EMULEX®

HBAnyware® Utility

Version 3.1

User Manual

Last Updated August 7, 2007

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 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 August 7, 2007

HBAnyware

Introduction

Emulex drivers have many options that you can modify to provide for different behavior. You can change these options using the HBAnyware® utility. The HBAnyware utility is client/server based and provides 'remote' configuration capability to other host platforms running the HBAnyware utility. This remote configuration capability can be provided either "in-band" (host systems on the same FC SAN) or "out-of-band" (from IP addresses of remote machines). The HBAnyware utility also enables the local and “in-band” discovery of Emulex and OEM branded Emulex host bus adapters (HBAs).

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. The client machine from which the request is being made does not need the HBAnyware package or even an installed Emulex HBA. You only need a standard web browser, or some other application capable of making HTTP requests. You do not even need the Java runtime as that too will be automatically downloaded if it is not already present.

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.

Note: The Linux 2.6 SCSI midlayer provides a number of additional services compared to earlier Linux 2.4 kernels. For an overview of 2.6 SCSI and Emulex driver changes, see the white paper on the Linux section of the Emulex Web site.

- The HBAnyware utility is a user-friendly graphical environment. Use the HBAnyware utility to do any of the following:
    - Discover local and remote hosts, host bus adapters (HBAs), targets and LUNs
    - Enables the local and “in-band” discovery of Emulex and OEM branded Emulex HBAs
    - Reset HBAs
    - Set HBA driver parameters
    - Set driver parameters simultaneously to multiple HBAs using Batch Update
    - Set global driver parameters to HBAs
    - Update firmware on a single HBA or multiple HBAs using Batch Update
    - Enable or disable the Boot BIOS
    - Run diagnostic tests on HBAs
    - Manage out-of-band HBAs
    - Manage local and in-band remote HBAs
    - Locate HBAs using beaconing
    - Launch HBAnyware directly from your Web browser

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.

Starting the HBAnyware Utility

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

To start HBAnyware:

Note: For in-band management, remote 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.

1. su to 'root'.
2. Run the script:

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

Starting the HBAnyware Security Configurator

Prerequisites

- Ensure 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 setup the OOB hosts or they will not be seen by the security configurator. See the Out-of-Band SAN Management topics for information.

Procedure

To start the HBAnyware Security Configurator:

1. su to 'root'.
2. Change to the application installation directory. Type:

```
./install ssc
```

3. Run the script:

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

Starting HBAnyware from the Command Line

Procedure

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=Util01

  The HBAnyware utility will show HBAs in the host named Util01.

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

Changing Management Mode

During installation you selected a management mode, however you can change it if you enabled that option during installation.

The HBAnyware utility enables you to choose three types of host/HBA management:

- Strictly Local Management - This setting only allows management of HBAs on this host. Management of HBAs on this host from other hosts is not allowed.
- Local Management Plus - This setting only allows management of HBAs on this host, but management of HBAs on this host from another host is possible.
- Full Management - This setting enables you to manage HBAs on this host and other hosts that allow it.

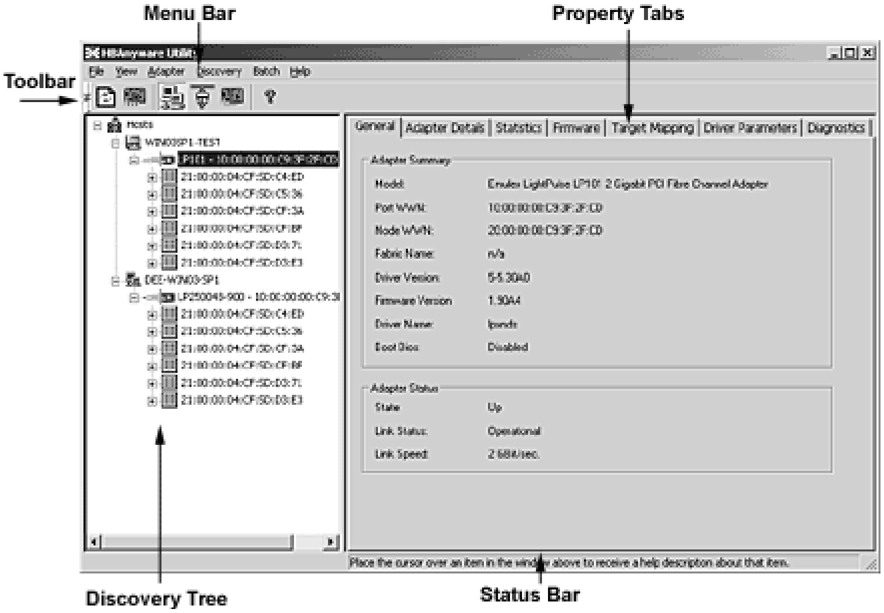
To change management mode:

1. Run the following script:

   ```
   /usr/sbin/hbanyware/set_operating_mode
   ```
2. Choose the management type you want.

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.


Menu Bar
Property Tabs
Toolbar
Discovery Tree
Status Bar
HBAnyware Utility
File View Adapter Discovery Batch Help
General | Adapter Details | Statistics | Firmware | Target Mapping | Driver Parameters | Diagnostics

Hosts
WIN03SP1-TEST
LP101 - 10:00:00:00:C9:3F:2F:CD
21:00:00:04:CF:5D:C4:ED
21:00:00:04:CF:5D:C5:36
21:00:00:04:CF:5D:CF:3A
21:00:00:04:CF:5D:CF:BF
21:00:00:04:CF:5D:D3:71
21:00:00:04:CF:5D:D3:E3
DEE-WIN03-SP1
LP250049-900 - 10:00:00:00:C9:3
21:00:00:04:CF:5D:C4:ED
21:00:00:04:CF:5D:C5:36
21:00:00:04:CF:5D:CF:3A
21:00:00:04:CF:5D:CF:BF
21:00:00:04:CF:5D:D3:71
21:00:00:04:CF:5D:D3:E3

Adapter Summary

Model:	Emulex LightPulse LP101 2 Gigabit PCI Fibre Channel Adapter
Port WWN:	10:00:00:00:C9:3F:2F:CD
Node WWN:	20:00:00:00:C9:3F:2F:CD
Fabric Name:	n/a
Driver Version:	5-5.30A0
Firmware Version:	1.90A4
Driver Name:	lpxnds
Boot Bios:	Disabled

Adapter Status

State:	Up
Link Status:	Operational
Link Speed:	2 GBit/sec.

Place the cursor over an item in the window above to receive a help description about that item.

Figure 1: HBAnyware window

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.

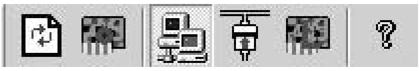


Figure 2: The Toolbar

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 13 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.

Discovery-Tree Icons

Discovery-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 gray 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

The status bar is located near the bottom of the HBAnyware utility window. The status bar displays messages about certain HBAnyware utility functions, such as “Discovery in process”.

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 Command-Line Interface

The CLI (command-line interface) Client component of HBAnyware 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: HBAnyware must be running on all remote hosts that are to be discovered and managed. Remote capabilities of HBAnyware are subject to fabric zoning configuration. Remote hosts to be discovered and managed by HBAnyware must be in the same zone.

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 of the host bus adapter (HBA) that is the target of the command. For example, the following command displays the port attributes for the HBA with the specified World Wide Port Name:

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

Entering /usr/sbin/hbanyware/hbacmd <no qualifiers> displays a list of command options.

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. 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.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.

The CLI Client Command Reference

Version

Syntax: `./hbacmd VERSION (This command is not case sensitive.)`

Description: The current version of the HBAnyware CLI Client application

Parameters: N/A

List HBAs

Syntax: `./hbacmd LISTHBAS (This command is not case sensitive.)`

Description: A list of the discovered manageable Emulex HBAs and their World Wide Node Names.

Parameters: N/A

Display HBA Attributes

Syntax: `./hbacmd HBAAttrib <wwpn>`

Description: A list of attributes for the HBA with the specified World Wide Port Name.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Port Attributes

Syntax: `./hbacmd PortAttrib <wwpn>`

Description: A list of attributes for the port with the specified World Wide Port Name.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Port Statistics

Syntax: `./hbacmd PortStat <wwpn>`

Description: A list of statistics for the port with the specified World Wide Port Name.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Server Attributes

Syntax: `./hbacmd ServerAttrib <wwpn>`

Description: A list of attributes for the specified server.

Parameters: wwpn- The World Wide Port Name of the server.

Download

Syntax: `./hbacmd DOWNLOAD <wwpn> <filename>`

Description: Loads the specified firmware image to the (HBA) with the specified WWPN.

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

Filename- The pathname of the firmware image that is to be loaded. This can be any file that is accessible to the CLI client application, but we recommend that you keep image files in the Emulex Repository folder or directory.

Reset Adapter

Syntax: `./hbacmd RESET <wwpn>`

Description: Resets the HBA with the specified World Wide Port Name.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Target Mapping

Syntax: `./hbacmd TargetMapping <wwpn>`

Description: A list of mapped targets for the port with the specified World Wide Port Name.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Persistent Binding

Syntax: `./hbacmd PersistentBinding <wwpn> <source>`

Description: This function returns a list of the current persistent binding data associated with the HBA specified by ObjectPort. The data may be retrieved either from the driver itself (live), or from a configuration file.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Source- Either C or L. C = Configuration. L = Live.

All Node Info

Syntax: `./hbacmd AllNodeInfo <wwpn>`

Description: This functions retrieves target information for all targets that are visible to the specified HBA. This includes all automapped, persistently-bound, and unmapped targets. Because this function returns information for any unmapped targets, it is a more inclusive call than Persistent Binding.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Set Persistent Binding

Syntax: `./hbacmd SetPersistentBinding <wwpn> <scope> <bindtype> <id> <scsibus> <scsitarget>`

Description: Creates a persistent binding between an FCP target and OS SCSI information.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

Scope- P, I, or B. P = Bind set permanently. I = Bind set immediately. B = Bind set immediately and permanently at reboot.

BindType- D, P, or N. D = Enable binding by D_ID. P = Enable binding by WWPN. N = Enable binding by WWNN.

ID- Either WWPN, WWNN, or D_ID (depending on BindType).

Remove All Persistent Binding

Syntax: `./hbacmd RemoveAllPersistentBinding <wwpn>`

Description: Removes all persistent bindings for the specified HBA. Only the configured bindings can be removed; rebooting is required to remove a live bindings.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

Remove Persistent Binding

Syntax: `./hbacmd RemovePersistentBinding <wwpn> <bindtype> <id> <scsibus> <scsitarget>`

Description: Removes a selected persistent binding. Only the configured bindings can be removed; rebooting is required in order to remove a live binding.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

BindType- D, P, or N. D = Enable binding by D_ID. P = Enable binding by WWPN. N = Enable binding by WWNN.

ID- Either WWPN, WWNN, or D_ID (depending on BindType).

Binding Capabilities

Syntax: `./hbacmd BindingCapabilities <wwpn>`

Description: The flags returned by this function represent all binding capabilities present in the HBA specified by ObjectPort.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

Binding Support

Syntax: `./hbacmd BindingSupport <wwpn> <source>`

Description: This function returns the subset of capabilities that is currently active on the specified HBA.

Parameters: wwpn- The World Wide Port Name of the HBA. The HBA can be either local or remote.

Source- Either C or L. C = Configuration. L = Live.

Set Binding Support

Syntax: `./hbacmd SetBindingSupport <wwpn> <bindflag>`

Description: This function installs a set of active capabilities in the specified HBA.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

Bindflag- D, P, N, A, DA, Pa, or NA. D = Enable binding by D_ID. P = Enable binding by WWPN. N = Enable binding by WWNN. A = Enable binding by AUTOMAP. DA = Enable binding by D_ID and AUTOMAP. PA = Enable binding by WWPN and AUTOMAP. NA = Enable binding by WWNN and AUTOMAP.

Driver Parameters

Syntax: `./hbacmd DriverParams <wwpn>`

Description: This function returns the driver parameters array of the specified HBA. Each entry in the array contains the parameter name and values for minimum value, maximum value, current value, and default value.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

Set Driver Parameters

Syntax: `./hbacmd SetDriverParams <wwpn> <ctrlword> <param> <value>`

Description: This function is used to assign a value to a member of the Driver Parameters array belonging to the HBA referenced by ObjectPort. Only one parameter can be set for each call to this function.

Parameters: wwpn- The World Wide Port Name of the port. The port can be either local or remote.

ctrlword- P, G, B or N. P = Permanent. G = Global. B = Both. N = Neither

Set BootBIOS

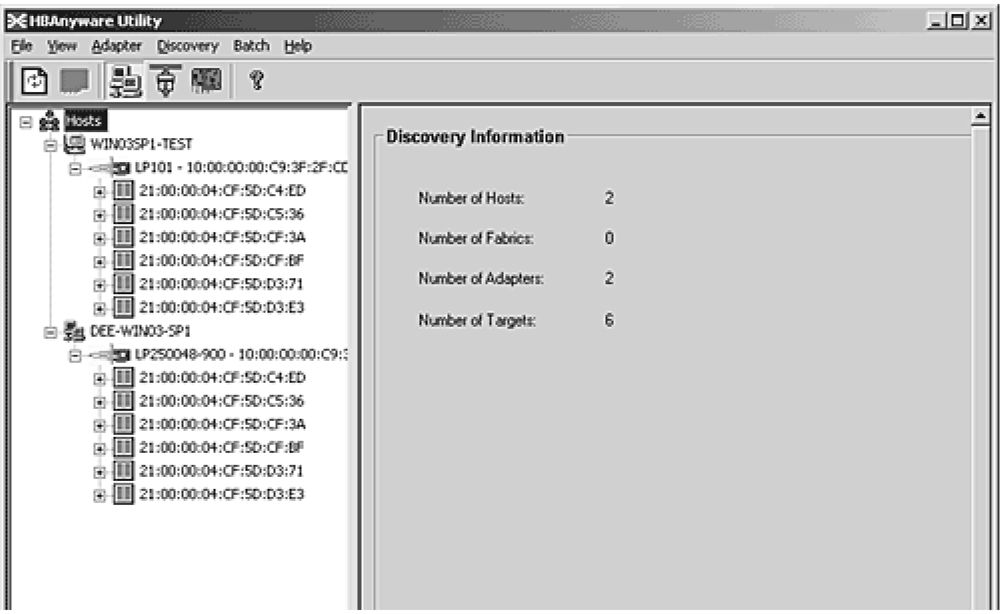
Syntax: `./hbacmd SetBootBios <wwpn> <ctrlword>`

Description: This function is used to enable/disable a BootBIOS firmware file that is present on an HBA. When you download a firmware file which has a Boot BIOS file attached, you have an option to enable or disable this boot file, depending upon the current state of this boot file.

Parameters: ctrlword- E or D. E = Enabled. D = Disabled.

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 “The HBAnyware Utility Window Element Definitions” on page 4.



Hosts
- WIN03SP1-TEST
  - LP101 - 10:00:00:00:C9:3F:2F:CD
    - 21:00:00:04:CF:5D:C4:ED
    - 21:00:00:04:CF:5D:C5:36
    - 21:00:00:04:CF:5D:CF:3A
    - 21:00:00:04:CF:5D:CF:BF
    - 21:00:00:04:CF:5D:D3:71
    - 21:00:00:04:CF:5D:D3:E3
- DEE-WIN03-SP1
  - LP250048-900 - 10:00:00:00:C9:3
    - 21:00:00:04:CF:5D:C4:ED
    - 21:00:00:04:CF:5D:C5:36
    - 21:00:00:04:CF:5D:CF:3A
    - 21:00:00:04:CF:5D:CF:BF
    - 21:00:00:04:CF:5D:D3:71
    - 21:00:00:04:CF:5D:D3:E3

Discovery Information

Number of Hosts:	2
Number of Fabrics:	0
Number of Adapters:	2
Number of Targets:	6

Figure 3: Discovery information

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

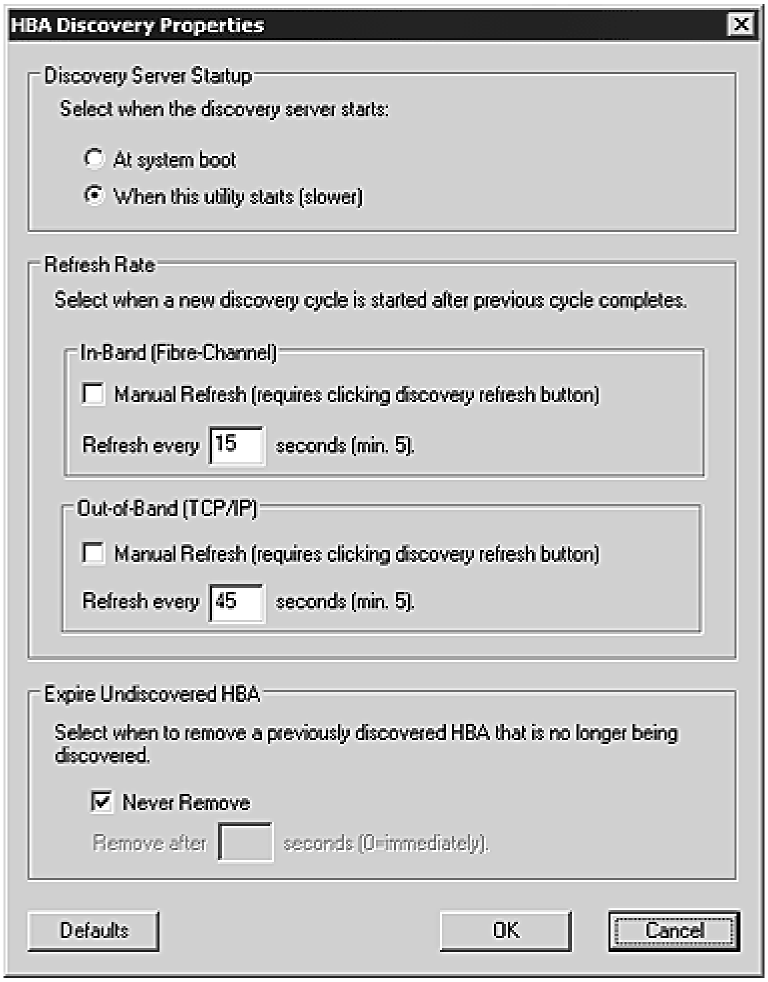
Note: The HBAnyware utility must be installed and the elxhbamgr process(es) must be running on all remote hosts that you want to discover and manage.

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.

When an in-band HBA becomes undiscovered (as seen by the HBAnyware utility running remotely) the target WWPN changes color from black (normal) to blue and the target information is removed from the discovery-tree until the undiscovered HBA timer has expired (See Configuring Discovery Settings on page 12). Similarly, when an out-of-band host is no longer seen by the HBAnyware utility, the HBAs on that host will change from black (normal) to blue, and the target information is not removed from the discovery-tree until the undiscovered HBA timer has expired.

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.



HBA Discovery Properties

Discovery Server Startup

Select when the discovery server starts:

○ At system boot

● When this utility starts (slower)

Refresh Rate

Select when a new discovery cycle is started after previous cycle completes.

In-Band (Fibre-Channel)

□ Manual Refresh (requires clicking discovery refresh button)

Refresh every 15 seconds (min. 5).

Out-of-Band (TCP/IP)

□ Manual Refresh (requires clicking discovery refresh button)

Refresh every 45 seconds (min. 5).

Expire Undiscovered HBA

Select when to remove a previously discovered HBA that is no longer being discovered.

☑ Never Remove

Remove after ___ seconds (0=immediately).

Figure 4: HBA Discovery Properties dialog box

To configure discovery settings:

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

Sorting HBA Information

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

Sort 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.

Sort 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.

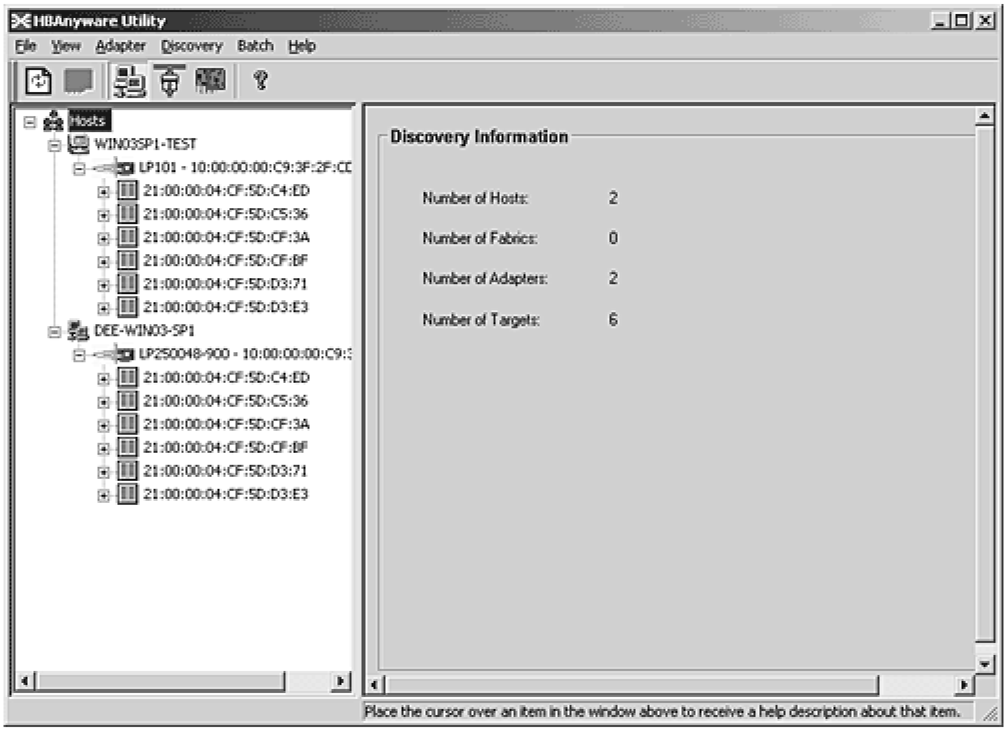
Viewing HBA Information

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. 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.



Discovery Information

Number of Hosts: 2

Number of Fabrics: 0

Number of Adapters: 2

Number of Targets: 6

Place the cursor over an item in the window above to receive a help description about that item.

Figure 5: 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

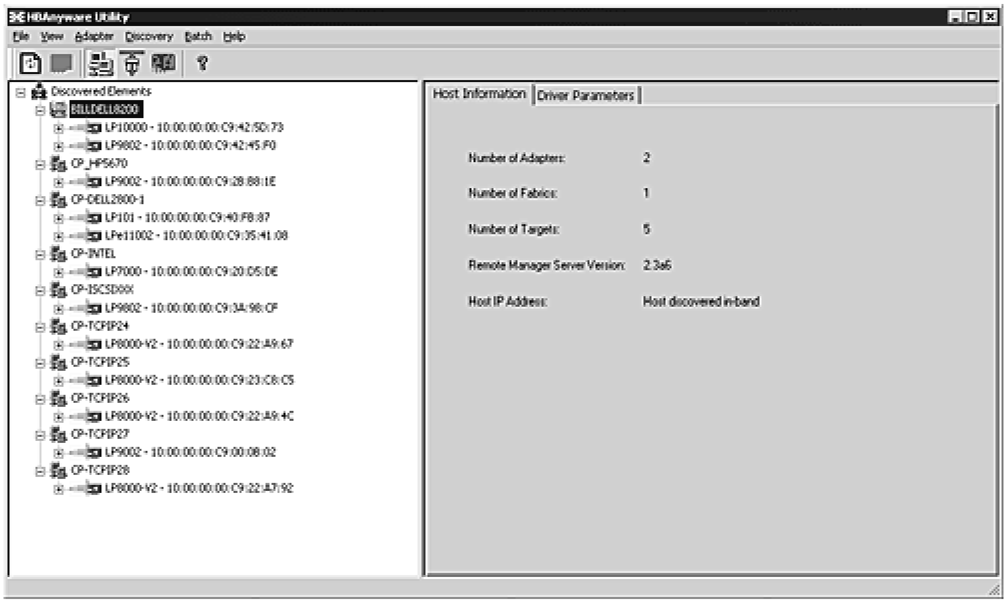
There are two tabs that show host information: the Host Information tab and the host Driver Parameters tab. The Host Information tab is read-only. The host Driver Parameters tab enables you to view and define HBA driver settings for a specific host.

To view the Host Information and Driver Parameters tabs:

1. 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.
2. Select a host in the discovery-tree.
3. Select the **Host Information** tab or the **Host Driver Parameters** tab.

The Host Information Tab

The Host Information tab displays information for the selected host including the number of adapters in the selected host, the number of fabrics to which it is connected and so on.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
BILLDELL8200
LP10000 - 10:00:00:00:C9:42:5D:73
LP9802 - 10:00:00:00:C9:42:45:F0
CP_HP5670
LP9002 - 10:00:00:00:C9:28:88:1E
CP-DELL2800-1
LP101 - 10:00:00:00:C9:40:F8:87
LPe11002 - 10:00:00:00:C9:35:41:08
CP-INTEL
LP7000 - 10:00:00:00:C9:20:D5:DE
CP-ISCSDXXX
LP9802 - 10:00:00:00:C9:3A:98:CF
CP-TCPIP24
LP8000-V2 - 10:00:00:00:C9:22:A9:67
CP-TCPIP25
LP8000-V2 - 10:00:00:00:C9:23:C8:C5
CP-TCPIP26
LP8000-V2 - 10:00:00:00:C9:22:A9:4C
CP-TCPIP27
LP9002 - 10:00:00:00:C9:00:08:02
CP-TCPIP28
LP8000-V2 - 10:00:00:00:C9:22:A7:92
Host Information
Driver Parameters

Number of Adapters:	2
Number of Fabrics:	1
Number of Targets:	5
Remote Manager Server Version:	2.3a6
Host IP Address:	Host discovered in-band

Figure 6: 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.

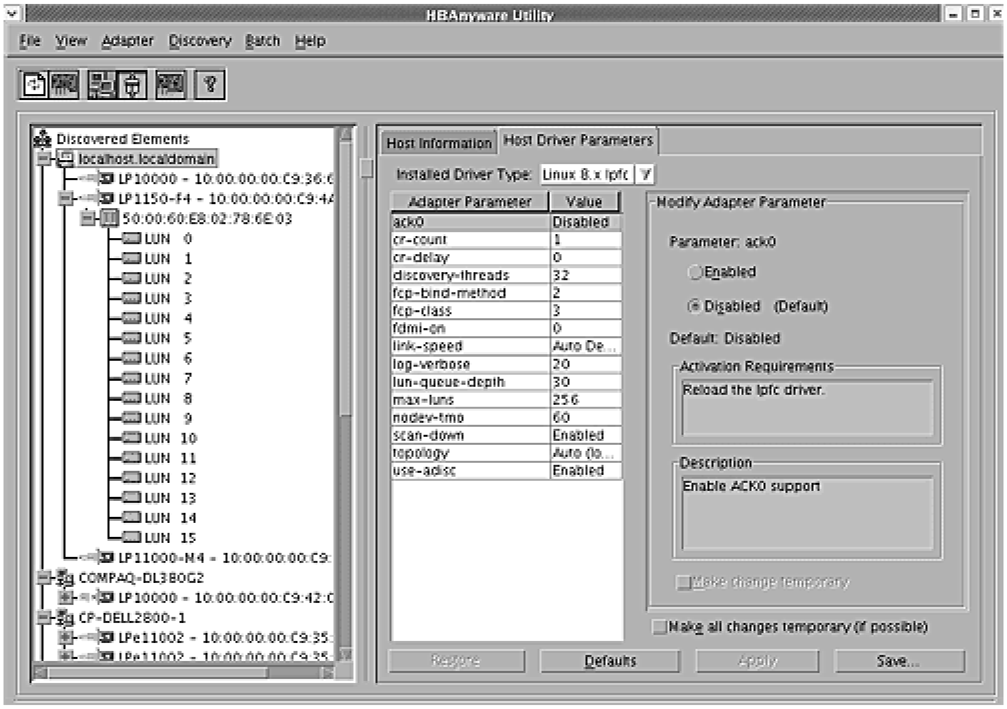
The Host Driver Parameters Tab

The Host Driver Parameters tab 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).

Note: For the Linux 2.6 kernel, most driver parameters are set globally. You can set the lpfc_log_verbose, lpfc_nodev_tmo and lpfc_use_adisc locally.

For more information on changing the parameters for a single HBA, see “Setting Driver Parameters for an HBA” on page 33.

For more information changing the parameters for the host, see “Setting Driver Parameters for a Host” on page 35.



Installed Driver Type: Linux 8.x lpfc

Adapter Parameter	Value
ack0	Disabled
cr-count	1
cr-delay	0
discovery-threads	32
fcp-bind-method	2
fcp-class	3
fdmi-on	0
link-speed	Auto De...
log-verbose	20
lun-queue-depth	30
max-luns	256
nodev-tmo	60
scan-down	Enabled
topology	Auto (lo...
use-adisc	Enabled

Modify Adapter Parameter

Parameter: ack0

○ Enabled

● Disabled (Default)

Default: Disabled

Activation Requirements

Reload the lpfc driver.

Description

Enable ACK0 support

□ Make change temporary

□ Make all changes temporary (if possible)

Figure 7: Host Driver Parameters tab

Driver Parameter Tab Field Definitions

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.

- 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

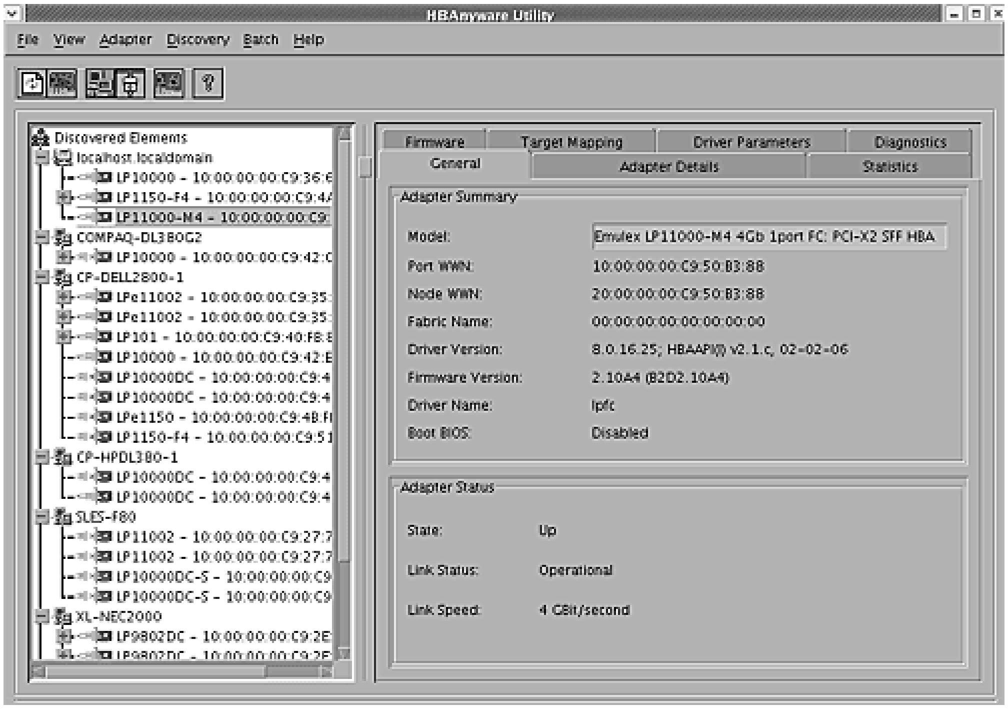
- Restore - Click to save and restore parameters to this last saved value, if you have made changes to parameters and have not saved them by clicking **Apply**.
- Defaults - Click to reset all parameter values to their default (out-of-box) values.
- Apply - Click to apply any driver parameter changes. 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. Select **Host** or **Fabric** sort.
2. Select an HBA in the discovery-tree.


HBAnyware Utility
File
View
Adapter
Discovery
Batch
Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:C
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:F8:E
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:4B:F
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
Firmware
Target Mapping
Driver Parameters
Diagnostics
General
Adapter Details
Statistics

Adapter Summary

Model: Emulex LP11000-M4 4Gb 1port FC: PCI-X2 SFF HBA
Port WWN: 10:00:00:00:C9:50:B3:88
Node WWN: 20:00:00:00:C9:50:B3:88
Fabric Name: 00:00:00:00:00:00:00:00
Driver Version: 8.0.16.25; HBAAPI(I) v2.1.c, 02-02-06
Firmware Version: 2.10A4 (B2D2.10A4)
Driver Name: lpfc
Boot BIOS: Disabled

Adapter Status

State: Up
Link Status: Operational
Link Speed: 4 GBit/second

Figure 8: 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.

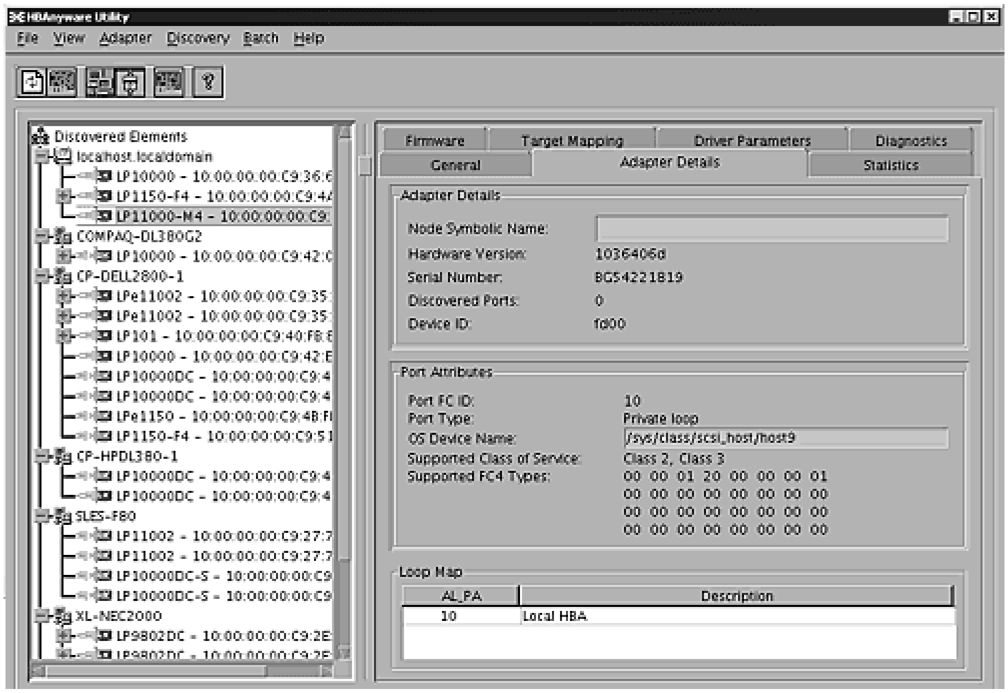
Viewing Detailed HBA Information

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

To view the detailed attributes:

1. Select **Host** or **Fabric** sort.
2. Select an HBA in the discovery-tree.

3. Select the **Adapter Details** tab.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:0
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:F8:E
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:4B:Fl
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
Firmware
Target Mapping
Driver Parameters
Diagnostics
General
Adapter Details
Statistics

Adapter Details

Node Symbolic Name:
Hardware Version: 1036406d
Serial Number: BG54221819
Discovered Ports: 0
Device ID: fd00

Port Attributes

Port FC ID: 10
Port Type: Private loop
OS Device Name: /sys/class/scsi_host/host9
Supported Class of Service: Class 2, Class 3
Supported FC4 Types:

```
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
```

Loop Map

AL_PA	Description
10	Local HBA

Figure 9: 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 - Counts the number of mapped and unmapped ports found during discovery by the Emulex HBA driver. The mapped ports are targets and the unmapped ports are non targets such as switches or HBAs.
- 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 OS.
- 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

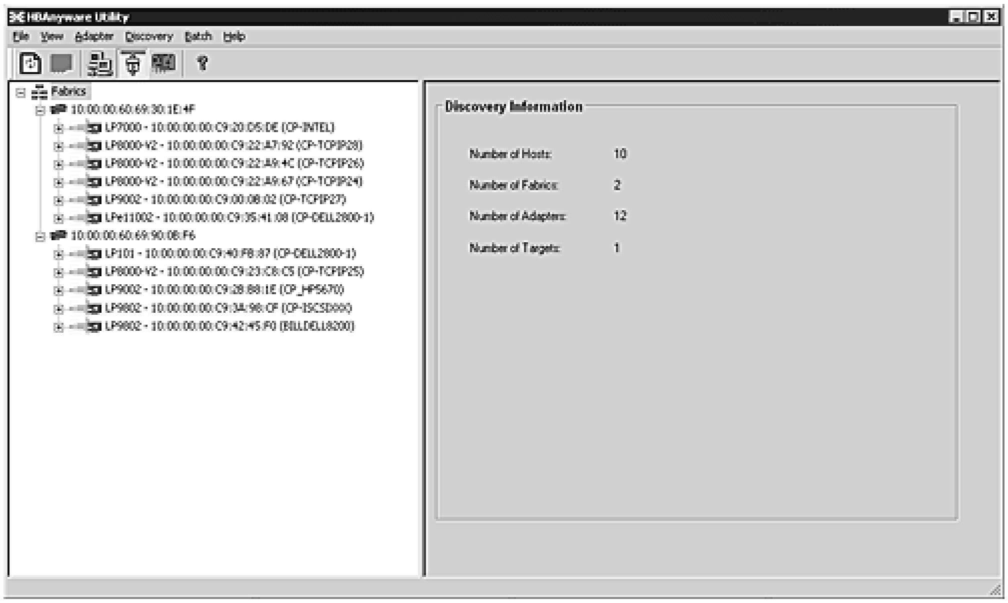
- The loop map shows the different ports present in the loop, and is present only if the port (HBA) is operating in loop mode. The simplest example would be to connect a JBOD directly to an HBA. When this is done, the port type will be a private loop, and the loop map will have an entry for the HBA, 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. 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.
2. Click on a fabric address in the discovery-tree. The Discovery Information tab shows information about the selected fabric.



Fabrics
- 10:00:00:60:69:30:1E:4F
  - LP7000 - 10:00:00:00:C9:20:D5:DE (CP-INTEL)
  - LP8000-V2 - 10:00:00:00:C9:22:A7:92 (CP-TCPIP28)
  - LP8000-V2 - 10:00:00:00:C9:22:A9:4C (CP-TCPIP26)
  - LP8000-V2 - 10:00:00:00:C9:22:A9:67 (CP-TCPIP24)
  - LP9002 - 10:00:00:00:C9:00:08:02 (CP-TCPIP27)
  - LPe11002 - 10:00:00:00:C9:35:41:08 (CP-DELL2800-1)
- 10:00:00:60:69:90:08:F6
  - LP101 - 10:00:00:00:C9:40:F8:87 (CP-DELL2800-1)
  - LP8000-V2 - 10:00:00:00:C9:23:C8:C5 (CP-TCPIP25)
  - LP9002 - 10:00:00:00:C9:28:88:1E (CP_HP5670)
  - LP9802 - 10:00:00:00:C9:3A:98:CF (CP-ISCSDXXX)
  - LP9802 - 10:00:00:00:C9:42:45:F0 (BILLDELL8200)

Discovery Information

Number of Hosts:	10
Number of Fabrics:	2
Number of Adapters:	12
Number of Targets:	1

Figure 10: Discovery information

Discovery Information Field Definitions

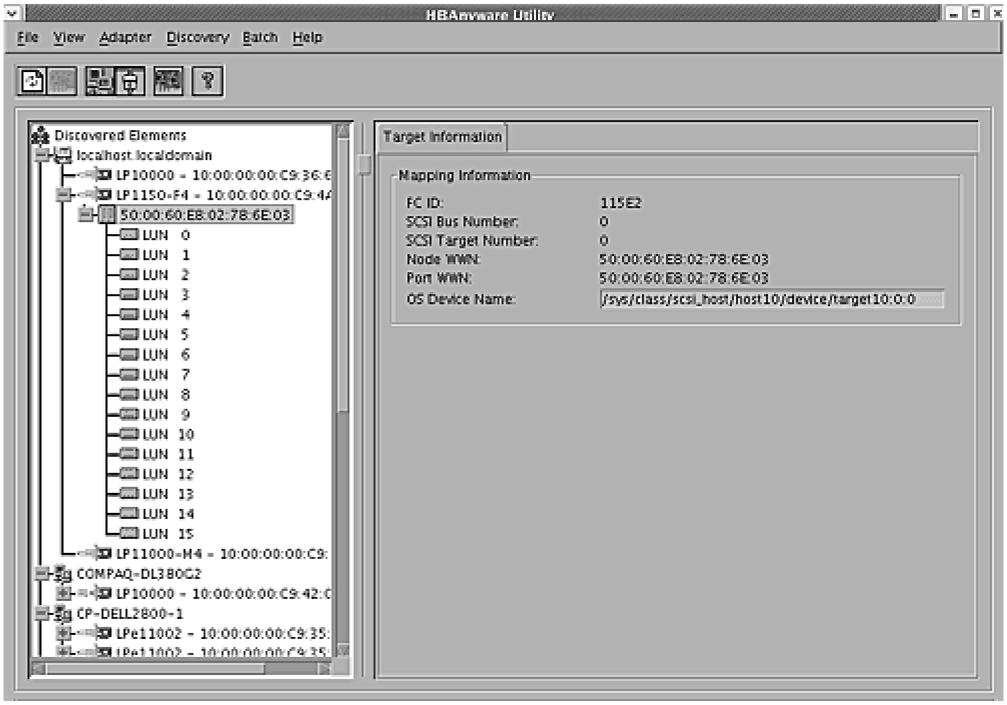
- Number of Hosts - The number of hosts discovered or seen by this host on the selected fabric.
- Number of Fabrics - The number fabrics identified during discovery.
- Number of Adapters - The number of HBAs discovered by this host on the selected fabric.
- Number of Targets - The number of storage devices 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. 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.
2. Click a target in the discovery-tree. The Target Information tab appears.



Mapping Information

FC ID:	115E2
SCSI Bus Number:	0
SCSI Target Number:	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

Figure 11: Target Information tab

Target Information Field Definitions

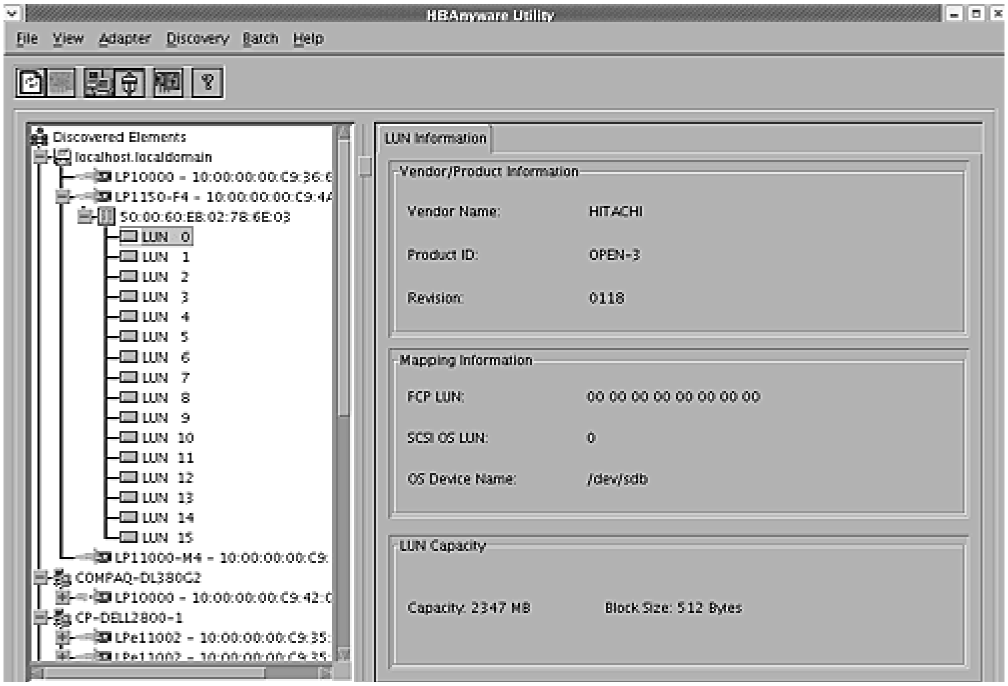
- Mapping Information Area
  - FC ID - The Fibre Channel ID for the target; assigned automatically in the firmware.
  - SCSI Bus Number - Defines the SCSI bus to which the target is mapped.
  - SCSI Target Number - The target's identifier on the SCSI bus.
  - Node WWN - A unique 64-bit number, in hexadecimal, 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 OS device name.

Viewing LUN Information

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

To view the LUN information:

1. 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.
2. Select a LUN in the discovery-tree.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
50:00:60:E8:02:78:6E:03
LUN 0
LUN 1
LUN 2
LUN 3
LUN 4
LUN 5
LUN 6
LUN 7
LUN 8
LUN 9
LUN 10
LUN 11
LUN 12
LUN 13
LUN 14
LUN 15
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:0
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LUN Information

Vendor/Product Information

Vendor Name: HITACHI

Product ID: OPEN-3

Revision: 0118

Mapping Information

FCP LUN: 00 00 00 00 00 00 00 00

SCSI OS LUN: 0

OS Device Name: /dev/sdb

LUN Capacity

Capacity: 2347 MB   Block Size: 512 Bytes

Figure 12: LUN Information tab

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 OS to map to the specific LUN.
    - OS Device Name - The name assigned by the operating system (OS) 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.

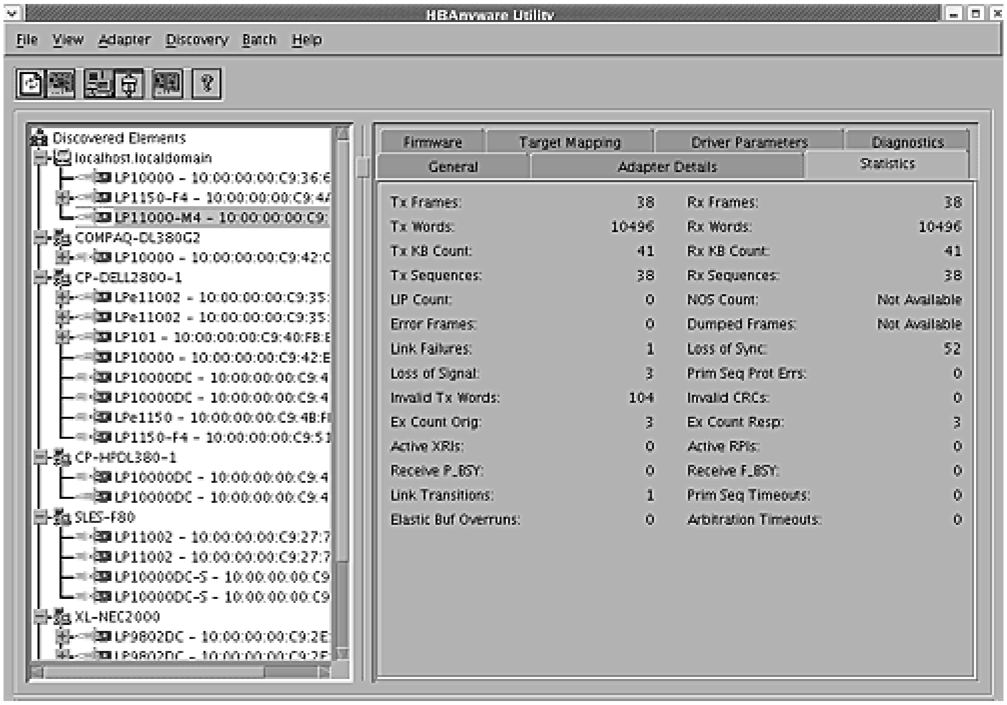
  - Capacity - The capacity of the LUN, in megabytes.
  - Block Length - The length of a logical unit block in bytes.

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. Select **Host** or **Fabric** sort.
2. Select an HBA in the discovery-tree.
3. Click the **Statistics** tab.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:C
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:FB:E
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:4B:F
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
Firmware
Target Mapping
Driver Parameters
Diagnostics
General
Adapter Details
Statistics

Tx Frames:	38	Rx Frames:	38
Tx Words:	10496	Rx Words:	10496
Tx KB Count:	41	Rx KB Count:	41
Tx Sequences:	38	Rx Sequences:	38
LIP Count:	0	NOS Count:	Not Available
Error Frames:	0	Dumped Frames:	Not Available
Link Failures:	1	Loss of Sync:	52
Loss of Signal:	3	Prim Seq Prot Errs:	0
Invalid Tx Words:	104	Invalid CRCs:	0
Ex Count Orig:	3	Ex Count Resp:	3
Active XRIs:	0	Active RPIs:	0
Receive P_BSY:	0	Receive F_BSY:	0
Link Transitions:	1	Prim Seq Timeouts:	0
Elastic Buf Overruns:	0	Arbitration Timeouts:	0

Figure 13: 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.

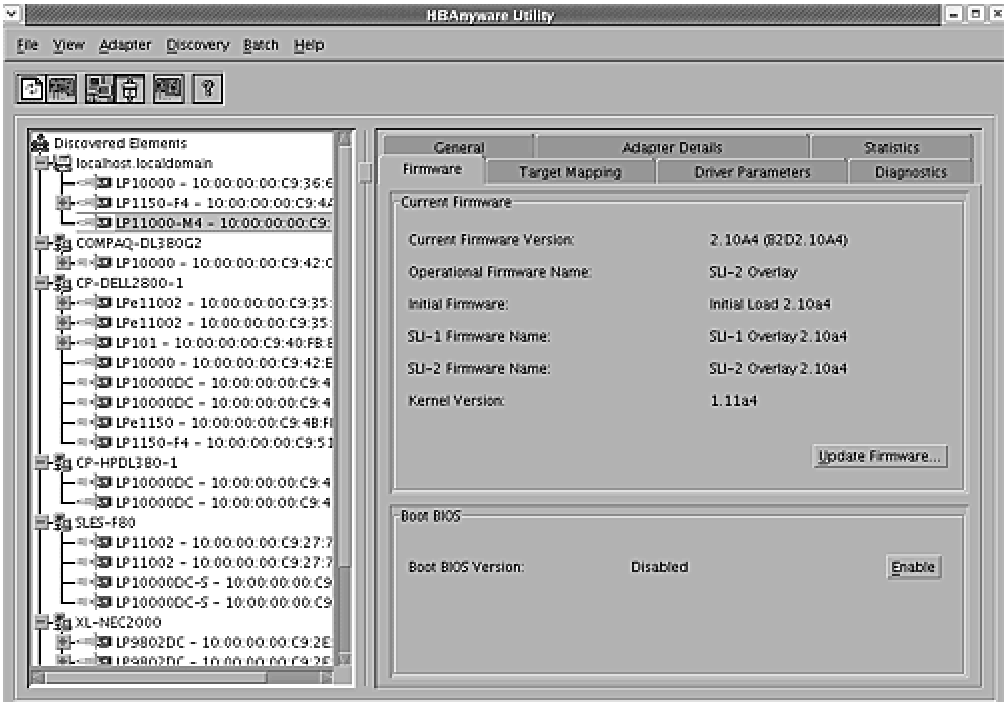
- Error Frames - The number of frames received with cyclic redundancy check (CRC) errors.
- Link Failures - The number of times the link failed. A link failure is a possible cause of a timeout.
- Loss of Signal - The number of times the signal was lost.
- Invalid Tx Words - The total number of invalid 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 is incremented 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.

To view the firmware information:

1. Select **Host** or **Fabric** sort.
2. Select an HBA in the discovery-tree.
3. Select the **Firmware** tab.


HBAnyware Utility
File
View
Adapter
Discovery
Batch
Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:C
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:F8:E
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:4B:F
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
General
Adapter Details
Statistics
Firmware
Target Mapping
Driver Parameters
Diagnostics
Current Firmware
Update Firmware...
Boot BIOS
Enable

Current Firmware Version: 2.10A4 (82D2.10A4)

Operational Firmware Name: SLI-2 Overlay

Initial Firmware: Initial Load 2.10a4

SLI-1 Firmware Name: SLI-1 Overlay 2.10a4

SLI-2 Firmware Name: SLI-2 Overlay 2.10a4

Kernel Version: 1.11a4

Boot BIOS Version: Disabled

Figure 14: 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 BootBIOS 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 Using HBAnyware” topic on page 27 for more information.

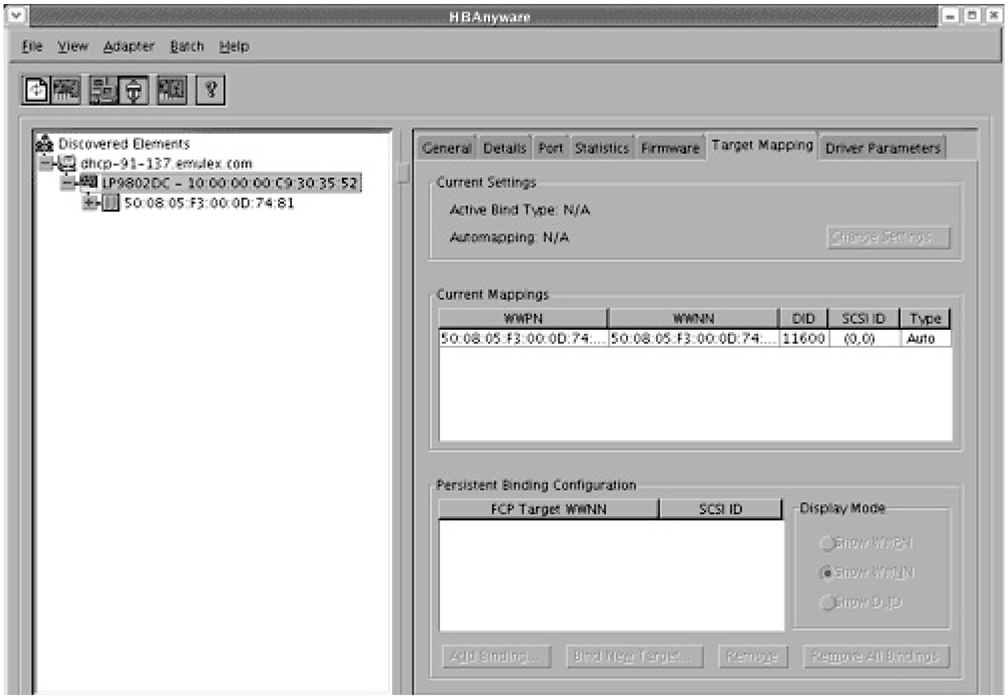
Viewing Target Mapping

Use this tab to view target mapping. The Target Mapping tab is read-only.

Note: Persistent binding is not supported by the Linux 2.6 kernel or by the Emulex version 8 driver for Linux.

To view target mapping:

1. Select **Host** or **Fabric** sort.
2. Select the HBA in the discovery-tree whose target mapping information you wish to view.
3. Select the **Target Mapping** tab.


HBAnyware
File View Adapter Batch Help
General Details Port Statistics Firmware Target Mapping Driver Parameters
Change Settings...
Display Mode
○ Show WWPN
● Show WWNN
○ Show D_ID
Add Binding... Bind New Target... Remove Remove All Bindings

Discovered Elements
dhcp-91-137.emulex.com
LP9802DC - 10:00:00:00:C9:30:35:52
50:08:05:F3:00:0D:74:81

Current Settings

Active Bind Type: N/A

Automapping: N/A

Current Mappings

WWPN	WWNN	DID	SCSI ID	Type
50:08:05:F3:00:0D:74:...	50:08:05:F3:00:0D:74:...	11600	(0,0)	Auto

Persistent Binding Configuration

FCP Target WWNN	SCSI ID

Figure 15: Target Mapping tab

Target Mapping Field Definitions

Current Settings Area

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

Current Mappings Table

- This table lists current mapping information for the selected HBA.

Persistent Binding Configuration Table

- N/A

Display Mode Radio Buttons

- N/A

Target Mapping Buttons

- N/A

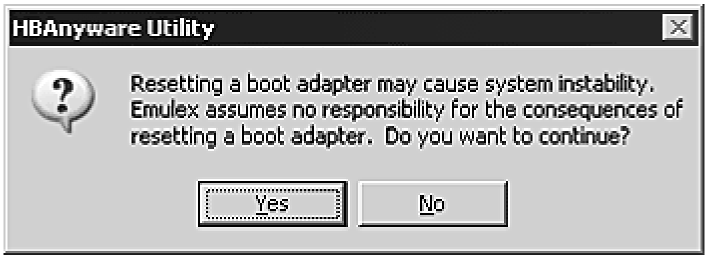
Resetting HBAs

You can reset HBAs using HBAnyware.

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

To reset the HBA using the HBAnyware utility:

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



Resetting a boot adapter may cause system instability. Emulex assumes no responsibility for the consequences of resetting a boot adapter. Do you want to continue?

Figure 16: Reset Warning dialog box

4. 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

You can update firmware on local and remote HBAs using HBAnyware.

Prerequisites

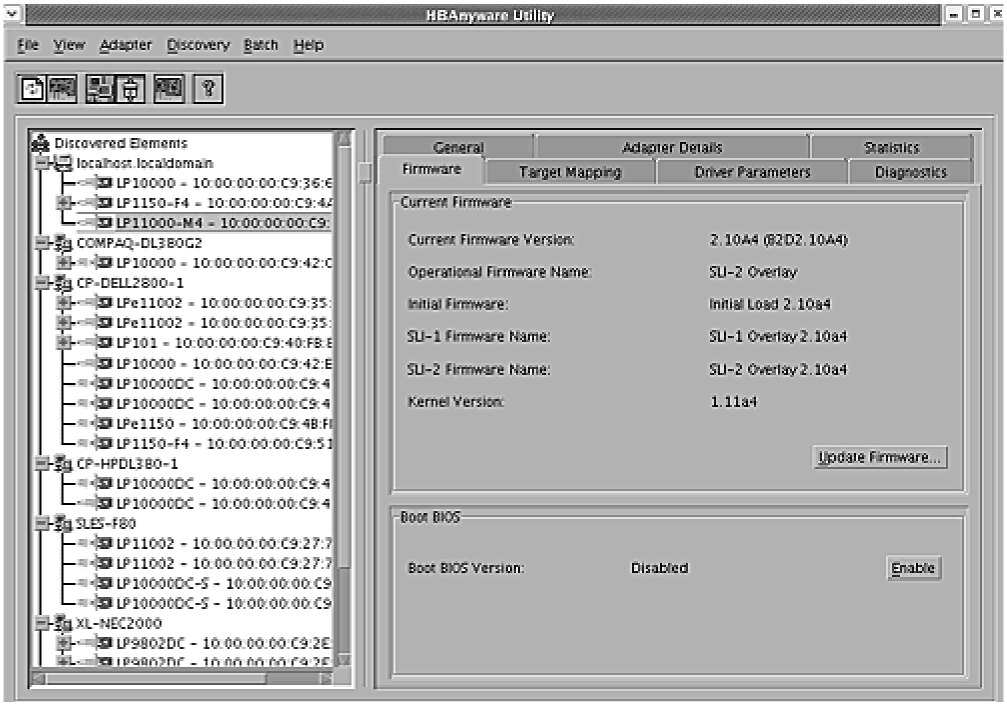
- The Emulex driver is installed properly.
- The HBAnyware utility is installed properly.
- The firmware file has been downloaded from the Emulex Web site and extracted.

Note: For OEM branded HBAs, see the OEM’s Web site or contact the OEM’s customer service department or technical support department for the firmware files.

Procedure

To update firmware:

1. In the discovery-tree, select the HBA whose firmware you wish to update.
2. Select the **Firmware** tab.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:C
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:F8:E
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:4B:F
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
General
Adapter Details
Statistics
Firmware
Target Mapping
Driver Parameters
Diagnostics
Update Firmware...
Enable

Current Firmware

Current Firmware Version: 2.10A4 (B2D2.10A4)

Operational Firmware Name: SLI-2 Overlay

Initial Firmware: Initial Load 2.10a4

SLI-1 Firmware Name: SLI-1 Overlay 2.10a4

SLI-2 Firmware Name: SLI-2 Overlay 2.10a4

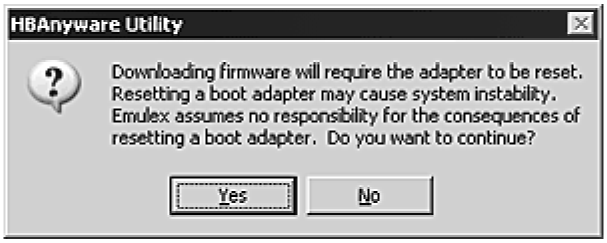
Kernel Version: 1.11a4

Boot BIOS

Boot BIOS Version: Disabled

Figure 17: Firmware tab

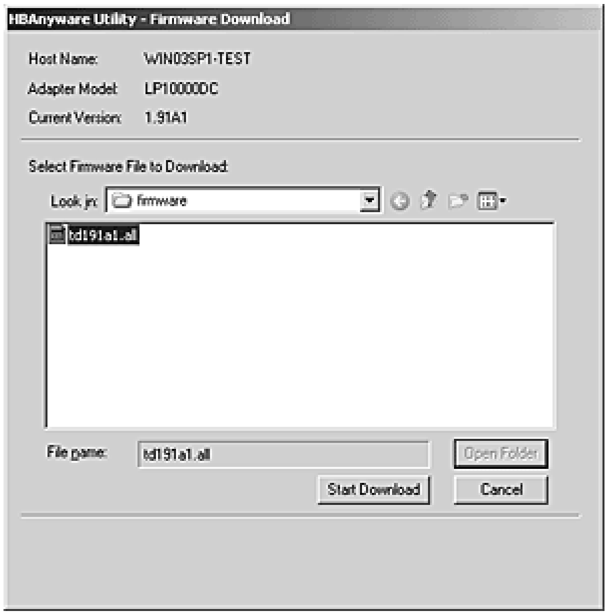
3. Click **Update Firmware**. The following warning screen appears:



Downloading firmware will require the adapter to be reset. Resetting a boot adapter may cause system instability. Emulex assumes no responsibility for the consequences of resetting a boot adapter. Do you want to continue?

Figure 18: Firmware Warning dialog box

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


HBAnyware Utility - Firmware Download

Host Name: WIN03SP1-TEST

Adapter Model: LP10000DC

Current Version: 1.91A1

Select Firmware File to Download:

Look in: firmware

td191a1.all

File name: td191a1.all

Figure 19: Firmware Download dialog box

5. Navigate to the extracted firmware file you wish to download. Select the file and click **Start Download**. A status bar shows the progress of the download and indicates when the download is complete.
6. Click **Close**. The Firmware tab displays the updated firmware information for the selected HBA.

If you are updating the firmware on a dual-channel HBA, repeat steps 1 through 6 to update the firmware on the second port or use the “Updating Firmware (Batch Mode) Using the HBAnyware Utility” procedure on page 29.

Note: If the state of the boot code on the board has changed, this change will be reflected immediately on the General tab.

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 Emulex driver is installed.
- HBAnyware is installed.
- 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.

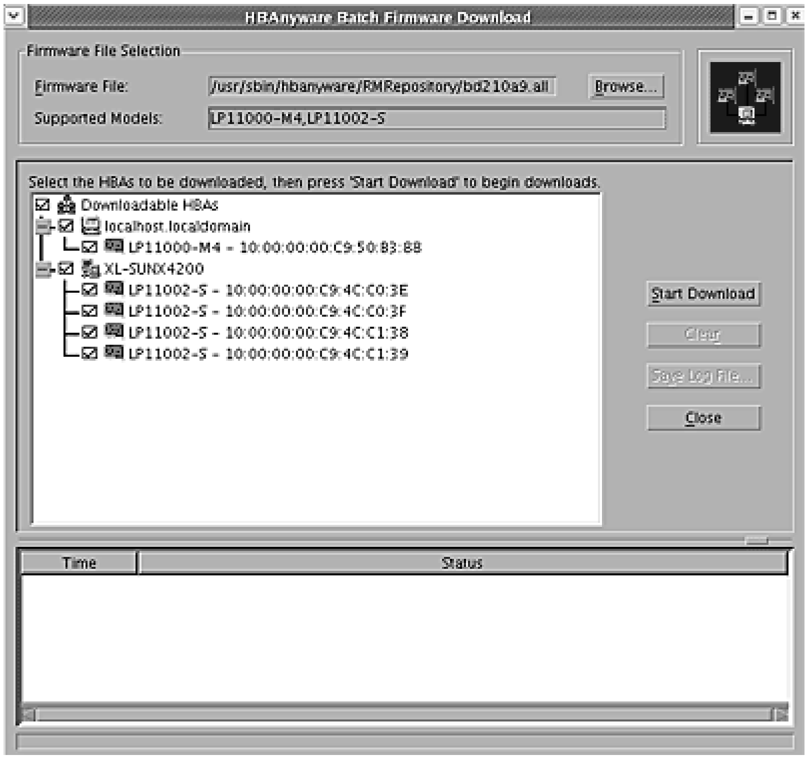
Procedure

To batch load firmware:

1. From the menu bar, select **Batch** and click **Download Firmware.**

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

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



HBAnyware Batch Firmware Download

Firmware File Selection

Firmware File: /usr/sbin/hbanyware/RMRepository/bd210a9.all

Supported Models: LP11000-M4,LP11002-S

Select the HBAs to be downloaded, then press 'Start Download' to begin downloads.

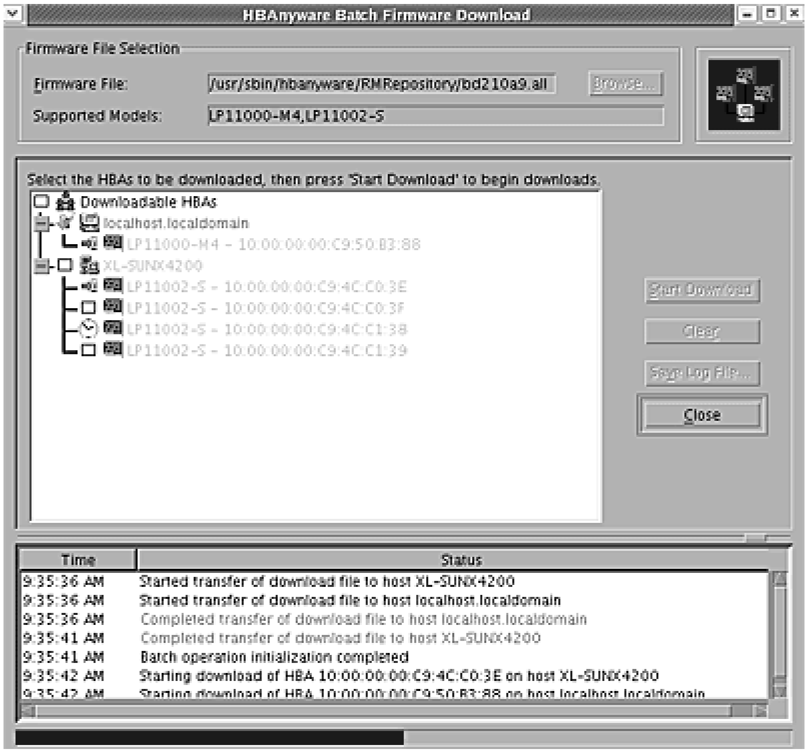
```
☑ Downloadable HBAs
☑ localhost.localdomain
   ☑ LP11000-M4 - 10:00:00:00:C9:50:83:88
☑ XL-SUNX4200
   ☑ LP11002-S - 10:00:00:00:C9:4C:C0:3E
   ☑ LP11002-S - 10:00:00:00:C9:4C:C0:3F
   ☑ LP11002-S - 10:00:00:00:C9:4C:C1:38
   ☑ LP11002-S - 10:00:00:00:C9:4C:C1:39
```

Time	Status

Figure 20: 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.

3. Make your selections and click **Start Download**.
4. 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.



Firmware File: /usr/sbin/hbanyware/RMRepository/bd210a9.all

Supported Models: LP11000-M4,LP11002-S

Select the HBAs to be downloaded, then press 'Start Download' to begin downloads.

```
□ Downloadable HBAs
  localhost.localdomain
    LP11000-M4 - 10:00:00:00:C9:50:83:88
□ XL-SUNX4200
    LP11002-S - 10:00:00:00:C9:4C:C0:3E
  □ LP11002-S - 10:00:00:00:C9:4C:C0:3F
    LP11002-S - 10:00:00:00:C9:4C:C1:38
  □ LP11002-S - 10:00:00:00:C9:4C:C1:39
```

```
Time         Status
9:35:36 AM   Started transfer of download file to host XL-SUNX4200
9:35:36 AM   Started transfer of download file to host localhost.localdomain
9:35:36 AM   Completed transfer of download file to host localhost.localdomain
9:35:41 AM   Completed transfer of download file to host XL-SUNX4200
9:35:41 AM   Batch operation initialization completed
9:35:42 AM   Starting download of HBA 10:00:00:00:C9:4C:C0:3E on host XL-SUNX4200
9:35:42 AM   Starting download of HBA 10:00:00:00:C9:50:83:88 on host localhost.localdomain
```

Figure 21: Firmware Download dialog box with completed download

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

Enabling or Disabling an HBA's BIOS

Enabling the BIOS is a two-step process:

1. Enable the HBA BIOS (x86 BootBIOS, FCode or EFIBoot) to read the Emulex boot code on the HBA.
2. Enable the HBA to boot from SAN (using the BIOS utility).

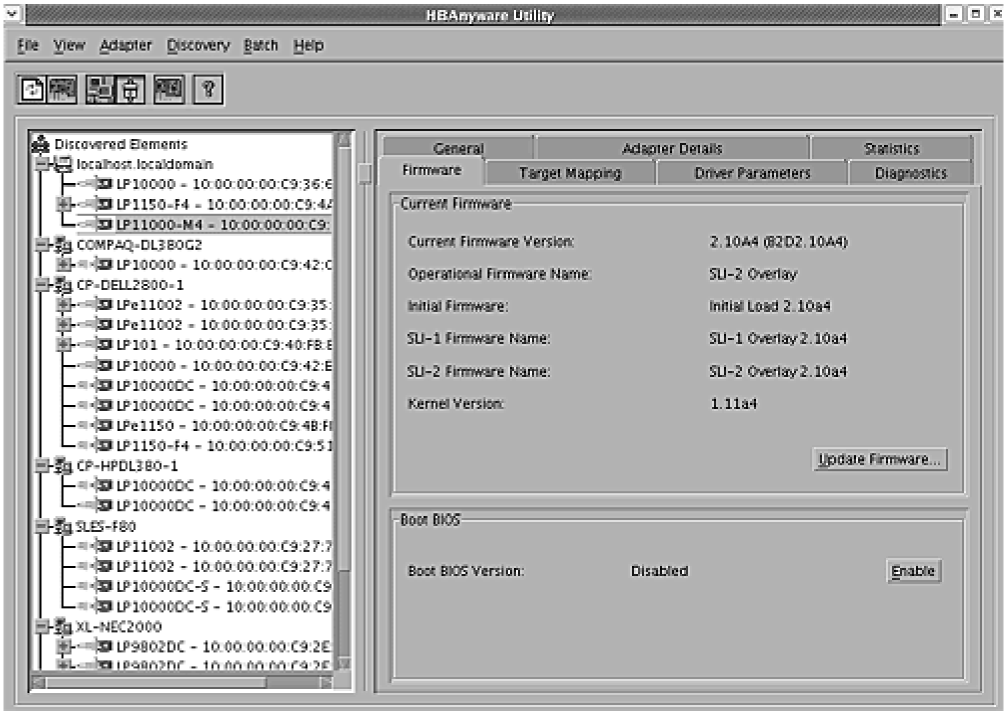
Prerequisites

- The Emulex driver is installed properly.

Procedure

To enable or disable the HBA BIOS:

1. In the discovery-tree, select the HBA whose BIOS you wish to enable or disable.
2. Select the **Firmware** Tab.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:C
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:F8:E
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:4B:F
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
General
Adapter Details
Statistics
Firmware
Target Mapping
Driver Parameters
Diagnostics
Current Firmware
Update Firmware...
Boot BIOS
Enable

Current Firmware Version: 2.10A4 (B2D2.10A4)

Operational Firmware Name: SLI-2 Overlay

Initial Firmware: Initial Load 2.10a4

SLI-1 Firmware Name: SLI-1 Overlay 2.10a4

SLI-2 Firmware Name: SLI-2 Overlay 2.10a4

Kernel Version: 1.11a4

Boot BIOS Version: Disabled

Figure 22: Firmware tab with BIOS disabled

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

   Or

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

   Note: If the BIOS state on the board changes, the change reflects immediately on the General tab

   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.

Configuring the Driver

You can configure the driver using the following methods:

Note: Driver parameter changes made using the HBAnyware utility persist if the driver is uninstalled. To return to the default settings, you must modify the settings in modprobe.conf.

- Setting driver parameters using the HBAnyware utility.
- Specifying parameters when loading the driver manually.

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_nodev_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.

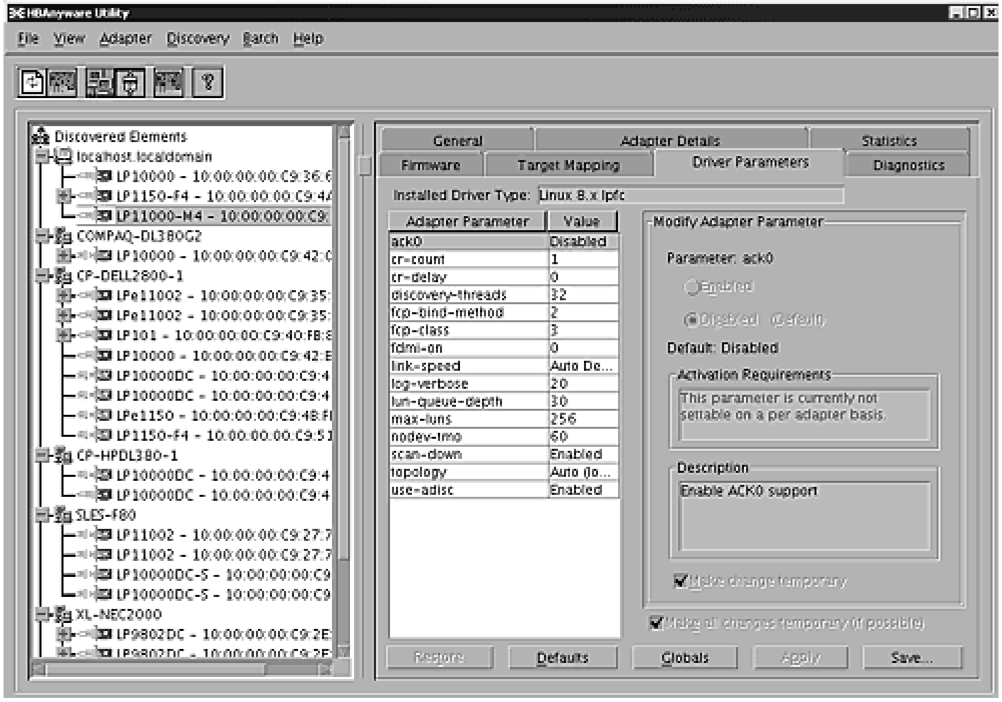
You can also apply driver parameters for one HBA to other HBAs in the system using the Driver Parameters tab. When you define parameters for an HBA, you create a .dpv file. The .dpv file contains the parameters for that HBA. After you create the .dpv file, the HBAnyware utility enables you to apply the .dpv file parameters to multiple HBAs in the system, thereby simplifying multiple HBA configuration. See “Creating the Batch Mode Driver Parameters File” on page 36 for more information.

Note: The Linux 2.6 kernel only supports setting the log_verbose, nodev_tmo and use_adisk driver parameters for individual HBAs. You must apply other driver parameters to all HBAs contained in the host.

Setting Driver Parameters for an HBA

To change the driver parameters for an HBA:

1. 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.
2. In the discovery-tree, select the HBA whose parameters you wish to change.
3. Select the **Driver Parameters** tab. The parameter values for the selected HBA are displayed.


HBAnyware Utility
File View Adapter Discovery Batch Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:6
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:0
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:FB:8
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:48:FI
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
General
Adapter Details
Statistics
Firmware
Target Mapping
Driver Parameters
Diagnostics
Restore
Defaults
Globals
Apply
Save...

Installed Driver Type: Linux 8.x lpfc

Adapter Parameter	Value
ack0	Disabled
cr-count	1
cr-delay	0
discovery-threads	32
fcp-bind-method	2
fcp-class	3
fdmi-on	0
link-speed	Auto De...
log-verbose	20
lun-queue-depth	30
max-luns	256
nodev-tmo	60
scan-down	Enabled
topology	Auto (lo...
use-adisc	Enabled

Modify Adapter Parameter

Parameter: ack0

○ Enabled

● Disabled (Default)

Default: Disabled

Activation Requirements

This parameter is currently not settable on a per adapter basis.

Description

Enable ACK0 support

☑ Make change temporary

☑ Make all changes temporary (if possible)

Figure 23: Driver Parameters tab - HBA selected

4. 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.
5. 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".
6. 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.
7. 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.
8. 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**.

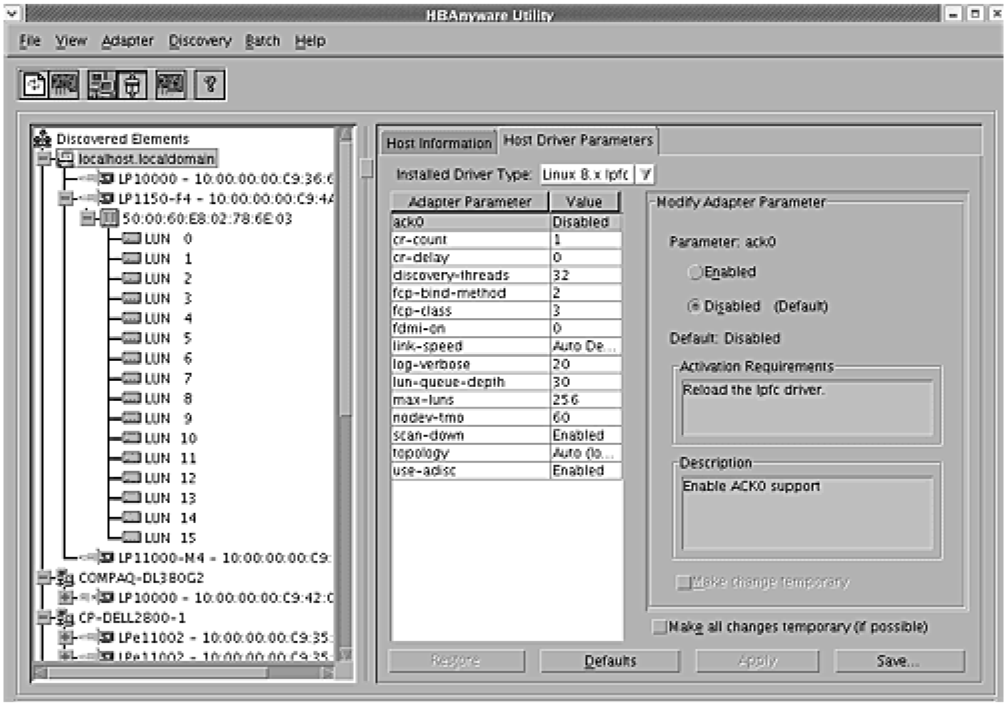
Resetting All Default Values

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. 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.
2. In the discovery-tree, click the host whose HBA driver parameters you wish to change.
3. Select 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.
4. 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.



Installed Driver Type: Linux 8.x lpfc

Adapter Parameter	Value
ack0	Disabled
cr-count	1
cr-delay	0
discovery-threads	32
fcp-bind-method	2
fcp-class	3
fdmi-on	0
link-speed	Auto De...
log-verbose	20
lun-queue-depth	30
max-luns	256
nodev-tmo	60
scan-down	Enabled
topology	Auto (lo...
use-adisc	Enabled

Modify Adapter Parameter

Parameter: ack0

○ Enabled

● Disabled (Default)

Default: Disabled

Activation Requirements: Reload the lpfc driver.

Description: Enable ACK0 support

□ Make change temporary

□ Make all changes temporary (if possible)

Figure 24: Driver Parameters tab - host selected

5. 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).
6. 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.
7. 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.
8. 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**.

Changing Non-dynamic Parameter Values (Linux)

To change non-dynamic parameter values:

1. Navigate to the /usr/sbin/hbanyware directory and run the scripts to stop the HBAnyware utility processes. Type:

   ```
   ./stop_hbanyware
   ```
2. Stop all I/O to lpfc attached devices.
3. Unload the lpfcdfc driver. Type:

   ```
   rmmod lpfcdfc
   ```
4. Unload the lpfc driver. Type:

   ```
   rmmod lpfc
   ```
5. Reload the driver.Type:

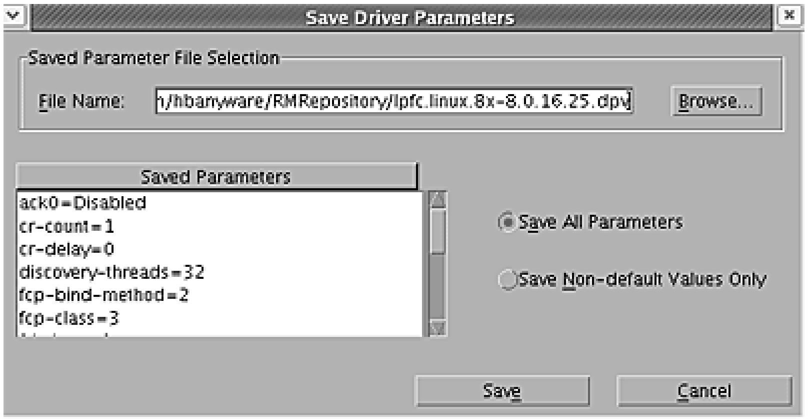
   ```
   modprobe lpfc
   modprobe lpfcdfc
   ```
   The HBAnyware services will start automatically when you launch the application.

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.depths file. The.depths file contains the parameters for that HBA. After you create the.depths file, the HBAnyware utility enables you to apply the.depths file parameters to multiple HBAs in the system, thereby simplifying multiple HBA configuration.

To create the.depths file:

1. Select the HBA whose parameters you want to apply to other HBAs from the discovery-tree.
2. Select the **Driver Parameters** tab. Set the driver parameters.
3. 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.



File Name: h/hbanyware/RMRepository/lpfc.linux.8x-8.0.16.25.dpv

Saved Parameters

ack0=Disabled
cr-count=1
cr-delay=0
discovery-threads=32
fcp-bind-method=2
fcp-class=3

● Save All Parameters

○ Save Non-default Values Only

Figure 25: Save Driver Parameters dialog box

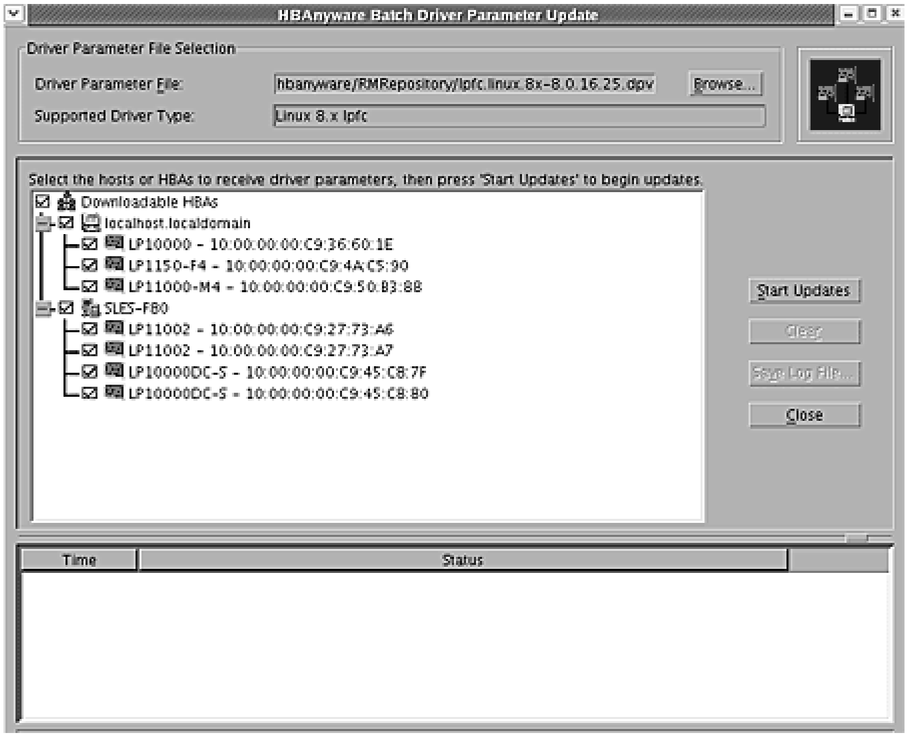
4. The two radio buttons allow you to choose the type of parameters to save. You can save all parameters or only those parameters whose current values differ from their corresponding default values.
5. A list of the saved parameters and their current values show in the Saved Parameters box.
6. Click **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 36 to learn how to create the .dpv file.

To assign batch mode parameters to HBAs:

1. From Batch menu 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.
2. 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.



HBAnyware Batch Driver Parameter Update
Driver Parameter File Selection
Browse...
Start Updates
Clear
Save Log File...
Close
Time
Status

Driver Parameter File: hbanyware/RMRepository/lpfc.linux.8x-8.0.16.25.dpv

Supported Driver Type: Linux 8.x lpfc

Select the hosts or HBAs to receive driver parameters, then press 'Start Updates' to begin updates.

- ☑ Downloadable HBAs
- ☑ localhost.localdomain
  - ☑ LP10000 - 10:00:00:00:C9:36:60:1E
  - ☑ LP1150-F4 - 10:00:00:00:C9:4A:C5:90
  - ☑ LP11000-M4 - 10:00:00:00:C9:50:B3:8B
- ☑ SLES-FB0
  - ☑ LP11002 - 10:00:00:00:C9:27:73:A6
  - ☑ LP11002 - 10:00:00:00:C9:27:73:A7
  - ☑ LP10000DC-S - 10:00:00:00:C9:45:C8:7F
  - ☑ LP10000DC-S - 10:00:00:00:C9:45:C8:80

Figure 26: Batch Driver Parameters Update dialog box

3. Click **Start Updates**. The HBAnyware 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 Topology

The Driver Parameters tab allows you to change the topology for a single HBA or for all HBAs in one host.

To change topology:

1. In the discovery- tree, click the HBA or the host.
2. Select the **Driver Parameters** tab.
3. Select the **Topology** parameter.
4. Select a new value from the drop-down list.
5. Click **Apply**.
6. Reset the HBA to make this change effective.

Mapping and Masking

Automapping SCSI Devices

The driver defaults to automatically mapping SCSI devices. The procedures in this section apply if the default has been changed.

To automap SCSI devices:

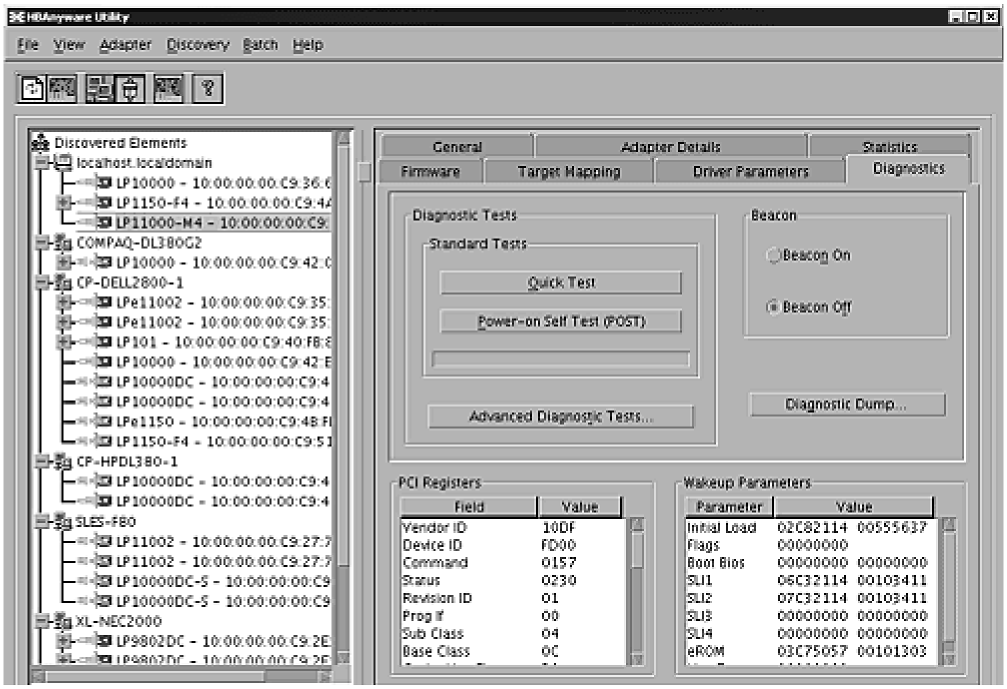
1. Display driver parameters for the host or HBA - select the **Driver Parameters** tab or the **Host Driver Parameters** tab.
2. Select the **AutoMap HBA** parameter. Several fields about the parameter appear on the right side of the screen.
3. Select **Enabled**.
4. If you want a temporary change (where the parameter reverts to its last permanent setting when the system reboots), check the "**Make change temporary**" box. This option is available only for dynamic parameters.
5. If you need to make changes to multiple parameters, and you want all the changes temporary, check the "**Make all changes temporary**" box. This setting overrides the setting of the "Make change temporary" box. Only dynamic parameters can be temporary.
6. To apply your changes, click **Apply**.
7. Reboot the system for this change to take effect.

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 44)
  - Internal Loopback (see page 44)
  - External Loopback (see page 44)
  - Power-On Self Test (POST) (see page 41)
  - Echo (End-to-End) (see page 45)
  - Quick Test (see page 40)
- Perform a diagnostic dump (see page 41)
- View PCI registers and wakeup parameter (see page 42)
- Control HBA beaconing (see page 41)

Note: Diagnostic test functionality is only supported for HBAs that were discovered out-of-band and for HBAs that are installed in the local host.


HBAnyware Utility
File
View
Adapter
Discovery
Batch
Help
Discovered Elements
localhost.localdomain
LP10000 - 10:00:00:00:C9:36:(
LP1150-F4 - 10:00:00:00:C9:4A
LP11000-M4 - 10:00:00:00:C9:
COMPAQ-DL380G2
LP10000 - 10:00:00:00:C9:42:(
CP-DELL2800-1
LPe11002 - 10:00:00:00:C9:35:
LPe11002 - 10:00:00:00:C9:35:
LP101 - 10:00:00:00:C9:40:F8:
LP10000 - 10:00:00:00:C9:42:E
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
LPe1150 - 10:00:00:00:C9:48:F
LP1150-F4 - 10:00:00:00:C9:51
CP-HPDL380-1
LP10000DC - 10:00:00:00:C9:4
LP10000DC - 10:00:00:00:C9:4
SLES-F80
LP11002 - 10:00:00:00:C9:27:7
LP11002 - 10:00:00:00:C9:27:7
LP10000DC-S - 10:00:00:00:C9
LP10000DC-S - 10:00:00:00:C9
XL-NEC2000
LP9802DC - 10:00:00:00:C9:2E
LP9802DC - 10:00:00:00:C9:2E
General
Adapter Details
Statistics
Firmware
Target Mapping
Driver Parameters
Diagnostics
Diagnostic Tests
Standard Tests
Quick Test
Power-on Self Test (POST)
Advanced Diagnostic Tests...
Beacon
Diagnostic Dump...
PCI Registers
Wakeup Parameters

○ Beacon On

● Beacon Off

PCI Registers

Field	Value
Vendor ID	10DF
Device ID	FD00
Command	0157
Status	0230
Revision ID	01
Prog If	00
Sub Class	04
Base Class	0C

Wakeup Parameters

Parameter	Value
Initial Load	02C82114 00555637
Flags	00000000
Boot Bios	00000000 00000000
SLI1	06C32114 00103411
SLI2	07C32114 00103411
SLI3	00000000 00000000
SLI4	00000000 00000000
eROM	03C75057 00101303

Figure 27: Diagnostics tab

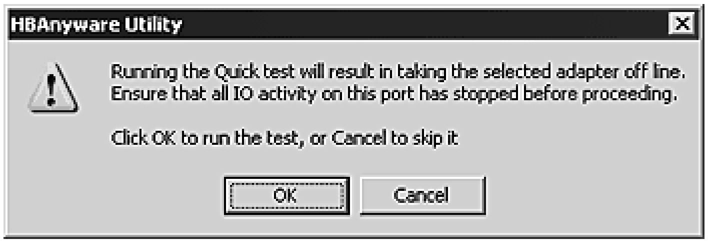
All functions are supported locally and remotely, except for the dump feature which is only supported locally.

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. From the discovery-tree, select the HBA on which you wish to run the Quick Test.
2. Select the **Diagnostics** tab and click **Quick Test**. A warning message appears.



HBAnyware Utility

Running the Quick test will result in taking the selected adapter off line.
Ensure that all IO activity on this port has stopped before proceeding.

Click OK to run the test, or Cancel to skip it

Figure 28: Quick Test Warning Window

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

Running a POST

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:

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

Using Beaconing

The beaconing 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 beaconing, 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 beaconing mode. This cycle repeats indefinitely until you disable this feature or you reset the HBA.

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

To enable or disable beaconing:

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

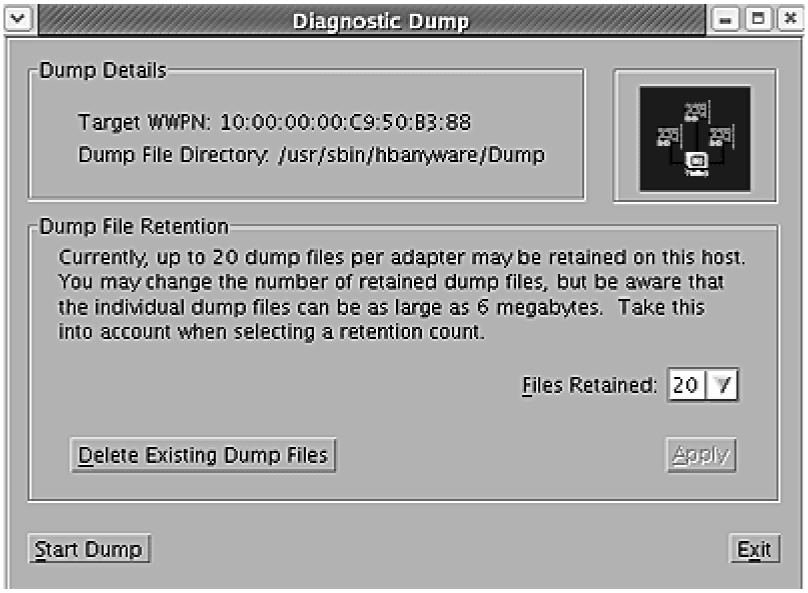
Creating Diagnostic Dumps

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. From the discovery-tree, select a local HBA whose diagnostic information you wish to dump.
2. 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.



Diagnostic Dump

Dump Details

Target WWPN: 10:00:00:00:C9:50:B3:88

Dump File Directory: /usr/sbin/hbanyware/Dump

Dump File Retention

Currently, up to 20 dump files per adapter may be retained on this host. You may change the number of retained dump files, but be aware that the individual dump files can be as large as 6 megabytes. Take this into account when selecting a retention count.

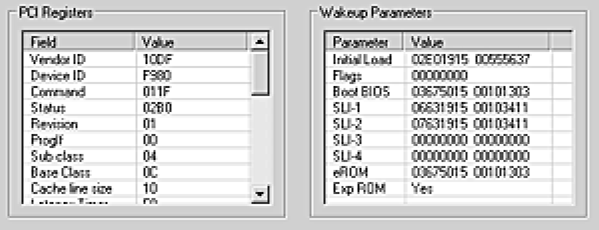
Files Retained: 20

Figure 29: Diagnostic Dump dialog box

3. 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:



PCI Registers

Field	Value
Vendor ID	10DF
Device ID	F980
Command	011F
Status	0280
Revision	01
ProgIf	00
Sub class	04
Base Class	0C
Cache line size	10

Wakeup Parameters

Parameter	Value
Initial Load	02E01915 00555637
Flags	00000000
Boot BIOS	03675015 00101303
SLI-1	06631915 00103411
SLI-2	07631915 00103411
SLI-3	00000000 00000000
SLI-4	00000000 00000000
eROM	03675015 00101303
Exp ROM	Yes

Figure 30: 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:

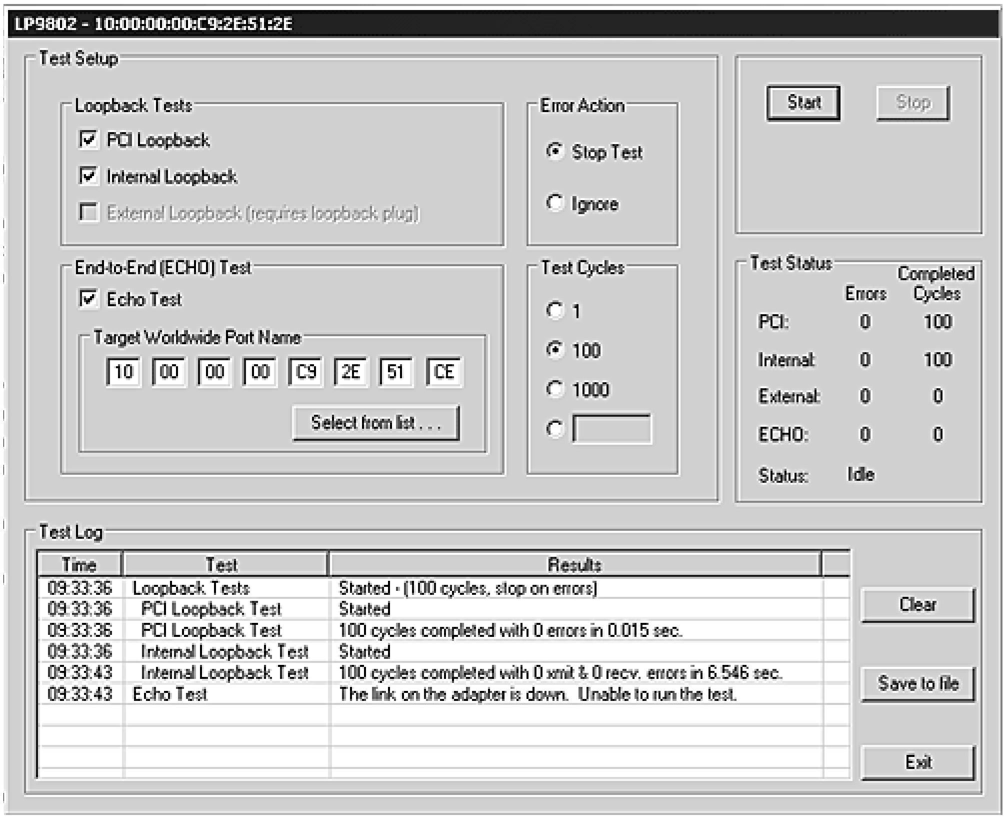
1. Click **Advanced Diagnostics Test** on the Diagnostics tab to view the Advanced Diagnostics dialog box.

   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.



LP9802 - 10:00:00:00:C9:2E:51:2E

Test Setup

Loopback Tests
☑ PCI Loopback
☑ Internal Loopback
☐ External Loopback (requires loopback plug)

Error Action
● Stop Test
○ Ignore

End-to-End (ECHO) Test
☑ Echo Test

Target Worldwide Port Name
10 00 00 00 C9 2E 51 CE

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.
```

Figure 31: Advanced Diagnostics

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:

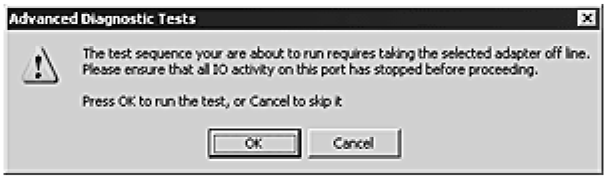
- Stop Test - The error will be logged and the test aborted. No further tests will run.
- Ignore - Log the error and proceed with the next test cycle.

To run loopback tests:

1. From the discovery-tree, select the HBA on which you wish to run the Loopback Test.
2. 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.

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



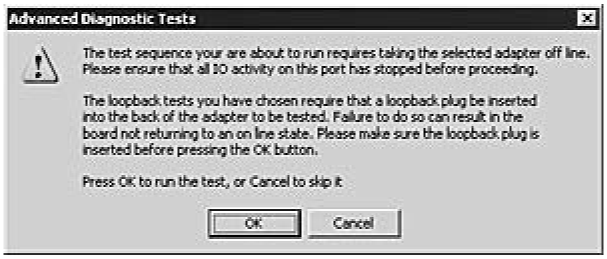
Advanced Diagnostic Tests

The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.

Press OK to run the test, or Cancel to skip it

Figure 32: HBAnyware Utility, Advanced Diagnostic Tests Warning

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



Advanced Diagnostic Tests

The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.

The loopback tests you have chosen require that a loopback plug be inserted into the back of the adapter to be tested. Failure to do so can result in the board not returning to an on line state. Please make sure the loopback plug is inserted before pressing the OK button.

Press OK to run the test, or Cancel to skip it

Figure 33: HBAnyware Utility, Advanced Diagnostic Tests Warning for External Loopback

5. 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.

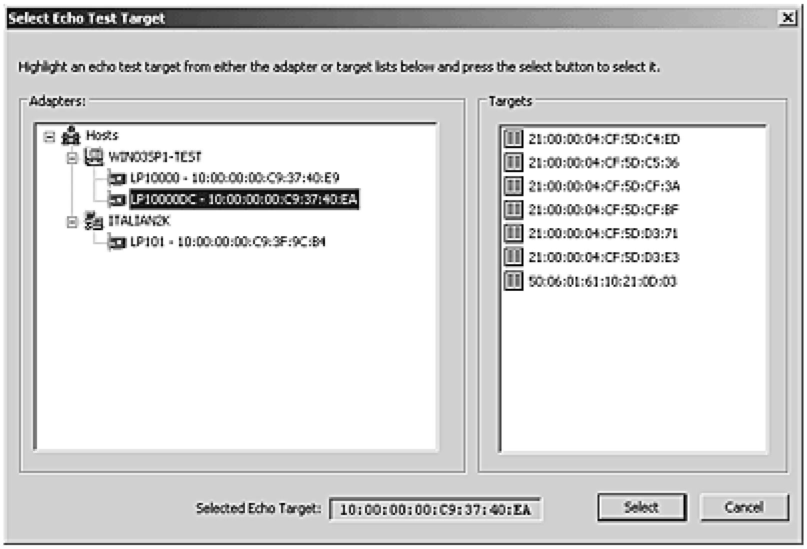
To run end-to-end echo tests:

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** (see Figure 34 on page 46).
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.



Select Echo Test Target

Highlight an echo test target from either the adapter or target lists below and press the select button to select it.

Adapters:

- Hosts
  - WIN03SP1-TEST
    - LP10000 - 10:00:00:00:C9:37:40:E9
    - LP10000DC - 10:00:00:00:C9:37:40:EA
  - ITALIAN2K
    - LP101 - 10:00:00:00:C9:3F:9C:B4

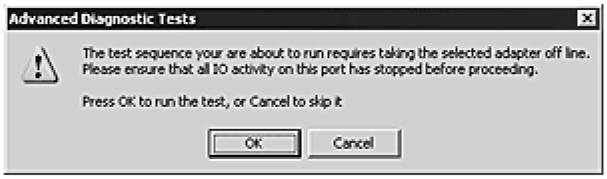
Targets

- 21:00:00:04:CF:5D:C4:ED
- 21:00:00:04:CF:5D:C5:36
- 21:00:00:04:CF:5D:CF:3A
- 21:00:00:04:CF:5D:CF:BF
- 21:00:00:04:CF:5D:D3:71
- 21:00:00:04:CF:5D:D3:E3
- 50:06:01:61:10:21:0D:03

Selected Echo Target: 10:00:00:00:C9:37:40:EA

Figure 34: HBAnyware Utility, Select Echo Test Target Window

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



Advanced Diagnostic Tests

The test sequence your are about to run requires taking the selected adapter off line. Please ensure that all IO activity on this port has stopped before proceeding.

Press OK to run the test, or Cancel to skip it

Figure 35: 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.

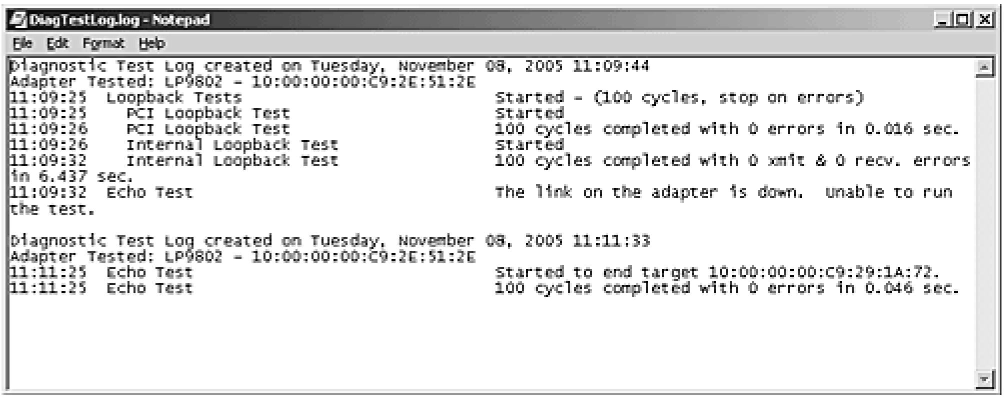
Saving the Log File

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:



```
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 36: 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) SAN management is achieved by sending the remote management requests over a LAN using the Ethernet TCP/IP protocol to remote hosts.

In-band SAN 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:

- An OOB 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.

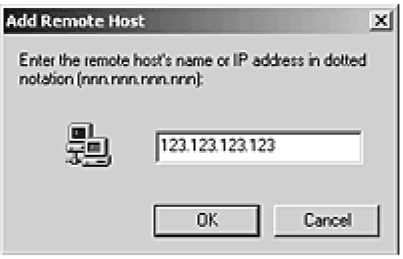
Adding a Single Host

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.



Enter the remote host's name or IP address in dotted notation (nnn.nnn.nnn.nnn):

123.123.123.123

Figure 37: HBAnyware Utility, Add Remote Host Dialog Box

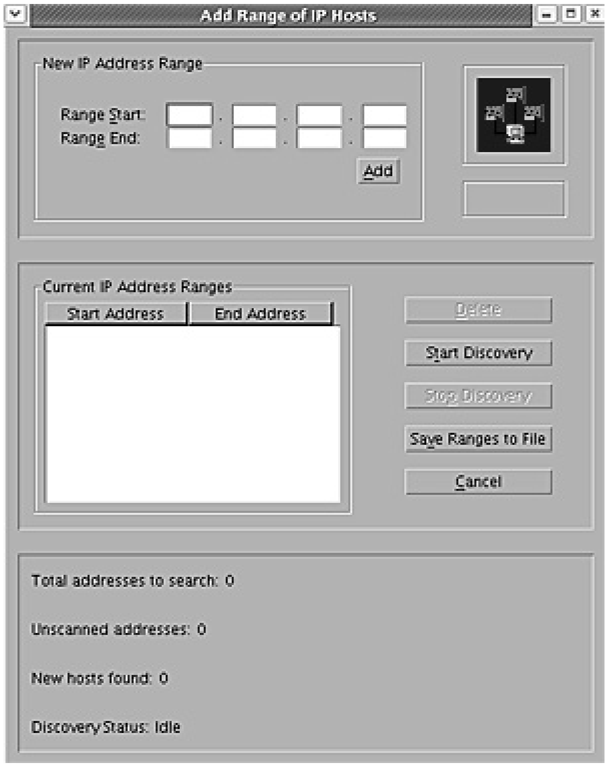
3. Enter the name or the IP address of the host to be added. Entering the IP address is the best way to add a new host.

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.



Total addresses to search: 0

Unscanned addresses: 0

New hosts found: 0

Discovery Status: Idle

Figure 38: HBAnyware 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 HBAnyware 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**. The HBAnyware utility 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. 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.
2. 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**.
3. Click **OK** to remove the selected hosts.

HBAnyware Security

Introduction

After you install the base HBAnyware software, which includes the HBAnyware utility and remote server, on a group of systems, the HBAnyware utility on 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.

You can use the HBAnyware utility security package to control which HBAnyware enabled systems can remotely access and manage HBAs on other systems in a Fibre Channel network. HBAnyware security is systems-based, not user-based. Anyone with access to a system that has been granted HBAnyware client access to remote HBAs can manage those HBAs. Any unsecured system is still remotely accessible by the HBAnyware client software (HBAnyware utility).

The HBAnyware security software provides two main security features:

1. Prevent remote HBA management from systems that you do not want to have this capability.
2. Prevent 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.

The first time you run the HBAnyware Security Configurator on a system in an environment where no security as been configured, the initial Access Control Group (ACG) is created. At this point, only this system has remote access to the HBAs in the systems in the ACG. They are no longer remotely accessible from any other system.

Subsequently, you can create additional Access Sub-Groups (ASGs). This grants systems in the ACG the ability to remotely access the HBAs of other selected systems in the ACG.

Starting the HBAnyware Security Configurator

Prerequisites

Before you can start the HBAnyware Security Configurator, you must have the following items installed on your system:

- The Emulex driver
- The HBAnyware Utility
- The HBAnyware Security Configurator

Note: Before you start the Configurator, you must 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.

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.

Any system that is part of the security installation and that is offline when the HBAnyware Security Configurator starts will not be available for security configuration changes even if it is brought online while the Configurator is running.

Procedure

To start the HBAnyware Security Configurator:

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

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

Running the Configurator for the First Time/Creating the ACG

When you install the HBAnyware utility Security software on a system and run the HBAnyware utility Security Configurator for the first time, that system becomes the Master Security Client (MSC). All of the available servers are discovered and are available to be part of the system Access Control Group (ACG). You select the systems to add to the ACG, and the security configuration updates on all of the selected servers as well as on the initial system. This selection constitutes the participating platforms in this security installation.

To create the ACG:

1. Start the HBAnyware utility Security Configurator for the first time in an unsecure environment. A warning message appears.
2. Click **OK**. The Access Control Group tab appears:

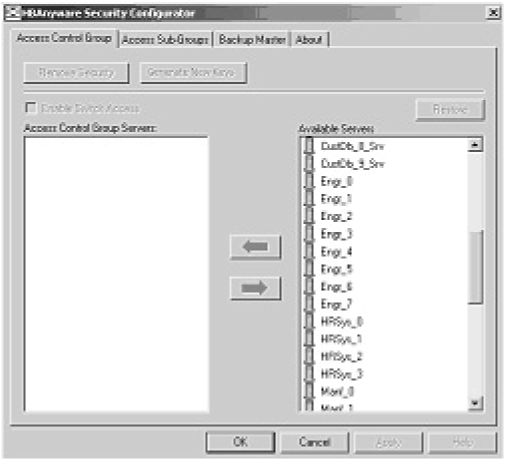
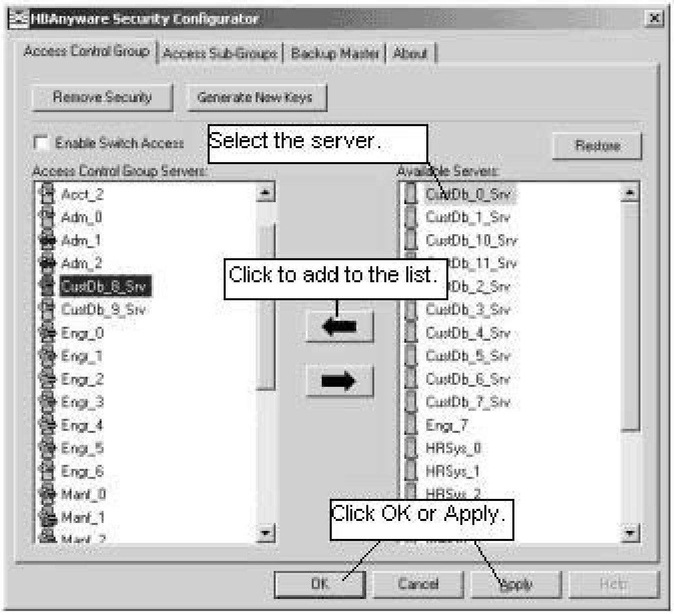


Figure 39: Access Control Group tab - No ACG Servers

3. Select the unsecured servers that you want to add to the ACG from the Available Servers list.



Select the server.

Click to add to the list.

Click OK or Apply.

Figure 40: Access Control Group tab with ACG Servers

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

Designating a Master Security Client

The first time you run the HBAnyware Security Configurator on any system in a Fibre Channel network, that system becomes the MSC (Master Security Client). See “Running the Configurator for the First Time” on page 51 for more information.

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 the Master Security Client (MSC), allows you to select the systems that belong to the ACG.

Access Control Group Tab on the MSC

On the 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 updates 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 update 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:

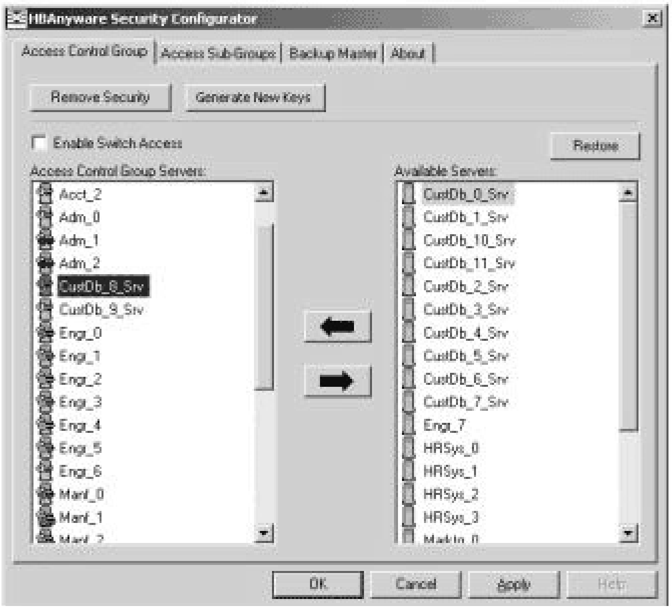
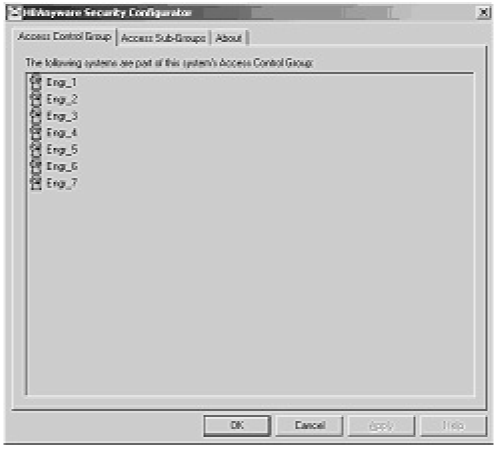


Figure 41: Access Control Group tab on an MSC System

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:



The following systems are part of this system's Access Control Group:

Figure 42: Access Control Group tab on a Non_MSC System

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.

Run the Configurator for the First Time/Create the ACG

When you install the HBAnyware Security software on a system and run the HBAnyware Security Configurator for the first time, that system becomes the Master Security Client (MSC). All of the available servers are discovered and available to become part of the system Access Control Group (ACG). Select the systems to add to the ACG, and the security configuration updates all of the selected servers as well as on the initial system. This selection constitutes the participating platforms in this security installation.

To create the ACG:

1. Start the HBAnyware Security Configurator for the first time in an unsecure environment. The computer from which you run the Configurator becomes the MSC. The “Unsecured System” message appears.
2. Click **OK.** The Access Control Group tab appears (Figure 39).
3. Select the unsecured servers that you want to add to the ACG from the Available Servers list (Figure 41).
4. Click the **left arrow** to add the servers to the Access Control Group Servers list.
5. Click **OK** or **Apply**.

Adding a Server to the ACG

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

To add servers to the ACG:

1. On the Access Control Group tab, from the Available Servers list, select the unsecured servers to add to the ACG (Figure 41).
2. Click the **left arrow** to add the server to the Access Control Group Servers list.
3. Click **OK** or **Apply**.

Deleting a Server from the ACG

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

1. On the Access Control Group tab, from the Access Control Group Servers list, select the secured systems to delete from the ACG (Figure 41).
2. Click the **right arrow** to remove the servers from the Access Control Group Servers list.
3. 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. On the Access Control Group tab, click **Remove Security**. A warning message appears.
2. 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 appears (see Figure 40 on page 52).
2. On the Access Control Group tab, click **Generate New Keys**. A dialog box warns you that you are about to generate new security keys for all systems.
3. Click **Yes**. The new keys generate and are 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 **Restore** (Figure 41).

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).

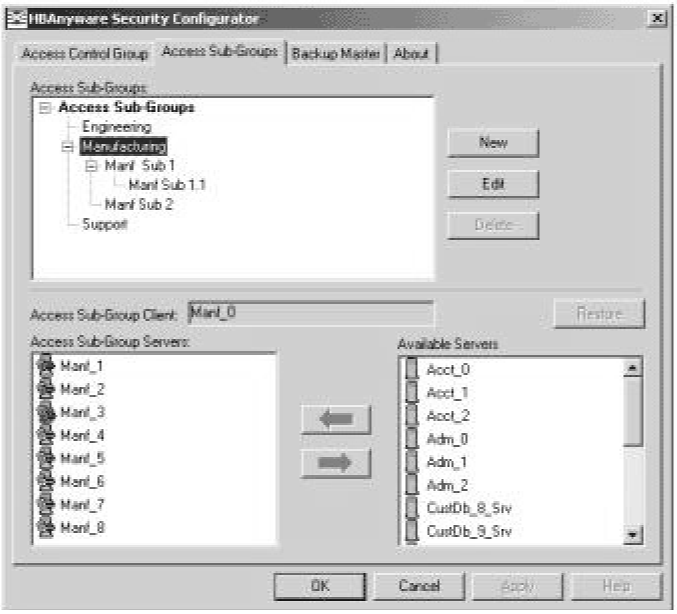
To enable switch access:

1. From the Access Control Group tab, check **Enable Switch Access**. (Figure 41).

Access Sub-Groups

Introduction

Use the Access Sub-Group tab 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, we recommend 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 shows in the Access Sub-Groups tab as a tree. You can create, modify and delete ASGs at each level in this tree.



Access Sub-Groups:

- Access Sub-Groups
  - Engineering
  - Manufacturing
    - Manf Sub 1
      - Manf Sub 1.1
    - Manf Sub 2
  - Support

Access Sub-Group Client: Manf_0

Access Sub-Group Servers:

Manf_1
Manf_2
Manf_3
Manf_4
Manf_5
Manf_6
Manf_7
Manf_8

Available Servers

Acct_0
Acct_1
Acct_2
Adm_0
Adm_1
Adm_2
CustDb_8_Srv
CustDb_9_Srv

Figure 43: Access Sub-Groups tab with Sub-Groups Created

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

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 HBAnyware Security Configurator is run on the new client, the ACG shows the servers that were configured in the ASG by its parent client.

To create an ASG:

1. Click the **Access Sub-Groups** tab.

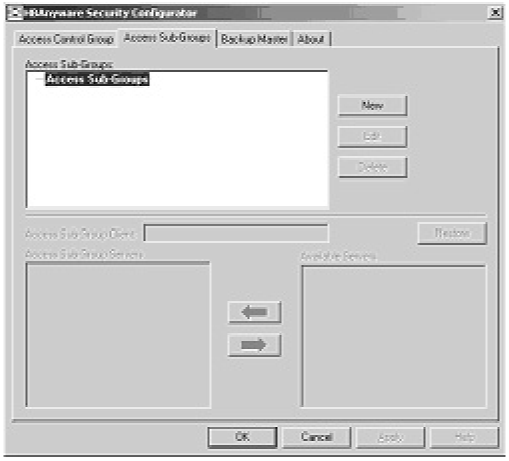
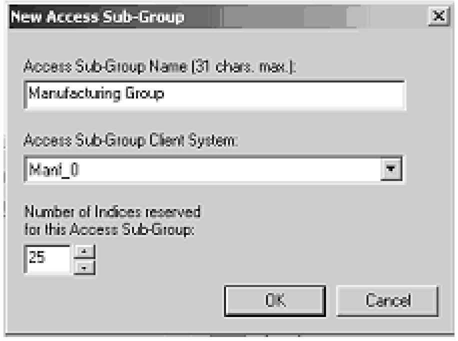


Figure 44: Access Sub-Groups tab with No Sub-Groups Created

2. Click **New**. The New Access Sub-Group dialog box appears:



Access Sub-Group Name (31 chars. max.): Manufacturing Group

Access Sub-Group Client System: Manl_0

Number of Indices reserved for this Access Sub-Group: 25

Figure 45: New Access Sub-Group dialog box

3. 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 you can subsequently create on the new client's system.
4. Click **OK** in the New Access Sub-Group dialog box. The ASG is created.

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 you can subsequently create 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 want 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. Click the Access Sub-Group tab (see Figure 44 on page 57).
2. The name of the ASG appears in the Access Sub-Groups tree. From the Available Servers list, select the servers to add to the ASG.

   Note: Out-of-band servers will appear in the Available Servers list even though the ASG client system may not have discovered them yet. These servers can still be added to the Access Sub-Group Servers list.

3. Click the **left arrow** to move the servers to the Access Sub-Group Servers list.
4. 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, you must delete those child ASGs 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 **OK** or **Apply**.

Restoring an ASG to Its Last Saved Configuration

You can restore an Access Sub-Group (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 (see Figure 44 on page 57).
2. Select the ASG whose configuration you want to restore.
3. Click **Restore**.
4. Click **OK** or **Apply** to save your changes.

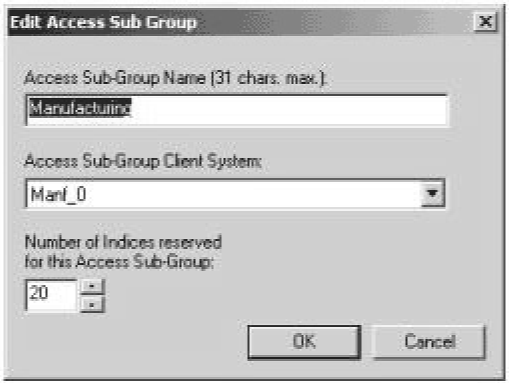
Editing an ASG

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

To edit an ASG:

1. Click the **Access Sub-Group** tab (see Figure 44 on page 57).
2. Select the ASG you want to edit.

3. Click **Edit**. The Edit Access Sub-Group dialog box appears:.



Edit Access Sub Group

Access Sub-Group Name (31 chars. max.): Manufacturing

Access Sub-Group Client System: Manf_0

Number of Indices reserved for this Access Sub-Group: 20

Figure 46: Edit Access Sub Group dialog box

4. 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 is 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 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' to reserve for the client system of the new ASG. This number reflects the number of subsequent 'child' ASGs that you can subsequently create on the new client's system. See page 58 for examples.
5. 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 HBAnyware 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:

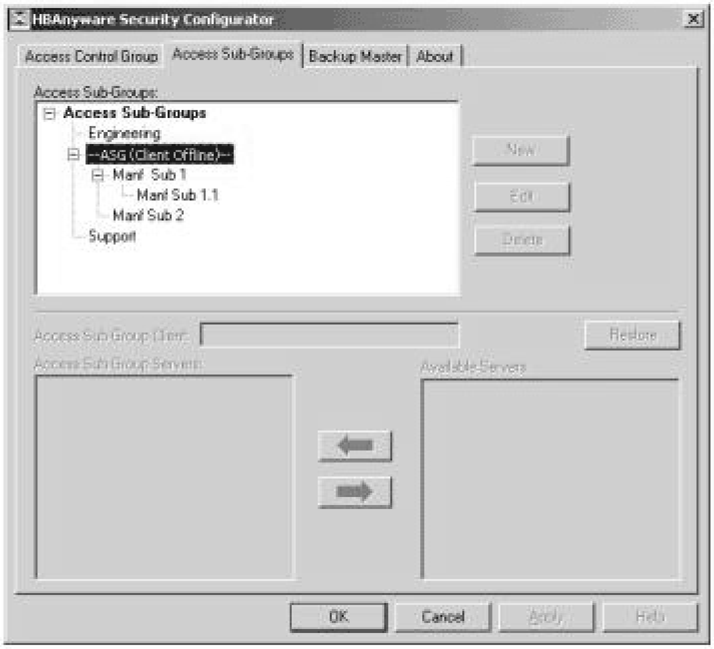


Figure 47: Access Sub-Groups tab - Client System Offline

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, we recommend 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 is 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 shows the ASGs, but you cannot change the ASGs (see Figure 41 on page 53).

The Backup Master tab is available only when the HBAnyware 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 you start the HBAnyware Security Configurator 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 HBAnyware 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.

A Backup Master system receives all the updates that the MSC makes to the security configuration, therefore it is very important that the Backup Master is online when the HBAnyware 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

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 you select the Backup Master tab on the MSC, it looks similar to the following:

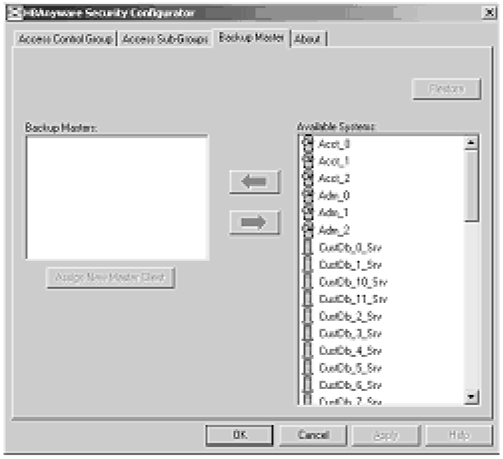


Figure 48: Backup Master tab - First Time Selected

Creating a Backup Master

To create a Backup Master:

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

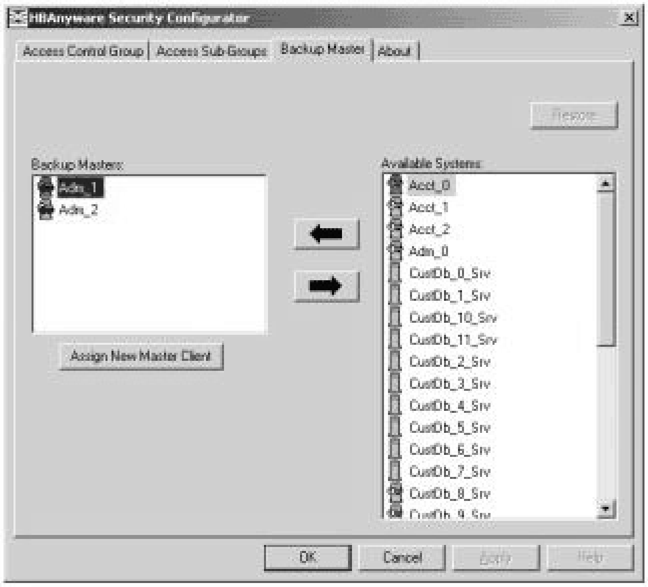


Figure 49: Backup Master tab with Backup Masters

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.

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 connects to multiple fabrics, select its Backup Master from the Available Systems list connected to the same fabrics as the MSC.

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

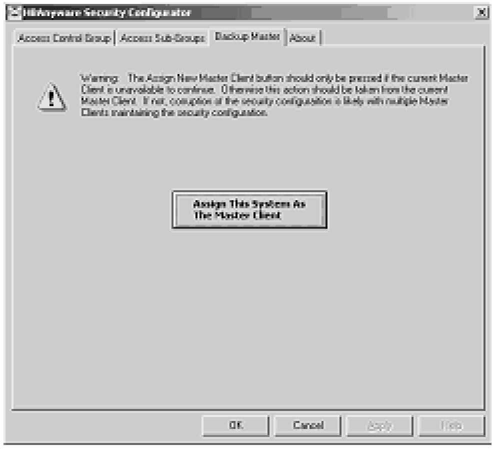
1. On the MSC, start the HBAnyware Security Configurator.
2. Click the Backup Master tab (see Figure 49)
3. In the Backup Masters list, select the Backup Master system that you want to reassign as the MSC.
4. Click **Assign New Master Client**. A dialog box appears and asks if you want to proceed.
5. Click **Yes** on the dialog box. 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 you can no longer boot the MSC or 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.



Warning: The Assign New Master Client button should only be pressed if the current Master Client is unavailable to continue. Otherwise this action should be taken from the current Master Client. If not, corruption of the security configuration is likely with multiple Master Clients maintaining the security configuration.

Figure 50: 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.
6. Restart the HBAnyware Security Configurator to run the former Backup Master as the MSC.