Emulex® OneCommand® Manager Command Line Interface for LightPulse® Adapters

User Guide
Release 12.0

Table of Contents

Chapter 1: Introduction 7

1.1 Abbreviations 8

1.2 OneCommand Manager Secure Management 9

1.2.1 OneCommand Manager Secure Management Configuration Requirements 10

1.3 Secure Management Installation 11

1.3.1 Linux and Solaris 11

1.3.2 Windows 11

1.4 Setting Secure Management Mode for Linux and Solaris 11

1.4.1 Using OneCommand Manager with Secure Management Enabled 12

Chapter 2: Installing and Uninstalling the CLI 13

2.1 Linux 13

2.1.1 Citrix 13

2.1.2 Installing in Linux without an Existing OneCommand CLI Kit 13

2.1.3 Installing in Linux with an Existing OneCommand CLI Kit 14

2.1.4 Uninstalling in Linux 15

2.1.5 Uninstalling Older HBAnyware Kits in Linux 15

2.2 Solaris 16

2.2.1 Installing in Solaris 16

2.2.2 Uninstalling in Solaris 17

2.3 VMware ESXi 17

2.4 Windows 17

2.4.1 Installing in Windows by Attended Installation 18

2.4.2 Installing in Windows by Unattended Installation 18

2.4.3 Uninstalling in Windows 19

2.5 Starting and Stopping Daemon Processes for Linux and Solaris Installations 20

Chapter 3: Updating the OneCommand Manager CLI to the OneCommand Manager Enterprise Kit 21

3.1 Linux 21

3.2 Solaris 21

3.3 Windows 21

Chapter 4: CLI Client Command Usage 22

4.1 Overview 22

4.1.1 CLI in Read-Only Mode 22

4.2 HbaCmd Syntax Usage 22

4.3 Secure Management CLI Interface 23

4.3.1 Device Management Using the Secure Management Interface 23

4.3.2 Syntax Rules for the Secure Management Interface 23

4.4 CIM Client Interface 24
4.4.1 Device Management Using the CIM Interface 24
4.4.2 Syntax Rules for the CIM Interface 24
Chapter 5: CLI Client Command Descriptions 26
5.1 Help 31
5.2 Attributes Commands 31
5.2.1 HbaAttributes 31
5.2.2 PortAttributes 32
5.2.3 PortStatistics 33
5.2.4 ServerAttributes 34
5.2.5 SetPhyPortSpeed 34
5.2.6 SetPortEnabled 35
5.3 Authentication Commands 36
5.3.1 AuthConfigList 36
5.3.2 DeleteAuthConfig 36
5.3.3 GetAuthConfig 36
5.3.4 GetAuthStatus 37
5.3.5 InitiateAuth 37
5.3.6 RemoveAdapterAuthConfig 37
5.3.7 RemoveAuthConfig 38
5.3.8 SetAuthConfig 38
5.3.9 SetAuthConfigParams 39
5.3.10 SetAuthConfigSecret 39
5.3.11 SetPassword 40
5.4 Boot Commands 41
5.4.1 EnableBootCode 41
5.4.2 GetBootParams 41
5.4.3 SetBootParam 42
5.4.4 SetPortSpeed 43
5.5 DCB Commands 43
5.5.1 GetDCBParams 43
5.5.2 GetPGInfo 44
5.5.3 SetCnaPGBW 44
5.5.4 SetDCBParam 45
5.5.5 SetDCBPriority 46
5.6 Diagnostic Commands 47
5.6.1 D_PortTest 47
5.6.2 EchoTest 49
5.6.3 FcTraceRoute 50
5.6.4 GetBeacon 52

5.6.5 GetXcvrData 52
5.6.6 LoadList 53
5.6.7 LoopBackTest 53
5.6.8 LoopMap 54
5.6.9 PciData 54
5.6.10 PostTest 55
5.6.11 SetBeacon 56
5.6.12 Wakeup 56
5.7 Driver Parameter Commands 56
5.7.1 DriverConfig 57
5.7.2 GetDriverParams 57
5.7.3 GetDriverParamsGlobal 57
5.7.4 SaveConfig 58
5.7.5 SetDriverParam 58
5.7.6 SetDriverParamDefaults 59
5.8 Dump Commands 59
5.8.1 DeleteDumpFiles 59
5.8.2 Dump 59
5.8.3 GetDumpDirectory 60
5.8.4 GetDumpFile 60
5.8.5 GetDumpFileNames 61
5.8.6 GetRetentionCount 61
5.8.7 SetDumpDirectory 61
5.8.8 SetRetentionCount 62
5.9 FCoE Commands 62
5.9.1 GetFCFInfo 63
5.9.2 GetFIPParams 63
5.9.3 SetFIPParam 64
5.10 Firmware Commands 64
5.10.1 getfwparams 64
5.10.2 setfwparam 65
5.11 LUN Masking Commands 65
5.11.1 GetLunList 66
5.11.2 GetLunUnMaskByHBA 66
5.11.3 GetLunUnMaskByTarget 66
5.11.4 RescanLuns 67
5.11.5 SetLunMask 67
5.12 LUN ExpressLane Commands 67
5.12.1 GetExpressLaneLunList 68
5.12.2 SetExpressLaneLunState 68

5.12.3 GetLunXLaneConfig 69
5.12.4 SetLunXLaneConfig 70
5.13 Miscellaneous Commands 71
5.13.1 AddHost 71
5.13.2 Download 71
5.13.3 ExportSANInfo 72
5.13.4 FecEnable 73
5.13.5 GetCimCred 73
5.13.6 GetVPD 73
5.13.7 ListHBAs 74
5.13.8 RemoveHost 74
5.13.9 Reset 75
5.13.10 SetCimCred 75
5.13.11 TargetMapping 75
5.13.12 Version 76
5.14 Persistent Binding Commands 76
5.14.1 AllNodeInfo 77
5.14.2 BindingCapabilities 77
5.14.3 BindingSupport 77
5.14.4 PersistentBinding 77
5.14.5 RemoveAllPersistentBinding 78
5.14.6 RemovePersistentBinding 78
5.14.7 SetBindingSupport 78
5.14.8 SetPersistentBinding 79
5.15 vPort Commands 79
5.15.1 CreateVPort 80
5.15.2 DeleteVPort 80
5.15.3 ListVPorts 80
5.15.4 VPortTargets 81
5.16 WWN Management Commands 81
5.16.1 ChangeWWN 81
5.16.2 GetWWNCap 82
5.16.3 ReadWWN 82
5.16.4 RestoreWWN 83
Appendix A: OneCommand Manager Error and Return Messages 83
Appendix B: License Notices 85
B.1 Secure Hash Algorithm (SHA-1) Notice 85
B.2 OpenPegasus Licensing Notice 85
B.3 OpenSSL Notice 85

Chapter 1: Introduction

The OneCommand® Manager command line interface (CLI) is a comprehensive management utility for Emulex® adapters. The CLI provides support for commonly used commands without requiring the installation of the OneCommand Manager graphical user interface (GUI). The OneCommand Manager CLI console application name is HbaCmd. At the command line interface, a single operation is performed by entering `hbacmd`, followed by a CLI client command and its possible parameters.

The OneCommand Manager application can be installed on multiple operating systems: Windows, Linux, and Solaris. For VMware ESXi hosts, use the OneCommand Manager application for VMware vCenter. For details, refer to the *Emulex OneCommand Manager for VMware vCenter for LightPulse Adapters User Guide*. You can also manage adapters using the OneCommand Manager CLI on Windows, but you must install and use the appropriate Emulex CIM Provider on those VMware hosts.

NOTE: The Solaris operating system is supported only on PowerPC (PPC) converged network adapters (CNAs).

NOTE: For VMware ESXi hosts, when advanced adapter management capabilities are required (for example, port disablement), use the OneCommand Manager for VMware vCenter Server. For more details, refer to the *Emulex OneCommand Manager for VMware vCenter for LightPulse Adapters User Guide*.

This product supports the following Emulex LightPulse® host bus adapters (HBAs) and converged fabric adapters (CFAs):

- LPe12000-series adapters
- LPe15000-series adapters
- LPe16000-series adapters, including PPC CNAs
- LPe31000-series adapters
- LPe32000-series adapters

For supported versions of operating systems and platforms, go to www.broadcom.com.

1.1 Abbreviations

API	application programming interface
BIOS	basic input-output system
CFA	converged fabric adapter
CIMOM	CIM Model Object Manager
CLI	command line interface
CNA	converged network adapter
CSV	comma separated value
DAC	direct-attach copper
D_ID	destination identifier
DCB	Data Center Bridging
DCBX	Data Center Bridging Capabilities Exchange
DH	Diffie-Hellman
DHCHAP	Diffie-Hellman Challenge Handshake Authentication Protocol
ETS	Enhanced Transmission Selection
FA-PWWN	Fabric Assigned WWN
FAT	file allocation table
FC	Fibre Channel
FCF	Fibre Channel over Ethernet Forwarder
FCoE	Fibre Channel over Ethernet
FEC	forward error correction
FIP	FCoE Initialization Protocol
GFO	Get Fabric Object
GUI	graphical user interface
HBA	host bus adapter
IP	internet protocol
LDAP	Lightweight Directory Access Protocol
LLDP	Link Layer Discovery Protocol
LUN	logical unit number
MAC	Media Access Control
NIC	network interface card
NVRAM	nonvolatile random access memory
OAS	Optimized Access Storage
OB	open boot
OS	operating system
PAM	pluggable authentication module
PCI	Peripheral Component Interconnect
PPC	PowerPC
PFC	priority flow control
PG	priority group
POST	power-on self-test
PXE	Pre-boot execution Environment

QSFP	Quad Small Form-factor Pluggable
RHEL	Red Hat Enterprise Linux
Rx	receive
SAN	storage area network
SCSI	Small Computer Systems Interface
SFCB	Small Footprint CIM Broker
SFP	small form-factor pluggable
SLES	SUSE Linux Enterprise Server
TCP	Transmission Control Protocol
Tx	transmit
UEFI	Unified Extensible Firmware Interface
VLAN	virtual local area network
VLAN ID	VLAN identifier
VPD	vital product data
vPort	virtual port
WWN	World Wide Name
WWNN	World Wide Node Name
WWPN	World Wide Port Name
XML	Extensible Markup Language

1.2 OneCommand Manager Secure Management

OneCommand Manager Secure Management enables system administrators to further enhance the active management security of their networks. Using Secure Management, administrators can define each user's privileges for managing both local and remote adapters. When running in Secure Management mode, users must specify their user name and password to run the OneCommand Manager CLI. When users are authenticated, only they can perform the functions allowed by the OneCommand Manager user group to which they belong. If your systems are running in an LDAP or Active Directory domain, the OneCommand Manager CLI will authenticate the user with those defined in that domain. For Linux and Solaris systems, this is accomplished using PAM.

NOTE: OneCommand Manager Secure Management is supported on Linux, Solaris, and Windows, but it is not supported on VMware hosts. For VMware hosts, the CIM credentials are used.

Administrators set up user accounts such that a user belongs to one of the OneCommand Manager user groups. The user groups define the management capabilities for the user. Table 1: Secure Management User Privileges defines the OneCommand Manager user groups and each group's management capabilities.

Table 1: Secure Management User Privileges

Group Name	OneCommand Manager Capability
ocmadmin	Allows full active management of local and remote adapters
ocmlocaladmin	Permits full active management of local adapters only
ocmuser	Permits read-only access of local and remote adapters
ocmlocaluser	Permits read-only access of local adapters

On Linux or Solaris systems, the *unix getent group* utility can be run on the target host system's command shell to verify the correct configuration of the groups. The groups, and users within the groups, appear in the output of this command.

NOTE: Although users can belong to the administrator group or be a root user, they will not have full privileges to run the OneCommand Manager unless they are also a member of the ocmadmin group. Otherwise, when Secure Management is enabled, a root user or an administrator can manage only local adapters (similar to the ocmlocaladmin user).

Remote management operations between two machines is allowed or denied depending on the Secure Management status of the machines, and the domains to which the machines belong. The following tables (Table 2: Active Commands: Machines on Same Domain, Table 3: Active Commands: Machines on Different Domains, and Table 4: Passive Commands: Machines on Any Domain) list the expected behavior for each machine domain condition (assuming appropriate user credentials are used).

Table 2: Active Commands: Machines on Same Domain

	Remote Server (Secure)	Remote Server (Not Secure)
Client (Secure)	Allowed	Denied [a]
Client (Not Secure)	Denied	Allowed

a. Informs you of an unsecured server that you might want to secure.

Table 3: Active Commands: Machines on Different Domains

	Remote Server (Secure)	Remote Server (Not Secure)
Client (Secure)	Denied[a]	Denied [b]
Client (Not Secure)	Denied	Allowed

a. Allowed if the user name and password are the same on both domains.

b. Informs you of an unsecured server that you might want to secure.

Table 4: Passive Commands: Machines on Any Domain

	Remote Server (Secure)	Remote Server (Not Secure)
Client (Secure)	Allowed	Allowed
Client (Not Secure)	Allowed	Allowed

1.2.1 OneCommand Manager Secure Management Configuration Requirements

For systems to run in the OneCommand Manager Secure Management environment, they must be configured to provide the following two capabilities:

- Authentication – On Linux and Solaris, this is accomplished by using the PAM interface and must be configured as follows:
  - On Solaris, place the correct value in the auth section of the `/etc/pam.d/other` file, or its earlier equivalent, `/etc/pam.conf`.

NOTE: For Solaris systems, you must use `useradd -G groupname` for authentication to work. You cannot use a lowercase **g**.

  - On Linux, it is the `/etc/pam.d/passwd` file auth section, or the equivalent.

- User Group Membership – From the host machine, OneCommand Manager Secure Management must be able to access the OneCommand Manager group to which the user belongs. For Linux and Solaris systems, it uses the `getgrnam` and `getgrid` C-library API calls. The equivalent to the API calls can be obtained by typing `getent group` from the shell command line. If the four OneCommand Manager group names are listed with their member users, the system is ready to use OneCommand Manager Secure Management.

1.3 Secure Management Installation

The enabling or disabling of the Secure Management feature is specified at OneCommand Manager installation time. This can be accomplished either interactively or by using dedicated installation switches on Windows, Linux, and Solaris. On Linux and Solaris, if the OneCommand Manager groups described in Table 1: Secure Management User Privileges are not configured on the machine at the time of the OneCommand Manager installation, the installation will fail when the Secure Management feature is selected.

NOTE: Only a user with administrator or root privileges can enable or disable the Secure Management feature on a local host machine.

Management mode cannot be used if Secure Management is enabled.

1.3.1 Linux and Solaris

This section describes the Secure Management installation options for the Linux and Solaris operating systems.

1.3.1.1 Interactive Installation

Enterprise OneCommand Manager installations performed in Interactive mode ask if OneCommand Manager Secure Management mode should be enabled. If the answer is **yes**, the other management mode questions are skipped. If the answer is **no** to the OneCommand Manager Secure Management mode question, the management mode installation questions follow.

1.3.1.2 Unattended Installation with Install Script Switch Option Support

Enterprise OneCommand Manager installations performed in Unattended mode provide a switch option to enable OneCommand Manager Secure Management. If the OneCommand Manager Secure Management switch is not used with the installation, Secure Management is disabled.

1.3.2 Windows

During OneCommand Manager installations performed in Interactive mode, you are presented with a management mode window where you can select **Secure Management** as the management mode.

1.4 Setting Secure Management Mode for Linux and Solaris

To set the Secure Management mode for the Linux and Solaris operating systems, perform these steps:

1. Log on as root.
2. Set Secure Management:
   – To set Secure Management mode for Linux, type the following command:
   ```
   # /usr/sbin/ocmanager/set_operating_mode
   ```
   – To set Secure Management mode for Ubuntu 14, type the following command:

```
# /opt/emulex/ocmanager/scripts/set_operating_mode.sh
```

– To set Secure Management mode for Solaris, type the following command:

```
# /opt/ELXocm/ocmanager/set_operating_mode
```

Example

The following example text is displayed:

```
Do you want to enable Secure Management feature for OneCommand? (s/u)
The secure management feature requires OneCommand groups be configured on the LDAP network or the
local host machine to provide for OneCommand operation.
Enter 's' to select secure management. (LDAP/NIS OCM group configuration required)
Enter 'u' to run without secure management (default.
Enter the letter 's' or 'u': s
```

1.4.1 Using OneCommand Manager with Secure Management Enabled

To run the OneCommand Manager CLI when Secure Management mode is enabled, you must include your user name and password each time you type a command.

The syntax for entering your user name and password is the following:

hbacmd <m=sec> <u=*userid*> <p=*password*> <*command*>

For example:

```
>hbacmd m=sec u=jsmith p=password download 00-12-34-56-78-9A oc11-4.6.96.2.ufi
```

User names and passwords authenticate the commands. After the credentials are authenticated, the OneCommand Manager CLI determines which one of the four user groups you belong to and allows command usage as appropriate.

Chapter 2: Installing and Uninstalling the CLI

This chapter details prerequisites and procedures for installing and uninstalling the OneCommand Manager CLI in the following operating systems: Linux, Solaris, and Windows. It also describes the Secure Management capability and the procedure for starting and stopping daemon processes.

2.1 Linux

The following instructions are for installing and uninstalling the OneCommand Manager CLI on Linux operating systems. You can install Linux with or without an existing OneCommand CLI kit. Additionally, you can install the OneCommand Manager CLI for Citrix-based operating systems.

2.1.1 Citrix

Citrix is based on CentOS Linux; however, for the OneCommand Manager CLI, Citrix is more comparable to VMware—a hypervisor-style server for managing virtual machines. Citrix XenServer 6.5 and 7.0 operating systems require the OneCommand Manager CLI installation.

2.1.2 Installing in Linux without an Existing OneCommand CLI Kit

NOTE: For Secure Management, prior to installation, OneCommand groups must be configured on the LDAP network or the local host machine for Secure Management operation. See Section 1.2.1, OneCommand Manager Secure Management Configuration Requirements, for configuration instructions.

2.1.2.1 Linux OneCommand Manager Requirements

For new systems, install the specific Linux driver rpm files before installing the OneCommand Manager CLI.

2.1.2.1.1 Libnl Library

On RHEL 6.x and 7.x, the OneCommand Core rpm file requires the `Libnl` library. This library is not installed by default, but it can be obtained from the operating system distribution media.

- For i386 RHEL, use the 32-bit `libnl` library.
- For x86_64 RHEL, use the 64-bit `libnl` library.
- For PowerPC RHEL, use the 64-bit `libnl` library.

2.1.2.1.2 libhbaapi Library

To install the OneCommand Manager CLI in Linux without an existing OneCommand CLI, perform these steps:

1. Copy the applications kit tar file to a directory on the installation machine.
2. Change to the directory where you copied the tar file.
3. Untar the file:
   `tar zxvf elxocmcore-<supported_os>-<app_ver>-<rel>.tgz`
4. Change to the Core kit directory created in step 3.
   `cd elxocmcore-<supported_os>-<app_ver>-<rel>`

5. Run the `install.sh` script.
   ```
   ./install.sh
   ```

The Core kit consists of three or four rpm files for each supported architecture and each supported version of Linux. For example:

- `elxocmlibhbaapi-*.rpm` (on 64-bit platforms that support 32-bit applications, there are two of these files)
- `elxocmcore-*.rpm`
- `elxocmcorelibs-*.rpm`

6. When you are prompted, choose whether to enable Secure Management for OneCommand:
   ```
   Do you want to enable Secure Management feature for OneCommand? (s/u)
   Enter 's' to select secure management. (LDAP/NIS OCM group configuration required)
   Enter 'u' to run without secure management (default).
   Enter the letter 's' or 'u'.
   ```

If you enter u, an additional prompt is given for the management mode:

```
You selected: Secure Management Disabled
Select desired mode of operation for OneCommand Manager:
Enter the number 1, 2, 3, or 4: 1
You selected: 'Local Only Mode'
```

1 Strictly Local Management:	Only manage the adapters on this host. Management of adapters on this host from other hosts is not allowed.
2 Local Management Plus:	Only manage the adapters on this host. Management of adapters on this host from other hosts is allowed.
3 Full Management:	Manage the adapters on this host and other hosts that allow it. Management of the adapters on this host from another host is allowed.
4 Management Host:	Manage the adapters on this host and other hosts that allow it. Management of the adapters on this host from another host is not allowed.

2.1.2.1.3 Unattended Installation

The `install.sh` script can be run in Noninteractive (unattended or quiet) mode. Enter the following command to view the syntax:

```
./install.sh --help
```

To perform an unattended, silent installation, enter the following command, perform these steps:

```
#./install.sh –q2
```

NOTE: The management mode default for unattended installation is Local Management Plus.

2.1.3 Installing in Linux with an Existing OneCommand CLI Kit

NOTE: The OneCommand Manager Core kit cannot be installed if a previous version of the HBAnyware utility is installed.

Two options are available for installing the OneCommand Manager CLI on a Linux system with an existing OneCommand CLI kit:

- Updating an existing installation – Preserve existing settings
- Performing a clean install – Overwrite existing settings

2.1.3.1 Updating the CLI (Preserving Existing Settings)

To update the OneCommand Manager CLI and preserve settings, you must install the current Core kit as detailed in Section 2.1.2, Installing in Linux without an Existing OneCommand CLI Kit. The `.rpm` file handles the configuration file update. The install script executes an rpm file update (`rpm -U *.rpm`) to update the installed version of the core kit to the current version.

NOTE: There is no update path from an HBAnyware 4.x or 3.x core kit to a OneCommand Manager 5.1 or later core kit. You must uninstall previous versions of the HBAnyware utility before installing a OneCommand Manager core kit. For information on uninstalling older versions of HBAnyware, see Section 2.1.5, Uninstalling Older HBAnyware Kits in Linux.

2.1.3.2 Performing a Clean Install (Removing Existing Settings)

1. Uninstall the existing OneCommand Manager CLI using the uninstall script included in the tar file or in the `/usr/sbin/ocmanager/scripts` directory. The configuration files are backed up by rpm with a `.rpmsave` extension.

   For Ubuntu 14 (PPC CNAs only), use the uninstall script in the following location:
   `/opt/emulex/ocmanager/scripts/uninstall.sh`

NOTE: If an HBAnyware CLI or Enterprise kit is installed, follow the procedure in Section 2.1.5, Uninstalling Older HBAnyware Kits in Linux.

2. Install the specific rpm file for your driver for Linux version. For information on installing the rpm file, see Section 2.1.2, Installing in Linux without an Existing OneCommand CLI Kit.

2.1.4 Uninstalling in Linux

To uninstall the OneCommand Manager CLI in Linux, perform these steps:

1. Log on as root.
2. Perform one of the following tasks:
   - Run the `uninstall_ocmanager.sh` script located in `/usr/sbin/ocmanager/scripts`.
   - Run the `uninstall.sh` script located in the installation tar file.
   - For Ubuntu 14 (PPC CNAs only), use the uninstall script in the following location:
   `/opt/emulex/ocmanager/scripts/uninstall.sh`

2.1.5 Uninstalling Older HBAnyware Kits in Linux

2.1.5.1 Uninstalling an Older HBAnyware Core Kit

Run the following command to remove the Core kit.

```
rpm -e elxlinuxcorekit
```

2.1.5.1.1 Uninstalling an Older HBAnyware Enterprise Kit

1. Perform one of the following tasks:
   - Run the uninstall script located in `/usr/sbin/hbanyware/scripts` to remove the Enterprise kit.
   - Run the uninstall script located in the tar file to remove the Enterprise kit.

   If the HBAnyware Security Configurator is installed, you must uninstall it before uninstalling the HBAnyware configuration utility. You must use the uninstall script that shipped with the version of OneCommand Security Configurator that you want to remove and proceed to step 2. If the Security Configurator is not installed, proceed to step 3.

2. If the HBAnyware Security Configurator is installed, follow these steps:
   a. Log on as root.
   b. Change to the directory containing the tar file.
   c. Extract the tar file using the `tar -xvf` command.
   d. Change to the newly created directory.
   e. Type the following uninstall script with the `ssc` parameter specified:
   `./uninstall ssc`
3. Uninstall the HBAnyware utility and the Application Helper module:
   a. Log on as root.
   b. Change to the directory containing the tar file.
   c. Extract the tar file using the `tar -xvf` command.
   d. Change to the newly created directory.
   e. Uninstall any previously installed versions. Type the following command:
   `./uninstall`

2.2 Solaris

The following instructions are for installing and uninstalling the OneCommand Manager CLI on Solaris operating systems.

2.2.1 Installing in Solaris

NOTE: For Secure Management, prior to installation, OneCommand groups must be configured on the LDAP network or the local host machine for Secure Management operation. See Section 1.2.1, OneCommand Manager Secure Management Configuration Requirements, for configuration instructions.

To install the OneCommand Manager CLI in Solaris, perform these steps:

1. Copy the OneCommand Manager core kit to a temporary directory on the system.
2. Untar the core kit by typing the following command:
   `tar xvf elxocmcore-solaris-<kit version>.tar`
3. Change to the newly created elxocmcore-solaris-<*kit version*> directory:
   `cd ./elxocmcore-solaris-<kit version>/`
4. Run the `install` script and follow the instructions.
   `./install`

NOTE: The `install` script can also be run in Noninteractive (unattended, quiet) mode. Enter the following command to view the syntax:
`./install --help`

If any of the following are already present on the system, the `install` script attempts to remove them first:
- HBAnyware utility
- OneCommand Manager Core kit
- OneCommand Manager Enterprise kit
- Solaris driver utilities

5. When you are prompted, choose whether to enable Secure Management for OneCommand:

```
Do you want to enable Secure Management feature for OneCommand? (s/u)
Enter 's' to select secure management. (LDAP/NIS OCM group configuration required)
Enter 'u' to run without secure management (default).
Enter the letter 's' or 'u'.
```

If you enter u here, an additional prompt is given for the management mode:

```
You selected: Secure Management Disabled
Select desired mode of operation for OneCommand Manager:
Enter the number 1, 2, 3, or 4: 1
You selected: 'Local Only Mode'
    1 Strictly Local Management: Only manage the adapters on this host. Management of
                                 adapters on this host from other hosts is not allowed.
    2 Local Management Plus:     Only manage the adapters on this host. Management of
                                 adapters on this host from other hosts is allowed.
    3 Full Management:           Manage the adapters on this host and other hosts that
                                 allow it. Management of the adapters on this host from
                                 another host is allowed.
    4 Management Host:           Manage the adapters on this host and other hosts that
                                 allow it. Management of the adapters on this host from
                                 another host is not allowed.
```

2.2.2 Uninstalling in Solaris

To uninstall the OneCommand Manager CLI in Solaris, perform these steps:

1. Log on as root.
2. Perform one of the following tasks:
   – Run `/opt/ELXocm/scripts/uninstall`.
   – Run the `uninstall` script located in the installation tar file.
   – Enter the command `pkgrm ELXocmcore`.

NOTE: The `uninstall` script can also be run in Noninteractive (quiet) mode. Enter the following command to view the syntax:

```
./uninstall --help
```

2.3 VMware ESXi

The OneCommand Manager CLI cannot be run on a VMware ESXi operating system. However, a VMware ESXi host can be accessed remotely from the Windows OneCommand Manager CLI if the Broadcom® Emulex CIM Provider is installed on the ESXi host. For instructions on installing Broadcom Emulex CIM Provider on VMware ESXi operating systems, refer to the *Emulex CIM Provider Package for LightPulse Adapters Installation Guide*.

2.4 Windows

The following instructions are for installing and uninstalling the OneCommand Manager CLI on Windows operating systems. Install the OneCommand Manager CLI in Windows in one of two ways:

- Attended installation – You are present during the installation. You are prompted for more information for the installation to continue.
- Unattended installation – You do not need to be present during the installation. Installation will complete on its own. Installation progress can be displayed as an option.

2.4.1 Installing in Windows by Attended Installation

To install the OneCommand Manager CLI, run the `installation.exe` file for a Windows Core driver kit that does not include the OneCommand Manager GUI, and follow the installation instructions.

Use the following syntax for the installation executable file:

`elxocmcore-windows-<arch>-<kit version>.exe`

- <*arch*> is either x64 or x86.
- <*kit version*> represents the complete kit version.

For example, at the command prompt, type the following command:

`elxocmcore-windows-x64-5.0.2.14-1.exe`

2.4.2 Installing in Windows by Unattended Installation

To install the OneCommand Manager CLI in Windows unattended, perform these steps:

1. From www.broadcom.com, download the x64 or x86 OneCommand Manager Core kit installation file to your system.
2. Use the following syntax for the installation executable file:
   `elxocmcore-windows-<arch>-<kit version>.exe <option>`
3. Activate the kit with switch `/q` or `/q2`.
   – The `/q` switch displays progress reports.
   – The `/q2` switch does not display progress reports.
4. Either enable Secure Management mode by adding the `sec=1` argument or disable it by adding `sec=0`. If the `sec` argument is not entered, Secure Management is disabled by default. See Section 1.2, OneCommand Manager Secure Management, for more information.

   To enable Secure Management mode, at the command prompt, type the following command:
   `elxocm-windows-<arch>-<kit version>.exe sec=1 /q2`
   To disable Secure Management mode, at the command prompt, type the following command:
   `elxocm-windows-<arch>-<kit version>.exe sec=0 /q2`

NOTE: Two management mode defaults are available for unattended installation:

- `mmode=3` (full management mode)
- `achange=1`

5. Select a management mode by adding the `mmode` argument, and select the ability to change the management mode by adding the `achange` argument with selected values as in the following example.

NOTE: If you enabled Secure Management mode in step 4 and attempt to enter an `mmode` value, a `conflicting parameters` error can occur.

For example, at the command prompt type the following command:

`elxocm-windows-x64-5.01.00.10-4.exe mmode=3 achange=1 /q2`

The following are the possible `mmode` values:

1 – Local Only Management mode

2 – Local Plus Management mode

3 – Full Management mode

4 – Local Plus Management mode and Read Only

5 – Full Management mode and Read Only

6 – Management host

The following are the possible achange values:

0 – Do not allow management mode to change

1 – Allow management mode to change

You can also set the following optional parameters:

– MHost – This optional switch allows a nonmanagement-host user to select a management host to register with. If this switch is not specified, the default value of 0 is used, and the capability will be disabled. If the switch is specified, the value can be a host name or an IP address, which is validated by the installer. An error message appears if mmode is set as Local Only management mode or Management Host mode.

– excl – This optional switch allows the nonmanagement-host user to select whether the OneCommand Manager application processes requests exclusively from the management host specified by the MHost switch. This option is only accepted if accompanied by a valid MHost value; otherwise, an error message appears. If this switch is not specified, the default value of 0 is used. If the switch is specified, the valid values are:

0 – Remotely managed by other hosts.

1 – Remotely managed by management host only.

– Mtcp – This optional switch allows you to enable or disable remote management and to specify the TCP/IP port number over which management occurs. If this switch is not specified, the default TCP/IP port number 23333 is used.

If the management host option is selected, you must select the default port number or enter a valid TCP/IP port number on the command line. A value of 0 will not be accepted.

If one of the nonmanagement host options is selected, you can enter the TCP/IP port number on the command line.

2.4.3 Uninstalling in Windows

You can uninstall the OneCommand Manager CLI in Windows in one of two ways:

- Through the Control Panel
- Through the command line

2.4.3.1 Uninstalling through the Control Panel

To uninstall the OneCommand Manager CLI in Windows through the Control Panel, perform these steps:

1. In the Control Panel, select **Programs and Features**.
2. If present, select **Emulex OCManager CLI** [*version*], and click **Uninstall/Change;** you are prompted to continue. Click **Yes**.

The OneCommand Manager CLI components are removed from the system.

2.4.3.2 Uninstalling through the Command Line

To uninstall the OneCommand Manager CLI in Windows through the command line, perform these steps:

1. Change to the appropriate uninstall directory:
   `cd <Installation Location>\Emulex\Util\Uninstall`
2. Type the following command:
   `uninstall_OCManager_Core.bat`

2.5 Starting and Stopping Daemon Processes for Linux and Solaris Installations

On Linux and Solaris machines, you can stop and start the OneCommand Manager daemon processes using the `stop_ocmanager` and `start_ocmanager` scripts, respectively. These are found in the following OneCommand Manager installation directories:

- Linux – `/usr/sbin/ocmanager`
- Ubuntu 14 – `/opt/emulex/ocmanager/scripts`:
  - `stop_ocmanger.sh`
  - `start_ocmanager.sh`
- Solaris – `/opt/ELXocm`

The `elxhbamgrd` daemon process (included with OneCommand Manager CLI) is affected by these scripts. It is a remote management daemon that services requests from OneCommand Manager clients running on remote host machines.

The daemon processes start at system boot time.

Chapter 3: Updating the OneCommand Manager CLI to the OneCommand Manager Enterprise Kit

NOTE: The full-featured OneCommand Manager Enterprise kit is not supported on Citrix XenServer 6.x, Citrix XenServer 7.x, or VMware ESXi server.

This chapter details procedures for updating the OneCommand Manager CLI to the OneCommand Manager Enterprise kit in Linux, Solaris, and Windows operating systems. An update can be performed only if the version of the OneCommand Manager Enterprise kit is the same or later than the OneCommand Manager CLI version.

NOTE: You cannot update a OneCommand Manager CLI with a previous version of the OneCommand Manager Enterprise kit.

3.1 Linux

To update from the OneCommand Manager CLI to the full-featured OneCommand Manager Enterprise kit in Linux, run the `install.sh` script of the OneCommand Manager Enterprise kit.

The install script executes an rpm file update (`rpm -U *.rpm`) to update the installed core kit to an enterprise kit.

3.2 Solaris

To update from the OneCommand Manager CLI to the full-featured OneCommand Manager Enterprise kit in Solaris, perform these steps:

1. Download the OneCommand Manager Enterprise kit to a temporary directory on your system.
2. Untar the OneCommand Manager Enterprise kit tar file:
   `tar xvf elxocm-solaris-<kit version>.tar`
3. Change to the newly created `elxocm-solaris-<kit version>` directory:
   `cd ./elxocm-solaris-<kit version>/`
4. Run the `install` script and follow the instructions:
   `./install`

The `install` script can also be run in Noninteractive (quiet) mode. To view the syntax, type the following command:
`/install --help`

3.3 Windows

To update from the OneCommand Manager CLI to the full-featured OneCommand Manager Enterprise kit in Windows:

From the desktop, run the `elxocm-windows-<kit version>.exe` file that contains the full application kit. Running this executable file removes the OneCommand Manager CLI and installs a full-featured version of the OneCommand Manager application that includes the CLI and the GUI.

Chapter 4: CLI Client Command Usage

The CLI Client component of the OneCommand Manager application provides access to the capabilities of the Remote Management library or the CIM interface from a console command prompt to get the management information.

4.1 Overview

The CLI Client is intended for use in command shells or scripted operations from within shell scripts or batch files. The CLI Client is a console application named `HbaCmd`. A single operation is performed by typing `hbacmd` at the command line, followed by a CLI client command and its possible parameters. For example:

```
hbacmd [cli options] <command> [parameters]
```

The CLI options are specified for running the CLI commands on remote hosts or with Secure Management.

When the specified operation is completed, the command prompt is displayed. For a majority of commands, the first parameter following the command is the WWPN or MAC address of the port that the command is to act upon.

4.1.1 CLI in Read-Only Mode

The CLI does not allow the execution of some commands if it is configured for Read-Only mode. The following error message is returned if such a command is attempted:

```
Error: Read-only management mode is currently set on this host. The requested command is not
permitted in this mode.
```

4.2 HbaCmd Syntax Usage

The following syntax rules and usage apply to the `HbaCmd` application:

- Parameters denoted within angle brackets < > are required.
- Parameters denoted within square brackets [ ] are optional.
- For Linux and Solaris (which are case-sensitive), program names must be in lowercase letters. Therefore, the command line must begin with `hbacmd` (rather than `HbaCmd`). Windows is not case-sensitive, so the program name is not required to be in all lowercase letters.
- To run the command on a remote host, an IP address or a host name must be specified using the h option with the following syntax:

  ```
  hbacmd [h=IP_Address[:port] | Hostname[:port]] <command> [parameters]
  ```

  – If the h option is omitted, the command is run on the local host.
  – If the h option is specified, the command is sent to the specified remote host (assuming it is specified correctly, the remote host is up, and the remote host is running the OneCommand Manager remote management agent.
  – The `:port` option is optional. If it is omitted, the OneCommand Manager remote management protocol uses the default TCP port. If it is specified, it uses the user-specified TCP port.
  – Examples

  Using the IP address:

  ```
  hbacmd h=138.239.91.121 ListHBAs
  ```

  Using the host name:

  ```
  hbacmd h=<host_name> ListHBAs
  ```

  – The h option is available for all commands except for the `AddHost`, `RemoveHost`, and `Version` commands.

- For FC and FCoE functions, the WWPN of the adapter must be specified. Where the WWPN is specified, each pair of numbers within the WWPN is separated by colons (`:`) or spaces ( ). If space separators are used, the entire WWPN must be enclosed in quotation marks (“ ”).

  For example, the following command displays the port attributes for the adapter with the specified WWPN:

  ```
  hbacmd PortAttributes 10:00:00:00:c9:20:20:20
  ```

- For NIC functions, the MAC address must be specified. Where a MAC address is specified, each pair of numbers within the MAC address is separated by a dash (`-`).

  For example, the following command displays the server attributes for the server where the NIC function is running the NIC port with the specified MAC address:

  ```
  hbacmd ServerAttributes 00-11-22-33-44-55
  ```

- For NIC functions, only the permanent MAC address is supported for the port address parameter on an `HbaCmd` command line.

  Normally, for a NIC function, the function’s permanent MAC address and current MAC address parameters are equal. However, it is possible to set a user-specified (current) MAC address that is different from the permanent MAC address. Also, for some implementations, it is possible to have multiple NIC functions with the same current MAC addresses, but with unique permanent MAC addresses. Therefore, to be sure that OneCommand Manager can access the correct function, only the permanent MAC address is supported.

NOTE: Both the permanent MAC address and the current MAC address are displayed by using the `ListHBAs` command. See Section 5.13.7, ListHBAs.

4.3 Secure Management CLI Interface

The Secure Management CLI interface is supported by the Linux, Solaris, and Windows operating systems.

NOTE: Users with root or administrator privileges on the local machine retain full configuration capability in the OneCommand Manager CLI without the use of credentials (local machine only).

4.3.1 Device Management Using the Secure Management Interface

To run the `HbaCmd` CLI client application when the Secure Management feature is enabled, each invocation must include a user name and password. The user name and password options are added to the existing `HbaCmd` command in the same way as they are for CIM commands, except the `<m=cim>` option is replaced by the `<m=sec>` option (to distinguish it from a CIM command). For example:

Without Secure Management (or if running as root or administrator):

```
hbacmd <cmd>
```

With Secure Management (as non-root or non-administrator user):

```
hbacmd <m=sec> <u=userid> <p=password> <cmd>
```

4.3.2 Syntax Rules for the Secure Management Interface

For the Secure Management interface, all of the syntax rules in Section 4.2, HbaCmd Syntax Usage, apply.

Example

In Windows, to download firmware on a PPC CNA managed on a remote host at IP address 192.168.1.122 using the Secure Management interface, run the following command:

```
hbacmd h=192.168.1.122 m=sec u=jsmith p=password download 00-12-34-56-78-9A
lancer_a11.2.123.45.grp
```

4.4 CIM Client Interface

NOTE: In Linux and Solaris, you cannot use `HbaCmd` as a CIM client.

4.4.1 Device Management Using the CIM Interface

VMware on the hypervisor-based ESXi platforms use the CIM as the only standard management mechanism for device management.

For VMware ESXi hosts, you can manage adapters using the OneCommand Manager CLI on Windows, but you must install and use the appropriate Broadcom Emulex CIM Provider on the VMware ESXi host. For installation, refer to the *CIM Provider Package for LightPulse Adapters Installation Guide*.

NOTE: For VMware ESXi hosts, if advanced adapter management capabilities are required, use the OneCommand Manager for VMware vCenter Server. For more details, refer to the *OneCommand Manager for VMware vCenter for LightPulse Adapters User Guide*.

4.4.2 Syntax Rules for the CIM Interface

For the CIM interface, all the syntax rules in Section 4.2, HbaCmd Syntax Usage, apply, except that the h option is required. Additionally, the `m=cim` parameter is required in the command line for getting the data from the ESXi host. For example:

```
hbacmd h=192.168.1.110 m=cim u=root p=password n=root/emulex listhbas
```

4.4.2.1 Syntax Options and Setting CIM Credentials

For issuing CIM-based commands, two main syntax options are available.

Option A

```
hbacmd <h=IP_Address[:port]> m=cim [u=userid] [p=password] [n=root/emulex] <command> <WWPN>
```

Option B

```
hbacmd <h=IP_Address[:port]> <m=cim> <command>
```

Before using the option B syntax, you must set the CIM credentials. Perform one of the following tasks:

- Set the default CIM credentials using the `SetCimCred` command (see Section 5.13.10, SetCimCred). This command sets only the CIM credentials. After you have set them, subsequent `HbaCmd` commands do not require you to specify the CIM credentials on the command line.

  Command syntax:

  ```
  hbacmd setcimcred <username> <password> <namespace> <portnum>
  ```

- Add the host IP address with CIM credentials using the `AddHost` command.

  Command syntax:

  ```
  hbacmd <m=cim> [u=userid] [p=password] [n=namespace] addhost <IP_Address>
  ```

4.4.2.1.1 Default CIM Credentials

If you specify the command with the CIM method `m=cim` without specifying the CIM credentials (*`userid`*, *`password`*, or *`namespace`*), the default value for the missing CIM credential is obtained in the following order:

1. The information entered using the `addhost` command is looked up.
2. If no values exist, the information entered using the `setcimcred` command is used.
3. If no values exist, the following defaults are used:

```
username=root
password=root
namespace=root/emulex
portnum=5988
```

4.4.2.2 Example of Using the CIM Interface to Display Adapters

In Windows, to display a list of adapters managed for a specified host using the CIM interface, run the following command:

```
hbacmd h=10.192.113.128 m=cim u=root p=root n=root/emulex listhbas
```

For a list of `HbaCmd` commands supported through the CIM interface, see Table 6, CLI Client Command Reference.

Chapter 5: CLI Client Command Descriptions

CLI Client commands are organized by command groups. Two tables are presented for your convenience; a table organized by command group and another by alphabetically listing CLI Client commands.

The following table shows each command group with a short description and the commands in each group. After you determine the command group of interest, click the command link and go directly to the command you selected.

Table 5: CLI Client Command Reference Functional Groups

Command Group	Description	Commands
Attributes Commands	This group manages the display of adapter, port, server attributes, and port statistics for each adapter specified. You can also set the port speed on PPC CNAs.	HbaAttributes ServerAttributes SetPhyPortSpeed SetPortEnabled
Authentication Commands	These commands configure a DHCHAP connection between an FC port and a switch port.	AuthConfigList DeleteAuthConfig GetAuthConfig GetAuthStatus InitiateAuth RemoveAdapterAuthConfig RemoveAuthConfig SetAuthConfig SetAuthConfigParams SetAuthConfigSecret SetPassword
Boot Commands	This group manages the commands that enable or disable network boot for NIC ports or the boot code for FC adapter ports. You can also show and change FC and FCoE boot parameters.	EnableBootCode GetBootParams SetBootParam SetPortSpeed
DCB Commands	These commands display and set the DCB and LLDP parameters for FCoE and NIC ports on PPC CNAs.	GetDCBParams GetPGInfo SetCnaPGBW SetDCBParam SetDCBPriority
Diagnostic Commands	This group provides commands that enable you to detect cabling problems, to examine transceiver data, and to flash memory load lists. Additionally, you can run specific diagnostic tests, such as the Loopback test and the POST.	D_PortTest EchoTest FcTraceRoute GetBeacon GetXcvrData LoadList LoopBackTest LoopMap PciData PostTest SetBeacon Wakeup

Table 5: CLI Client Command Reference Functional Groups (Continued)

Command Group	Description	Commands
Driver Parameter Commands	Use the driver parameter commands to show, set, and save the driver parameter values. You can also change the parameters back to factory default values.	DriverConfig GetDriverParams GetDriverParamsGlobal SaveConfig SetDriverParam SetDriverParamDefaults
Dump Commands	Use the diagnostic dump feature to create a dump file for a selected adapter. Dump files contain information, such as firmware version, driver version, and operating system information. This information is useful for troubleshooting an adapter, but it is unavailable in Read-Only mode.	DeleteDumpFiles Dump GetDumpDirectory GetDumpFile GetDumpFileNames GetRetentionCount SetDumpDirectory SetRetentionCount
FCoE Commands	This group of commands manages the FIP parameters and displays the FCF for an FCoE+NIC PPC CNA.	GetFCFInfo GetFIPParams SetFIPParam
Firmware Commands	These commands enable you to view and set firmware parameters.	getfwparams setfwparam
LUN Masking Commands	The commands in this group manage LUN masking activities. LUN masking is supported only for FC ports.	GetLunList GetLunUnMaskByHBA GetLunUnMaskByTarget RescanLuns SetLunMask
LUN ExpressLane Commands	This group of commands enables, disables, and displays the ExpressLane™ status on a particular LUN. You can also assign a frame priority to an ExpressLane LUN if the adapter and the switch support it. LUN ExpressLane commands do not apply to PPC CNAs.	GetExpressLaneLunList SetExpressLaneLunState GetLunXLaneConfig SetLunXLaneConfig
Miscellaneous Commands	This group contains commands that do not belong in other groups.	AddHost Download ExportSANInfo FecEnable GetCimCred GetVPD ListHBAs Reset SetCimCred TargetMapping Version

Table 5: CLI Client Command Reference Functional Groups (Continued)

Command Group	Description	Commands
Persistent Binding Commands	This group of commands facilitates persistent binding operations. These commands are supported only for FC and FCoE ports.	AllNodeInfo BindingCapabilities BindingSupport PersistentBinding RemoveAllPersistentBinding RemovePersistentBinding SetBindingSupport SetPersistentBinding
vPort Commands	vPort commands manage virtual ports and functions only on FC and FCoE adapters. In Linux, VPorts do not persist across system reboots.	CreateVPort DeleteVPort ListVPorts VPortTargets
WWN Management Commands	WWN management validates WWNs to avoid WWPN duplication; however, WWNN duplication is acceptable. You might see error and warning messages if a name duplication is detected. Make sure that the activation requirement is fulfilled after each WWN is changed or restored. If pending changes exist, some diagnostic and maintenance features are not available.	ChangeWWN GetWWNCap ReadWWN RestoreWWN

Table 6: CLI Client Command Reference lists each command alphabetically and shows the operating system and CIM Interface support for each command. A linked page number for each command is provided for your convenience. A check mark (✓) designates a supported command for a particular operating system and CIM interface.

NOTE: For VMware ESXi, two options support the CLI:

- Using the OneCommand Manager CLI on Windows with the appropriate Emulex CIM Provider installed on a VMware host. These commands are covered in this section.
- Using the OneCommand Manager for VMware vCenter command line interface (`elxvcpcmd`). Although the available commands are listed in Table 6 for your convenience, refer to the *OneCommand Manager for VMware vCenter for LightPulse Adapters User Guide* for specific information.

Table 6: CLI Client Command Reference

Command	Linux		Solaris	Windows	CIM	elxvcpcmd	Section
	RHEL, SLES, Ubuntu, Oracle	Citrix					
AddHost	✓	✓	✓	✓	✓		Section 5.13.1, AddHost
AllNodeInfo	✓	✓	✓	✓	✓		Section 5.14.1, AllNodeInfo
AuthConfigList			✓	✓			Section 5.3.1, AuthConfigList
BindingCapabilities			✓	✓			Section 5.14.2, BindingCapabilities
BindingSupport			✓	✓			Section 5.14.3, BindingSupport
ChangeWWN	✓	✓	✓	✓	✓		Section 5.16.1, ChangeWWN
CreateVPort	✓		✓	✓			Section 5.15.1, CreateVPort
DPortTest	✓	✓		✓	✓		Section 5.6.1, D_PortTest
DeleteAuthConfig			✓	✓			Section 5.3.2, DeleteAuthConfig

Table 6: CLI Client Command Reference (Continued)

Command	Linux		Solaris	Windows	CIM	elxvcpcmd	Section
	RHEL, SLES, Ubuntu, Oracle	Citrix					
DeleteDumpFiles	✓	✓	✓	✓	✓		Section 5.8.1, DeleteDumpFiles
DeleteVPort	✓		✓	✓			Section 5.15.2, DeleteVPort
Download	✓	✓	✓	✓	✓		Section 5.13.2, Download
DriverConfig	✓	✓		✓			Section 5.7.1, DriverConfig
Dump	✓	✓	✓	✓	✓		Section 5.8.2, Dump
EchoTest	✓	✓	✓	✓			Section 5.6.2, EchoTest
EnableBootCode	✓	✓	✓	✓	✓		Section 5.4.1, EnableBootCode
ExportSANInfo	✓	✓	✓	✓			Section 5.13.3, ExportSANInfo
FcTraceRoute	✓	✓		✓	✓		Section 5.6.3, FcTraceRoute
FecEnable	✓	✓	✓	✓	✓		Section 5.13.4, FecEnable
GetBeacon	✓	✓	✓	✓	✓		Section 5.6.4, GetBeacon
GetAuthConfig			✓	✓			Section 5.3.3, GetAuthConfig
GetAuthStatus			✓	✓			Section 5.3.4, GetAuthStatus
GetBootParams	✓	✓	✓	✓			Section 5.4.2, GetBootParams
GetCimCred				✓			Section 5.13.5, GetCimCred
GetDCBParams	✓	✓	✓	✓	✓		Section 5.5.1, GetDCBParams
GetDriverParams	✓	✓	✓	✓	✓		Section 5.7.2, GetDriverParams
GetDriverParamsGlobal	✓	✓	✓	✓	✓		Section 5.7.3, GetDriverParamsGlobal
GetDumpDirectory	✓	✓	✓	✓	✓		Section 5.8.3, GetDumpDirectory
GetDumpFile	✓	✓	✓	✓	✓		Section 5.8.4, GetDumpFile
GetDumpFileNames	✓	✓	✓	✓	✓		Section 5.8.5, GetDumpFileNames
GetExpressLaneLUNList	✓	✓		✓	✓		Section 5.12.1, GetExpressLaneLunList
GetFCFInfo	✓	✓	✓	✓	✓		Section 5.9.1, GetFCFInfo
GetFIPParams	✓	✓	✓	✓	✓		Section 5.9.2, GetFIPParams
GetFwParams	✓	✓		✓	✓	✓	Section 5.10.1, getfwparams
GetLunList				✓		✓	Section 5.11.1, GetLunList
GetLunUnMaskByHBA				✓			Section 5.11.2, GetLunUnMaskByHBA
GetLunUnMaskByTarget				✓			Section 5.11.3, GetLunUnMaskByTarget
GetPGInfo	✓	✓	✓	✓	✓		Section 5.5.2, GetPGInfo
GetRetentionCount	✓	✓	✓	✓	✓		Section 5.8.6, GetRetentionCount
GetVPD	✓	✓	✓	✓	✓		Section 5.13.6, GetVPD
GetWWNCap	✓	✓	✓	✓	✓		Section 5.16.2, GetWWNCap
GetXcvrData	✓	✓	✓	✓	✓		Section 5.6.5, GetXcvrData
HbaAttributes	✓	✓	✓	✓	✓		Section 5.2.1, HbaAttributes
Help	✓	✓	✓	✓	N/A		Section 5.1, Help
InitiateAuth			✓	✓			Section 5.3.5, InitiateAuth
ListHBAs	✓	✓	✓	✓	✓		Section 5.13.7, ListHBAs
ListVPorts	✓	✓	✓	✓	✓		Section 5.15.3, ListVPorts
LoadList	✓	✓	✓	✓	✓	✓	Section 5.6.6, LoadList

Table 6: CLI Client Command Reference (Continued)

Command	Linux		Solaris	Windows	CIM	elxvcpcmd	Section
	RHEL, SLES, Ubuntu, Oracle	Citrix					
LoopBackTest	✓	✓	✓	✓	✓	✓	Section 5.6.7, LoopBackTest
LoopMap	✓	✓	✓	✓			Section 5.6.8, LoopMap
PciData	✓	✓	✓	✓	✓	✓	Section 5.6.9, PciData
PersistentBinding		✓	✓	✓			Section 5.14.4, PersistentBinding
PortAttributes	✓	✓	✓	✓	✓	✓	Section 5.2.2, PortAttributes
PortStatistics	✓	✓	✓	✓	✓	✓	Section 5.2.3, PortStatistics
PostTest	✓	✓	✓	✓	✓	✓	Section 5.6.10, PostTest
ReadWWN	✓	✓	✓	✓	✓	✓	Section 5.16.3, ReadWWN
RemoveAllPersistent Binding			✓	✓			Section 5.14.5, RemoveAllPersistentBinding
RemoveAdapterAuth Config	✓	✓	✓	✓			Section 5.3.6, RemoveAdapterAuthConfig
RemoveAuthConfig	✓	✓	✓	✓			Section 5.3.7, RemoveAuthConfig
RemovePersistentBinding			✓	✓			Section 5.14.6, RemovePersistentBinding
RemoveHost	✓	✓	✓	✓	✓		Section 5.13.8, RemoveHost
RescanLuns				✓			Section 5.11.4, RescanLuns
Reset	✓	✓	✓	✓	✓	✓	Section 5.13.9, Reset
RestoreWWN	✓	✓	✓	✓	✓	✓	Section 5.16.4, RestoreWWN
SaveConfig	✓	✓	✓	✓		✓	Section 5.7.4, SaveConfig
ServerAttributes	✓	✓	✓	✓	✓	✓	Section 5.2.4, ServerAttributes
SetAuthConfig			✓	✓			Section 5.3.8, SetAuthConfig
SetAuthConfigParams	✓	✓	✓	✓			Section 5.3.9, SetAuthConfigParams
SetAuthConfigSecret	✓	✓	✓	✓			Section 5.3.10, SetAuthConfigSecret
SetBeacon	✓	✓	✓	✓	✓	✓	Section 5.6.11, SetBeacon
SetBindingSupport			✓	✓			Section 5.14.7, SetBindingSupport
SetBootParam	✓	✓	✓	✓			Section 5.4.3, SetBootParam
SetCnaPGBW	✓	✓	✓	✓	✓	✓	Section 5.5.3, SetCnaPGBW
SetCimCred				✓			Section 5.13.10, SetCimCred
SetDCBParam	✓	✓	✓	✓	✓	✓	Section 5.5.4, SetDCBParam
SetDCBPriority	✓	✓	✓	✓	✓	✓	Section 5.5.5, SetDCBPriority
SetDriverParam	✓	✓	✓	✓	✓	✓	Section 5.7.5, SetDriverParam
SetDriverParamDefaults	✓	✓	✓	✓		✓	Section 5.7.6, SetDriverParamDefaults
SetDumpDirectory					✓	✓	Section 5.8.7, SetDumpDirectory
SetExpressLaneLUNState	✓	✓		✓	✓	✓	Section 5.12.2, SetExpressLaneLunState
SetFIPParam	✓	✓	✓	✓	✓	✓	Section 5.9.3, SetFIPParam
SetFwParam	✓	✓		✓	✓	✓	Section 5.10.2, setfwparam
SetPortSpeed	✓	✓	✓	✓	✓	✓	Section 5.4.4, SetPortSpeed
SetLunMask							Section 5.11.5, SetLunMask
SetPassword			✓	✓			Section 5.3.11, SetPassword
SetPersistentBinding			✓	✓			Section 5.14.8, SetPersistentBinding

Table 6: CLI Client Command Reference (Continued)

Command	Linux		Solaris	Windows	CIM	elxvcpcmd	Section
	RHEL, SLES, Ubuntu, Oracle	Citrix					
SetPhyPortSpeed	✓	✓	✓	✓	✓		Section 5.2.5, SetPhyPortSpeed
SetPortEnabled	✓	✓	✓	✓	✓		Section 5.2.6, SetPortEnabled
SetRetentionCount	✓	✓	✓	✓	✓		Section 5.8.8, SetRetentionCount
TargetMapping	✓	✓	✓	✓	✓		Section 5.13.11, TargetMapping
Version	✓	✓	✓	✓	✓		Section 5.13.12, Version
VPortTargets	✓	✓	✓	✓	✓		Section 5.15.4, VPortTargets
Wakeup	✓	✓	✓	✓			Section 5.6.12, Wakeup

5.1 Help

This command displays command information for the `HbaCmd` application. Without using its optional parameters, the `Help` command lists all the commands in their respective groups. Using the optional parameter *`GroupName`*, it lists the commands in a group. Using the optional parameter *`CmdName`*, it shows the details for a specific command.

Supported By

Linux, Solaris, and Windows

Syntax

`Help [`*`GroupName`*`] [`*`CmdName`*`]`

Parameters

`GroupName`	This optional parameter lists the commands in a particular group.
`CmdName`	This optional parameter shows the details for a particular CLI command.

Examples

This `Help` command example lists all the commands in their respective groups:

```
hbacmd help
```

This `Help` command example shows the details for the `SetDCBParam` command:

```
hbacmd help setdcbparam
```

5.2 Attributes Commands

The Attributes Command group manages the display of adapter, port, function, server attributes, and port statistics for each adapter specified. You can also set the port speed on PPC CNAs in NIC+FCoE mode.

5.2.1 HbaAttributes

This command shows a list of all adapter attributes for the adapter. The type of information listed might vary according to the adapter model.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`HbaAttributes <WWPN|MAC>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`MAC`	The MAC address of a NIC function.

Example

```
HBA Attributes for 10:00:00:90:fa:94:26:af

Host Name:                WIN-9ILVRDLR7JC
Manufacturer:             Emulex Corporation
Serial Number:            VA53900065
Model:                    LPe32002-M2
Model Desc:               Emulex LightPulse LPe32002-M2 2-Port 32Gb Fibre Channel Adapter
Node WWN:                 20 00 00 90 fa 94 26 af
Node Symname:             Emulex LPe32002-M2 FV11.1.38.61 DV11.0.247.0
HN:                       WIN-9ILVRDLR7JC
OS:                       Windows 2012 R2
HW Version:               0000000C
FW Version:               11.1.38.61
Vendor Spec ID:           10DF
Number of Ports:          1
Driver Name:              elxfc
Driver Version:           11.0.247.0
Device ID:                E300
HBA Type:                 LPe32002-M2
Operational FW:           11.1.38.61
IEEE Address:             00 90 fa 94 26 af
Boot Code:                Enabled
Boot Version:             11.1.38.56
Board Temperature:        Normal
Function Type:            FC
Sub Device ID:            E300
PCI Bus Number:           32
PCI Func Number:          0
Sub Vendor ID:            10DF
IPL Filename:             H62LEX1
Service Processor FW Name: 11.1.38.61
ULP FW Name:              11.1.38.61
FC Universal BIOS Version:    11.1.38.56
FC x86 BIOS Version:          11.1.38.56
FC EFI BIOS Version:          11.1.38.48
FC FCODE Version:             11.0.150.0
Flash Firmware Version:       11.1.38.61
```

5.2.2 PortAttributes

This command shows a list of attributes for the adapter-specified function. The type of information listed might vary according to the adapter model.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`PortAttributes <WWPN|MAC>`

Parameters

`WWPN` The WWPN of an FC or FCoE function.

`MAC` The MAC address of a NIC function.

Example

```
hbacmd h=10.192.32.197 portattributes 10:00:00:00:c9:88:88:89
Port Attributes for 10:00:00:00:c9:88:88:89
Node WWN: 0 00 00 00 c9 88 88 89
Port WWN: 10 00 00 00 c9 88 88 89
Port Symname:
Port FCID: 0000
Port Type: Unknown
Port State: Link Down
Port Service Type: 8
Port Supported FC4: 00 00 01 00 00 00 00 01
     00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00
Port Active FC: 00 00 01 00 00 00 00 01
     00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00
     00 00 00 00 00 00 00 00
Port Supported Speed: 4 8 16 Gbit/sec
Configured Port Speed: Auto Detect
Port Speed: Not Available
Max Frame Size: 2048
OS Device Name: \\.\Scsi5:
Num Discovered Ports: 0
Fabric Name: 00 00 00 00 00 00 00 00
Function Type: FC
FEC: Disabled
```

5.2.3 PortStatistics

This command shows all function statistics for the specified function. The type of information listed can vary according to the adapter model.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`PortStatistics <WWPN>`

Parameters

`WWPN` The WWPN of an FC or FCoE function.

5.2.4 ServerAttributes

This command shows a list of server attributes for the server where the specified function is running. The type of information listed can vary according to the adapter model.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`ServerAttributes <WWPN|MAC>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`MAC`	The MAC address of a NIC function.

5.2.5 SetPhyPortSpeed

This command sets the port speed on PPC CNAs.

PPC CNAs have configurable physical port speeds. Depending on the port module or transceiver installed in the physical port, the speed settings can be forced to a specific value (for example, 1 Gb) or to a range of values for auto-negotiation with the switch (for example, 10 Gb/1 Gb/100 Mb). Three values can be configured: port speed mode, speed values, and the DAC cable length.

The configurable port speeds are based on the port module type and the mode defined by the port speed *Mode* parameter. For the default port speed mode, the speed setting is not required.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`SetPhyPortSpeed <WWPN|MAC> <Mode> [Speed [Length]]`

Parameters

`WWPN`	The WWPN of an FCoE function.
`MAC`	The MAC address of a NIC function.
`Mode`	The Mode number: `0` = Default `1` = Auto-negotiate; requires the `Speed` parameter `2` = Force; requires the `Speed` and `Length` parameters If the adapter's port speed value and the switch's port speed value conflict, the link will not be brought up.

`Speed`	The speed string of the PHY port. Some valid string values include `100Mb`, `1Gb`, and `10Gb`. The `PortAttributes` command lists all the valid speeds in Auto-negotiate and Force modes. **Auto-negotiated Speeds** A comma-separated list of available auto-negotiated speeds is displayed by the `PortAttributes` command for PPC CNAs in NIC+FCoE mode. For combinations of speeds, each speed is separated by a slash, for example, `10Gb/1Gb/100Mb`. If the port does not support auto-negotiated speeds, this property is displayed as `Not Supported`. **Forced Speeds** A comma-separated list of available forced speeds is displayed by the `PortAttributes` command for PPC CNAs in NIC+FCoE mode. Combinations of speeds for forced speeds are not available. If the port does not support forced speeds, this property is displayed as `Not Supported`. If the `Mode` parameter is `1` or `2`, the `Speed` parameter is required. If the `Mode` parameter is `0`, the `Speed` parameter is ignored.
`Length`	The length of the DAC cable in meters. Valid values are `0` to `10`. A length value of `0` indicates an optical cable. A Length value is required if you are using a 10Gb SFP and QSFP transceiver interface type. If the `Mode` parameter is `0`, `Speed` and `Length` parameters are ignored, and if the `Mode` parameter is `1`, the `Length` parameter is ignored.

Examples

The following example configures the PHY port to a forced speed of 1 Gb/s with a cable length of 10 meters:

```
hbacmd setphyportspeed 00-00-c9-ad-ad-ac 2 1Gb 10
```

The following example tries to configure the PHY port to a forced speed of 100 Mb/s:

```
hbacmd setphyportspeed 00-00-c9-a9-41-88 2 100Mb
```

If the command is successful, the following is displayed:

```
Successfully changed speed settings on port.
```

If the `Mode` parameter is `2`, this command results in the following error because you must include a value for the `Length` parameter:

```
ERROR: <431>: Cable length required for force mode and interface type
```

5.2.6 SetPortEnabled

This command enables or disables a port. When a port is disabled, packets are not transmitted or received on the port.

NOTE: Make sure that all I/O traffic on the port is stopped before disabling the port.

NOTE: If the `SetPortEnabled` command disables an FC port, the adapter must be reset to activate the new value.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`SetPortEnabled <`*`WWPN|MAC`*`> <`*`PortEnable`*`>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function on the port.
`MAC`	The MAC address of a NIC function on the port.

`PortEnable`	The port-enabled state: `0` = Disabled `1` = Enabled

5.3 Authentication Commands

These commands configure a DHCHAP connection between an FC function and a switch port.

5.3.1 AuthConfigList

This command returns the list of WWPNs that have an authentication connection configuration with the specified adapter.

Supported By

Linux, Solaris, and Windows

Syntax

`AuthConfigList <WWPN>`

Parameters

`WWPN`	The WWPN of an FC function.

5.3.2 DeleteAuthConfig

This command deletes the authentication configuration on LPe12000-series adapters only.

NOTE: The `RemoveAuthConfig` command is deprecating this command.

Supported By

Linux, Solaris, and Windows

Syntax

`DeleteAuthConfig <WWPN1> <WWPN2> <PasswordType> <Password>`

Parameters

`WWPN1`	The WWPN of an FC function.
`WWPN2`	Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the WWPN for a target.
`PasswordType`	`1` = ASCII `2` = Hexadecimal (binary) `3` = Password not yet defined
`Password`	The current password value.

5.3.3 GetAuthConfig

This command retrieves the authentication configuration for the adapter.

Supported By

Linux, Solaris, and Windows

Syntax

`GetAuthConfig <WWPN1> <WWPN2>`

Parameters

`WWPN1` The WWPN of an FC function.

`WWPN2` Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the WWPN for a target.

5.3.4 GetAuthStatus

This command returns the current status for the authentication connection specified by WWPN1 and WWPN2 (adapter and the switch). It includes the current authentication state (connected or failed). Currently authenticated connections specify the hash algorithm and DH group used in the DHCHAP associated with this connection. Failed status includes the failure reason.

Supported By

Linux, Solaris, and Windows

Syntax

`GetAuthStatus <WWPN1> <WWPN2>`

Parameters

`WWPN1` The WWPN of an FC function.

`WWPN2` Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the WWPN for a target.

5.3.5 InitiateAuth

This command initiates the authentication configuration on the adapter.

Supported By

Linux, Solaris, and Windows

Syntax

`InitiateAuth <WWPN1> <WWPN2>`

Parameters

`WWPN1` The WWPN of an FC function.

`WWPN2` Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the WWPN for a target.

5.3.6 RemoveAdapterAuthConfig

This command removes or deletes all authentication configuration entries for an FC adapter.

NOTE: Not supported on LPe12000-series adapters.

Supported By

Linux, Solaris, and Windows

Syntax

`RemoveAdapterAuthConfig <WWPN>`

Parameters

`WWPN` The WWPN of the port whose configurations you want to delete.

5.3.7 RemoveAuthConfig

This command removes or deletes one or more authentication configuration entries for an FC port.

NOTE: Use the `AuthConfigList` command to get the list of entity pairs.

Supported By

Linux, Solaris, and Windows

Syntax

`removeAuthConfig <WWPN> <Entity pair 1> <Entity pair 2> <Entity pair N>`

Parameters

`WWPN`	The WWPN of the FC port whose configuration you want to delete.
`Entity pair`	LocalEntity,RemoteEntity `LocalEntity` = Source WWPN `RemoteEntity` = Destination WWPN Use `all` to delete the entire authentication configuration.

5.3.8 SetAuthConfig

This command sets the authentication configuration on LPe12000-series adapters only.

NOTE: The `SetAuthConfigParams` command is deprecating this command.

Supported By

Linux, Solaris, and Windows

Syntax

`SetAuthConfig <WWPN1> <WWPN2> <PasswordType> <Password> <Param> <Value>`

NOTE: Where multiple parameters and values are used, separate them using commas.

Parameters

`WWPN1`	The WWPN of an FC function.
`WWPN2`	Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the WWPN for a target.
`PasswordType`	`1` = ASCII 2 = Hexadecimal (binary) 3 = Password not yet defined
`Password`	The current password value.

`Param`	The parameter names: ■ `Mode` ■ `Timeout` ■ `Bidirectional` ■ `Hash-priority` ■ `DH-priority` ■ `Re-authentication` ■ `Re-authentication-interval`
`Value`	The value is based on the type of <*Param*>: ■ `Mode`: `disabled`, `enabled`, or `passive` ■ `Timeout`: time in seconds ■ `Bi-directional`: `disabled` or `enabled` ■ `Hash-priority`: `md5` or `sha1` (`md5` = first md5, then sha1; `sha1` = first sha1, then md5) ■ `DH-priority`: `1`, `2`, `3`, `4`, `5`; any combination up to 5 digits ■ `Re-authentication`: `disabled` or `enabled` ■ `Re-authentication-interval`: `0`, `10` to `3600`, in seconds

5.3.9 SetAuthConfigParams

This command sets one or more authentication configuration parameters for the FC port.

Supported By

Linux, Solaris, and Windows

Syntax

`setauthconfigParams <WWPN1> <WWPN2> <Mode> <DH-priority> <Hash-priority> <Timeout> <Bi-directional> <Re-authentication> <Re-authentication-interval>`

Parameters

`WWPN1`	The WWPN of an FC function.
`WWPN2`	Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the actual WWPN for a target.
`Mode`	`disabled`, `enabled`, or `passive`
`DH-priority`	`1`, `2`, `3`, `4`, `5`; any combination up to 5 digits
`Hash-priority`	`md5` or `sha1` (`md5` = first md5, then sha1; `sha1` = first sha1, then md5)
`Timeout`	Time in seconds
`Bi-directional`	`disabled` or `enabled`
`Re-authentication`	`disabled` or `enabled`
`Re-authentication interval`	`0`, `10` to `3600`, in seconds

5.3.10 SetAuthConfigSecret

This commands sets the local or remote secret on the adapter for an authenticated connection to the switch.

NOTE: This command is deprecating the `SetPassword` command.

Supported By

Linux, Solaris, and Windows

Syntax

`setauthconfigsecret <WWPN1> <WWPN2> <Flag> <Nst> <Nsv>`

Parameters

`WWPN1` The WWPN of an FC function.

`WWPN2` Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the actual WWPN for a target.

`Flag` `1` = Local (secret used by the adapter when the adapter authenticates to the switch, and when using bidirectional authentication)
`2` = Remote (secret used when switch initiates authentication to the HBA and when using bidirectional authentication)

`Nst` Current secret type.
`1` = ASCII
`2` = Hexadecimal (binary)

`Nsv` New secret value.
`1` = ASCII
`2` = Hexadecimal (binary)

5.3.11 SetPassword

This command sets the password on LPe12000-series adapters only for an authenticated connection to the switch.

NOTE: The `SetAuthConfigSecret` command is deprecating this command.

Supported By

Linux, Solaris, and Windows

Syntax

`SetPassword <WWPN1> <WWPN2> <Flag> <Cpt> <Cpw> <Npt> <Npw>`

Parameters

`WWPN1` The WWPN of an FC function.

`WWPN2` Either use `ff:ff:ff:ff:ff:ff:ff:ff` for a switch, or use the actual WWPN for a target.

`Flag` `1` = Local (password used by the adapter when the adapter authenticates to the switch)
`2` = Remote (password used by the adapter when the switch authenticates to the adapter)

`Cpt` Current password type.
`1` = ASCII
`2` = Hexadecimal (binary)
`3` = Password not yet defined

`Cpw` Current password value.

`Npt` New password type.
`1` = ASCII
`2` = Hexadecimal (binary)

`Npw` New password value.

5.4 Boot Commands

The Boot Commands group manages the commands that enable or disable the network boot for NIC ports or the boot code for FC and FCoE adapter ports. You can also show and change FC and FCoE boot parameters.

CAUTION! Using the EnableBootCode or SetBootParam commands on an older FC adapter (for example, LPe12000) that is being used to boot from SAN is not advisable. After the command has completed, the system performs an adapter reset, which might cause a loss of connectivity to the SAN and possible loss of data. To perform these commands on an older FC adapter, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot from SAN host.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be used.

5.4.1 EnableBootCode

This command enables or disables boot code. If the boot code is disabled, the adapter does not boot from the SAN, regardless of the value of the *EnableBootFromSan* boot parameter. If the boot code is enabled, the adapter boots from SAN if the *EnableBootFromSan* parameter is also enabled.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

```
EnableBootCode <WWPN> <Flag>
```

Parameters

WWPN	The WWPN of an FC function.
Flag	D = Disable the boot code. E = Enable the boot code.

Examples

The following example enables boot code:

```
hbacmd EnableBootCode 10:00:00:00:c9:20:20:20 e
```

5.4.2 GetBootParams

This command shows the FC or FCoE boot parameters. If any arguments are missing or invalid, an error is reported. If all arguments are correct, the data is displayed in tabular form.

Supported By

Linux, Solaris, and Windows

Syntax

```
GetBootParams <WWPN> <Type>
```

Parameters

`WWPN`	The WWPN of an FC function.
`Type`	`X86`, `OpenBoot`, or `UEFI`.

5.4.3 SetBootParam

This command changes the FC and FCoE boot parameters. You can change function parameters and boot device parameters for x86, OpenBoot, and EFI boot.

- If you change adapter parameters, omit the `BootDev` keyword and value; otherwise, an error is reported.
- If you change boot device parameters for OpenBoot, omit the `BootDev` keyword and value; otherwise, an error is reported.
- For boot device parameters for x86 or EFI, you must provide the `BootDev` keyword and value.

Supported By

Linux, Solaris, and Windows

Syntax

`SetBootParam <WWPN> <Type> <AdapterParam> <Value1> [BootDev <Value2>]`

Parameters

`WWPN`	The WWPN of an FC or FCoE port.
`Type`	{`x86`, `EFI`, `OB`}
`AdapterParam`	The parameter name.
`Value1`	The parameter value.
`BootDev`	The boot device.
`Value2`	The boot device entry number: {0 to 7}.

Adapter Parameters	Boot Type	Value
`DefaultAlpa`	All	{ Value }
`EnableAdapterBoot`	All	{ State } (`0`=Disable, `1`=Enable)
`EnableBootFromSan`	All	{ State } (`0`=Disable, `1`=Enable)
`LinkSpeed`	All	{ `0`, `1`, `2`, `4`, `8` } This parameter is available only LPe12000-series adapters Use the `SetPortSpeed` command instead for all other adapters.
`PlogiRetryTimer`	All	{ `0`, `1`, `2`, `3` }
`Topology`	All	{ `0`, `1`, `2`, `3` }
`AutoScan`	x86	{ `0`, `1`, `2`, `3` }
`AutoBootSectorEnable`	x86	{ State } (`0`=Disable, `1`=Enable)
`EDD30Enable`	x86	{ State } (`0`=Disable, `1`=Enable)
`EnvVarEnable`	x86	{ State } (`0`=Disable, `1`=Enable)
`SpinupDelayEnable`	x86	{ State } (`0`=Disable, `1`=Enable)
`StartUnitCommandEnable`	x86	{ State } (`0`=Disable, `1`=Enable)
`BootTargetScan`	EFI	{ `0`, `1`, `2` }
`DevicePathSelection`	EFI	{ `0`, `1` }
`MaxLunsPerTarget`	EFI	{ Value }
`ResetDelayTimer`	EFI	{ Value }

SfsFlag	OB	{ State } (0=Disable, 1=Enable)
Boot Device Parameters		
D_ID	All	{ Value [*BootDev* <*Value2*>] }
LUN	All	{ Value [*BootDev* <*Value2*>] }
TargetWwpn	All	{ Value [*BootDev* <*Value2*>] }
TargetID	OB	{ Value }

5.4.4 SetPortSpeed

This command sets the link speed for a specific port on an LPe16000-series, LPe3100-series, or LPe32000-series adapter.

NOTE: This command is not supported on LPe12000-series adapters. Use the `LinkSpeed` parameter of the `SetBootParam` command instead.

NOTE: This command is not supported on PPC CNAs. Use the `SetPhyPortSpeed` command instead.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`SetPortSpeed <WWPN> <LinkSpeed>`

Parameters

WWPN	The WWPN of an FC port.
LinkSpeed	Numeric value representing a supported link speed. For a list of port speeds supported by the adapter, use the `PortAttributes` command to display `Port Supported Speed`. Specify a value of `0` to configure Auto Detect mode.

NOTE: A port reset is required to activate the new settings.

5.5 DCB Commands

This command group controls the DCB and LLDP parameters for FCoE and NIC adapter ports on PPC CNAs.

5.5.1 GetDCBParams

This command shows the active and configured DCB and LLDP settings on a port of a PPC CNA. The active parameters show what the adapter port is currently running, and the configured parameters show the value that the adapter port's DCB parameter is set to.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetDCBParams <WWPN|MAC>`

Parameters

WWPN	The WWPN of an FCoE function on the port.

MAC	The MAC address of a NIC function on the port.

Example

```
hbacmd GetDCBParams 00-00-c9-93-2f-d8
```

5.5.2 GetPGInfo

This command shows the ETS priority group bandwidth percentages for a port of a PPC CNA. Additionally, this command displays the number of priority groups supported by an adapter.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

```
GetPGInfo <WWPN|MAC>
```

Parameters

WWPN	The WWPN address of an FCoE function on the port.
MAC	The MAC address of a NIC function on the port.

Example

```
hbacmd getpginfo 00-00-c9-93-2f-d8
```

5.5.3 SetCnaPGBW

This command sets the ETS priority group bandwidth percentages on a port of a PPC CNA according to the following rules:

- Bandwidths (BW0–BW7) for priority groups 0 to 7 (PG0 to PG7) must total 100 (for 100 percent).
- Bandwidth can be assigned to a priority group that has priorities.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

```
SetCnaPGBW <WWPN|MAC> <BW0–BW7>
```

Parameters

WWPN	The WWPN of an FCoE function on the port.
MAC	The MAC address of a NIC function on the port.
BW0–BW7	The bandwidths allocated for the priority groups 0 to 7.

Example

This command sets the bandwidth of PG0 to 50%, PG1 to 50%, and PG2 to PG7 to 0%.

```
hbacmd SetCnaPGBW 10:00:00:00:c9:3c:f7:88 50 50 0 0 0 0 0 0
```

5.5.4 SetDCBParam

This command configures the DCB and LLDP settings on a PPC CNA. Use the `GetDCBParams` command to obtain valid parameter names for use in this command.

NOTE: You cannot set DCBX mode. If you attempt to specify a *dcbxmode* parameter, an error message is displayed.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`SetDCBParam <WWPN|MAC> <Param> <Value>`

Parameters

`WWPN`	The WWPN of an FCoE function on the port.
`MAC`	The MAC address of a NIC function on the port.
`Param`	The parameter name. See DCB Settings for `<Param>` and `<Value>` and LLDP Settings for `<Param>` and `<Value>`.
`Value`	The parameter value. See DCB Settings for `<Param>` and `<Value>` and LLDP Settings for `<Param>` and `<Value>`.

DCB Settings for <Param> and <Value>

<Param>	**Description and <Value>**
`DCBXState`	The DCBX protocol state. `0` = Disabled `1` = Enabled
`PFCEnable`	Flow control in both directions (transmit and receive). `0` = Disabled `1` = Enabled
`FCoEPriority`	This parameter is only applicable for ports running FCoE. A single priority must be specified. The range of valid values is `0` to `7`. Only one priority can be specified for each invocation of this command and must be for a protocol running on the port. If more than one protocol priority can be set, they must be unique values.
`PFCPriority`	A list of comma-separated values where multiple PFC priorities are supported. The comma-separated list can contain up to seven values ranging from `0` to `7`.
`defaults`	Use to set the DCB parameters (including priority groups) to their default values. For example: `hbacmd SetDCBParam <WWPN|MAC> defaults`

LLDP Settings for <Param> and <Value>

<Param>	**Description and <Value>**
`TxState`	Transmit State: DCBX uses LLDP to exchange parameters between two link peers. For the DCBX protocol to operate correctly, both LLDP Rx and Tx must be enabled. If either Rx or Tx is disabled, DCBX is disabled. `0` = Disabled `1` = Enabled
`RxState`	Receive State: DCBX uses LLDP to exchange parameters between two link peers. For the DCBX protocol to operate correctly, both LLDP Rx and Tx must be enabled. If either Rx or Tx is disabled, DCBX is disabled. `0` = Disabled `1` = Enabled
`TxPortDesc`	Transmit Port Description: Provides a description of the port in an alphanumeric format. `0` = Disabled `1` = Enabled

`TxSysDesc`	Transmit System Description: Provides a description of the network entity in an alphanumeric format. `0` = Disabled `1` = Enabled
`TxSysName`	Transmit System Name: Provides the system's assigned name in an alphanumeric format. `0` = Disabled `1` = Enabled
`TxSysCap`	Transmit System Capabilities: `0` = Disabled `1` = Enabled

Example

```
hbacmd SetDCBParam 00-00-c9-3c-f7-88 fcoepriority 3
```

5.5.5 SetDCBPriority

This command sets the PFC priorities and the ETS priority groups, priorities. The values must be set according to the following rules:

- The priorities range from 0 to 7.
- A priority (0 to 7) must exist in only one priority group.
- All priorities must appear once in any of the eight (PG0 to PG7) priority groups, or if available, PG15.
- To not specify priorities for a priority group, use a dash (`-`).
- Any assigned PFC priority must be assigned as the single priority in a priority group (for example, no other priorities allowed in a group assigned the PFC priority).
- Any PG assigned one or more priorities must also be assigned a nonzero bandwidth value (see Section 5.5.3, SetCnaPGBW).

The following rules are specific to FCoE+NIC PPC CNAs:

- A maximum of two PFC priorities can be assigned.
- If FCoE is running on the port, one of the PFC priorities must match the FCoE priority.

The following rules are specific to NIC PPC CNAs

- Only one PFC priority can be assigned.
- In NIC-Only mode, PFC is disabled by default. To enable PFC, NIC ETS must be enabled.

  To enable NIC ETS, load the NIC driver with the `tx_prio` driver parameter set to `1`.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

```
SetDcbPriority <WWPN|MAC> <PFC> <PG0> <PG1> <PG2> <PG3> <PG4> <PG5> <PG6> <PG7> [PG15]
```

Parameters

`WWPN`	The WWPN of an FCoE function on a port.
`MAC`	The MAC address of a NIC function on a port.
`PFC`	The PFC priority that is a comma-separated list of up to eight values, ranging from `0` to `7`.
`PG0-PG7`	Priority group membership that is a comma-separated list of priorities ranging from `0` to `7`. Each set of priorities for a group must be separated by a space. All priorities (`0` to `7`) must be assigned to a PGID.

Example

```
hbacmd SetDCBPriority 10:00:00:00:c9:3c:f7:88 3 0,1,2,4,5,6,7 3 0 0 0 0 0 0
```

5.6 Diagnostic Commands

The Diagnostic Commands group provides commands that enable you to detect cabling problems, examine transceiver data, and to flash memory load lists. Additionally, you can run specific diagnostic tests, such as the Loopback test and POST test.

CAUTION! Using the `LoopBackTest`, `PciData`, or `Post` commands on an older FC adapter (for example, LPe12000) that is being used to boot from SAN is not advisable. After the command has completed, the system performs an adapter reset, which might cause a loss of connectivity to the SAN and possible loss of data. To perform these commands on an older FC adapter, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot from SAN host.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be used.

5.6.1 D_PortTest

D_Port, also called ClearLink, is a set of diagnostic tests that detects physical cabling issues that result in increased error rates and intermittent behavior.

This command is supported only for LPe16000-series, LPe31000-series, and LPe32000-series FC adapters connected to D_Port-enabled Brocade switches.

Bidirectional D_Port testing is supported. The switch or initiator can initiate D_Port testing.

NOTE: When initiating the D_Port tests from the adapter port, do not enable D_Port on the switch port.

The `DPortTest` command runs a series of tests, including local electrical loopback, loopback to the remote optics, loopback from the remote port to the local optics, and a full-device loopback test with data integrity checks. It also provides an estimate of cable length, from the switch to the adapter, to validate that a proper buffering scheme is in place.

The various tests allow some fault isolation, so you can distinguish faults that are the result of marginal cables, optics modules, and connectors or optics seating. If the adapter, firmware, SFP, or switch do not support D_Port testing, an error is generated.

These tests run with the physical connection in an offline diagnostic state, so normal I/O cannot be sent through the physical port while the test is in progress. While the port is in D_Port mode, the link appears down on that port, similar to an unplugged cable.

NOTE: If you are using D_Port in a boot from SAN configuration, the configuration must have redundant paths to the boot LUN, and only one of the redundant adapter ports should be set to D_Port.

Supported By

Linux, Windows, and Windows+CIM Provider on a VMware host

Syntax

`DPortTest <WWPN>`

Parameters

`WWPN` The WWPN of the FC function on the adapter.

Considerations when using D_Port

- A test failure occurs if the `DPortTest` command is run with a switch that does not support D_Port testing.
- Typing **CTRL+C** while the D_Port tests are running terminates the tests and the completed results are displayed.
- If the Overall Test Result is FAILED, you must either rerun the tests successfully, or reset the adapter port to bring up the link.
- If a test phase fails, the D_Port diagnostics are stopped automatically. As a result, test phases that would have occurred after the failure are not displayed.
- If more than one error is reported in a single test phase, multiple lines are displayed showing each error.

Examples

Successful test and test failure examples are below.

Successful Test

```
>hbacmd DPortTest 10:00:00:00:c9:d1:a2:d0

Running D_Port Tests. Please wait. Polling for results.........................

D_Port Test Status:     Passed
Buffers Required:       1
Frame Size:             2112
Round Trip Latency:     1898 nanoseconds
Estimated Cable Length: 172  meters

================================================================================
Test Phase                Result    Latency   Local Errors   Remote Errors
================================================================================
Electrical Loopback       Passed    122
Optical Loopback          Passed    1898
Reverse Optical Loopback  Skipped   0
Link Traffic              Passed    0
```

Test Failures

```
>hbacmd DPortTest 10:00:00:00:c9:d1:a2:d0

Running D_Port Tests. Please wait. Polling for results.......................

D_Port Test Status:     Failed
Buffers Required:       0
Frame Size:             0
Round Trip Latency:     0    nanoseconds
Estimated Cable Length: 0    meters

================================================================================
Test Phase                Result    Latency   Local Errors   Remote Errors
================================================================================
Electrical Loopback       Failed    n/a

>hbacmd DPortTest 10:00:00:00:c9:d1:a2:d0
```

```
Running D_Port Tests. Please wait. Polling for results.....................

D_Port Test Status:     Failed
Buffers Required:       0
Frame Size:             0
Round Trip Latency:     0    nanoseconds
Estimated Cable Length: 0    meters

================================================================================
Test Phase                Result    Latency   Local Errors   Remote Errors
================================================================================
Electrical Loopback       Passed    0
Optical Loopback          Failed    n/a

>hbacmd DPortTest 10:00:00:00:c9:d1:a2:d0

Running D_Port Tests. Please wait. Polling for results.....................

D_Port Test Status:     Failed
Buffers Required:       1
Frame Size:             2112
Round Trip Latency:     1898 nanoseconds
Estimated Cable Length: 172  meters

================================================================================
Test Phase                Result    Latency   Local Errors   Remote Errors
================================================================================
Electrical Loopback       Passed    127
Optical Loopback          Passed    1898
Reverse Optical Loopback  Skipped   0
Link Traffic              Failed    n/a
```

5.6.2 EchoTest

This command runs the Echo test on FC functions.

NOTE: The `EchoTest` command fails if the target WWPN does not support the `ECHO ELS` command.

Supported By

Linux and Windows

Syntax

`EchoTest <WWPN Source> <WWPN Destination> <Count> <StopOnError> <Pattern>`

Parameters

`WWPN Source`	The WWPN of the originating FC function.
`WWPN Destination`	The WWPN of the destination (echoing) FC functions.
`Count`	The number of times to run the test. Use `0` to run the test indefinitely.
`StopOnError`	Checks if the test must be halted on error: `0` = No halt `1` = Halt on error
`Pattern`	Hexadecimal data pattern to transmit (up to 8 characters).

5.6.3 FcTraceRoute

This command issues an FC trace route request for the communication path between an FC initiator port and an FC target port. It is supported only on LPe16000-series, LPe31000-series, and LPe32000-series adapters.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`FcTraceRoute <WWPN> <Target WWPN>`

Parameters

`WWPN`	The WWPN of the FC port to use as the FC trace route source.
`Target WWPN`	The WWPN of the an FC target to use as the FC trace route endpoint

Successful Test

```
>hbacmd fctraceroute 10:00:00:90:fa:5d:05:a9 50:06:01:60:90:20:5C:38

Test to be run: FC Trace Route (FTR)

FC trace route test status:
Test pending. Polling for results…

Test running ..........

FC Trace Route test suceeded - Results:

  Initiator Port: 10:00:00:90:FA:5D:05:A9
  Target Port   : 50:06:01:60:90:20:5C:38

  Hop 1
    Switch Name:       30:00:05:01:39:27:01:27
    Domain ID:         0000003F
    Ingress Port Name: 30:09:05:01:39:27:01:27
    Ingress Port Num:  9
    Egress Port Name:  30:2a:0F:01:39:27:01:27
    Egress Port Num:   42

  Hop 2
    Switch Name:       10:00:00:29:33:44:41:0F
    Domain ID:         0000001C
    Ingress Port Name: 10:1C:00:29:33:44:41:0F
    Ingress Port Num:  28
    Egress Port Name:  10:08:00:29:33:44:41:0F
    Egress Port Num:   8

  Hop 3
    Switch Name:       01:00:00:00:33:44:41:29
    Domain ID:         0000003D
    Ingress Port Name: 01:01:00:00:33:44:41:29
    Ingress Port Num:  1
    Egress Port Name:  01:02:00:00:33:44:41:29
    Egress Port Num:   2
```

```
Hop 4
  Switch Name:       01:00:00:00:33:44:41:29
  Domain ID:         0000003D
  Ingress Port Name: 01:02:00:00:33:44:41:29
  Ingress Port Num:  2
  Egress Port Name:  01:01:00:00:33:44:41:29
  Egress Port Num:   1

Hop 5
  Switch Name:       10:00:00:29:33:44:41:0F
  Domain ID:         0000001C
  Ingress Port Name: 10:08:00:29:33:44:41:0F
  Ingress Port Num:  8
  Egress Port Name:  10:1C:00:29:33:44:41:0F
  Egress Port Num:   28

Hop 6
  Switch Name:       30:00:05:01:39:27:01:27
  Domain ID:         0000003F
  Ingress Port Name: 30:2a:0F:01:39:27:01:27
  Ingress Port Num:  42
  Egress Port Name:  30:09:05:01:39:27:01:27
  Egress Port Num:   9
```

5.6.4 GetBeacon

This command shows the current beacon state (either on or off).

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetBeacon <WWPN|MAC>`

Parameters

`WWPN`	The WWPN of the FC or FCoE function on the port.
`MAC`	The MAC address of the NIC function on the port.

5.6.5 GetXcvrData

This command shows transceiver data for a port on an adapter.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetXcvrData <WWPN|MAC> [Type]`

Parameters

`WWPN`	The WWPN of an FC or FCoE function on the port.
`MAC`	The MAC address of a NIC function on the port.

`Type`	The type of SFP data to display: `1` = Formatted SFS data (default) `2` = Raw SFS data (not supported by Windows+CIM Provider on a VMware host)

Example

```
hbacmd GetXcvrData 00-00-c9-93-2f-d6
```

5.6.6 LoadList

This command shows the flash memory load list data for the FC function on the adapter. It is supported only on LPe12000-series adapters.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`LoadList <WWPN>`

Parameters

`WWPN`	The WWPN of the FC function on the adapter.

5.6.7 LoopBackTest

This command runs one of the loopback tests available on the adapter port specified by the WWPN or MAC address.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`LoopBackTest <WWPN|MAC> <Type> <Count> <StopOnError> [Pattern]`

Parameters

`WWPN`	The WWPN of an FC or FCoE function on the port.
`MAC`	The MAC address of a NIC function on the port.
`Type`	The type of Loopback test to run: `0` = PCI Loopback test; not supported on PPC CNAs `1` = Internal Loopback test; not supported on PPC CNAs `2` = External Loopback test (requires loopback plug) `4` = PHY Loopback test; supported only on PPC CNAs in NIC+FCoE mode `5` = MAC Loopback test; supported only on PPC CNAs in NIC+FCoE mode
`Count`	Number of times to run the test. Possible values are `1` to `99999`. To run the test infinitely, use `0`.
`StopOnError`	Checks if the test must be halted on error. `0` = No halt `1` = Halt
`Pattern`	An optional parameter that specifies 1–8 hexadecimal bytes to use for loopback data (for example, `1a2b3c4d`).

Example

```
hbacmd LoopBackTest 10:00:00:00:c9:20:20:20 1 120 0
```

5.6.8 LoopMap

This command shows the arbitrated loop map data on an FC function.

Supported By

Linux, Solaris, and Windows

Syntax

`LoopMap <WWPN>`

Parameters

`WWPN` The WWPN of the FC function.

5.6.9 PciData

This command shows the PCI configuration data (if available).

The PCI registers displayed are specific to the function referenced in the OneCommand Manager CLI. For example, if you specify the WWPN for the FCoE function, the PCI registers for that FCoE function are returned. If you specify the MAC address for the NIC function on that same physical port, the PCI registers for that NIC function are returned.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`PciData <WWPN|MAC>`

Parameters

`WWPN` The WWPN of an FC or FCoE function.

`MAC` The MAC address of a NIC function.

Example

```
hbacmd pcidata 10:00:B0:5A:DA:01:B1:0D
```

The example output:

```
Vendor ID:            0x10DF        Device ID:            0xE300
Command:              0x0546        Status:               0x0010
Revision ID:          0x01          Prog If:              0x00
Subclass:             0x04          Base Class:           0x0C
Cache Line Size:      0x10          Latency Timer:        0x00
Header Type:          0x80          Built In Self Test:   0x00
Base Address 0:       0x92C0800C    Base Address 1:       0x00000000
Base Address 2:       0x00000000    Base Address 3:       0x00000000
Base Address 4:       0x00000000    Base Address 5:       0x00000000
CIS:                  0x00000000    SubVendor ID:         0x1590
SubSystem ID:         0x0214        ROM Base Address:     0x00000000
Interrupt Line:       0x00          Interrupt Pin:        0x02
Minimum Grant:        0x00          Maximum Latency:      0x00
Capabilities Ptr:     0x54

FeatureEnable:                   0x00000000
PwrMgt Caps/Nxt/ID:              0x00036001
```

```
PwrMgt Ctl/Stat:                  0x00000008
MSI Ctl/Nxt/ID:                   0x018A7805
MSI Lo Address:                   0x00000000
MSI High Address:                 0x00000000
MSI Data:                         0x00000000
MSI Mask Bits:                    0x00000000
MSI Pending Bits:                 0x00000000
MSI-X Ctl/Nxt/ID:                 0x81FF9411
MSI-X Table Offset:               0x00004000
MSI-X PBA Offset:                 0x00003400
VPD Address/Nxt/ID:               0x00000003
VPD Data:                         0x51000D820000000000000000
PCIE Capabilities/Nxt/ID:         0x0002F810
PCIE Device Cap. Reg:             0x10008724
PCIE Device Status & Control:     0x00095136
PCIE Link Capabilities:           0x0041DC83
PCIE Link Status & Control:       0x10830040
Slot Capabilities Register:       0x00000000
Slot Status & Control Register:   0x00000000
Root Capabilities & Ctl Register: 0x00000000
Root Status Register:             0x00000000
Device Capabilities 2 Register:   0x0010001F
Device StatusControl 2 Register:  0x00000000
Link Capabilities 2 Register:     0x0000000E
Link Status 2 & Ctl 2 Register:   0x00000000
Slot Capabilities 2 Register:     0x00000000
Slot Status Control 2 Register:   0x00000000
Enhanced Cap Header AER:          0x00000000
Uncorrectable Error Status:       0x00000000
Uncorrectable Error Mask:         0x00000000
Uncorrectable Error Severity:     0x00000000
Correctable Error Status:         0x00000000
Correctable Error Mask:           0x00000000
Adv. Error Cap & Control:         0x00000000
Header Log 0x0:                   0x00000000
Header Log 0x4:                   0x00000000
Header Log 0x8:                   0x00000000
Header Log 0xC:                   0x00000000
Enhanced Cap Header PBUDG:        0x00000000
Data Select Reg:                  0x00000000
Data Register:                    0x00000000
Power Budget:                     0x00000000
```

5.6.10 PostTest

This command runs the POST on the adapter.

NOTE: This command is supported only on LPe12000-series adapters.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`PostTest <WWPN>`

Parameters

`WWPN` The WWPN of the FC port.

5.6.11 SetBeacon

This command turns the beacon on or off on the adapter port.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`SetBeacon <WWPN|MAC> <BeaconState>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function on the port.
`MAC`	The MAC address of a NIC function on the port.
`BeaconState`	Indicates the state of the beacon. `0` = Off `1` = On

5.6.12 Wakeup

This command shows the firmware's wakeup parameters for the FC function on the adapter.

NOTE: This command is supported only on LPe12000-series adapters.

Supported By

Linux, Solaris, and Windows

Syntax

`Wakeup <WWPN>`

Parameters

`WWPN` The WWPN of an FC function.

5.7 Driver Parameter Commands

The Driver Parameter Commands group controls the driver parameters. You also can change the parameters back to factory default values.

NOTE: Driver Parameter commands are supported only for FC and FCoE ports.

The `DriverConfig` and `SetDriverParamDefaults` commands are not supported for Solaris.

Considerations

- Driver parameters set to temporary or global values (using the `T` and `G` flags, respectively) must be read using the GetDriverParams command to view the current value of the parameter. The `GetDriverParamsGlobal` command returns only permanently set driver parameter values.

Additionally, if temporary and global values are set for one or more driver parameters, the `SaveConfig` command must be run with the `N` flag (using the `N` flag is analogous to using the `GetDriverParams` command) to force the driver parameter values for the specified adapter to be saved. Inaccurate values can be saved if the `G` flag is used for this command.

- The list of available driver parameters that can be configured are different depending on the operating system and protocol (FC or FCoE).

5.7.1 DriverConfig

This command sets all driver parameters to the values in the `.dpv` file type. The `.dpv` file's driver type must match the driver type of the host operating system adapter.

Supported By

Linux and Windows

Syntax

`DriverConfig <WWPN> <FileName> <Flag>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`FileName`	The name of the `.dpv` file, which is stored in the Emulex Repository directory.
`Flag`	`G` = Make the change global (all FC or FCoE functions on this host). `N` = Make the change non-global (function-specific).

5.7.2 GetDriverParams

This command shows the name and value of each parameter.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetDriverParams <WWPN>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.

5.7.3 GetDriverParamsGlobal

This command shows the name and the global value of each driver parameter.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetDriverParamsGlobal <WWPN>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.

5.7.4 SaveConfig

This command saves the specified adapter's driver parameters to a file. The resulting file contains a list of driver parameter definitions in ASCII file format with definitions delimited by a comma. Each definition has the following syntax: `<parameter-name>=<parameter-value>`

The command saves either the values of the global set, or those specific to the adapter in the Emulex Repository directory.

Supported By

Linux, Solaris, and Windows

Syntax

`SaveConfig <WWPN> <FileName> <Flag>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`FileName`	The name of the file that contains the driver parameters list.
`Flag`	`G` = Save the global parameter set. `N` = Save the local (function-specific) parameter set.

5.7.5 SetDriverParam

This command changes a driver parameter and designates the scope of the change.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`SetDriverParam <WWPN> <Flag1> <Flag2> <Param> <Value>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`Flag1`	`L` = Make the change local for only this function. `G` = Make the change global (all FC or FCoE functions on this host).
`Flag2`	`P` = Make the change permanent (persists across reboot). For Linux, to make a permanent change that persists across reboots, you must set `Flag1` to `G` (Global). `T` = Make the change temporary.
`Param`	Name of the parameter to modify.
`Value`	New parameter value, decimal or hexadecimal (`0xNNN`).

Example

To enable dynamic target mode:

```
hbacmd SetDriverParam 10:00:00:00:c9:ff:ff:ff L P enable-dtm 1
```

To disable dynamic target mode, set the flags to `0`.

5.7.6 SetDriverParamDefaults

This command changes all values to the default for the adapter.

Supported By

Linux and Windows

Syntax

`SetDriverParamDefaults <WWPN> <Flag1> <Flag2>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`Flag1`	`L` = Make the change local for only this function. `G` = Make the change global (applies to all FC or FCoE functions on this host).
`Flag2`	`P` = Make the change permanent (the change persists across reboot). `T` = Make the change temporary.

5.8 Dump Commands

The Diagnostic Dump feature enables you to create a dump file for a selected adapter. Dump files contain information, such as firmware version, driver version, and operating system information. This information is useful when you are troubleshooting an adapter, but it is unavailable in Read-Only mode.

CAUTION! Disruption of service can occur if a diagnostic dump is run during I/O activity.

The dump files created are text files (`.txt` extension) and binary files. The extension for binary files depends on the following adapter types:

- LPe16000-series, LPe31000-series, and LPe32000-series adapters – `.bin` extension
- LPe12000-series adapters – `.dmp` extension

5.8.1 DeleteDumpFiles

This command deletes all diagnostic dump files for an adapter.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`DeleteDumpFiles <WWPN|MAC>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function on the adapter.
`MAC`	The MAC address of a NIC port function on the adapter.

5.8.2 Dump

This command creates a diagnostic dump file in the `HbaCmd` dump file directory.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`Dump <WWPN|MAC>`

Parameters

`WWPN`	The WWPN of an FC or FCoE port.
`MAC`	The MAC address of a NIC port.

5.8.3 GetDumpDirectory

This command shows the dump file directory for the adapters in the host.

NOTE: The dump directory can be set only on VMware ESXi hosts.

The dump directory applies to all adapters in the server. A separate dump directory for each adapter does not exist.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetDumpDirectory [WWPN|MAC]`

Parameters

`WWPN`	Obsolete; ignored if specified.
`MAC`	Obsolete; ignored if specified.

5.8.4 GetDumpFile

This command gets the user-specified dump file to the local client's dump directory. The dump directory (local and remote) is named `Dump`. The dump files are copied from the dump directory of the remote host to the dump directory of the local host. Therefore, if the remote host option is not specified (h=*IP_Address*`[`*:port*`]`), this command returns an error because the source and destination directories are the same.

Dump directory:

- Windows – *SystemDrive_Letter*`:\Program Files\Emulex\Util\Dump`
- Linux – `/var/opt/emulex/ocmanager/Dump`
- Solaris – `/opt/ELXocm/Dump`
- VMware ESXi – The dump directory set using the `SetDumpDirectory` command.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`GetDumpFile <h=`*IP_Address*`[:`*port*`]>[`*WWPN*`|`*MAC*`] <`*filename*`>`

Parameters

`WWPN`	Obsolete; ignored if specified.

`MAC`	Obsolete; ignored if specified.
`filename`	The name of the dump file to be copied from the remote host.

Example

```
hbacmd h=10.192.193.154  GetDumpFile  BG-HBANYWARE-15_10000000c97d1314_20100120-032820421.dmp
```

5.8.5 GetDumpFileNames

This command gets the names of the files in the host's dump directory.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

```
GetDumpFileNames [WWPN|MAC]
```

Parameters

`WWPN`	Obsolete; ignored if specified.
`MAC`	Obsolete; ignored if specified.

Example

```
hbacmd GetDumpFileNames
```

5.8.6 GetRetentionCount

This command shows the maximum number of diagnostic dump files to keep.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

```
GetRetentionCount [WWPN|MAC] <value>
```

Parameters

`WWPN`	Obsolete; ignored if specified.
`MAC`	Obsolete; ignored if specified.
`Value`	The number of dump files to retain.

Example

```
hbacmd getRetentionCount 6
```

5.8.7 SetDumpDirectory

This command sets the dump directory (valid only on VMware ESXi hosts).

Supported By

Windows+CIM Provider on a VMware host

To use the `SetDumpDirectory` command, you must have a directory (which must be a storage partition) mapped under `/vmfs/volumes` where the files are dumped. This directory points to the internal hard disk or an external storage area and can also be mapped using the vSphere Client utility from VMware.

The application checks for the dump directory and creates the dump files in that location.

In a remote environment, you can use the `SetDumpDirectory` command from a host running any operating system (including Linux, Solaris, and Windows), but only to a remote host that is running VMware ESXi.

NOTE: The dump directory applies to all adapters in the server. A separate dump directory for each adapter does not exist.

Syntax

`SetDumpDirectory <DumpDirectoryName>`

Parameters

`DumpDirectoryName`	The directory under `/vmfs/volumes` that you created to store the dump files.

Example

This example shows the dump directory set to `/vmfs/volumes/ocm-datastore:`

```
hbacmd h=10.192.203.173 m=cim u=root p=Swamiji001 n=root/emulex SetDumpDirectory
10:00:00:00:c9:61:f2:64 ocm-datastore
```

5.8.8 SetRetentionCount

This command specifies the maximum number of diagnostic dump files for the adapter. When the count reaches the limit, the next dump operation deletes the oldest file.

NOTE: The retention count applies to all adapters in the server.

Supported By

Linux, Solaris, Windows, and Windows+CIM Provider on a VMware host

Syntax

`SetRetentionCount [WWPN|MAC] <Value>`

Parameters

`WWPN`	Obsolete; ignored if specified.
`MAC`	Obsolete; ignored if specified.
`Value`	The number of dump files to retain.

Example

```
hbacmd SetRetentionCount 6
```

5.9 FCoE Commands

The FCoE Commands group manages the FIP parameters and displays the FCF for an FCoE function.

NOTE: These commands are supported only on FCoE+NIC PPC CNAs.

5.9.1 GetFCFInfo

This command shows the FCF information of the FCoE function.

Supported By

Linux

Syntax

`GetFCFInfo <WWPN>`

Parameters

`WWPN` The WWPN of an FCoE function.

Example

```
hbacmd GetFCFInfo 10:00:00:00:c9:3c:f7:88
Number of FCFs:1
Active FCFs:1
Entry 0:
   State: 1
   Priority:133
   Fabric Name:10:00:00:05:1E:0C:54:49
   Switch Name:10:00:00:05:1E:0C:54:49
   MAC:   00:05:9B:71:3D:71
   FC Map:0x0EFC00
   VLAN IDs:
   LKA Period:8
```

5.9.2 GetFIPParams

This command gets the FIP parameters of an FCoE function.

Supported By

Linux

Syntax

`GetFIPParams <WWPN>`

Parameters

`WWPN` The WWPN of an FCoE function.

Example

```
hbacmd h=10.231.140.83 getfipparams 10:00:00:00:c9:bc:a9:31
Param Description      Param Name       Value
-----------------      ----------       -----
Primary Fabric Name    pfabric          FF:FF:FF:FF:FF:FF:FF:FF
Primary Switch Name    pswitch          FF:FF:FF:FF:FF:FF:FF:FF
DCB VLan ID            vlanid           Any VLAN ID is valid
```

5.9.3 SetFIPParam

This command sets the FIP parameters of an FCoE function.

Supported By

Linux

Syntax

`SetFIPParam <WWPN> <Param> <Value>`

Parameters

`WWPN` The WWPN of an FCoE function.

`Param` The FIP parameter name:

- pfabric
- pswitch
- vlanid
- fcmap
- cinvlanid

`Value` The value based on the FIP parameter name:

- pfabric: 8-byte fabric name (format XX:XX:XX:XX:XX:XX:XX:XX)
- pswitch: 8-byte switch name (format XX:XX:XX:XX:XX:XX:XX:XX)
- vlanid: 2-byte VLAN ID [0–4095] or *any* for any VLANID
- fcmap: 3-byte FC_map, 0x0EFCxx
- cinvlanid: 2-byte VLAN_ID [0–4095]

Example

```
hbacmd SetFIPParam 10:00:00:00:c9:5b:3a:6d fcmap 0x0efc99
```

5.10 Firmware Commands

These commands enable you to view and configure firmware parameters.

5.10.1 getfwparams

This command displays a list of all configurable firmware parameters.

Supported By

Windows, Linux, and Windows+CIM Provider on a VMware host

Syntax

`getfwparams <WWPN>`

Parameters

`WWPN` The WWPN of the adapter port.

Example

```
hbacmd getfwparams 10:00:00:90:fa:94:88:cd

FW Params for 10:00:00:90:fa:94:88:cd. Values in HEX format.
```

```
DX                Param      Low     High      Def      Cur      Dyn
00:             FA-PWWN        0        1        0        0        5
01:                 FEC        0        1        1        1        1
02:        DYNAMIC-DPORT       0        1        0        0        1
```

5.10.2 setfwparam

This command enables you to configure firmware parameters.

Supported By

Windows, Linux, and Windows+CIM Provider on a VMware host

Syntax

`setfwparam <WWPN> <param> <value>`

Parameters

`WWPN`	The WWPN of the adapter port.
`param`	The parameter to modify. `FA-PWWN`- Enables or disables the Fabric Assigned WWN (FA-PWWN) parameter. Disabled is the default setting. **NOTE:** You must reset the adapter port to activate new firmware parameter setting, and you must reload the OneCommand Manager application to display the new setting. **NOTE:** When a new WWPN is assigned using FA-PWWN, persistently stored configuration information associated with the original WWPN, such as driver parameters and LUN frame priority settings, is not applied to the newly assigned WWPN. The configuration information associated with the original WWPN must be reconfigured for the new WWPN.
`Value`	`0` = Disables the parameter. `1` = Enables the parameter.

Example

```
hbacmd setfwparam 10:00:00:90:fa:94:2e:ca fa-pwwn 1
Set FW Parameter FA-PWWN=1 for 10:00:00:90:fa:94:2e:ca
Reset adapter port to activate new firmware parameter setting.
```

5.11 LUN Masking Commands

The LUN Masking Commands group manages LUN masking activities. LUN masking commands are supported only for FC functions.

NOTE: Linux, Solaris and Windows+CIM Provider on a VMware host do not support the following commands:

- `GetLunUnMaskByHBA`
- `GetLunUnMaskByTarget`
- `RescanLuns`
- `SetLunMask`

5.11.1 GetLunList

This command queries for the presence of any masked LUNs.

Supported By

Windows

Syntax

`GetLunList <HBA WWPN> <Target WWPN> <Option>`

Parameters

`HBA WWPN`	The WWPN of an FC function on the adapter.
`Target WWPN`	The WWPN of the target.
`Option`	`0` = Get information from the driver `1` = Get information from the configuration

5.11.2 GetLunUnMaskByHBA

This command queries for the presence of any unmasked LUNs by FC functions.

Supported By

Windows

Syntax

`GetLunUnMaskByHBA <HBA WWPN> <Option>`

Parameters

`HBA WWPN`	The WWPN of an FC port.
`Option`	`0` = Get information from the driver `1` = Get information from the configuration

5.11.3 GetLunUnMaskByTarget

This command queries for any unmasked LUNs by target.

Supported By

Windows

Syntax

`GetLunUnMaskByTarget <HBA WWPN> <Target WWPN> <Option>`

Parameters

`HBA WWPN`	The WWPN of an FC function.
`Target WWPN`	The WWPN of the target.
`Option`	`0` = Get information from the driver `1` = Get information from the configuration

5.11.4 RescanLuns

This command rescans LUNs to find any new LUNs.

Supported By

Windows

Syntax

`RescanLuns <HBA WWPN> <Target WWPN>`

Parameters

`HBA WWPN`	The WWPN of an FC function.
`Target WWPN`	The WWPN of the target.

5.11.5 SetLunMask

This command masks the specified LUNs.

Supported By

Windows

Syntax

`SetLunMask <HBA WWPN> <Target WWPN> <Option> <Lun> <LunCount> <MaskOp>`

Parameters

`HBA WWPN`	The WWPN of an FC function.
`Target WWPN`	The WWPN of the target.
`Option`	`0` = Get information from the driver `1` = Get information from the configuration (make persistent) `2` = Send information to both
`Lun`	The starting LUN number.
`LunCount`	The number of LUNs.
`MaskOp`	`A` = Mask LUN `B` = Clear unmask target level `C` = Clear unmask HBA level `D` = Unmask LUN `E` = Unmask target level `F` = Unmask HBA level

5.12 LUN ExpressLane Commands

The LUN ExpressLane Commands group enables, disables, and displays the ExpressLane status on a particular LUN.

The OneCommand Manager application allows you set special priority queuing for selected LUNs by making them ExpressLane LUNs. ExpressLane LUN performance is superior to that of regular LUNs. You can enable ExpressLane LUNs attached to both physical and virtual ports. ExpressLane LUN assignments persist across system reboots.

NOTE: ExpressLane is not supported on LPe12000-series adapters or on PPC CNAs.

For Linux operating systems, if ExpressLane LUNs are created, the vPort needs to be re-created after a system boot because the ExpressLane LUNs do not persist across system reboots. If the vPort is re-created with the same WWPN to which the ExpressLane LUN was previously assigned and that same LUN is then detected, it becomes an ExpressLane LUN again.

5.12.1 GetExpressLaneLunList

This command displays LUNs on a target and their respective ExpressLane status.

Supported By

Linux, Windows, and Windows + CIM Provider on a VMware host

NOTE: For Linux and VMware operating systems, only ExpressLane-enabled LUNs are shown by this command. LUNs without ExpressLane-enabled support are not shown.

Syntax

`GetExpressLaneLunList <WWPN> [vport=<vPort WWPN>] <Target WWPN> <Option>`

Parameters

`WWPN`	The WWPN of the FC function connected to the target or physical WWPN if virtual ports are selected.
`vPort WWPN`	The WWPN of an optional vPort allowing you to get the ExpressLane LUNs of a vPort.
`Target WWPN`	The WWPN of the target LUNs.
`Option`	`0` = Get information from driver `1` = Get information from configuration

Example

```
hbacmd h=10.192.87.198 GetExpressLaneLunList 10:00:00:00:00:87:01:98 20:22:d4:ae:52:6e:6f:08 0

Number of LUNs: 4
      FCP_LUN          OS_LUN       ExpressLane
------------------     ------       -------------
0000 0000 0000 0000    0            No
0001 0000 0000 0000    1            Yes
0002 0000 0000 0000    2            No
0003 0000 0000 0000    3            Yes
```

5.12.2 SetExpressLaneLunState

This command enables or disables ExpressLane on a particular LUN.

NOTE: ExpressLane cannot be enabled for masked LUNs.

Supported By

Linux, Windows, and Windows + CIM Provider on a VMware host

Syntax

`SetExpressLaneLunState <WWPN> [vport=<vPort WWPN>] <Target WWPN> <Lun> <State> <Option>`

Parameters

`WWPN`	The WWPN of the FC function connected to the target or physical WWPN if virtual ports are selected.

`vPort WWPN`	The WWPN of an optional vPort allowing you to set the state of a vPort LUN.
`Target WWPN`	The WWPN of the target LUNs.
`LUN`	The LUN number on which to set the ExpressLane status. Obtain the LUN number from the output of the `GetExpressLaneLunList` command under the OS LUN column.
`State`	`0` = Disable ExpressLane `1`= Enable ExpressLane
`Option`	`0` = Set ExpressLane LUN state in driver to temporary, until reboot `1` = Set ExpressLane LUN state in the configuration to persist across reboots `2` = Set ExpressLane LUN state in both driver and in the configuration to persist across reboots

Example

```
hbacmd h=10.192.87.198 SetExpressLaneLUNState 10:00:00:00:00:87:01:98 20:22:d4:ae:52:6e:6f:08 2 1 2
```

5.12.3 GetLunXLaneConfig

This command displays the frame priority value for ExpressLane LUNs on the specified target.

Supported By

Linux, Windows, and Windows + CIM Provider on a VMware host

Syntax

```
hbacmd GetLunXLaneConfig <WWPN> [vport=<vPort WWPN>] <Target WWPN> <Option>
```

Parameters

`WWPN`	World-wide port name of any FC function on the adapter.
`vPort WWPN`	The WWPN of an optional vPort.
`Target WWPN`	The WWPN of the target connected to the LUNs.
`Option`	`0` = Get the information from the driver. `1` = Get the information from the configuration.

Example

```
hbacmd GetLunXLaneConfig 10:00:00:00:c9:55:55:56 50:06:01:60:10:20:5C:38 0

Supported Priority Levels: High, Medium, Low

                              Priority   Priority
    FCP_LUN          OS_LUN   Level      Value
------------------- -------- ---------- ----------
0000 0000 0000 0000    0        High       113
0001 0000 0000 0000    1        High       113
0002 0000 0000 0000    2        Medium     92
0009 0000 0000 0000    9        Low        53
```

5.12.4 SetLunXLaneConfig

If the adapter and switch support it, the `SetLunXLaneConfig` command enables you to configure the ExpressLane Optimized Access Storage (OAS) state and the frame priority levels, or values, for ExpressLane LUNs. Switches can provide up to three priority levels, Low, Medium, and High, but they might provide fewer options.

NOTE: If the switch connected to the FC initiator does not support LUN specific frame priority levels using the Get Fabric Object (GFO), you must manually enter the frame priority values in the range of 0–127 for all ExpressLane-enabled LUNs.

You can also use the `SetLunXLaneConfig` command to disable ExpressLane on all LUNs in a single operation.

Use the `GetLunXLaneConfig` command to determine if frame priority levels are supported.

The following rules apply when using the `SetLunXLaneConfig` command:

- The ExpressLane (OAS) state and priority levels, or values, is saved automatically to both the driver and configuration settings. You cannot specify where to save the configuration.
- The priority parameter is only required if the ExpressLane state parameter is set to `1` (enable).
  - You cannot disable the ExpressLane OAS state with the priority level, or value, parameter set.
  - You cannot disable all LUNs with the priority level, or value, parameter set.
- The `EnableXLane` driver parameter must be enabled.

NOTE: `EnableXLane` is disabled when `vmid_priority_tagging` and `max_vmid` parameters are enabled on VMware hosts.

Supported By

Linux, Windows, and Windows + CIM Provider on a VMware host

Syntax

`hbacmd SetLunXLaneConfig <WWPN> [vport=<vPort WWPN>] <Target WWPN> <LUN> <State> <PriorityLevel|PriorityValue>`

Parameters

`WWPN`	The World Wide Port Name of any FC function on the adapter.
`vPort WWPN`	The WWPN of an optional vPort.
`Target WWPN`	The WWPN of the target connected to the LUNs.
`LUN`	The LUN number. (The OS_LUN from the `GetExpressLaneLunList` command to set.) Use `ALL` to disable ExpressLane for all LUNs.)
`State`	`0`=disable ExpressLane `1`=enable ExpressLane
`PriorityLevel`	The levels are high, medium, or low. (Use the `GetSmartSanPriorities` command to get an accurate list of the supported priority levels). This value must be omitted if the `State`=0.
`PriorityValue`	A value within the range of 0– 127. This value is only allowed if priority levels are not supported by the switch. This value must be omitted if the `State`=0.

Example

```
hbacmd SetLunXLaneConfig 10:00:00:00:c9:55:55:56 50:06:01:60:10:20:5C:38 0 1 low

ExpressLane configuration successfully changed on the specified LUN(s)
```

5.13 Miscellaneous Commands

Commands in the Miscellaneous Command group do not fit in other groups. See specific commands for adapter limitations.

5.13.1 AddHost

This command adds a host to the hosts file for remote TCP/IP management in the OneCommand Manager application. The adapters for these hosts are also presented by the `ListHBAs` command (see Section 5.13.7, ListHBAs).

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

To add non-VMware ESXi hosts:

```
AddHost <hostname|IP_address>[:Port_Number]
```

Parameters

`hostname`	The name of the host to add to the hosts file.
`IP_address`	The IP address (IPv4 or IPv6) of the host to add to the hosts file. Example IPv4: `10.192.80.102` Example IPv6: `fe80::6445:80e9:9878:a527`
`Port_Number`	The optional IP port number used to access remote host. Example: `10.192.80.102:9876` **NOTE:** When specifying IPv6 address with `Port_Number`, it must be enclosed in `[ ]`. Example: `[fe80::6445:80e9:9878:a527]:9876`

- An attempt is made to contact the host to confirm remote access before adding it to the host list. If the attempt fails, the host is not added.
- The h option (for specifying an optional IP address or host name) after `hbacmd` is not available for the `AddHost` command.

To add VMware ESXi hosts to Windows using the OneCommand Manager application:

```
m=cim [u=<username>] [p=<password>] [n=<namespace>] AddHost  <IP_Address>
```

If the *username*, *password*, and *namespace* are not specified, see Section 4.4.2.1.1, Default CIM Credentials.

Parameters

`host_address`	The IP address (using the IPv4 or IPv6 format) or the host name.

5.13.2 Download

This command downloads a firmware image to the port function or adapter specified by the WWPN or MAC address.

Considerations

- If you attempt to update unauthenticated firmware for an LPe31000-series or LPe32000-series adapter, the following error message is displayed:

```
ERROR: Download Failed due to invalid firmware digital signature. Please contact customer support
for additional help.
ERROR: <203>: Failed validating firmware digital signature
```

- If you attempt to update unsecured firmware for an LPe31000-series or LPe32000-series adapter, the following error message is displayed:
  `ERROR: Download Failed due to missing digital signature in firmware file. Please contact customer support for additional help.`
  `ERROR: <209>: Firmware digital signature missing`
- For LPe16000-series, LPe31000-series, and LPe32000-series firmware downloads, the OneCommand Manager application accepts only `.grp` files.
- For LPe16000-series, LPe31000-series, and LPe32000-series adapters, the WWPN (and MAC address for PPC CNAs) identifies the adapter, and the updated firmware applies to the entire adapter.
- If you attempt to download firmware that is not compatible with the adapter, the following error message is displayed:
  `ERROR: <24>: This firmware version is not supported on this board model.`
- For LPe12000-series adapters, you update the firmware and boot code on each FC port/function. The firmware and boot code are two separate binaries. You must flash both the firmware and boot binaries to update LPe12000-series adapters.

CAUTION! Updating firmware or boot code on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the update has completed, the system performs an adapter reset, which might cause a loss of connectivity to the SAN and a possible loss of data. To update firmware on an LPe12000-series adapter, you must make sure that the adapter is not currently being used to boot from SAN. Perform one of the following:

- Move the adapter to be updated to a non-boot from SAN host, and perform the update from that location.
- If the host with the adapter that needs to be updated is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be updated because it is no longer being used for boot from SAN.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`Download <WWPN|MAC> <FileName>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function on the adapter.
`MAC`	The MAC address of a NIC function on the adapter.
`FileName`	The name and location of the firmware image (any file accessible to the CLI client).

5.13.3 ExportSANInfo

For reporting purposes, this command captures the SAN information in `.xml` for XML-formatted files and `.csv` for CSV-formatted files.

NOTE: This command can take a long time on large SAN configurations because of the large amount of information that must be obtained and reported. The output can also be redirected to a file if required.

Supported By

Linux, Solaris, and Windows

Syntax

`ExportSANInfo [format]`

NOTE: The h option (for specifying an optional IP address or host name) after `hbacmd` is not available for the `ExportSANInfo` command.

Parameters

`format` An optional parameter that specifies the format of the adapter information:
`csv` = CSV-formatted files
`xml` = XML-formatted files
Leaving the format blank shows the data in xml format (default).

5.13.4 FecEnable

This command enables or disables FEC on LPe16000-series, LPe31000-series, and LPe32000-series FC adapters.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

FecEnable *WWPN <0|1>*

Parameters

`WWPN` The WWPN of the FC function.
`0` Disables FEC on the function
`1` Enables FEC on the function

5.13.5 GetCimCred

This command shows the default credentials set for the CIM client.

NOTE: The password is encrypted.

Supported By

Windows

Syntax

`GetCimCred`

Parameters

None.

5.13.6 GetVPD

This command shows the port's VPD.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`GetVPD <WWPN|MAC>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`MAC`	The MAC address of a NIC function.

5.13.7 ListHBAs

This command shows a list of the manageable Broadcom Emulex adapters found by local discovery. For a NIC port on a PPC CNA, the MAC address is displayed instead of the WWPN. The node WWN and fabric WWN are not displayed. The type of information listed can vary according to the adapter model.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`ListHBAs [local] [m=model] [pt=type] [down]`

Parameters

`local`	Displays only local adapters.
`m=model`	Model filter. Append * to the end of the model name for a wildcard match. For example: LPe16*
`pt=type`	The port type filter. Valid types are `NIC`, `FC`, and `FCoE`.
`down`	Displays only the NIC functions of PPC CNAs on the local system in which the adapter's ARM processor has stopped. This parameter detects adapters that might not respond to commands from the OneCommand Manager CLI or application.

5.13.8 RemoveHost

This command removes a host from the hosts file used for TCP/IP management in the OneCommand Manager application GUI. The <*host_address*> can be an IP address that uses the IPv4 or IPv6 format, or it can be a host name.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

For the remote management interface:
`RemoveHost host_address`

For VMware ESXi using the CIM interface:
`m=cim RemoveHost <IP_Address>`

NOTE: The h option (for specifying an optional IP address or host name) after `hbacmd` is not available for the `RemoveHost` command.

Parameters

`host_address`	The host to remove.
`IP_Address`	The IP address of the host to remove.

5.13.9 Reset

This command resets an FC or FCoE function. A reset can require several seconds to complete, especially for remote devices. When the reset is completed, the system command prompt is displayed.

NOTE: This command applies only to FC and FCoE functions.

For PPC CNA FCoE functions, this command only resets the driver to update changed driver parameters that require a driver reset. It does not cause a hardware reset of the FCoE function.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`Reset <WWPN>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.

5.13.10 SetCimCred

This command sets the default CIM credentials. You must specify all four credentials: *`username`*, *`password`*, *`namespace`*, and *`portnum`*. Default credentials are used if any credential is not in the `hbacmd` command argument. After the default credentials for a host are set, any other command can be issued by specifying `m=cim`.

Supported By

Windows

Syntax

`SetCimCred <username> <password> <namespace> <portnum>`

NOTE: Use this command to set only the CIM credentials. After this is finished, subsequent `hbacmd` commands do not require you to specify the CIM credentials in the command line.

Parameters

`username`	The logon user ID of the VMware ESXi.
`password`	The logon password of the VMware ESXi.
`namespace`	The namespace where the Emulex CIM provider is registered in the SFCB CIMOM of VMware ESXi, specifically `root/emulex`.
`portnum`	The port number of the SFCB that CIMOM is listening to, that is, `5988` (HTTP) or `5989` (HTTPS).

5.13.11 TargetMapping

This command shows a list of mapped targets and the LUNs for an FC or FCoE function on a port.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`TargetMapping <WWPN>`

Parameters

`WWPN` The WWPN of an FC or FoE adapter.

5.13.12 Version

This command shows the current version of the OneCommand Manager CLI Client.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

For the remote management interface:
`Version`

NOTE: The `h` option (for specifying an optional IP address or host name) after `hbacmd` is not available for the `Version` command.

For VMware ESXi using the CIM interface:
`h=<IP address> m=<cim Version>`

Parameters

`h` The IP address of the VMware ESXi.

`m` The CIM version of the VMware ESXi.

5.14 Persistent Binding Commands

The Persistent Binding Commands group facilitates persistent binding operations.

In a remote environment, you can perform persistent bindings operations from a host running any operating system (including Linux or VMware ESXi), but only to a remote host that is running Windows or Solaris.

For a binding to take effect immediately (that is, `SetPersistentBinding parameter`: `Scope` = `I` or `B`), the <*SCSIBus*> and <*SCSITarget*> parameters must match the SCSI bus and SCSI target to which the FC or FCoE target is already automapped. If automapping is disabled, the binding takes effect immediately if the FC or FCoE target is not already persistently bound, and the specified <*SCSIBus*> and <*SCSITarget*> parameters are available to be persistently bound. Also, the <*BindType*> parameter must match the currently active bind type. Otherwise, you are notified that you must reboot the system to cause the persistent binding to become active.

These commands are supported only for FC and FCoE ports.

The following persistent binding commands are not supported on Linux or on Windows + CIM Provider on a VMware host:

- `BindingCapabilities`
- `BindingSupport`
- `PersistentBinding`
- `RemoveAllPersistentBinding`
- `RemovePersistentBinding`
- `SetBindingSupport`
- `SetPersistentBinding`

5.14.1 AllNodeInfo

This command shows target node information for each target accessible by the adapter.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`AllNodeInfo <WWPN>`

Parameters

`WWPN` The WWPN of an FC or FCoE function.

5.14.2 BindingCapabilities

This command shows the binding capabilities of the adapter. If a binding is configured, it is maintained across reboots.

Supported By

Solaris and Windows

Syntax

`BindingCapabilities <WWPN>`

Parameters

`WWPN` The WWPN of an FC or FCoE function.

5.14.3 BindingSupport

This command shows the binding support for an FC or FCoE function.

Supported By

Solaris and Windows

Syntax

`BindingSupport <WWPN> <Source>`

Parameters

`WWPN` The WWPN of an FC or FCoE function.

`Source` `C` = Configuration support
`L` = Live support

5.14.4 PersistentBinding

This command specifies the set of persistent binding information (configuration or live state) that is requested.

Supported By

Citrix, Solaris and Windows

Syntax

`PersistentBinding <WWPN> <Source>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`Source`	`C` = Configuration support `L` = Live support

5.14.5 RemoveAllPersistentBinding

This command removes all persisting bindings for an FC or FCoE function.

Supported By

Solaris and Windows

Syntax

`RemoveAllPersistentBinding <WWPN>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.

5.14.6 RemovePersistentBinding

This command removes persistent binding between an FC or FCoE target and a SCSI bus and target. The binding to be removed can be to a target WWPN, a target WWNN, or a target D_ID.

Supported By

Solaris and Windows

Syntax

`RemovePersistentBinding <WWPN> <BindType> <ID> <SCSIBus> <SCSITarget>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`BindType`	`P` = Remove binding by WWPN `N` = Remove binding by WWNN `D` = Remove binding by D_ID
`ID`	The type of ID based on `<BindType>`: Target WWPN if `<BindType>` = `P` Target WWNN if `<BindType>` = `N` Target D_ID if `<BindType>` = `D`
`SCSIBus`	The bus number of the SCSI device.
`SCSITarget`	The target number of the SCSI device.

5.14.7 SetBindingSupport

This command enables and sets the binding support for an FC or FCoE function.

Supported By

Solaris and Windows

Syntax

`SetBindingSupport <WWPN> <BindFlag>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`BindFlag`	The type of binding support for the adapter: `D` = Binding by D_ID (not available for Windows driver) `P` = Binding by WWPN `N` = Binding by WWNN (not available for Windows driver) `A` = Binding by automap (not available for Windows driver) `DA` = Binding by D_ID and automap `PA` = Binding by WWPN and automap `NA` = Binding by WWNN and automap

5.14.8 SetPersistentBinding

This command sets a persistent binding between an FC or FCoE target and a SCSI bus target. The binding can be to a target WWPN, a target WWNN, or a target D_ID.

Supported By

Solaris and Windows

Syntax

`SetPersistentBinding <WWPN> <Scope> <BindType> <TargetId> <SCSIBus> <SCSITarget>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`Scope`	`P` = Permanent binding (survives reboot) `I` = Immediate binding `B` = Binding is both permanent and immediate
`BindType`	`P` = Enable binding by WWPN `N` = Enable binding by WWNN `D` = Enable binding by D_ID
`TargetId`	If <`BindType`> = `P`, Target WWPN If <`BindType`> = `N`, Target WWNN If <`BindType`> = `D`, Target D_ID
`SCSIBus`	The bus number of the SCSI device.
`SCSITarget`	The target number of the SCSI device.

5.15 vPort Commands

The vPort Commands group manages virtual ports and functions on FC and FCoE adapters.

NOTE: In Linux, vPorts do not persist across system reboots. vPorts must be re-created after a system reboot.

5.15.1 CreateVPort

This command creates a virtual port with an automatically generated WWPN or a user-specified virtual WWPN on the specified physical port. If you specify `auto`, the virtual WWPN is generated automatically. Otherwise, you must specify the virtual WWPN for this parameter. If creation is successful, the WWPN is displayed as part of the output from the command. The *vname* optional parameter can be specified for the virtual port's name.

Supported By

Linux, Solaris, and Windows

Syntax

`CreateVPort <physical WWPN> auto [vname]`

-or-

`CreateVPort <physical WWPN> <virtual WWPN> <virtual WWNN> [vname]`

Parameters

`physical WWPN`	The WWPN of an FC or FCoE function.
`auto`	The virtual WWPN is automatically generated for the virtual port.
`vname`	The virtual port's name (optional).
`virtual WWPN`	The virtual WWPN to create.
`virtual WWNN`	The virtual WWNN to create.

5.15.2 DeleteVPort

This command deletes the virtual port specified by a physical and virtual WWPN.

Supported By

Linux, Solaris, and Windows

Syntax

`DeleteVPort <physical WWPN> <virtual WWPN>`

Parameters

`physical WWPN`	The WWPN of an FC or FCoE function.
`virtual WWPN`	The WWPN of the virtual port.

5.15.3 ListVPorts

This command lists virtual ports on the specified physical FC or FCoE function. Leaving the physical WWPN parameter blank lists all virtual ports on all manageable hosts that support virtual ports.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`ListVPorts <physical WWPN>`

Parameters

`physical WWPN` The WWPN of an FC or FCoE function.

5.15.4 VPortTargets

This command lists targets visible to the specified virtual port.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`VPortTargets <physical WWPN> <virtual WWPN>`

Parameters

`physical WWPN` The WWPN of an FC or FCoE function.

`virtual WWPN` The WWPN of the virtual port.

5.16 WWN Management Commands

NOTE: These commands are supported only for FC or FCoE functions.

The WWN Management Commands group validates WWNs carefully to avoid WWPN duplication, but WWNN duplication is acceptable. You might see error and warning messages if a name duplication is detected. Fulfill the activation requirement after each WWN is changed or restored. If pending changes exist, some diagnostic and maintenance features are not available.

CAUTION! Using the `ChangeWWN` or `RestoreWWN` commands on an LPe12000-series adapter that is being used to boot from SAN is not advisable. After the command is completed, the system performs an adapter reset, which might cause a loss of connectivity to the SAN and possible loss of data. To perform these commands, you must make sure that the adapter is not currently being used to boot from SAN.

Do one of the following:

- Move the target adapter to a non-boot from SAN host.
- If the host with the target adapter is also hosting other boot from SAN adapters, perform a boot from SAN using one of the other boot from SAN adapters. The target adapter can now be used.

5.16.1 ChangeWWN

This command allows you to change WWPNs and WWNNs, and it allows you to change the WWN to volatile or nonvolatile. If you attempt to select volatile on an adapter that does not support volatile WWNs, a `Not Supported` error is returned.

NOTE: This command is disabled when FA-PWWN is enabled on the adapter port.

When a volatile change is supported, a reboot is required to activate the new value. Volatile names are active until system power-down or adapter power-cycle.

For VMware ESXi:

- After changing the WWN of a function, update your zoning settings before you reboot your ESXi server. If the zoning is not updated before your reboot, the subsequent boot could take a long time.

- After changing the WWN of a function, you must reboot the ESXi system before trying to access the adapter on that system. For information on rebooting the ESXi system, refer to the VMware documentation.
- If you are using the CIM interface to access functions, after changing the WWN of a function, you must restart the CIMOM (that is, SFCB) on the ESXi system before trying to access the function on that system. For information on restarting the CIMOM, refer to the VMware documentation.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`ChangeWWN <WWPN> <New WWPN> <New WWNN> <Type>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`New WWPN`	The WWPN of the FC or FCoE function.
`New WWNN`	The WWNN of an FC or FCoE function.
`Type`	`0` = Volatile `1` = Nonvolatile

5.16.2 GetWWNCap

This command shows if volatile change is supported for the WWPN.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`GetWWNCap <WWPN>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.

5.16.3 ReadWWN

This command reads different types of WWNs.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`ReadWWN <WWPN> <Type>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`Type`	`0` = Volatile `1` = Nonvolatile `2` = Factory default `3` = Current `4` = Configured

5.16.4 RestoreWWN

This command changes the WWNs to the factory default or nonvolatile values. The change is nonvolatile.

NOTE: A reboot is required to activate the new value.

NOTE: This command is disabled when FA-PWWN is enabled on the adapter port.

For VMware ESXi:

- After changing the WWN of an function, you must reboot the ESXi system before trying to access the adapter on that system. For information on rebooting the ESXi system, refer to the VMware documentation available from the VMware website.
- If you are using the CIM interface to access adapters, after changing the WWN of a function, you must restart the CIMOM (that is, SFCB) on the ESXi system before trying to access the function on that system. For information on restarting the CIMOM, refer to the VMware documentation available from the VMware website.

Supported By

Linux, Solaris, Windows, and Windows + CIM Provider on a VMware host

Syntax

`RestoreWWN <WWPN> <Type>`

Parameters

`WWPN`	The WWPN of an FC or FCoE function.
`Type`	`0` = Restore default WWNs `1` = Restore NVRAM WWNs

Appendix A: OneCommand Manager Error and Return Messages

Table 7: OneCommand Manager Error and Warning Messages contains a list of some of the error messages that might be encountered during a OneCommand Manager session.

Table 7: OneCommand Manager Error and Warning Messages

Error Message	Commands	Description
Error: Read-only management mode is currently set on this host. The requested command is not permitted in this mode.	Active management commands that change a property on an adapter or host.	This message is returned when some commands are attempted while the CLI is configured for read-only mode. See Section 4.1.1, CLI in Read-Only Mode.
Not supported.	`ChangeWWN`	If a volatile change is requested on an adapter that does not support volatile WWNs, it returns a `Not Supported` error. See Section 5.16.1, ChangeWWN.
RETURN CODE: <0>: Success, no further action is needed.	`Download`	The firmware download completed without errors.
ERROR: HBACMD_GetDumpFile: RM_GetDumpFile call failed (2) ERROR: <2>: Not Supported	`GetDumpFile`	Dump files are copied from the Dump directory of the remote host to the Dump directory of the local host. Specifying a local port identifier for this command returns an error because the source and destination directory are the same. See Section 5.8.4, GetDumpFile.
ERROR: <4>: Invalid argument	`getfwparams` `setfwparam`	This message is returned when there is a problem with the command. See Section 5.10, Firmware Commands.
ERROR: <5>: Illegal WWN format	`getfwparams` `setfwparam`	This message is returned when the WWN format is incorrect. See Section 5.10, Firmware Commands.
ERROR: <24>: This firmware version is not supported on this board model.	`Download`	This message is returned when the firmware version is incompatible with the adapter. Download compatible firmware. See Section 5.13.2, Download.
ERROR: <35>: Unable to allocate buffer	`getfwparams`	This message is returned when the command cannot allocate a buffer. See Section 5.10, Firmware Commands.
ERROR: <180>: Authentication: User unknown	All	The specified user name is not valid or could not be authenticated by the system. See Section 1.2, OneCommand Manager Secure Management, for more information.
ERROR: <181>: Authentication: Insufficient credentials	All	The specified user name and password are valid and the user is a member of a OneCommand Manager group. However, the OneCommand Manager group does not have sufficient privileges to execute the specified command. See Section 1.2, OneCommand Manager Secure Management, for more information.

Table 7: OneCommand Manager Error and Warning Messages (Continued)

Error Message	Commands	Description
ERROR: <183>: Secure Mgmt: user not a member of OCM group	All	The specified user name and password could be authenticated, but the user is not a member of a OneCommand Manager group. See Section 1.2, OneCommand Manager Secure Management, for more information.
ERROR: Download Failed due to invalid firmware digital signature. Please contact customer support for additional help. ERROR: <203>: Failed validating firmware digital signature	`Download`	If you attempt to update unauthenticated firmware for a secure LPe31000-series or LPe32000-series adapter, this error message is displayed. See Section 5.13.2, Download.
ERROR: <206>: Authentication Failed	All	This indicates either a valid user name with an invalid password, or a general user authentication error. See Section 1.2, OneCommand Manager Secure Management, for more information.
ERROR: Download Failed due to missing digital signature in firmware file. Please contact customer support for additional help. ERROR: <209>: Firmware digital signature missing	`Download`	If you attempt to update unsecured firmware for a secure LPe31000-series or LPe32000-series adapter, this error message is displayed. See Section 5.13.2, Download.
RETURN CODE: <247>: Download succeeded, but a reboot is required to activate the new firmware.	`Download`	Reboot the system to activate the new firmware.
ERROR: <251>: Hardware or firmware does not support command	`getfwparams` `setfwparam`	This message is returned when the hardware or firmware does not support the command. See Section 5.10, Firmware Commands.
Error: <431> Cable length required for force mode and interface type.	`SetPhyPortSpeed`	This error is displayed when a length value is not included when the mode is set to 2. Example: `hbacmd setphyportspeed 00-00-c9-a9-41-88 2 100Mb` See Examples.

Appendix B: License Notices

B.1 Secure Hash Algorithm (SHA-1) Notice

/*
* Written by Aaron D. Gifford <me@aarongifford.com>
*
* Copyright 1998, 2000 Aaron D. Gifford. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in the
* documentation and/or other materials provided with the distribution.
* 3. Neither the name of the copyright holder nor the names of contributors
* may be used to endorse or promote products derived from this software
* without specific prior written permission.
*
* THIS SOFTWARE IS PROVIDED BY THE AUTHOR(S) AND CONTRIBUTORS ``AS IS'' AND
* ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
* ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) OR CONTRIBUTORS BE LIABLE
* FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
* DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
* OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
* LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
* OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
* SUCH DAMAGE.
*/

B.2 OpenPegasus Licensing Notice

Licensed to The Open Group (TOG) under one or more contributor license agreements. Refer to the OpenPegasusNOTICE.txt file distributed with this work for additional information regarding copyright ownership.
Each contributor licenses this file to you under the OpenPegasus Open Source License; you may not use this file except in compliance with the License.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:
The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

B.3 OpenSSL Notice

This is a copy of the current LICENSE file inside the CVS repository.
LICENSE ISSUES
==========
The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.
OpenSSL License

/* ==
* Copyright (c) 1998-2011 The OpenSSL Project. All rights reserved.
*
* Redistribution and use in source and binary forms, with or without
* modification, are permitted provided that the following conditions
* are met:
*

```
* 1. Redistributions of source code must retain the above copyright
* notice, this list of conditions and the following disclaimer.
*
* 2. Redistributions in binary form must reproduce the above copyright
* notice, this list of conditions and the following disclaimer in
* the documentation and/or other materials provided with the
* distribution.
*
* 3. All advertising materials mentioning features or use of this
* software must display the following acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
*
* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to
* endorse or promote products derived from this software without
* prior written permission. For written permission, please contact
* openssl-core@openssl.org.
*
* 5. Products derived from this software may not be called "OpenSSL"
* nor may "OpenSSL" appear in their names without prior written
* permission of the OpenSSL Project.
*
* 6. Redistributions of any form whatsoever must retain the following
* acknowledgment:
* "This product includes software developed by the OpenSSL Project
* for use in the OpenSSL Toolkit (http://www.openssl.org/)"
*
* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY
* EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
* IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR
* PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR
* ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
* SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT
* NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES;
* LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
* HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT,
* STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE)
* ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED
* OF THE POSSIBILITY OF SUCH DAMAGE.
* ====================================================================
*
* This product includes cryptographic software written by Eric Young
* (eay@cryptsoft.com). This product includes software written by Tim
* Hudson (tjh@cryptsoft.com).
*
*/

Original SSLeay License
-----------------------

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)
* All rights reserved.
*
* This package is an SSL implementation written
* by Eric Young (eay@cryptsoft.com).
* The implementation was written so as to conform with Netscapes SSL.
*
* This library is free for commercial and non-commercial use as long as
* the following conditions are aheared to. The following conditions
* apply to all code found in this distribution, be it the RC4, RSA,
* lhash, DES, etc., code; not just the SSL code. The SSL documentation
* included with this distribution is covered by the same copyright terms
* except that the holder is Tim Hudson (tjh@cryptsoft.com).
*
* Copyright remains Eric Young's, and as such any Copyright notices in
* the code are not to be removed.
* If this package is used in a product, Eric Young should be given attribution
* as the author of the parts of the library used.
* This can be in the form of a textual message at program startup or
* in documentation (online or textual) provided with the package.
*
```


BROADCOM®