVEL: Notice
MESSAGE: Firmware download
ACTION: No action needed, informational. If problems persist report these errors to Technical Support.

MSG_ID: 1521 Notice: Firmware Download Complete

VERBOSE_MASK: LOG_FIRMWARE (0x00008000)
DESCRIPTION: This indicates that an attempt to download a firmware image was successful.
SEVERITY LEVEL: Notice
MESSAGE: Firmware download complete
ACTION: No action needed, informational.

MSG_ID: 1522 Error: Firmware Download Failed

VERBOSE_MASK: LOG_FIRMWARE (0x00008000)

DESCRIPTION: This indicates that an attempt to download a firmware image was failed.

SEVERITY LEVEL: Error

MESSAGE: Firmware download failed

ACTION: Check your hardware configuration. If problems persist, report these errors to Technical Support.

Common Transport Events

MSG_ID: 1600 Debug: CT sent

VERBOSE_MASK: LOG_CT (0x00010000)

DESCRIPTION: This indicates that a CT command is being sent.

SEVERITY LEVEL: Debug

MESSAGE: CT sent

ACTION: No action needed, informational.

MSG_ID: 1601 Debug: CT comp

VERBOSE_MASK: LOG_CT (0x00010000)

DESCRIPTION: This indicates that a CT command completed normally.

SEVERITY LEVEL: Debug

MESSAGE: CT comp

ACTION: No action needed, informational.

MSG_ID: 1610 Error: Stray CT completion

VERBOSE_MASK: LOG_CT(0x00010000)

DESCRIPTION: This indicates that a CT command completion was received without issuing a corresponding CT command. This error could indicate a driver or firmware problem.

SEVERITY LEVEL: Error

MESSAGE: Stray CT completion

ACTION: No action needed. If problems persist, report these errors to Technical Support.

MSG_ID: 1611 Debug: Abnormal CT completion

VERBOSE_MASK: LOG_CT(0x00010000)

DESCRIPTION: This indicates that a CT command completed with a status error in the IOCB. It could mean the FC device on the network is not responding. The driver will automatically retry this CT command if needed.

SEVERITY LEVEL: Debug

MESSAGE: Abnormal CT completion

ACTION: Check physical connections to FC network and the state of the remote PortID.

MSG_ID: 1620 Debug: CT rcvd

VERBOSE_MASK: LOG_CT(0x00010000)

DESCRIPTION: This indicates that an unsolicited CT command was received.

SEVERITY LEVEL: Debug

MESSAGE: CT rcvd

ACTION: No action needed, informational.

MSG_ID: 1621 Debug: Unsolicited CT dropped

VERBOSE_MASK: LOG_CT(0x00010000)

DESCRIPTION: This indicates that an unsolicited CT command was received and then dropped for some reason.

SEVERITY LEVEL: Debug

MESSAGE: Unsolicited CT dropped.

ACTION: No action needed, informational.

MSG_ID: 1622 Debug: CT reply

VERBOSE_MASK: LOG_CT(0x00010000)

DESCRIPTION: This indicates that a reply is being sent for an unsolicited CT command.

SEVERITY LEVEL: Debug

MESSAGE: CT reply

ACTION: No action needed, informational.

MSG_ID: 1630 Error: Invalid CT command found

VERBOSE_MASK: LOG_CT(0x00010000)

DESCRIPTION: This indicates that a CT command was found with an invalid command code.

SEVERITY LEVEL: Error

MESSAGE: Invalid CT command found

ACTION: No action needed. If problems persist, report these errors to Technical Support.

Appendix

Introduction

Use Cases

Note: The concurrent production use of emlxs (Leadville) and lpfc on a given server is not supported. Transient co-existence is required in some migration use cases but must be discontinued before going into production.

Different use cases will drive different migration scenarios:

Server Platform	Existing lpfc Configuration	Targeted FC Environment	See Section...
x64 and x86	Not applicable	All cases	<i>Installing or Updating the FCA Utilities Using the emlxu_install Script</i> on page 5
SPARC	No Emulex lpfc driver	emlxs (any supported HBA)	<i>Introduction</i> on page 1
	Existing lpfc driver, no FC boot	emlxs (any supported HBA)	<i>Introduction</i> on page 1
	Lpfc to emlxs migration with FC boot		<i>Migrating a Configuration with FC Boot</i> on page 166
	Emulex HBAs – not emlxs supported	Supported Emulex HBAs	<i>Migrating Non-emlxs HBAs to emlxs HBAs</i> on page 166
	Emulex HBAs	Sun-branded HBAs	<i>Migrating an lpfc Configuration to emlxs – Adding Sun-Branded HBAs</i> on page 168

The unsupported sample migration scripts include support for migration in Sun Cluster environments.

This revision does not cover migration of a boot drive, or of logical unit numbers (LUNs) accessed through multipathing software such as EMC PowerPath or Veritas DMP, or of volume managers such as Sun SVM or Veritas VxVM.

Migrating from the Solaris lpfc Driver to the Solaris SFS Driver

If the Emulex lpfc driver for Solaris is already installed, you can migrate to the Solaris SFS driver either by customizing and running the unsupported sample scripts provided by Emulex, or by manually performing a set of procedures.

Operational Differences Between lpfc and SFS

Device discovery operation is different between SFS and lpfc as follows:

- lpfc discovers all fabric target devices by default.
- The FCA driver discovers direct-attach and loop targets, but not fabric attached targets, by default. Use `cfgadm` to indicate which fabric targets you want the driver to discover.
- Firmware download:
 - Sun-branded HBAs: the SFS FCA driver includes the adapter firmware and overrides any firmware version previously residing on the adapter. You cannot update the firmware manually.
 - Emulex SFS-supported HBAs: the Emulex-provided `emlxadm` tool provides a `download_fw` command. Syntax and details are provided in the *Emulex FCA Utilities Reference Manual*.
- Universal Boot download, including OpenBoot (FCode):
 - Sun-branded 2-Gb HBAs: use Sun-provided `luxadm`.
 - Sun-branded 4-Gb HBAs: use the Emulex-provided `emlxadm` tool, which provides a `download_fcode` command (syntax and details are provided in the *Emulex FCA Utilities Reference Manual*).
 - Emulex SFS-supported 2-Gb HBAs: use either `luxadm` or `emlxadm`.
 - Emulex SFS-supported 4-Gb HBAs: use `emlxadm`.

Sample Script File Details

Emulex provides unsupported sample scripts to help you migrate from the Solaris lpfc driver to the Solaris SFS driver. These scripts are available on the SFS driver pages on the Emulex web site. You can customize these scripts and run them to automate the migration process.

start_emlxs_migration.sh

The `start_emlxs_migration.sh` sample script performs the following tasks:

1. Verifies required packages are installed (3 packages - lpfc driver, leadville driver, and the HBAnyware Utility).
2. Cleans up any device-dangling links by running the operating system utility: `devfsadm -C`.
3. Obtains and saves the following information for each HBA in the system:
 - OS device name for the HBA (i.e. reflects PCI path).
 - OS logical controller number for the HBA.
 - Obtains a target number and wwn for all targets configured for each HBA and obtains the number of Luns configured for each target.
4. Writes data to files.

5. Verifies that the system boot device is not an Emulex HBA (if so, the sample script exits with an explanation).
6. Obtains and verifies the FCode version for each HBA in the system. If the FCode version is not compatible, the sample script errors, then exits.
7. Sets the FCode SFS bit to 1 on each adapter.
8. Calls the operating system's add/remove driver utility to configure `/etc/driver_aliases`.
9. Prompts you to reboot the system.

The `adapterN.migrate` and `targetN.migrate` files are generated by the start sample script. These files verify the migration process. Only attached and operational targets are migrated.

- `adapterN.migrate` - where *N* is the adapter number (one file for each adapter); primarily this file contains the adapter device path/name to link lpfc adapters to emlxs adapters across a reboot.
- `targetN.migrate` - where *N* is the adapter number (only adapters with targets configured have this file) - this file has target numbers and WWNs

finish_emlxs_migration.sh

The `finish_emlxs_migration.sh` sample script performs the following tasks:

1. Cleans up any device-dangling links by running the operating system utility: `devfsadm -C`.
2. Performs the following tasks for each HBA in the system:
 - a. Reads the device name from the file that was generated by `start_emlxs_migration.sh`.
 - b. Greps with the `ls -l /dev/cfg` command to acquire the emlxs (Leadville) controller number.
 - c. Writes the lpfc controller number and the emlxs controller number to the map file.
 - d. Constructs a target device name using the target WWN format (e.g. `c3::21000004cf92913c`) for each target in the target file.
3. Uses the `cfgadm -al` command to grep the target device name output and determine if the target device is already configured. Configures the device if necessary with the `cfgadm -c configure` command.
4. Greps with the `/etc/vfstab` command and replaces any lpfc-based storage device entry with its new emlxs-based (Leadville) storage device name entry using the target WWN device name format (e.g. `c3::21000004cf92913c`).
5. Executes a `mountall -l` if any lpfc storage device entry has been replaced with a new Leadville storage device name. Forces the operating system to re-mount local devices with `/etc/vfstab` command.

The `controllermap.migrate` and the `lpfccontroller.migrate` are map files that are generated by the finish sample script.

- `controllermap.migrate` - a file with entries that map the lpfc controller number to the emlxs controller number.
- `lpfccontroller.migrate` - one file with entries that map the adapter lpfc controller numbers to the lpfc adapter numbers (for `/etc/vfstab` parsing).

Migrating a Configuration without FC Boot

Migrating Automatically

Automatic migration provides an equivalent FC storage setup running on the Solaris FC (Leadville) stack. Emulex's Solaris lpfc driver on the SPARC platform uses "sd" as the native SCSI driver, and works in Solaris 2.6, 7, 8, 9 and 10. Emulex's emlxs driver supports the Leadville stack using "ssd" as the SCSI driver. With this procedure, a SAN setup on the host seamlessly migrates from using lpfc to the same setup using emlxs.

Prerequisites

- SPARC server running Solaris 8, 9 or 10.
- Emulex's lpfc driver and associated application kit including HBAnyware installed on the host system.
- Emulex's emlxs driver (SUNWemlxs) installed on the host system.
- Emulex FCode version 1.50a4 or later pre-installed on all HBAs.

Things to Know Before You Migrate

- FC tape devices do not migrate to the emlxs environment. Configure devices after migration.
- lpfc.conf parameters do not migrate into the emlxs driver environment. Note custom configuration values before migration, as default parameters are used after migration. Customize applicable parameters after the migration completes.
- The Leadville stack does not support LUN-level masking. Verify that the system is properly configured to provide the same number of LUNs in emlxs as are contained in the original lpfc environment. For a specific target, any visible LUNs that are not configured in the lpfc environment are automatically configured into the emlxs environment.
- The Leadville stack natively supports mpxio. If you use multipathing or load balancing software, verify that the software functions properly in the new emlxs environment.

Limitations

- If an Emulex HBA is the boot adapter, the sample script exits without proceeding with migration.
- If an Emulex HBA is configured to use the IP over FC interface, the IP interface does not migrate to the emlxs environment.

Procedure

To automatically migrate from lpfc to emlxs:

1. Download the migrate.tar tarball file to the host system in which the lpfc driver is in control and untar it. The tarball file contains two sample script files and a subdirectory containing binary files that are used by the sample scripts.
2. Open the tarball file and view the `start_emlxs_migration.sh` and `finish_emlxs_migration.sh` sample script files. Make changes to these files as needed based upon your system configuration.
3. Login as root and run the `start_emlxs_migration.sh` customized script file (for details, see page 162). After `start_emlxs_migration.sh` is completed, reboot the host system.
4. Login as root and change directory (cd) to where the customized migration scripts are installed.
5. Run the `finish_emlxs_migration.sh` customized script file (for details, see page 163).

Migrating Manually

To migrate manually:

1. Back up all data and system disks.
2. Note current lpfc target and LUN information contained in the following files:
 - /etc/vfstab
 - /kernel/drv/lpfc.conf
 - /kernel/drv/sd.confPersistent binding of the lpfc driver's targets is recommended before performing migration.
3. Using Emulex Iputil or HBAAnyware utilities for lpfc (bundled as part of the driver kit available at <http://www.emulex.com/ts/downloads/solpci/sol.html>):
 - Update the FCode in all adapters to the latest version.
 - Verify that FCode is enabled.
4. Install the required SFS version or patch, as described in *Installing or Updating the Utilities Package Manually* on page 9. SFS will not recognize any existing adapter, as your existing HBAs remain lpfc-attached. Make sure the SFS version and driver patch support the adapters that are to be used.
5. Install the emlxdrv/emlxadm utility package.
6. Start emlxdrv and enter the command `set_emlxs_all`. This changes the bindings of all Emulex adapters from lpfc control to emlxs.
7. Reboot the system with the `shutdown` command.
8. Install any new Sun-branded or Emulex HBAs.
9. Boot to the ok prompt.
10. Issue the Emulex FCode `set-sfs-boot` command to change the Emulex HBA's device path from lpfc to eml. The change will not take effect until the system is reset.

Example:

```
{0} ok show-devs
.
.
.
/pci@8,600000/lpfc@2
.
.
.
{0} ok " /pci@8,600000/lpfc@2" select-dev
^

Space required
{0} ok set-sfs-boot
{0} ok unselect-dev
```

Repeat this step for all adapters in the system. Type `reset-all`, then boot the system to the OS.

11. Configure any targets that were used with the lpfc driver (`cfgadm -a` to display the target list, `cfgadm -c configure <ApId>` to configure the ApId's storage). The ApId can also be referenced in the `/kernel/drv/lpfc.conf` file (for example, `fcplib-WWPN="200400a0b816dc52:lpfc3t4"` could be configured by typing `cfgadm -c configure c6::200400a0b816dc52`).
12. Edit the `/etc/vfstab` file and replace the sd pathname (for example, `c3t4d1s6`) to the ssd pathname (for example, `c6t200400A0B816DC52d1s6`).
13. Redeploy all your targets to the new HBAs following the instructions in the *SAN Foundation Software 4.4 Configuration Manual*.
14. Remove older adapters that are not supported by emlxs.
15. Uninstall HBAnyware and lpfc as follows:
login as `root` or `su` to `root`, then type `pkgrm HBAnyware lpfc`.

Migrating a Configuration with FC Boot

Migrating Non-emlxs HBAs to emlxs HBAs

This case applies if you are currently running only HBAs that are not supported with emlxs, such as LP8000, and migrating to Sun-branded or FCA-recognized Emulex-branded HBAs. In this case, the migration involves procuring emlxs-recognized Sun-branded or Emulex HBAs.

To migrate non-Emulex HBAs to Emulex HBAs:

1. Back up all data and system disks.
2. Install SFS 4.4.7 or higher. It will not recognize any adapters because your existing HBAs remain lpfc-attached.
3. Shut down the system.
4. Install your new Sun-branded or Emulex HBA. Sun-branded HBAs will attach to the Leadville driver (emlxs). Emulex HBAs will attach to the Emulex SD driver (lpfc).
5. Boot the OS.

If you are migrating from one Emulex HBA family to a different family, perform the following additional steps. Otherwise, skip to step 6.

- a. Identify the device path of the new boot drive, using the following format:

```
# format
.
.
.
/pci@8,600000/lpfc@2/sd@1,0
.
.
.
```
- b. Use `emlxdrv` to change only the migrating lpfc-attached HBA family to emlxs. Do not migrate the boot lpfc adapter's family.
- c. Boot the system to the `ok` prompt
- d. Issue the `set-sfs-boot` command to change the remaining Emulex HBA device paths from lpfc to emlxs:

```
{0} ok show-devs
.
.
.
```

```

/pci@8,600000/lpfc@2
.
.
.

{0} ok " /pci@8,600000/lpfc@2" select-dev
{0} ok set-sfs-boot
{0} ok reset-all

```

- e. Boot the system to the OS.
6. Define or designate an alternate boot drive for DAS boot through SFS and the Sun or Emulex HBA. If the alternate boot drive is fabric-attached, configure the storage (by using a command such as `cfgadm -c configure <APID>`).
7. Use the `format` command to identify the alternate boot drive and take note of its path because will be used to boot from the added HBA.
8. Use the `ufsdump` and `ufsrestore` commands (see the *Emulex Remote Boot Guide for SFS Drivers*) to create a fabric boot disk. Follow the instructions until complete.
9. Shut down the server and get to the `ok` prompt.
10. Issue the `set-sfs-boot` command to change the remaining Emulex HBAs device paths from `lpfc` to `emlx`. Changes will not take effect until the system is reset.

Example:

```

{0} ok show-devs
.
.
.
/pci@8,600000/lpfc@2
.
.
.
{0} ok " /pci@8,600000/lpfc@2" select-dev
      ^
      Space required
{0} ok set-sfs-boot
{0} ok unselect-dev

```

Repeat for each HBA in the system. Type `reset-all`, then boot the system to the OS.

11. Boot the new device:
 - For a Sun-branded boot HBA:


```

{0} ok boot
/pci@8,600000/SUNW,emlxs@2/fp@0,0/disk@w21000004cf720664,0:a
          
```
 - For an Emulex boot HBA:


```

{0} ok boot /pci@8,600000/emlx@2/fp@0,0/disk@w21000004cf720664,0:a
          
```
12. Use `emlxdrv` to migrate all supported `lpfc`-attached HBAs to `emlxs`.
13. Reconfigure all FC targets to your `emlxs`-attached HBAs.
14. Remove any HBAs that are not supported by `emlxs` (such as LP8000).
15. Uninstall `lpfc`: login as `root` or `su` to `root`, then type `pkgrm lpfc`.

Migrating an lpfc Configuration to emlxs – Adding Sun-Branded HBAs

This case applies if you plan to migrate all or some of your existing HBAs from lpfc to emlxs, as well as adding Sun-branded HBAs.

The steps to follow are identical to *Migrating Non-emlxs HBAs to emlxs HBAs* on page 166, with the exception that step 14 (removing HBAs not supported by emlxs) may not apply.