Boot for NIC, iSCSI, and FCoE Protocols User Manual

Emulex, 3333 Susan Street

Costa Mesa, CA 92626

Table of Contents

List of Figures

List of Tables

1. Introduction

Overview

This manual describes installing, enabling, and configuring boot code for Emulex® network interface card (NIC), Internet Small Computer System Interface (iSCSI), and Fibre Channel over Ethernet (FCoE) universal converged network adapters (UCNAs). This manual also describes the Emulex boot from SAN implementation and its operation with distinct hardware and operating system requirements.

Boot from SAN is the process of booting a server directly from a disk operating system image located on a storage area network (SAN) by way of Emulex adapters using Emulex boot code. When booting from SAN, the storage device is typically identified by its world wide port name (WWPN) and a logical unit number (LUN). By extending the server system boot basic input/output system (BIOS), boot from SAN functionality is provided by the boot BIOS contained on an Emulex adapter in the server. When properly configured, the adapter then permanently directs the server to boot from a logical unit (disk) on the SAN as if it were a local disk.

Emulex provides the following types of boot code:

- Preboot eXecution Environment (PXE) boot for NIC adapters in x86 and x64 systems
- x86 BootBIOS for FCoE adapters in x86 and x64 systems
- iSCSI boot for iSCSI adapters in x86 and x64 systems
- UEFIBoot for iSCSI
- UEFIBoot for NIC and FCoE adapters in x64 systems. It provides system boot capability through the use of the UEFI (Unified Extensible Firmware Interface) Shell. It also functions on UEFI 2.1-based platforms through the HII (Human Interface Infrastructure) interface.
- OpenBoot for FCoE adapters in Sun SPARC systems (OpenBoot is also called FCode)

Note: Emulex drivers support multipath boot configurations. See your storage vendor's documentation for information on configuring multipath booting.

The Emulex boot code and the following utilities provide a variety of capabilities:

- Boot from SAN across the different networking protocols and operating systems
- UEFI configuration using the Emulex NIC, FCoE, and iSCSI Configuration Utilities
- PXESelect Utility
  - Configuring the port and controller
  - Configuring multichannel support, personality options, and advanced mode support
- FCoE Boot BIOS Utility

  - Scanning for target devices
  - Configuring boot devices, DCBX mode, and advanced adapter parameters
- iSCSISelect Utility
  - Setting up a basic configuration
  - Configuring and managing iSCSI initiators and targets

The OneConnect boot code is distributed, with the firmware, in a .UFI file. See the Emulex website for the Emulex utilities that enable you to install the firmware and boot code package.

Abbreviations

ACL	Access Control List
AL_PA	Arbitrated Loop Physical Address
API	application programming interface
ARP	Address Resolution Protocol
BBS	BIOS Boot Specification
BFS	byte file system
BIOS	basic input/output system
CEE	Converged Enhanced Ethernet
CHAP	Challenge Handshake Authentication Protocol
CIN	Cisco-Intel-Nuova
CLI	command line interface
DCB	Data Center Bridging
DCBX	Data Center Bridging Exchange Protocol
DHCP	Dynamic Host Configuration Protocol
DID	device ID
DMA	direct memory access
DNS	Domain Name System
EDD	Enhanced Disk Device
EFI	Extensible Firmware Interface
FC	Fibre Channel
FC-AL	Fibre Channel Arbitrated Loop
FCF	FC Forwarder
FCoE	Fibre Channel over Ethernet
FL_Port	fabric loop port
FTP	File Transfer Protocol
Gb/s	gigabits per second
GPT	GUID partition table

GUI	graphic user interface
GUID	Globally Unique Identifier
HBA	host bus adapter
HII	Human Interface Infrastructure
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
INTx	PCIe legacy interrupts, where "x" is variable
I/O	input/output
IOCTL	input/output control
IP	internet protocol
IQN	iSCSI qualified name
iSCSI	Internet Small Computer System Interface
JBOD	just a bunch of disks
KB	1024 bytes (Kilobyte or Kibibyte)
LDAP	Lightweight Directory Access Protocol
LED	light-emitting diode
LPVID	logical port VLAN ID
LUN	logical unit number
MAC	media access control
MBR	master boot record
MPIO	multipath I/O
MSI	message signaled interrupts
MSI-X	message signaled interrupts - extended
MTU	maximum transmission unit
NBP	network bootstrap program
NIC	network interface card (or controller)
NIS/NIS+	Network Information Service/Network Information Service Plus
NIV	Network Interface Virtualization
NLB	network loopback
NPIV	N_Port ID virtualization
NVRAM	non-volatile random-access memory
OCM	OneCommand Manager
OEM	original equipment manufacturer
OS	operating system
PCI	Peripheral Component Interconnect
PCIe	Peripheral Component Interconnect Express
PDU	protocol data unit

PF	physical function
PLOGI	port login
POST	power on self test
PXE	Preboot eXecution Environment
RAID	redundant array of independent disks
RHEL	Red Hat Enterprise Linux
RIS	Remote Installation Services
ROM	read-only memory
RPM	resource package manager
RSS	receive side scaling
SAN	storage area network
SCSI	Small Computer System Interface
SLES	SUSE Linux Enterprise Server
SLI	Service Level Interface
SNP	Simple Network Protocol
SR-IOV	single root I/O virtualization
TB	terabyte
TCP	transmission control protocol
TFTP	Trivial File Transfer Protocol
UCNA	universal converged network adapter
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UMC	universal multichannel
UNDI	Universal Network Device Interface
USB	Universal Serial Bus
VF	virtual function
VLAN	virtual local area network
VM	virtual machine
VMQ	virtual machine queue
vNIC	virtual NIC
WDS	Windows Deployment Server
WWN	world wide name
WWNN	world wide node name
WWPN	world wide port name
x	Used to designate a variable. For example, SP*x* includes SP1, SP2, etc.
ZB	zettabyte

2. Configuring PXE Boot for the NIC Protocol

This section describes using and configuring PXE (or 'pixie') to boot computers using a network interface independent of available data storage devices (such as hard disks) or installed operating systems.

The PXE protocol is a combination of Dynamic Host Control Protocol (DHCP) and Trivial File Transfer Protocol (TFTP) with subtle modifications to both. DHCP locates the appropriate boot server or servers, and TFTP downloads the initial bootstrap program and additional files.

Network booting enables you to perform the following tasks:

- Boot diskless systems such as thin clients and dedicated systems.
- Deploy software and operating systems for your systems.
- Automate system maintenance, such as backups.
- Automate system checking, such as virus scanning.
- Ensure a secure system.

Pre-OS

PXE can be used in a "pre-OS" environment. Pre-OS is the process of loading a small operating environment to perform a client management task before loading the final operating system from the local hard drive. For example, with a pre-OS you can scan the hard drive for viruses. This guarantees that the client is not infected before it starts. The Windows Deployment Services (WDS) uses this to install operation systems on local disks or Byte File System (BFS) disks.

PXE Boot Process

Once PXE Boot is enabled in the system UEFI/BIOS, the PXE client can boot up and start up the PXE boot read-only memory (ROM). This is the boot code physically located on the NIC adapter.

Note: To enable or disable PXE Boot, it must be enabled or disabled in the system UEFI/BIOS; see the documentation that accompanied the server for more information.

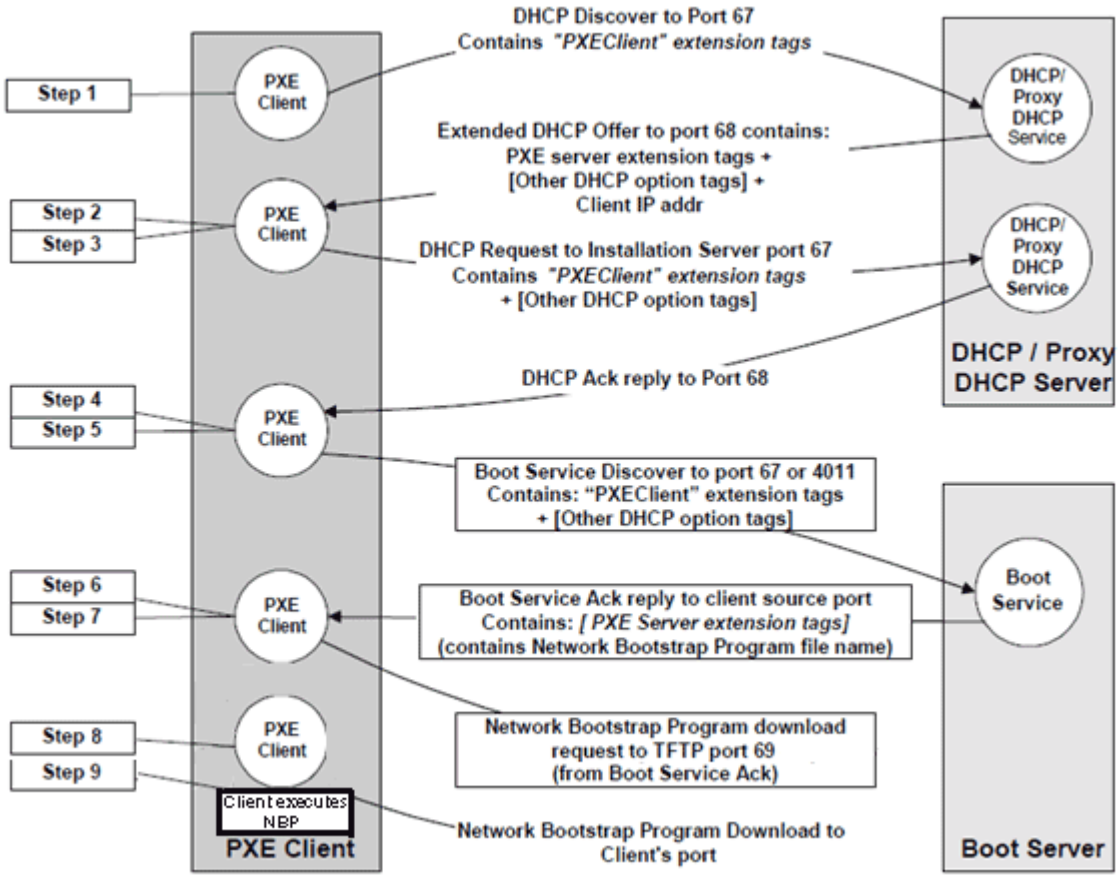

Figure 2-1 PXE Boot Process

Figure 2-1 shows the boot process.

1. The PXE boot ROM sends a DHCP request extended with PXE specific options (step 1).
2. The DHCP responses contain the DHCP options (DHCPOFFERs) that include the Network Bootstrap Program (NBP) filename and boot server lists (steps 2 through 5).
3. The PXE client attempts to download the specified NBP over TFTP from one of the specified boot servers (steps 6 and 7).
4. The PXE client executes the downloaded NBP (steps 8 and 9).

Note: If any of these steps fail, the boot process continues using the next available device in the boot sequence.

Remotely Installing with PXE for Windows Server 2008, 2008 R2, and 2012

For remote installation with PXE, a network driver for the Emulex adapter must be part of the client's installation image on the server. The current versions of Windows Server 2008 and Windows Server 2008 R2 do not include network drivers for the Emulex adapter; however, Windows Server 2012 does include the network driver for the Emulex adapter.

To add the image and installation using the driver with the Remote Installation Service Setup, select:

Start Menu > Programs > Administrative Tools Remote Installation Services Setup

(For more information, refer to *Microsoft Article ID Q246184 - How to Add Third-Party OEM Network Adapters to RIS Installations*.)

In addition to the network driver for the Emulex UCNA, you must configure the following services to use PXE for remote installations:

- DHCP server
- Remote Installation Services (RIS)
- Windows Deployment Server

Microsoft provides extensive documentation on deploying its operating systems for remote installations, and different setups may be required depending on your individual implementation. Microsoft provides step-by-step guides for its Windows Deployment Services for configuring your server, adding images, and installing an operating system. It also includes instructions for more advanced tasks like creating multicast transmissions, creating custom images, and performing an unattended installation.

For detailed information on deploying and managing remote installations on Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012, see the Microsoft website and visit Microsoft TechNet. Search on the bulleted terms above to access Microsoft's wide-ranging documentation on these subjects.

Remotely Installing with PXE for Linux and Citrix Servers

Linux allows for PXE installation over a network using the NFS, FTP, or HTTP protocols. If the system to be installed contains an Emulex NIC or UCNA with PXE Boot support, it can be configured to boot from files on another networked system rather than local media.

The Linux distributions provide extensive documentation on deploying and managing remote installations of the Linux operating system via PXE. See your appropriate distribution's documentation for instructions on how to deploy a PXE installation over your network.

Typically, for a PXE network installation, the Emulex NIC with PXE Boot support sends out a broadcast request for DHCP information. The DHCP server provides the client with an IP address, other network information such as the name server, the IP address or hostname of the TFTP server (which provides the files necessary to start the installation program), and the location of the files on the TFTP server.

The following steps must be performed to prepare for a PXE installation:

1. Configure the network (NFS, FTP, HTTP) server to export the installation tree.
2. Configure the files on the TFTP server necessary for PXE booting.
3. Configure which hosts are allowed to boot from the PXE configuration.
4. Start the TFTP service.
5. Configure DHCP.
6. Boot the client and start the installation.

For remote installation with PXE, a network driver for the Emulex UCNA must be part of the client's installation image on the server. Your current Linux distribution versions may or may not include network drivers for Emulex UCNAs. If they do, the driver may need to be added to your operating system’s installation image, or added during installation. See your appropriate distribution's documentation for instructions on how to add drivers during installation.

Using the PXESelect Utility

Navigating the PXESelect Utility

Use the following methods to navigate the PXESelect utility:

- Press the up/down arrows on your keyboard to move through and select menu options or configuration fields. When multiple adapters are listed, use the up/down arrows to scroll to the additional adapters.
- Press **<Tab>** to move to the next field, and **<Shift> <Tab>** to move to the previous field.
- Press **<Enter>** to accept a selection, select a menu option, to select a row in a configuration screen, or to change a configuration default.
- Press **<Esc>** to return to the previous menu or page, cancel a selection or dialog box, or exit the utility.

Running the PXESelect Utility

To run the PXESelect utility, start or restart your computer. When prompted, hold down **<Ctrl>** and press **<P>**. If you are running the PXESelect utility with multiple controllers, all your controllers are displayed when you start the utility. For example:

```
Press <Ctrl><P> for PXESelect(TM)Utility

Controller#0 Port#0 Base 0xFCE60000 at Bus:05 Dev:00 Fun:00
Controller#0 Port#1 Base 0xFCEA0000 at Bus:05 Dev:00 Fun:01
Controller#1 Port#0 Base 0xFC920000 at Bus:01 Dev:00 Fun:00
Controller#1 Port#1 Base 0xFC960000 at Bus:01 Dev:00 Fun:01
- Initializing ...Done.
```

The PXE Configuration menu appears after the boot BIOS initializes to begin your PXE configuration.

Setting Up a PXE Bootable Network

After the PXE boot BIOS initializes, you can use the PXESelect utility to set up a PXE bootable network by configuring your controllers.

To configure controllers for PXE boot:

1. At the Controller Selection Menu, select the controller you want to configure and press **<Enter>**.

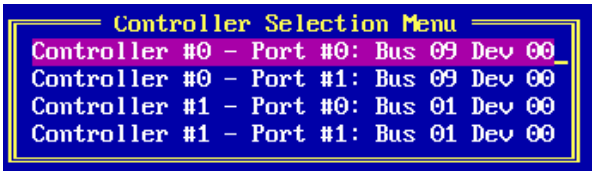

Figure 2-2 Controller Selection Menu

Note: The Controller Selection Menu only appears if there are two or more adapters connected.

Note: If your system supports multichannel, a MultiChannel menu appears automatically after you select the controller to allow you to enable multichannel functionality.

2. The Port Selection Menu appears. Select the port you want to configure and press **<Enter>**.

Figure 2-3 Port Selection Menu

The Port Configuration screen appears.

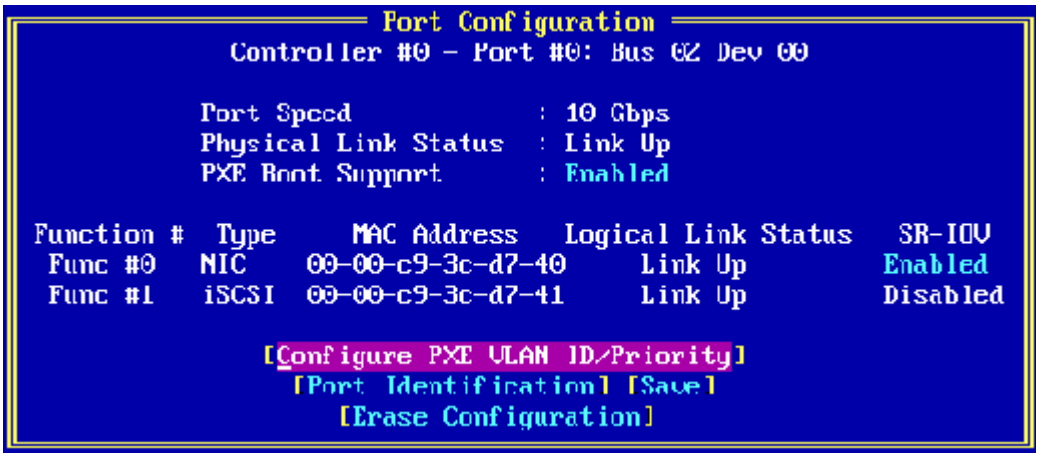

Figure 2-4 Port Configuration Screen

For some systems, there is a multichannel support option available as well as SR-IOV. When enabled, you can access up to eight virtual network interfaces.

To change the multichannel support option:

a. Use the **<Tab>** key to select the current setting and press **<Enter>**.

b. From the drop-down menu, select **Enabled** or **Disabled** and press **<Enter>**.

c. Select **Save** and press **<Enter>**. After making any changes to multichannel support, you are prompted to reboot the system immediately. For more information on multichannel, see the multichannel support documentation. For more information on SR-IOV configuration, see the *Emulex SR-IOV Setup README*.

3. To change PXE boot support:

a. Use the **<Tab>** key to select the current setting and press **<Enter>**.

b. From the drop-down menu, select **Enabled** or **Disabled** and press **<Enter>**.

c. Select **Save** and press **<Enter>**.

4. If your system BIOS supports SR-IOV, you can enable it. SR-IOV support can only be enabled for virtual channels.
   a. Use the **<Tab>** key to select the current setting and press **<Enter>**.
   b. From the drop-down menu, select **Enabled** or **Disabled** and press **<Enter>**.
   c. Select **Save** and press **<Enter>**.
5. To set a PXE VLAN ID, select **Configure PXE VLAN ID/Priority** and press **<Enter>**. The Configure PXE VLAN ID/Priority menu is displayed.

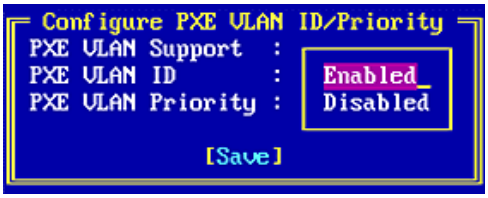

Figure 2-5 Configure PXE VLAN ID/Priority Menu

   a. Use the **<Tab>** key to select the current setting and press **<Enter>**.
   b. Select **Enabled** from the PXE VLAN Support drop-down menu and press **<Enter>**. Set a PXE VLAN ID number from 0-4094.
   c. Set the PXE VLAN Priority level from 0-7.
   d. Select **Save** and press **<Enter>**.
6. Reboot the system for the configuration to take effect.

Physically Identifying the Port

To physically determine which port you are configuring by blinking the link and activity LEDs of that port:

1. On the Port Configuration screen (Figure 2-4), select **Port Identification** and press **<Enter>**. The Port Identification screen appears.

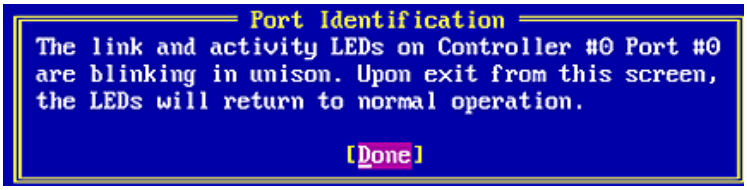

Figure 2-6 Port Identification Screen

2. The LEDs on your controller begin blinking. The selected port's LED status indicators blink on your controller until you select **Done** on this screen and press **<Enter>**.

Note: Not all controllers have LEDs that are visible externally. If you are using an add-in card in a blade server environment, the port identification or beaconing capability does not work.

Erasing Ports and Controller Configuration

To erase the ports and controller configuration:

1. On the Controller Configuration menu, select **Erase Configuration** and press **<Enter>**. A warning appears asking if you want to erase both ports of the controller. Press **<Y>** to delete the configuration. You will receive another warning asking to erase the controller configuration. Press **<Y>** to delete the configuration.
2. To exit the PXESelect utility, follow the instructions on the bottom of the individual menu screens until you are prompted to exit. Press **<Y>** to exit. The system automatically reboots and during system startup, PXE contacts the DHCP server for an IP address to boot from the network.

   Note: Depending on the memory allocation method supported, the PXESelect utility automatically reboots when changes are made to the system.

3. After you have successfully configured PXE boot, and depending on your individual system configuration, you will see a workspace or an installation image where you can install an operating system.

Multichannel Support

Note: Multichannel support is only available on Emulex OneConnect OCe11100-series UCNAs.

Multichannel, also known as universal multichannel (UMC), provides the ability to configure multiple PCI functions or I/O channels for each OneConnect port. Setting up multichannel may or may not depend on cooperation with adjacent switches. For additional information on multichannel support, see appendix E., "Multichannel for OneConnect OCe11100-series UCNAs," on page 189.

If multichannel functionality is supported on your system, PXESelect enables you to perform the following tasks:

- Enable or disable multichannel functionality
- Enable or disable each logical link
- Configure the bandwidth and Logical Port VLAN ID (LPVID) for each channel

Note: Your system may not support all multichannel options.

To enable and configure multichannel support:

1. After the BIOS initializes and you have selected your controller, the Controller Configuration menu appears. Select **MultiChannel Support** from the drop-down menu and press **<Enter>**. The Controller Configuration MultiChannel Support dialog box appears.
2. Select **Enabled** to activate multichannel support and press **<Enter>**.

3. Select **Save** and press **<Enter>**.

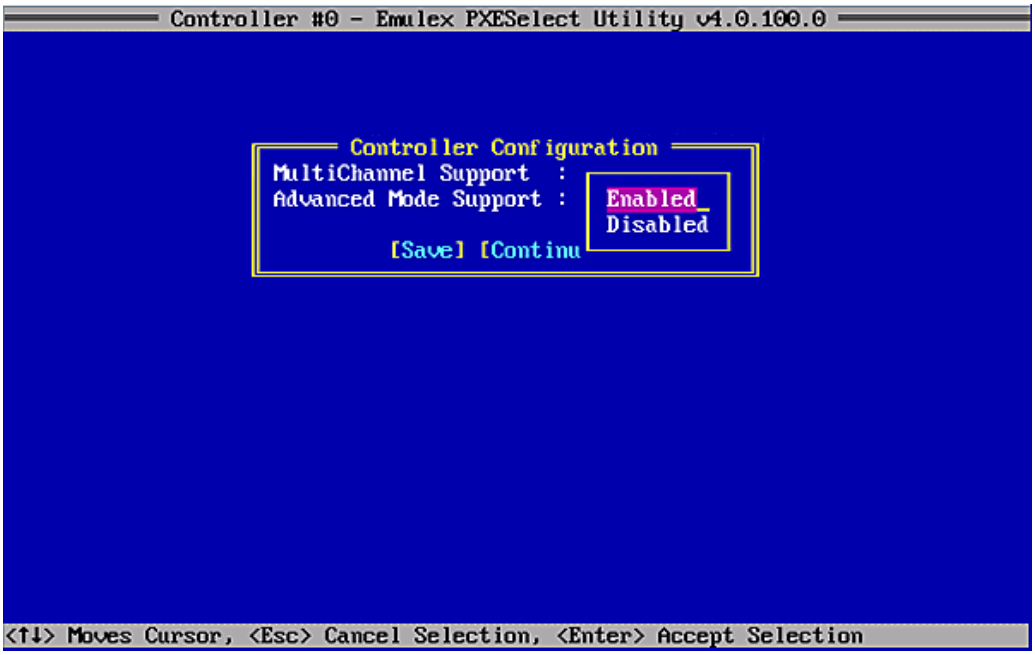

Figure 2-7 Controller Configuration MultiChannel Support Dialog Box

4. A warning message appears indicating that your system requires an immediate reboot upon enabling multichannel support. Press **<Y>** and then press **<Enter>** to reboot your system.
5. Once your system reboots, navigate to the Port Selection screen, select the port you want to configure and press **<Enter>**. The MultiChannel Configuration screen appears.

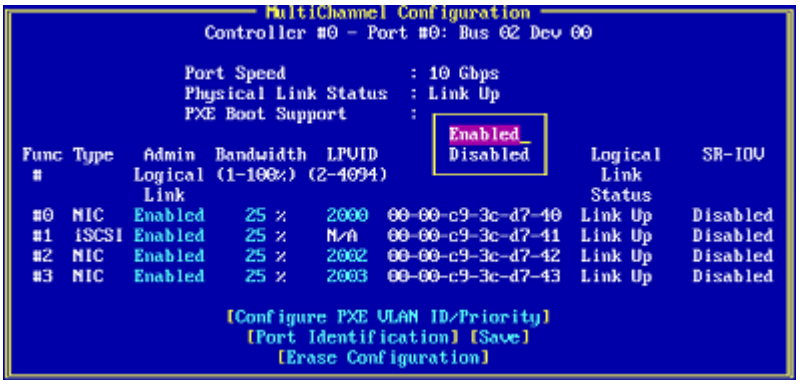

Figure 2-8 MultiChannel Configuration Screen

6. From the MultiChannel Configuration screen, you can enable or disable a logical link and configure the bandwidth percentage or LPVID per function.

   To enable or disable a logical link:

   a. Use the **<Tab>** key to select the current setting and press **<Enter>**.
   b. From the drop-down menu, select **Enabled** or **Disabled** and press **<Enter>**.
   c. Select **Save** and press **<Enter>**.

If you are configuring bandwidth, it must total 100% across all the functions on the selected port.

If you are configuring LPVID, set an LPVID number from 2-4094. For more information on using LPVID, see "Configuring LPVID" on page 28.

Note: SR-IOV support can only be enabled if multichannel support is disabled.

Note: If your system does not support some of the multichannel options, those unavailable options show as N/A in the MultiChannel Configuration menu.

Configuring LPVID

The LPVID is used to enforce a VLAN ID on all traffic originating from an IP address, channel, or PCI function. If the operating system for that PCI function has set up a VLAN ID, then the OS-configured VLAN ID takes precedence over the LPVID. If the operating system has not set up any VLAN IDs, then LPVID is used for tagging.

Note: In pre-OS environments, LPVIDs also need to be configured on the switch port.

Each LPVID must be unique and is relevant for NIC traffic only. The LPVID is not supported for storage functions. For iSCSI storage functions, you must configure a VLAN ID through iSCSISelect or through the host. For additional information, see the *Emulex OneConnect iSCSISelect User's Guide*.

Note: Emulex recommends that you do not perform VLAN ID setup and configuration on the virtual channels through the operating system when LPVID is enabled. When LPVID is enabled, the VLAN teaming options of HP and Emulex drivers cannot be used.

During PXE boot when the UNDI Driver (BIOS) is functional, the PXE VLAN is used. However, once the NIC driver is operational the LPVID is used.

For example:

```
PXE Install OS
PXE Server configured with VLAN 5
PXE VLAN=5
LPVID for function 0=5
```

Personality Option

The "personality" reflects the protocol, or protocols, of the adapter. This option specifies a list of available protocols that can be configured on an adapter. Depending on the personality for which the adapter is licensed, one of the following selections appears:

- NIC (iSCSI and FCoE are not allowed)
- NIC and iSCSI (FCoE is not allowed)
- NIC, iSCSI, and FCoE.

With this option, you can choose the personality that the adapter will run (if permitted on your system) by selecting it from the Controller Configuration drop-down menu. The menu only displays the available personalities, including both free and licensed personalities.

The NIC personality implies that all the enabled functions provide NIC/TOE functionality. iSCSI and FCoE personalities are enabled on one function per OneConnect port and include NIC functionality on the other enabled functions.

To select the personality of the adapter:

1. From the Controller Configuration menu, select **Personality** and press **<Enter>**. The Controller Configuration Screen-Personality dialog box appears.

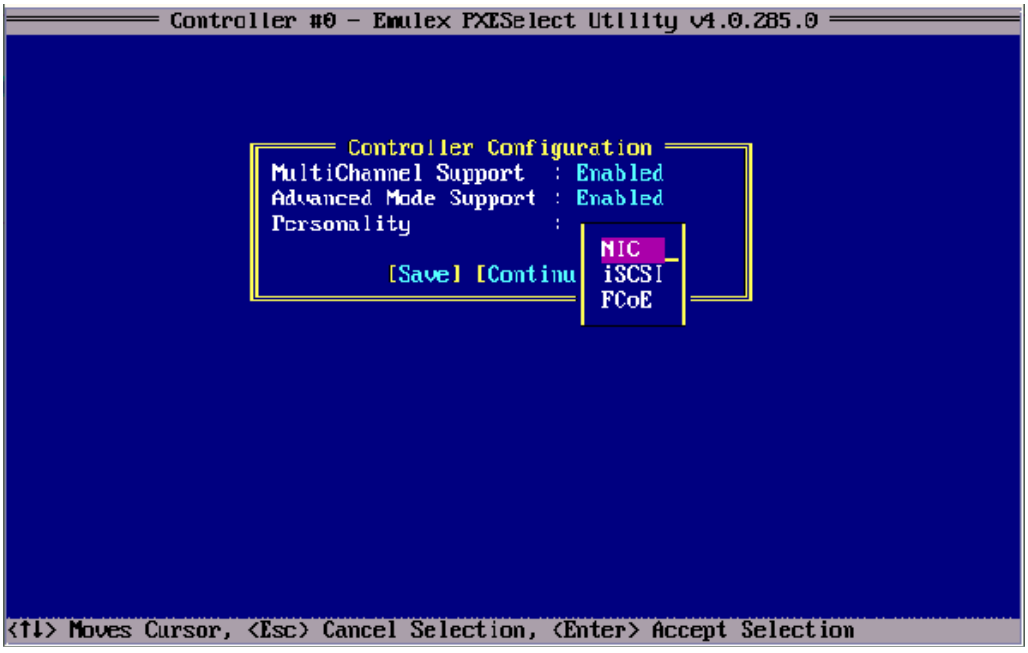

Figure 2-9 Personality Screen

2. From the drop-down menu, select **NIC, iSCSI**, or **FCoE** and press **<Enter>**.
3. Select **Save** and press **<Enter>**.

Advanced Mode Support

Advanced Mode is a driver compatibility option. With Advanced Mode enabled, you can run "advanced" drivers that have advanced options, including 4-port support and increased offload and virtualization capabilities. With Advanced mode disabled, you can run older drivers with later firmware versions.

Note: Advanced Mode support is available with OCe11100-series 2-port (the default setting is disabled) and 4-port controllers (the default setting is enabled). The Advanced Mode capability is not supported on OCe10100-series controllers (the default setting is disabled). Compatibility with legacy drivers requires that Advanced Mode support be disabled.

Note: On some 4–port-series LAN on motherboard (LOM) platforms, the Advanced Mode capability is not provided in the PXESelect utility. The Advanced Mode capability on these platforms is implicitly enabled by default and Advanced Mode-aware drivers must be implemented to fully utilize the advanced features of this functionality. Legacy Mode drivers will fail in creating the network interfaces on these platforms.

Table 2-1 Advanced Mode Capabilities (by Operating System)

Operating System	Advanced Mode Enabled	Advanced Mode Disabled (Legacy Mode)
Windows	16 RSS queues **Note:** Only supported on Windows Server 2008 R2 and 2012. Remains four queues for earlier Windows versions.	4 RSS Queues
	VMQ lookahead split **Note:** VMQs are only supported on Windows 2008 R2 and later versions.	Lookahead split is silently ignored. There may be a small performance penalty for VMQs.
	4-port	2-port
Linux and Citrix	4-port	2-port
	16 RSS Queues	4 RSS Queues
	VFs/PFs can be increased up to 30	
ESX	4-port	2-port
	For both 1500 and 9000 MTU: 16 NQs/PFs in non-VFA 4 NQs/PFs in VFA	1500 MTU – 8 NQ/PF in non-VFA and 4 NQ/PF in VFA. 9000 MTU – 4 NQ/PF in both VFA and non-VFA

For OCe11100-series UCNAs, the overall chip-wide maximum number of VFs is 60 (or 30 per port):

- Legacy Mode TOTAL VF Count = 30 (or 15 per port on 2-port adapters)
- Advanced Mode TOTAL VF Count = 60 (or 30 per port on 2-port adapters)

To enable Advanced Mode Support through PXESelect:

1. After the BIOS initializes and you have selected your controller, the Controller Configuration screen appears. Select **Advanced Mode Support** from the drop-down menu. The Controller Configuration Advanced Mode Support dialog box appears.

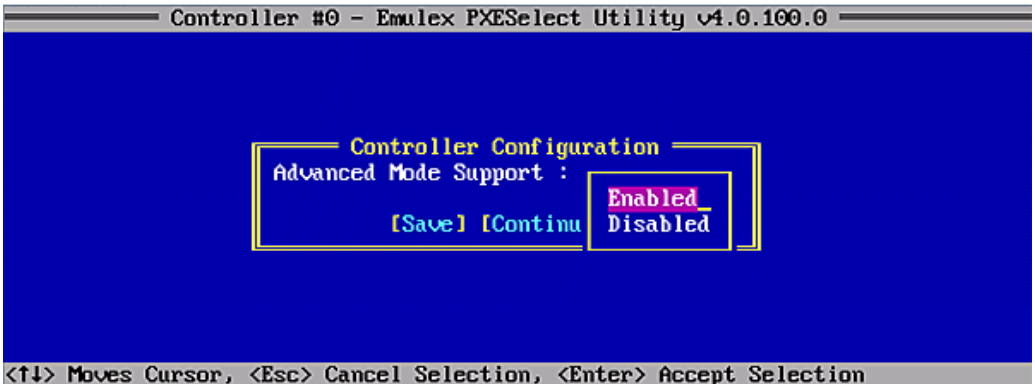

Figure 2-10 Controller Configuration Advanced Mode Support Dialog Box

2. From the drop-down menu, select **Enabled** or **Disabled** and press **<Enter>**.
3. Select **Save** and press **<Enter>**.
4. After enabling Advanced Mode Support, the Port Selection screen appears. Select the port you want to configure and press **<Enter>**. Continue to configure your controller.

PXE Boot Parameters Default Values

The default settings for the PXE Boot parameters are listed in the following table.

Table 2-2 PXE Boot Parameter Default Values

Parameter	Default Value	Valid Values
Advanced Mode	Enabled (OCe11100-series 4-port controllers) Disabled (OCe11100-series 2-port and OCe10100-series controllers)	Enabled Disabled
PXE Boot Support	The default for this parameter varies depending on the vendor configuration.	Enabled Disabled
SR-IOV	Disabled	Enabled Disabled
VLAN Support	Disabled	Enabled Disabled
VLAN ID	0	0-4094
VLAN Priority	0	0-7

Table 2-2 PXE Boot Parameter Default Values (Continued)

Parameter	Default Value	Valid Values
Multichannel Support	The default for this parameter varies depending on the vendor configuration.	Enabled Disabled
Function En/Dis	Disabled	Enabled Disabled
Bandwidth	0%	Must have a total of 100% across all ports.
LPVID	0	2–4094
Switch Option (IBM Virtual Fabric-capable configuration, if available)	IBM Virtual Fabric Mode	IBM Virtual Fabric Mode Switch Independent Mode
Switch Option (Cisco VNTag-capable configuration)	VNTag	Normal VNTag

3. Configuring Boot from SAN for the FCoE Protocol

When booting from SAN, the storage device is typically identified by its WWPN and a LUN. By extending the server system BIOS, boot from SAN capability is provided by the boot BIOS contained on an Emulex adapter in the server. When properly configured, the adapter then permanently directs the server to boot from a logical unit (disk) on the SAN as if it were a local disk.

Note: Not all procedures are required. Emulex adapters usually ship from the factory with the latest version of boot code installed and enabled, so you do not need to install or enable boot code in those cases. However, if boot code is not installed, you must install it, and, if it is not enabled, you must enable it. You may want to update the boot code if a more current version is available on the Emulex website at http://www.emulex.com.

This section describes how to set up a system to boot from SAN. This specific procedure to follow is determined by the system architecture and the operating system.

Windows Server 2008 and Windows Server 2012

Configuring Boot from SAN on Windows (x86 and x64)

To configure boot from SAN:

1. If necessary, install or update the boot code on the adapter (see chapter 6., “Installing, Updating, and Enabling Boot Code,” on page 72).
2. If necessary, enable the boot code on the adapter (see chapter 6., “Installing, Updating, and Enabling Boot Code,” on page 72).
3. Enable the adapter to boot from SAN (see “Enabling an Adapter to Boot from SAN” on page 54).
4. Configure boot devices (see “Configuring Boot Devices” on page 55).
5. If desired, configure the boot options on the adapter (see “Configuring Advanced Adapter Parameters” on page 62).
6. Install the operating system on an FC boot disk.

   For additional information, see “Installing Windows Server 2008 or 2012 on an FC Boot Disk (x86, x64, and UEFI)” on page 36.

Configuring Boot from SAN on Windows (UEFI)

To configure boot from SAN:

1. If necessary, install or update the boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
2. If necessary, enable the boot code on the adapter (see "Enabling an Adapter to Boot from SAN" on page 54).
3. Configure boot devices (see "Configuring Boot Devices" on page 55).
4. If desired, configure the boot options on the adapter (see "Configuring Advanced Adapter Parameters" on page 62).
5. Install the operating system on an FC boot disk:
   - For Windows Server 2008 or 2012, see "Installing Windows Server 2008 or 2012 on an FC Boot Disk (x86, x64, and UEFI)" on page 36.
   - For a new installation of Windows 2008 UEFI-Aware operating system on a UEFI-based x64 Server, see "Installing a New Windows Server 2008 or 2012 UEFI-Aware Operating System on a UEFI-based x64 Server" on page 34.

Installing a New Windows Server 2008 or 2012 UEFI-Aware Operating System on a UEFI-based x64 Server

This installation procedure assumes LUNs are created in the SAN storage device and zoned appropriately to the host adapter's WWN.

To install a new Windows Server UEFI-aware operating system:

1. From the server system UEFI setup, ensure that CD/DVD is the first device in the Boot Order list.
2. Enable the adapter BIOS setting to allow SAN boot in the Emulex UEFI configuration utility.
3. Configure the boot target and LUN in Emulex UEFI configuration utility to select the desired target.
4. Boot the host server with the Windows Server 2008 or 2012 DVD inserted. Follow the on-screen prompts to install the appropriate version of Windows Server 2008 or 2012.
5. The Windows installation exposes all available/visible LUNs as disks and partitions numbered 0 to N, where N is the highest number available. These numbers typically are the LUN numbers assigned by the array.
6. Select the disk on which you want to install the operating system.
7. Follow system prompts in the Windows installation.

   Note: The operating system image is installed with the GPT disk partition. See "GUID Partition Table" on page 35 for a brief description of GPT disk partitions.

8. After the installation is complete, a boot option variable called Windows Boot Manager is populated with a media device path pointing to the Windows boot

loader utility. Windows Boot Manager can be found in the Start Options menu of the Host Server UEFI.

9. The Windows Boot Manager option is inserted as the first boot option in the boot order list of the Host Server UEFI. The CD/DVD boot is the second device in the boot order list.
10. Upon reboot, the system boots from the LUN set up on the SAN.

Directing a UEFI-based Server to a Windows Server 2008 or 2012 Operating System Image (Installed as UEFI-Aware) Already Installed on the SAN

This installation procedure assumes a LUN exists in the SAN storage device, is zoned appropriately to the host adapter's WWN, and a UEFI-aware operating system resides on the target LUN.

To direct a UEFI-based server to a Windows Server operating system image:

1. Enable network boot in the Emulex UEFI configuration utility.
2. Configure the boot target and LUN in the Emulex UEFI configuration utility to point to your desired target.
3. Select **Boot Manager** from the System UEFI configuration manager.
4. Select **Add Boot Option**.
5. Identify the desired target in the list, and continue down the explorer path until you locate the bootmgfw.efi file. This file is the boot loader utility for your Windows 2008 or 2012 UEFI-aware operating system installation.
6. Input a boot device description (for example, Win2K8_UEFI_SAN) and optional data (if desired) for this device and select **Commit Changes**.
7. From the Windows Boot Manager, select **Change Boot Order**.
8. Move your previous input description name (Win2K8_UEFI_SAN) to the desired position in the boot order.
9. Select **Commit Changes**. The Start Options list now reflects the boot order changes.

   Upon reboot, the server is able to boot from this target LUN on the SAN.

GUID Partition Table

The Globally Unique Identifier (GUID) Partition Table (GPT) was introduced as part of the Extensible Firmware Interface (EFI) initiative. GPT provides a more flexible mechanism for partitioning disks than the older Master Boot Record (MBR) partitioning scheme that has been common to PCs. MBR supports four primary partitions per hard drive and a maximum partition size of 2 TB. If the disk is larger than 2 TB (the maximum partition size in a legacy MBR), the size of this partition is marked as 2 TB and the rest of the disk is ignored.

The GPT disk itself can support a volume up to 2^64 blocks in length (for 512-byte blocks, this is 9.44 ZB. A zettabyte is 1 billion terabytes. The GPT disk can also theoretically support unlimited partitions.

Note: By default, Microsoft Windows Server 2008 and 2012 installs with a GPT-formatted disk on an UEFI-Aware server.

For more information on the GUID partition table, see the Microsoft website and search for the terms: Windows and GPT FAQ.

Installing Windows Server 2008 or 2012 on an FC Boot Disk (x86, x64, and UEFI)

This procedure installs Windows Server 2008 or 2012 onto an unformatted FC disk drive and configures the system to boot from the SAN disk drive.

Note: The computer's system BIOS may require that another controller take precedence over the Emulex adapter during boot. If this occurs, you must disconnect or disable the other adapter. This allows you to configure and build your operating system on the drive connected to the Emulex adapter.

To install Windows Server on an FC boot disk:

1. From http://www.emulex.com, download the distribution executable file for the latest version of the Emulex driver to your local drive. The file you download is an executable (.exe) file.
2. In Windows Explorer, double-click the distribution executable file. Driver version information is displayed.
3. Click **Next** to access the Location window. The default installation location is displayed. If desired, browse to a different location.
4. Click **Install** to continue the installation. A progress window is displayed. As each task is completed, the corresponding check box is automatically selected. After all tasks are completed, a confirmation window is displayed.
5. Clear the **Run AutoPilot Installer** check box and click **Finish** to close the distribution executable file.
6. In Windows Explorer, navigate to the folder you specified in step 3.
7. In the \AutoPilot Installer\Drivers*drivername* folder, open the folder that corresponds to your computer type, such as x86. *drivername* is the type of driver you downloaded (for example, Storport Miniport).
8. Copy all the files in this folder onto a formatted floppy disk or a USB device.
9. Boot the target system with the Windows Server 2008 or 2012 setup media. The Install Windows splash screen is displayed.
10. Verify and if necessary change the language, time and date and keyboard values. Click **Next**. Another splash screen is displayed.
11. Click **Install Now**. The Where do you want to install Windows? screen is displayed.
12. Click **Load Driver**. Browse to the floppy disk or USB device specified in step 8 where the driver is located to load the Storport Miniport driver for the appropriate operating system. Once selected, the correct driver location and driver are displayed under the Select driver to be installed screen.

13. Select **Next**. After the driver is loaded, the Where do you want to install Windows? screen is displayed.
14. Select the same drive you configured as the boot device (for x86 and x64 systems, see "Configuring Boot Devices" on page 55. For UEFI systems, see "Adding Boot Devices" on page 140).

Linux, Citrix, and VMware

Configuring Boot from SAN on Linux, Citrix, or VMware (x86 and x64)

To configure boot from SAN:

1. If necessary, install or update the boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
2. If necessary, enable the boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
3. Enable the adapter to boot from SAN (see "Enabling an Adapter to Boot from SAN" on page 54).
4. If necessary, enable spinup delay (see "Enabling or Disabling the Spinup Delay" on page 65).
5. Configure boot devices (see "Configuring Boot Devices" on page 55).
6. If desired, configure the boot options on the adapter (see "Configuring Advanced Adapter Parameters" on page 62).
7. Use the driver on the operating system distribution disk to boot the system. If necessary, you can update the driver to the latest version.

Configuring Boot from SAN on Linux (UEFI)

To configure boot from SAN:

1. If necessary, install or update the latest boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
2. If necessary, enable the boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
3. Configure boot devices (see "Enabling an Adapter to Boot from SAN" on page 54).
4. If desired, configure the boot options on the adapter (see "Configuring Advanced Adapter Parameters" on page 62).
5. Use the driver on the operating system distribution disk to boot the system. If necessary, you can update the driver to the latest version.

Solaris

Configuring Boot from SAN on Solaris SFS (x86 and x64)

To configure boot from SAN:

1. If necessary, install or update the boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
2. If necessary, enable the boot code on the adapter (see chapter 6., "Installing, Updating, and Enabling Boot Code," on page 72).
3. Enable the adapter to boot from SAN (see "Enabling an Adapter to Boot from SAN" on page 54).
4. If necessary, enable spinup delay (see "Enabling or Disabling the Spinup Delay" on page 65).
5. Configure boot devices (see "Configuring Boot Devices" on page 55).
6. If desired, configure the boot options on the adapter (see "Configuring Advanced Adapter Parameters" on page 62).
7. Boot the Solaris installation CD and follow the prompts.

   Note: If you need help determining the LUNs to select for boot from SAN, see "Determining LUNs to Select for Boot from SAN" on page 38.

Determining LUNs to Select for Boot from SAN

To determine which LUNs to select:

1. Open a terminal window and leave it open.
2. In the terminal window, select the LUN you are going to use as the SAN boot disk (not the local drive) using the luxadm probe command. This shows all the available LUNs. Record this LUN information, which is used throughout this procedure. LUN 0 is used in the example:

   ```
   luxadm probe

   Found Fibre Channel device(s):
      Node WWN:50060e8003823800 Device Type:Disk device
      Logical Path:/dev/rdsk/c5t226000C0FF9833AFd6s2
      Node WWN:50060e8003823800 Device Type:Disk device
      Logical Path:/dev/rdsk/c5t226000C0FF9833AFd6s2
   Node WWN:50060e8003823800 Device Type:Disk device
   ```

3. Copy the /dev/rdsk/*nnn* part of the path statement for a drive.
4. In the terminal window, use the luxadm display command to show the WWPN or the LUN for which you selected the path in the prior step:

   ```
   luxadm display </dev/rdsk/nnn>
   ```

5. Record this LUN or WWPN information for use in the procedure.

Configuring Boot from SAN on Solaris SFS (SPARC)

To configure boot from SAN:

1. If necessary, install or update the boot code on the adapter (see chapter 6., “Installing, Updating, and Enabling Boot Code,” on page 72).
2. If necessary, enable the boot code on the adapter (see chapter 6., “Installing, Updating, and Enabling Boot Code,” on page 72).
3. Type the following at the OBP prompt:

   ```
   show-devs
   ```

   The ID information for each found adapter is displayed, such as:

   ```
   /pci@22,600000/pci@0/pci@9/pci@0/pci@9/emlx@0
   ```

4. Enable boot from SAN on each Emulex adapter in the system by typing the following set of commands, replacing adapter_id with the ID information (such as shown above), for each Emulex adapter in turn. There is a space between the first quotation mark and the first character of the adapter ID.

   ```
   " adapter_id" select-dev [for example,
   “/pci@22,600000/pci@0/pci@9/pci@0/pci@9/emlx@0” select-dev]
   set-sfs-boot
   unselect-dev
   ```

5. After all Emulex adapters have been enabled to boot from SAN, reset the system with the following command:

   ```
   reset-all
   ```

6. After the system resets, boot the Solaris installation CD and follow the prompts.
7. After the installation completes successfully, you will be prompted to reboot or exit the system. Press **<!>** and then press the **<Enter>** key to go to the Unix prompt.
8. Once the Unix prompt appears, append the following line to the system file at /a/etc/system:

   ```
   set pcie:pcie_max_mps=0
   ```

9. Save and reboot server.

Installing Solaris from a Network Image

The system must have a DVD drive and must be part of the site's network and naming service. If you use a naming service, the system must already be in a service, such as NIS, NIS+, DNS, or LDAP. If you do not use a naming service, you must distribute information about this system by following your site's policies.

Note: This procedure assumes that the system is running the Volume Manager. If you are not using the Volume Manager to manage media, refer to the Sun Microsystems System Administration Guide: Devices and File Systems.

To install from a network image:

1. Log on as a superuser or equivalent.
2. Insert the Solaris DVD in the system's drive.
3. Create a directory to contain the DVD image.

   ```
   # mkdir -p install_dir_path
   ```

   Install_dir_path specifies the directory where the DVD image is to be copied.
4. Change to the Tools directory on the mounted disc.

   ```
   # cd /cdrom/cdrom0/Solaris_10/Tools
   ```

   Note: For Solaris 10 only:

   a. Remove the SUNWemlxu and SUNWemlxs from /install_dir_path/Solaris/Tools/Boot.
   b. Unzip the elxfc driver to a /temp directory:

      ```
      pkgadd -R /install_dir_path/Solaris/Tools/Boot -d /temp
      ```

   c. Modify the elxfc.conf file to use persistent binding. For more information, see the *Emulex Driver for Solaris User Manual*.
5. Copy the DVD image in the drive to the install server's hard disk.

   ```
   # ./setup_install_server install_dir_path
   ```

   install_dir_path specifies the directory where the DVD image is to be copied.

   Note: The `setup_install_server` command indicates whether you have enough disk space available for the Solaris Software disc images. To determine available disk space, use the `df -kl` command.
6. Decide whether you need to make the installation server available for mounting:

   If the installation server is on the same subnet as the system to be installed or you are using DHCP, you do not need to create a boot server. Proceed to step 7.

   If the install server is not on the same subnet as the system to be installed and you are not using DHCP, complete the following steps.

   a. Verify that the path to the install server's image is shared appropriately.

      ```
      # share | grep install_dir_path
      ```

      install_dir_path specifies the path to the installation image where the DVD image was copied:

- If the path to the install server's directory is displayed and anon=0 is displayed in the options, proceed to step 7.
- If the path to the install server's directory is not displayed or you do not have anon=0 in the options, continue and make the install server available to the boot server. Using the share command, add this entry to the /etc/dfs/dfstab file (all on one line):

```
share -F nfs -o ro,anon=0 -d "install server directory"
install_dir_path
```

b. Verify that the nfsd daemon is running, or start the nfsd daemon.

- If the install server is running the current Solaris release, or compatible version, type the following command:

```
# svcs -l svc:/network/nfs/server:default
```

  - If the nfsd daemon is online, continue to step c.
  - If the nfsd daemon is not online, start it. Type the following command:

```
# svcadm enable svc:/network/nfs/server
```

- If the install server is running the Solaris 9 operating system, or compatible version, type the following command:

```
# ps -ef | grep nfsd
```

  - If the nfsd daemon is running, continue to step c.
  - If the nfsd daemon is not running, start it.

```
# /etc/init.d/nfs.server start
```

c. Share the install server.

```
# shareall
```

7. Change directories to root (/).

```
# cd /
```

8. Eject the Solaris DVD.
9. (Optional) Patch the files that are located in the miniroot on the net install image that was created by setup_install_server. Patching a file might be necessary if a boot image has problems. For more information, see the *Sun Microsystems Solaris 10 10/08 Installation Guide*.

Installing Solaris by Migrating an Image from a Local SCSI Disk

To install Solaris by migrating an image from a local SCSI disk:

1. Type the following at the OBP prompt:

```
show-devs
```

   The ID information for each found adapter is displayed, such as:

```
/pci@5d,700000/emlx@1 select-dev
```

2. Select the Emulex adapter on which you want to enable boot from SAN by entering the path to the adapter, for example:

```
" /pci@5d,700000/emlx@1" select-dev
```

3. To view the current boot device ID, type:

```
show-devs
" /pci@5d,700000/emlx@1" select-dev /* to select emlx@1 (for
example) */
.boot-id
```

Make a note of the WWPN, DID, or AL_PA returned from the probe and write down the corresponding boot entry.

4. To enable boot from SAN, set the boot device ID to the SAN device from which you want to boot. For example:

```
" /pci@5d,700000/emlx@1" select-dev
wwpn|did|alpa lun target_id set-boot-id
unselect-dev
```

where:

- *wwpn*|*did*|*alpa* is the device WWPN, DID, or AL_PA of the storage device.
- *lun* is the LUN number in hexadecimal. To enter it in decimal, enter d# [*lun*].
- *target_id* is the target ID in hexadecimal. To enter it in decimal, enter d# [*target_id*].

Note: Emulex recommends using the WWPN in most cases. The DID and AL_PA may change between boots, causing the SAN boot to fail, unless the DID and AL_PA are specifically configured to not change between boots.

Example 1: alpa=e1, lun=100 (decimal) and target id=10 (decimal):

```
alpa e1 d# 100 d# 10 set-boot-id
```

Example 2: wwpn=50000034987AFE, lun=af (hexadecimal) and target id=10 (decimal):

```
wwpn 50000034987AFE af d# 10 set-boot-id
```

Example 3: did=6312200, lun=25 (hexadecimal) and target id=f (hexadecimal):

```
did 6312200 25 f set-boot-id
```

5. Boot to the original local disk to set up the FC disk that you just defined. Type:

```
boot local_disk
```

where *local_disk* is the complete path or the alias of the original boot disk.

6. Run the format utility:

```
format
```

7. Select the target disk to become the new boot disk (for example, c1t1d0).
8. Select the partition option and partition the disk as desired.
9. Select the label option and write a volume label to the target disk.

For help with the format utility, see the man page *man format*.

10. Install the boot on partition 0 of the target disk. (Type this command as one line.)

```
installboot /usr/platform/ `uname -i`/lib/fs/ufs/bootblk
/dev/rdsk/clt1d0s0
```

11. Create a filesystem for each partition that contains a mounted filesystem:

```
newfs -v /dev/rdsk/clt1d0s0 (becomes root)
newfs -v /dev/rdsk/clt1d0s6 (becomes usr)
newfs -v /dev/rdsk/clt1d0s7 (becomes export/home)
```

12. Create temporary mount points for the new partitions:

```
mkdir root2
mkdir usr2
mkdir export2
```

13. Mount, copy, then unmount the usr2 file system:

```
mount /dev/dsk/clt1d0s6 /usr2
c0t0d0s6 ufsdump 0f - /dev/rdsk/c0t0d0s6 | (cd /usr2; ufsrestore
rf -)
umount /usr2
```

14. Copy the export/home file system:

```
mount /dev/dsk/clt1d0s7 /export2
ufsdump 0f - /dev/rdsk/c0t0d0s7 | (cd /export2; ufsrestore rf -)
umount /export2
```

15. Perform copy:

```
mount /dev/dsk/clt1d0s0 /root2
ufsdump 0f - /dev/rdsk/c0t0d0s0 | (cd /root2; ufsrestore rf -)
```

16. Edit /root2/etc/vfstab, changing the controller number, target number and LUN number to point to the new FC boot disk. For example, if the FC boot disk is c1t1d0, replace all local disk entries of c0t0d0 with c1t1d0.

    Currently file shows:

```
/dev/dsk/c0t0d0s1 (swap)

/dev/dsk/c0t0d0s0 and /dev/rdsk/c0t0d0s0 (root)
/dev/dsk/c0t0d0s6 and /dev/rdsk/c0t0d0s6 (usr)
/dev/dsk/c0t0d0s7 and /dev/rdsk/c0t0d0s7 (export)
```

    Edit file to show:

```
/dev/dsk/c1t1d1s1 (swap)

/dev/dsk/clt1d0s0 and /dev/rdsk/c1t1d0s1 (root)
/dev/dsk/clt1d0s6 and /dev/rdsk/c1t1d0s6 (usr)
/dev/dsk/clt1d0s7 and /dev/rdsk/c1t1d0s7 (export)
```

17. Reboot the system:

```
sync
halt
reset-all
```

18. Boot to disk:

```
boot disk
```

The system should boot to the FC disk.

19. View the current dump device setting:

```
dumpadm
```

20. Change the dump device to the swap area of the FC drive:

```
dumpadm -d /dev/dsk/c1t1d0s1
```

where /dev/dsk/c1t1d0s1 is a sample path to the swap area of the FC drive.

Booting Solaris 10 from the Network on SPARC Machines

To boot from the network:

1. Set up the install server and the boot server (if required). See the topic for Network-Based Installations in the *Solaris 10 10/09 Installation Guide*.
2. Obtain the MAC address of the OCE port used for the net boot:
   a. Get the device path of the port from the show-devs command:

```
{0} ok show-devs
/pci@0/pci@0/pci@8/pci@0/pci@1/emlx@0,3
/pci@0/pci@0/pci@8/pci@0/pci@1/emlx@0,2
/pci@0/pci@0/pci@8/pci@0/pci@1/oce@0,1
/pci@0/pci@0/pci@8/pci@0/pci@1/oce@0
/pci@0/pci@0/pci@8/pci@0/pci@1/emlx@0,3/fp@0,0
```

   b. Select the OCE device to boot:

```
{0} ok " /pci@0/pci@0/pci@8/pci@0/pci@1/oce@0,1" select-dev
```

   c. Get the MAC address of the selected device from its properties:

```
{0} ok .properties
status                   okay
assigned-addresses       82020014 00000000 00100000 00000000 00004000
                         82020018 00000000 00120000 00000000 00020000
                         82020020 00000000 00140000 00000000 00020000
                         82020030 00000000 00180000 00000000 00080000
model                    OCe10102
fcode-version            4.0.0.0
reg                      00020000 00000000 00000000 00000000 00000000
                         02020014 00000000 00000000 00000000 00004000
                         03020018 00000000 00000000 00000000 00020000
                         03020020 00000000 00000000 00000000 00020000
                         02020030 00000000 00000000 00000000 00040000
compatible               pciex19a2,700.10df.e602.2
                         pciex19a2,700.10df.e602
                         pciex19a2,700.2
                         pciex19a2,700
                         pciexclass,020000
                         pciexclass,0200
max-frame-size           000005ee
address-bits             00000030
supported-network-types  ethernet,10000,null,full
```

```
copyright               Copyright (c) 2009-2011 Emulex. All rights
reserved.
name                    oce
device_type             network
manufacturer            Emulex
fcode-rom-offset        00016e00
interrupts              00000001
cache-line-size         00000010
class-code              00020000
subsystem-id            0000e602
subsystem-vendor-id     000010df
revision-id             00000002
device-id               00000700
vendor-id               000019a2
```

3. Add the MAC address from step 2 as an installation client to the Install/Boot server.
4. Power on the client machine and wait for the ok prompt.
5. Set the net device alias for the device selected in step 2.
   - If the net device alias is already set to the network device to be used for the net boot, skip this step.
   - If the net device alias is not set, set the net device alias to the network device that to be used for the net boot. Type:

     ```
     {0} ok devalias net <device_path>
     ```
6. Boot from the network.
   - If using the DHCP boot strategy, type:

     ```
     {0} ok boot net:dhcp
     ```
   - If using the RARP boot strategy, type:

     ```
     {0} ok boot net:rarp
     ```

4. Configuring x86/x64 Platforms for the iSCSI Protocol

iSCSI Overview

The Internet Small Computer System Interface (iSCSI) is an IP-based standard for linking data-storage devices over a network and transferring data by carrying SCSI commands over IP networks. An iSCSI network consists of one or more iSCSI storage units (targets) connected through a copper or optical networking cable to 10Gb Ethernet network switches and/or IP routers. One or more servers are connected to this network, which are responsible for transferring data to or from the storage units.

When an operating system receives a request, it generates the SCSI command and then sends an IP packet over an Ethernet connection. At the receiving end, the SCSI commands are separated from the request, and the SCSI commands and data are sent to the SCSI controller and then to the SCSI storage device. iSCSI also returns a response to the request using the same protocol.

Constructing a Basic iSCSI SAN

There are three main components that make up an iSCSI SAN:

- iSCSI Initiator(s) – The initiator allows a given machine access to the storage available in the iSCSI SAN. It requests all SCSI operations like read or write. An initiator is usually located on the host/server side, either as hardware (iSCSI adapter) or software (iSCSI software initiator). To transport block (SCSI) commands over the IP network, an iSCSI driver must be installed on the iSCSI host. An iSCSI driver is included with the OneConnect adapter. (For more information on iSCSI initiators, see chapter 8., “Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility,” on page 76.)
- iSCSI Target(s) – An iSCSI SAN has one or more iSCSI targets, which house and make available the storage used within the SAN. The iSCSI target is the storage device itself or an appliance that controls and serves volumes or virtual volumes. The target is the device that performs the SCSI command or bridges it to an attached storage device. iSCSI targets can be disks, RAID arrays, or even FC fabrics. (For additional information on iSCSI targets, see chapter 9., “Configuring and Managing iSCSI Targets with the iSCSISelect Utility,” on page 82.)
- Networking infrastructure – The networking infrastructure in an iSCSI SAN uses Ethernet transport. The configuration and complexity of the storage network depends on its intended function and the required capabilities.

Managing an iSCSI Session

To transmit information from an iSCSI initiator to an iSCSI target, the initiator must first establish a session with the target through an iSCSI login process. The login process:

- Starts a TCP/IP connection
- Verifies that the iSCSI initiator has access to the iSCSI target (authentication)
- Allows negotiation of various parameters

Logging into an iSCSI Session

An iSCSI session has two phases:

- Login Phase – iSCSI parameters are negotiated using login requests and responses.
- Full Featured Phase – Once security/authentication has occurred and operational parameters have been set, the initiator begins to perform SCSI I/Os.

Security

Because the iSCSI protocol operates in the Internet environment, security is critical. The iSCSI SAN uses the Challenge Handshake Authentication Protocol (CHAP) security method.

CHAP Authentication

CHAP is used to periodically verify the identity of the initiator by the target using a challenge/response mechanism. The challenge/response is established on the initial link and may repeated at any time afterward. For CHAP to work, the target must know the initiator's secret key, and the initiator must correctly respond to the challenge.

Although the authentication is only one-way, you can negotiate CHAP in both directions for mutual authentication, with the help of the same secret set.

Configuring for the iSCSI Protocol

This section provides instructions for configuring boot from SAN for iSCSI on various operating systems using the iSCSISelect utility. It also provides information on how to use the iSCSISelect utility to perform an MPIO boot configuration.

Setting Up Boot from SAN for iSCSI

In iSCSI target configuration, you have the option of setting dual network paths to a single boot LUN. You must follow these steps in this order to configure boot support successfully for each operating system.

1. Use the iSCSISelect utility to configure a boot target.

   Note: iSCSI must be enabled for the port before configuring a boot target.

2. Complete the normal operating system installation.

Windows Server

To set up boot from SAN for iSCSI on Windows Server:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Use the iSCSISelect utility to log into a target from one adapter and configure it for boot. (For more information, see chapter 8., "Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility," on page 76 and chapter 9., "Configuring and Managing iSCSI Targets with the iSCSISelect Utility," on page 82.)

   If the iSCSISelect utility is configured properly, a message during boot time indicates that the iSCSI disk was successfully connected.
3. Install a Windows Server operating system over the iSCSI LUN.

Linux and Citrix Servers

To set up boot from SAN for iSCSI on Linux or Citrix:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Use the iSCSISelect utility to log into a target from one adapter and configure it for boot. (For more information, see chapter 8., "Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility," on page 76 and chapter 9., "Configuring and Managing iSCSI Targets with the iSCSISelect Utility," on page 82.)

   If the iSCSISelect utility is configured properly, a message during boot time indicates that the iSCSI disk was successfully connected.
3. Install a Linux operating system over the iSCSI LUN. (For more information, refer to the *Emulex Driver for Linux User Manual*.)

ESX Server

To install and configure boot from SAN on ESX Server:

1. Log into the iSCSISelect utility pressing **<Ctrl+S>** when prompted.
2. Use the iSCSISelect utility to log into a target from one adapter and configure it for boot. (For more information, see chapter 8., "Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility," on page 76 and chapter 9., "Configuring and Managing iSCSI Targets with the iSCSISelect Utility," on page 82.)

   If the iSCSISelect utility is configured properly, a message during boot time indicates that the iSCSI disk was successfully connected.
3. Install an ESX Server operating system over the iSCSI LUN. (For more information, refer to the *Emulex Driver for VMware User Manual*.)

Booting from SAN for iSCSI MPIO

MPIO support allows the initiator to log in dual sessions to the same target. In this way I/O can be sent over either TCP/IP connection to the target. If one session fails another session can continue processing I/O without interruption to the application. In iSCSI target configuration, you have the option of setting dual network paths to a single boot LUN.

Note: Although MPIO boot support allows the initiator to log into multiple sessions, the iSCSI BIOS currently limits the number of sessions to two iSCSI sessions for a single boot LUN.

You must follow these steps in this order to configure MPIO boot support for each operating system.

1. Use the iSCSISelect utility to configure the first path to a boot target.
2. Complete normal operating system installation.
3. Install third-party MPIO software for your operating system.
4. Configure the second path to a single boot LUN through the iSCSISelect utility.

Windows Server

To install and configure MPIO on Windows Server:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Use the iSCSISelect utility to log into a target from one adapter and configure it for boot by following the steps in "Setting Up a Basic iSCSI Boot Configuration" on page 73.

   If the iSCSISelect utility is configured properly, a message during boot time indicates that the iSCSI disk was successfully connected.

   Note: Only one instance of the boot LUN must be visible to the server during the installation. The installation might fail if multiple instances of the boot LUN are available to the server. Emulex recommends that the Spanning Tree Protocol be disabled on any ports that are connected to Windows Server 2008 or 2012 hosts booting via iSCSI. The Spanning Tree Protocol is used to calculate the best path between switches where there are multiple switches and multiple paths through the network.

3. Install a Windows Server operating system over the iSCSI LUN.
4. Once Windows Server is installed, install the MPIO software (such as Microsoft iSCSI Initiator), and reboot the system.
5. After rebooting, ensure that the boot LUN is detected by the MPIO driver. This can be done by either of the following two methods:
   - For Windows Server 2008, Windows Server 2008 R2, and Windows Server 2012:
     - Look at the driver name for the disk device from Device Manager,

     -or-

- Use the MPIO GUI to check for device ID `MS FT2005iSCSIBusType_0x9` under the MPIO Devices tab. The Disk Manager does not show duplicate disks.

6. Reboot your system and log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
7. You can now add an additional boot path with the iSCSISelect utility.

   To add an additional boot path to the same iSCSI LUN:

   a. Follow the steps for the "Windows Server" on page 48 to set up the second path.
   b. At the Add/Ping iSCSI Target menu, make sure you set a valid ISID Qualifier before adding your target. For more information on the ISID Qualifier, see "Setting an ISID Value" on page 88.
   c. After you have logged into the target, from the iSCSI Target Configuration menu, set the Boot Target option for the second target to **Yes**.
   d. Press **<F7>** to display the LUNs behind the target.
   e. Select the same LUN you chose for your initial boot LUN, then press **<F3>** to set it to bootable.
8. After Windows Server boots up, the MPIO installs drivers on the second path and prompts for reboot. Reboot the server.

Linux and Citrix Servers

To install and configure MPIO on Linux or Citrix:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Use the iSCSISelect utility to log into a target from one adapter and configure it for boot by following the steps for the "Linux and Citrix Servers" on page 48.

   If the iSCSISelect utility is configured properly, a message during boot time indicates that the iSCSI disk was successfully connected.
3. Install a Linux operating system over the iSCSI LUN. (For more information refer to the *Emulex Driver for Linux User Manual*.)
4. Once Linux is installed, install the MPIO software and reboot the system.
5. After rebooting, ensure that the boot LUN is detected by the MPIO driver. Perform either of the following steps:
   - To see if the multipath is running, type:

     ```
     # /sbin/multipath
     ```

     -or-

   - To see if the multipath daemon is running, type:

     ```
     # ps -aelf | grep multipathd
     ```
6. If multipath is running, you can view the current multipath topology. To view the current multipath topology, type:

   ```
   # /sbin/multipath -l
   ```
7. Reboot your system and log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.

8. Use the iSCSISelect utility to add an additional boot path to the same iSCSI LUN. To do this, follow these steps:
   a. Follow the steps for the "Linux and Citrix Servers" on page 48 to set up the second path.
   b. When you get to the Add/Ping iSCSI Target menu, make sure you set a valid ISID Qualifier before adding your target. For more information on the ISID Qualifier, see "Setting an ISID Value" on page 88.
   c. After you have logged into the target, from the iSCSI Target Configuration menu, set the Boot Target option for the second target to **Yes**.
   d. Press **<F7>** to display the LUNs behind the target.
   e. Select the same LUN you chose for your initial boot LUN, then press **<F3>** to set it to bootable.
   f. Follow the instructions on the bottom of the menu screens until you are prompted to exit.
   g. Save your changes before you exit.
   h. Press **<Y>** to exit the iSCSISelect utility.
9. After Linux boots up, the MPIO installs drivers on the second path and prompts you to reboot. Reboot the server.

ESX 4.0, 4.1, or 5.0 Server

To install and configure MPIO on ESX Server:

1. Log into the iSCSISelect utility pressing **<Ctrl+S>** when prompted.
2. Use the iSCSISelect utility to log into a target from one adapter and configure it for boot by following the steps for the "ESX Server" on page 48.

   If the iSCSISelect utility is configured properly, a message during boot time indicates that the iSCSI disk was successfully connected.
3. Install an ESX server operating system over the iSCSI LUN. For more information refer to the *Emulex Driver for VMware User Manual*.
4. Once the ESX server is installed, install the MPIO software and reboot the system. The ESX Server is MPIO by default.
5. Use the iSCSISelect utility to add an additional boot path to the same iSCSI LUN. To do this, follow these steps:
   a. Follow the steps for the "ESX Server" on page 48 to set up your second path.
   b. When you access the Add/Ping iSCSI Target menu, set a valid ISID Qualifier before adding your target. For more information, see "Setting an ISID Value" on page 88.
   c. After you have logged into the target, from the iSCSI Target Configuration menu, set the Boot Target option for the second target to **Yes**.
   d. Press **<F7>** to display the LUNs behind the target.
   e. Select the same LUN you chose for your initial boot LUN, then press **<F3>** to set it to bootable.

f. Follow the instructions on the bottom of the menu screens until you are prompted to exit.
g. Save your changes before you exit.
h. Press **<Y>** to exit the iSCSISelect utility.

6. After the ESX Server boots up, the MPIO installs drivers on the second path and prompts for a reboot. Reboot the server.

5. Using the FCoE Boot BIOS Utility for x86 and x64 Architectures

Before using the FCoE BIOS utility, ensure that the boot code is loaded and enabled on the adapter as described in "Installing, Updating, and Enabling Boot Code" on page 72.

Note: This section reflects the most recent release of the FCoE BIOS utility. Some selections may not be available if you are using an older version of the utility.

Navigating the FCoE BIOS Utility

The FCoE BIOS utility has menus and configuration screens. Use the following methods to navigate them:

- Press the up/down arrows on your keyboard to move through and select menu options or configuration fields. When multiple adapters are listed, use the up/down arrows to scroll to the additional adapters.
- Press **<PageUp>** to scroll to the previous page.
- Press **<PageDn>** to scroll to the next page.
- Press **<Enter>** to select a menu option, to select a changed value, to select a row in a configuration screen or to change a configuration default.
- Press **<Esc>** to go back to the previous menu.

Starting the FCoE BIOS Utility

Note: Links must be established before entering the FCoE BIOS utility; otherwise, you will receive an error message.

To start the FCoE BIOS utility:

1. Turn on the computer and press and hold down **<Alt>** or **<Ctrl>** and press **<E>** immediately (within five seconds) when the Emulex bootup message to start the FCoE BIOS utility is displayed. An adapter listing is displayed (Figure 5-1).

   Note: If the bootup message does not appear, you must enable x86 BootBIOS. (For more information, see "Installing, Updating, and Enabling Boot Code" on page 72.)

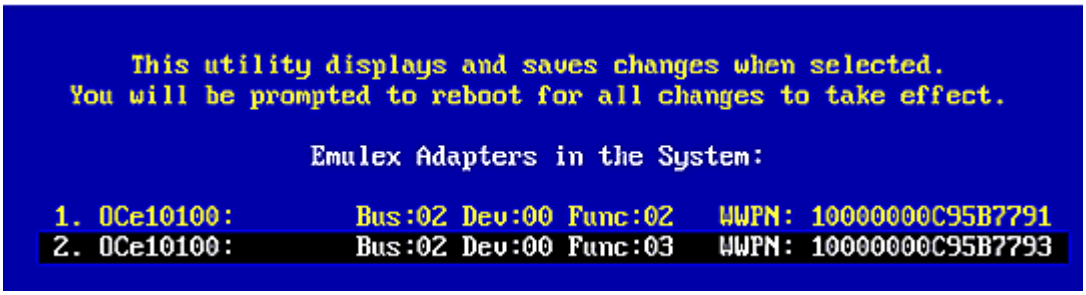

Figure 5-1 Emulex Adapter Listing

2. Select the adapter to configure and press **<Enter>**. The main configuration menu is displayed (Figure 5-2).

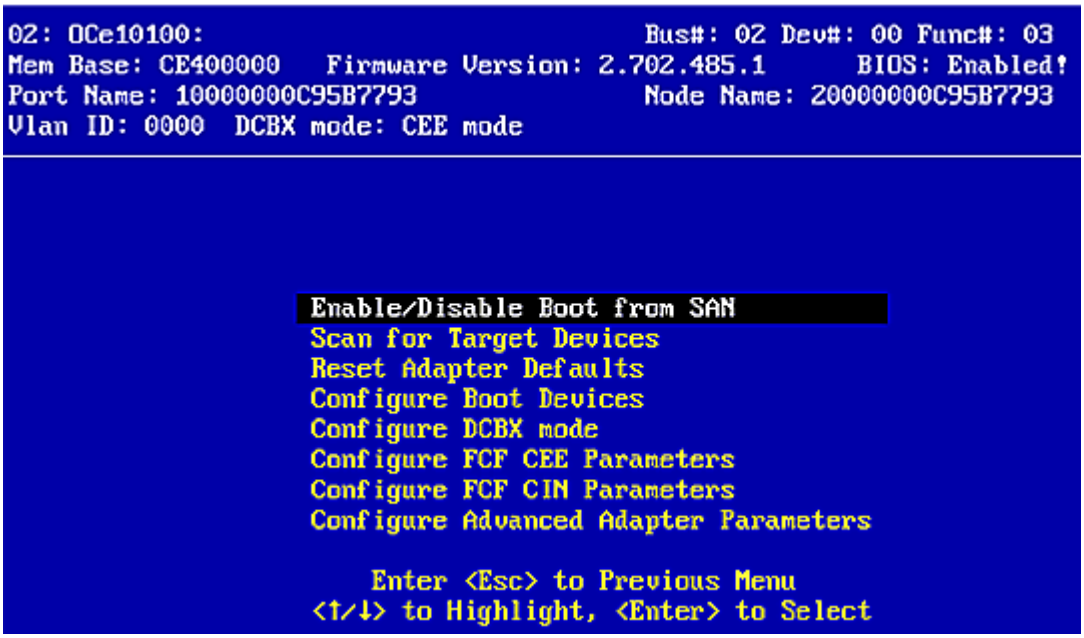

Figure 5-2 Main Configuration Menu

Under normal circumstances, you would first configure boot devices using the BIOS Utility (see "Configuring Boot Devices" on page 55). However, if the adapter is not enabled to boot from SAN, you must first enable the adapter to do so.

Enabling an Adapter to Boot from SAN

To enable an adapter to boot from SAN, from the Main configuration menu, select **Enable/Disable Boot from SAN** and press **<Enter>**.

Note: Adapters are disabled by default.

At least one adapter must be enabled to boot from SAN in order to use remote boot functionality. Once you enable an adapter, the status of the boot BIOS changes as shown in Figure 5-3.

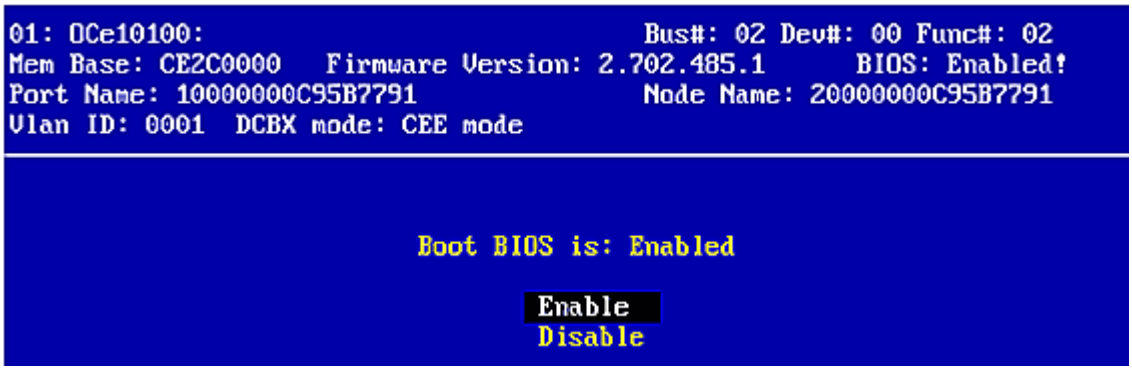

Figure 5-3 BIOS Status

Scanning for Target Devices

To scan for target devices:

1. From the Main configuration menu, select **Scan for Target Devices**. This option only displays a list of discovered target devices. It allows you to quickly verify zoning and SAN connectivity while providing a mechanism to log in ports for zoning.

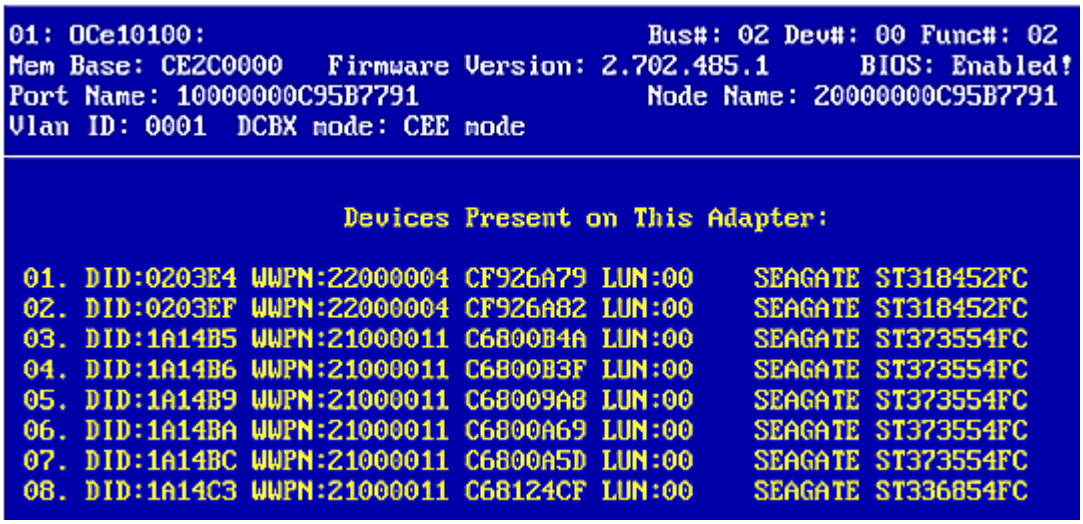

Figure 5-4 Devices Present on the Adapter

2. Press **<Esc>** to return to the Main configuration menu.

Configuring Boot Devices

Note: The FC protocol supports FC-AL (public and private loop) and fabric point-to-point. When operating in loop (FC-AL) topology, the system automatically determines whether it is configured for a public or private loop. The BIOS looks for a fabric loop (FL_Port) first. If a fabric loop is not detected, the BIOS looks for a private loop. The FCoE protocol does not support FC-AL.

To configure boot devices:

1. On the main configuration menu (Figure 5-2), select **Configure Boot Devices** and press **<Enter>**.

   A list of eight boot devices is shown (Figure 5-5). Emulex recommends that you configure only the bootable devices. The primary boot device is the first entry shown. It is the first bootable device. If the first boot entry fails due to a hardware error, the system boots from the second bootable entry. If the second boot entry fails, the system boots from the third bootable entry and so on.

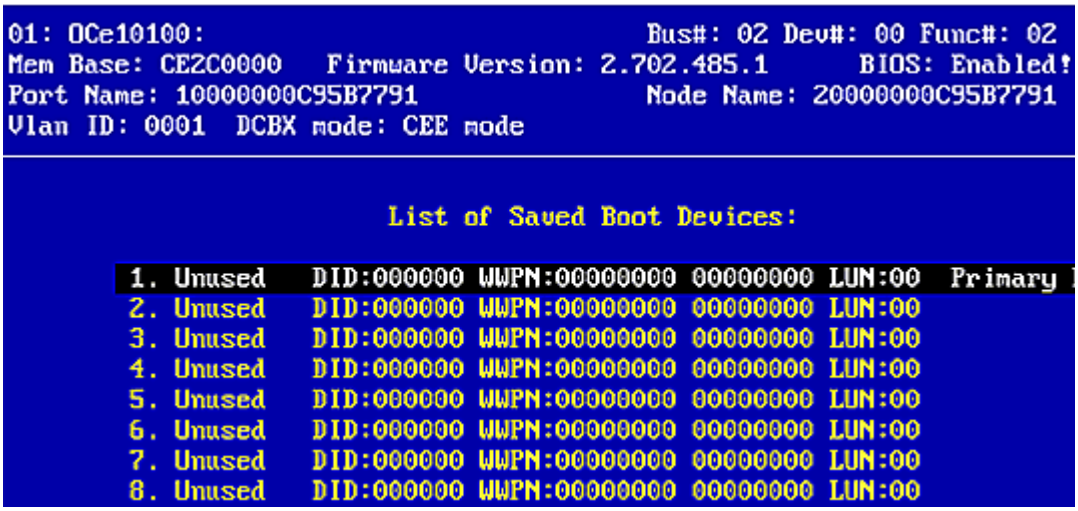

Figure 5-5 List of Saved Boot Devices Screen

2. Select a boot entry and press **<Enter>**. A screen similar to Figure 5-6 is displayed.

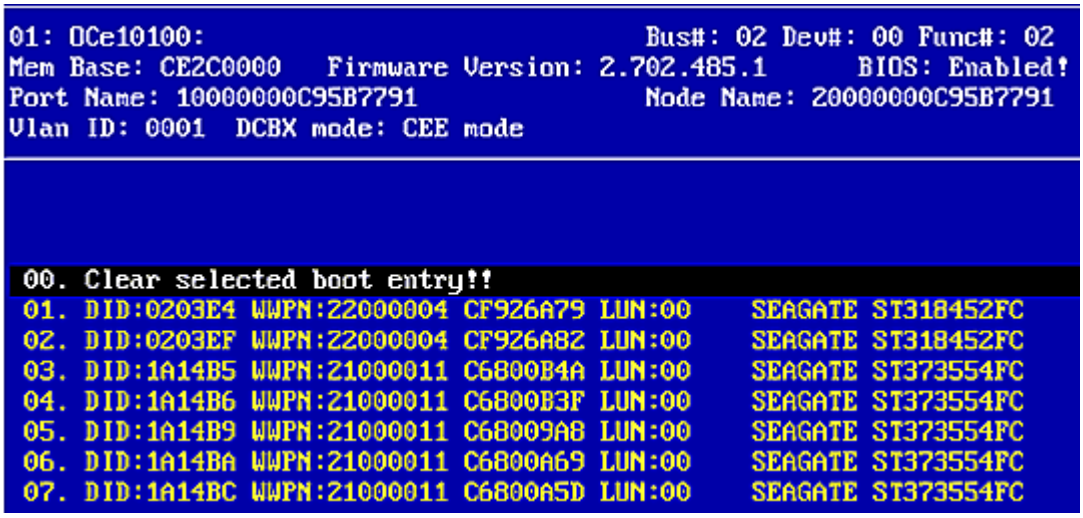

Figure 5-6 Device Selection List Example (Array) Screen

Note: To minimize the amount of time needed to locate the boot device, Emulex recommends that you select the drive with the lowest AL_PA as the boot device.

3. Select **<00>** and press **<Enter>** to clear the selected boot entry, or select a device to configure booting by WWPN or DID and press **<Enter>**.
4. If you select a device, you are asked for the starting LUN. Use the up and down arrows to enter the starting LUN in hexadecimal format and press **<Enter>**. (Figure 5-7). The starting LUN can be any number from 0 to 255.

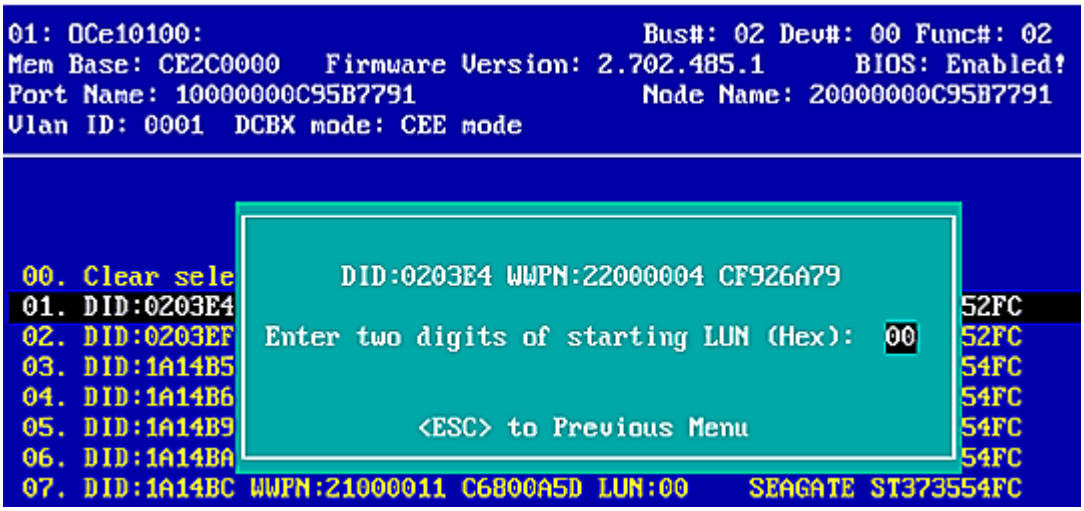

Figure 5-7 LUN Listing Screen

5. A screen similar to Figure 5-8 is displayed. Press **<Enter>**.

Figure 5-8 Boot Device Selected

The Boot Devices menu is displayed.

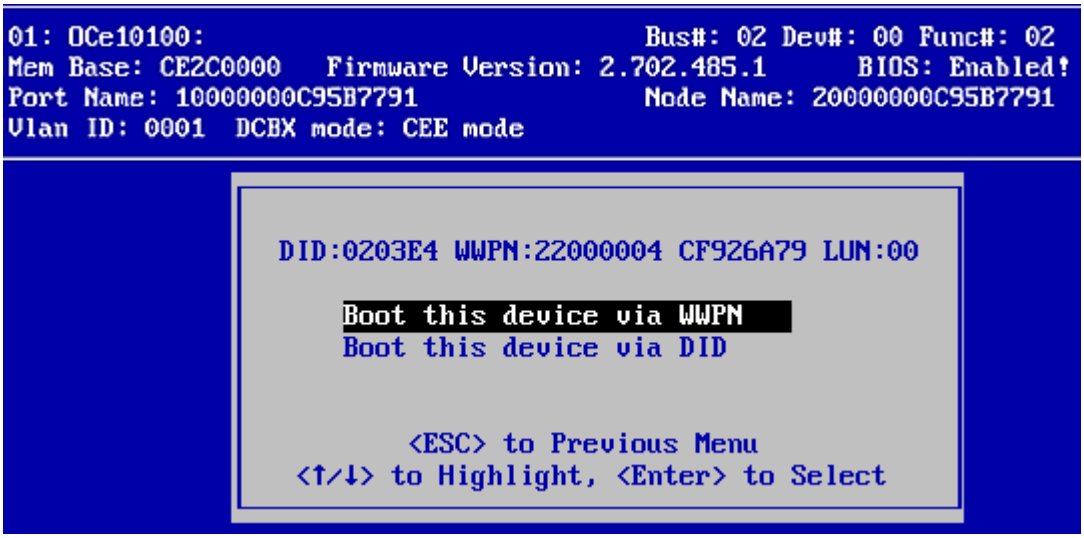

Figure 5-9 Boot Devices Menu

6. Use the up and down arrows to select the boot method. If you select to boot the device by WWPN, the WWPN of the earlier selected entry is saved in the flash memory. However, during the initial BIOS scan, the utility issues a Name Server Inquiry GID_PN (Get Port Identifier). Then, based on this DID, it continues with the remainder of the scanning.

   If you select to boot this device by DID, the earlier selected entry is saved in the flash memory.

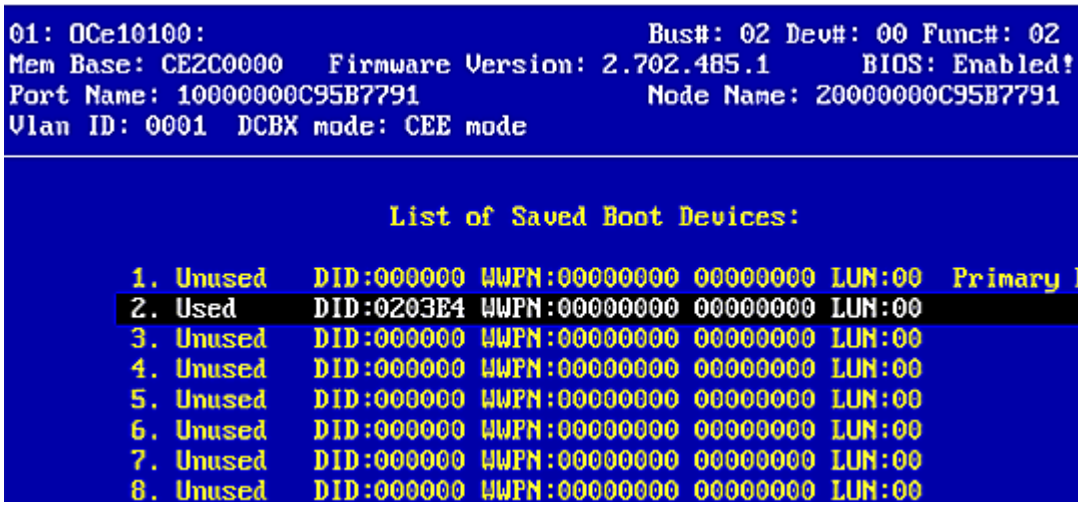

Figure 5-10 Primary Boot Device Set Up Screen

7. Press **<Enter>** to select the change.
8. Press **<Esc>** to return to the main configuration menu.
9. Reboot the system for the new boot path to take effect.

Configuring DCBX Mode

To configure Data Center Bridging Exchange Protocol (DCBX) mode for FCoE initialization protocol:

1. On the main configuration menu (Figure 5-2), select **Configure DCBX mode** and press **<Enter>**. The DCBX menu is displayed.

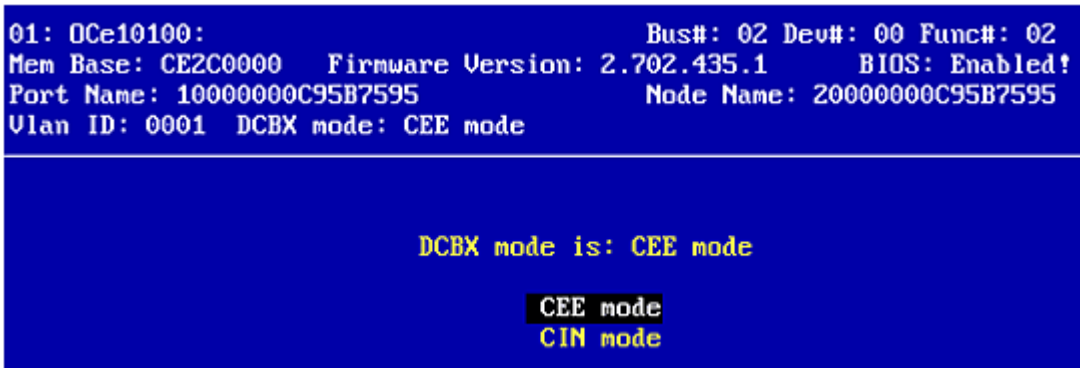

Figure 5-11 DCBX Menu

2. Use the arrow keys to select CEE (Converged Enhanced Ethernet) if the attached switch is CEE compatible, or select CIN (Cisco-Intel-Nuova) if the attached switch is CIN compatible. (For more information, see the FCoE switch documentation for your particular switch.)
3. Press **<Enter>** to select the mode.

Configuring CEE Parameters

To configure CEE parameters:

1. If multiple VLANs or FCoE switches are set up and you want to select a particular VLAN to boot from every time, select **Configure FCF CEE Parameters** from the main configuration menu (Figure 5-2) and press **<Enter>**. A list of discovered FCF is displayed.

Figure 5-12 FCF Listing

2. Select the FCF you want to boot from every time and save this to the adapter record by pressing **<Enter>**. The following message is displayed.

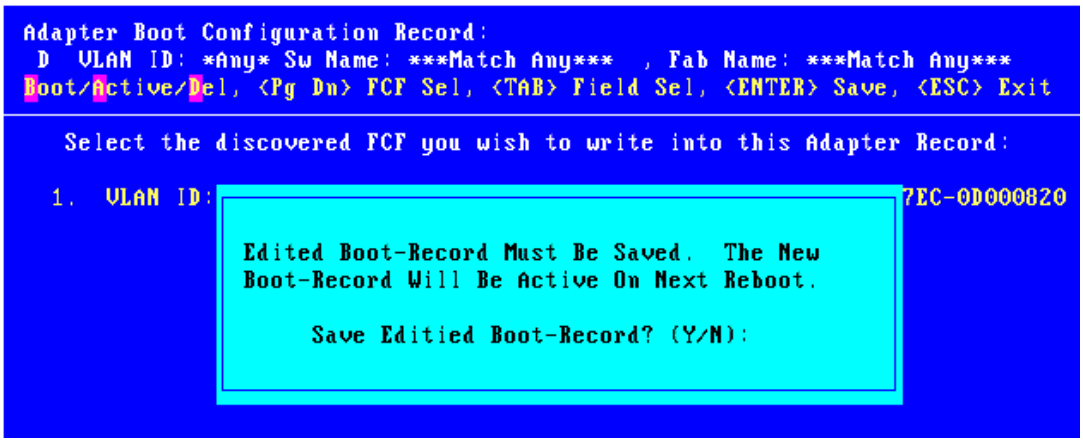

Figure 5-13 Save Edited Boot Record Dialog Box

3. Type **<Y>** to save the boot record. The main configuration menu is displayed.

Configuring CIN Parameters

To configure CIN parameters, on the main configuration menu (Figure 5-2), select **Configure FCF CIN Parameters** and press **<Enter>**. The CIN configuration menu is displayed.

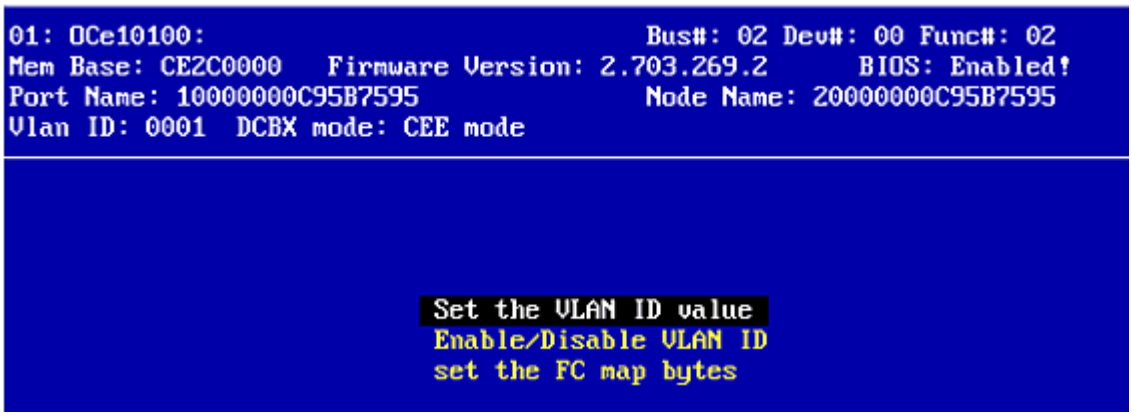

Figure 5-14 CIN Configuration Menu

Setting the VLAN ID Value

To set the VLAN ID value:

1. Select **Set the VLAN ID** from the CIN configuration menu and press **<Enter>**. The following screen is displayed.

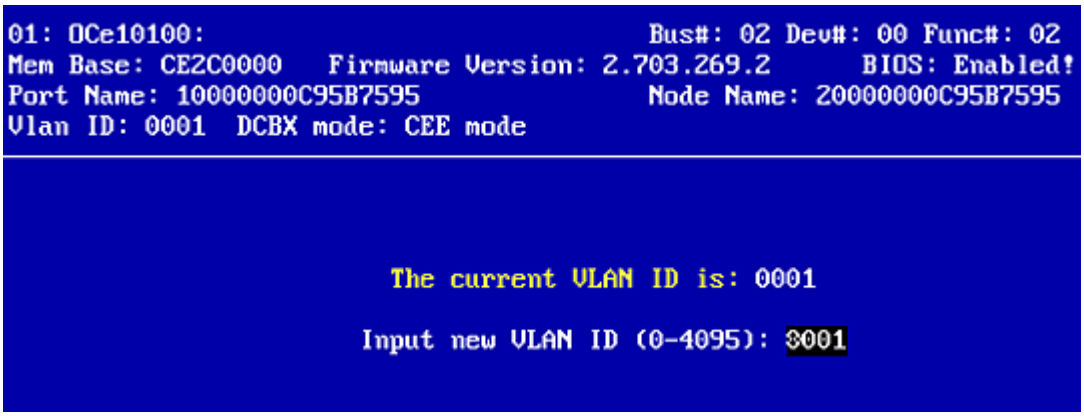

Figure 5-15 FCF CIN VLAN ID

2. Enter the VLAN on which the adapter FCoE services are available. Use the up and down arrow keys to change the value at the cursor and the left and right arrow keys to move the cursor.
3. Press **<Enter>** to save and return to the CIN configuration menu.
4. Press **<Esc>** to exit this screen without saving.

Enabling or Disabling VLAN ID

To enable or disable VLAN ID:

1. Select **Enable/Disable VLAN ID** from the CIN configuration menu. The following screen is displayed.

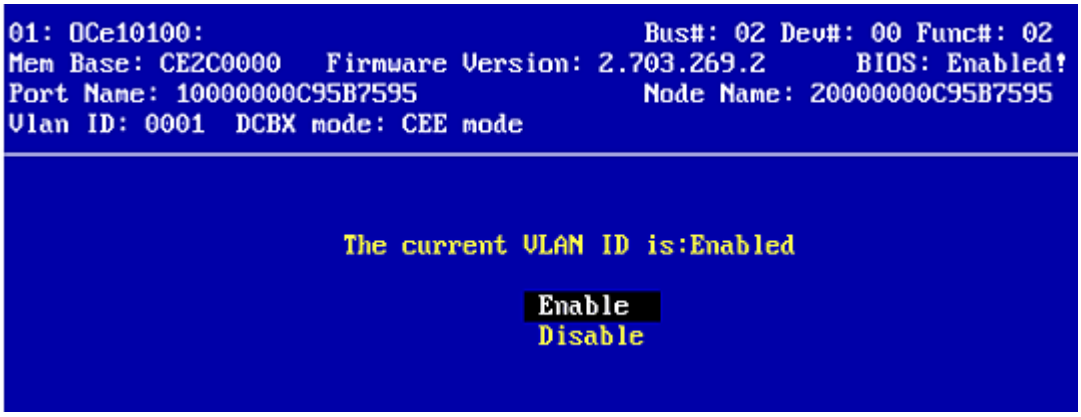

Figure 5-16 Enable or Disable VLAN ID Screen

2. Use the up and down arrows to highlight an option, then press **<Enter>** to select it.
3. Press **<Esc>** to return to the CIN configuration menu.

Setting the FC Map Bytes

To set the FC map bytes:

1. Select Set the **FC Map Bytes** from the CIN configuration menu and press **<Enter>**. The following screen is displayed.

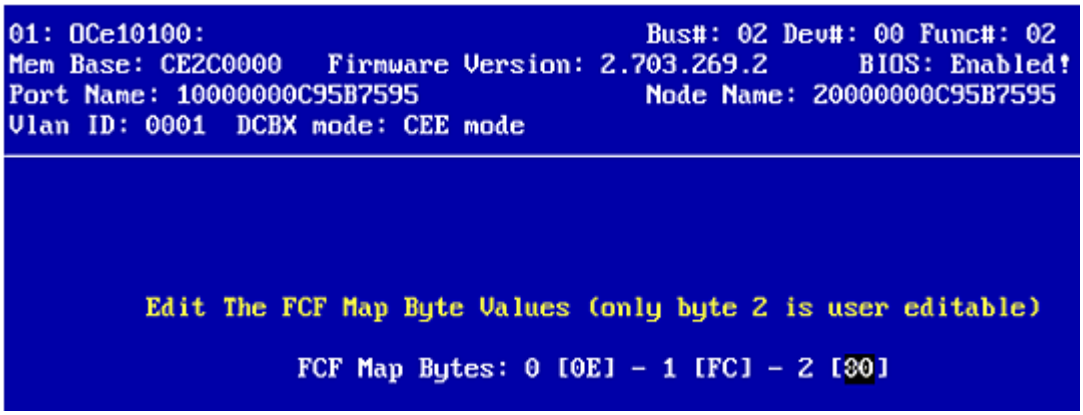

Figure 5-17 Set FCF Wrap Byte Screen

2. Enter the bit value that completes the fabric-provided MAC address. Use the up and down arrow keys to change the value at the cursor and the left and right arrow keys to move the cursor.
3. Press **<Enter>** to save and return to the CIN configuration menu.
4. Press **<Esc>** to exit this screen without saving.

Configuring Advanced Adapter Parameters

The BIOS utility has numerous options that can be modified to provide different behavior. Use the BIOS utility to perform the following tasks:

- Change the default AL_PA of the adapter
- Change the PLOGI retry timer
- Enable or disable spinup delay
- Set autoscan
- Enable or disable Enhanced Disk Drive (EDD) 3.0
- Enable or disable the start unit command
- Enable or disable the environment variable
- Enable or disable the auto boot sector

To access the adapter configuration menu, from the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed.

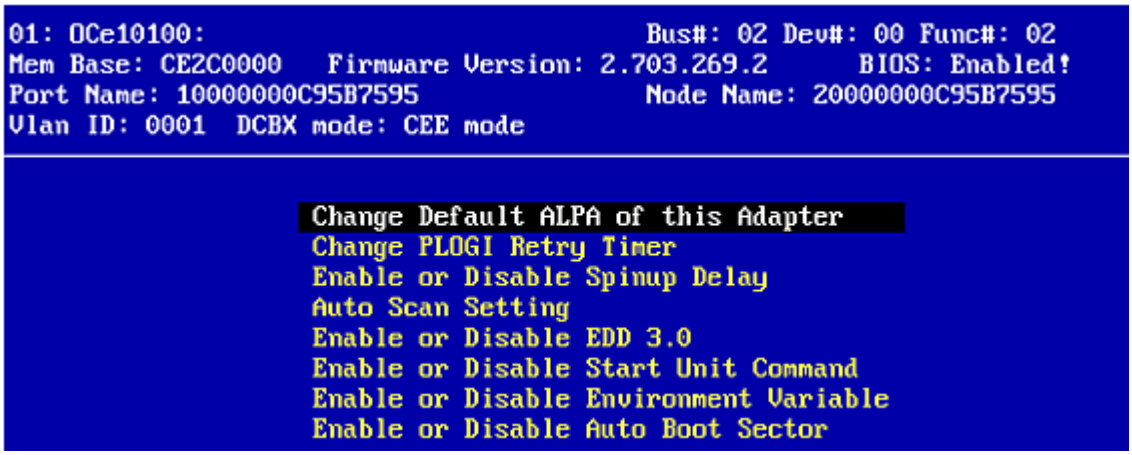

Figure 5-18 Advanced Adapter Configuration Menu

Default settings are acceptable for most installations.

To reset all values to their defaults, from the main configuration menu (Figure 5-2), select **Reset Adapter Defaults** and press **<Enter>**.

Changing the Default AL_PA

The default value of the AL_PA for the adapter BIOS is 00 (hex). All adapters or boot drives can be configured to other AL_PAs rather than their default values.

Note: This option applies only to arbitrated loop (FC-AL). The FCoE protocol does not support FC-AL.

To change the default AL_PA:

1. On the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).

2. Select **Change Default ALPA** of this adapter and press **<Enter>**. Information similar to Figure 5-19 is displayed.

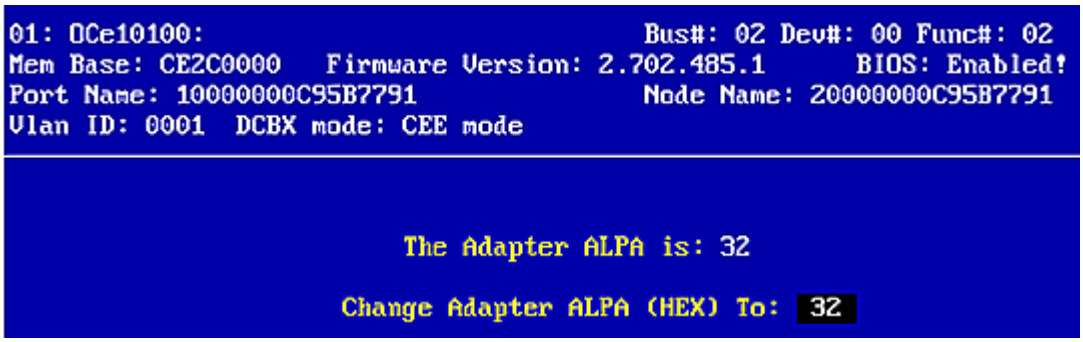

Figure 5-19 Change Default ALPA Screen

3. Change the default AL_PA, use the up and down arrow keys to scroll through the valid AL_PAs. Table 5-1 lists the valid AL_PA values.
4. Press **<Enter>** to accept the new value.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Note: If the adapter's AL_PA is changed, it does not show on the NVRAM AL_PA until the system has been reset.

Table 5-1 Valid AL_PA Values

0x00	0x01	0x02	0x04	0x08	0x0F	0x10	0x17
0x18	0x1B	0x1D	0x1E	0x1F	0x23	0x25	0x26
0x27	0x29	0x2A	0x2B	0x2C	0x2D	0x2E	0x31
0x32	0x33	0x34	0x35	0x36	0x39	0x3A	0x3C
0x43	0x45	0x46	0x47	0x49	0x4A	0x4B	0x4C
0x4D	0x4E	0x51	0x52	0x53	0x54	0x55	0x56
0x59	0x5A	0x5C	0x63	0x65	0x66	0x67	0x69
0x6A	0x6B	0x6C	0x6D	0x6E	0x71	0x72	0x73
0x74	0x75	0x76	0x79	0x7A	0x7C	0x80	0x81
0x82	0x84	0x88	0x8F	0x90	0x97	0x98	0x9B
0x9D	0x9E	0x9F	0xA3	0xA5	0xA6	0xA7	0xA9
0xAA	0xAB	0xAC	0xAD	0xAE	0xB1	0xB2	0xB3
0xB4	0xB5	0xB6	0xB9	0xBA	0xBC	0xC3	0xC5
0xC6	0xC7	0xC9	0xCA	0xCB	0xCC	0xCD	0xCE
0xD1	0xD2	0xD3	0xD4	0xD5	0xD6	0xD9	0xDA
0xDC	0xE0	0xE1	0xE2	0xE4	0xE8	0xEF	

Changing the PLOGI Retry Timer

This option is especially useful for Tachyon-based RAID arrays. Rarely, a Tachyon-based RAID array resets itself and the port goes offline temporarily. When the port returns to operation, the PLOGI (port login) retry interval scans the loop to discover this device. The PLOGI retry interval is the time it takes for one PLOGI to scan the whole loop. You can choose:

- No PLOGI Retry: 0 msec – default
- 50 msec takes 5 to 6 seconds per device (if 126 AL_PAs are on the loop)
- 100 msec takes 12 seconds per device (if 126 AL_PAs are on the loop)
- 200 msec takes 22 seconds per device (if 126 AL_PAs are on the loop)

To set the interval for the PLOGI retry timer:

1. On the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Change PLOGI Retry Timer** and press **<Enter>**. Information similar to Figure 5-20 is displayed.

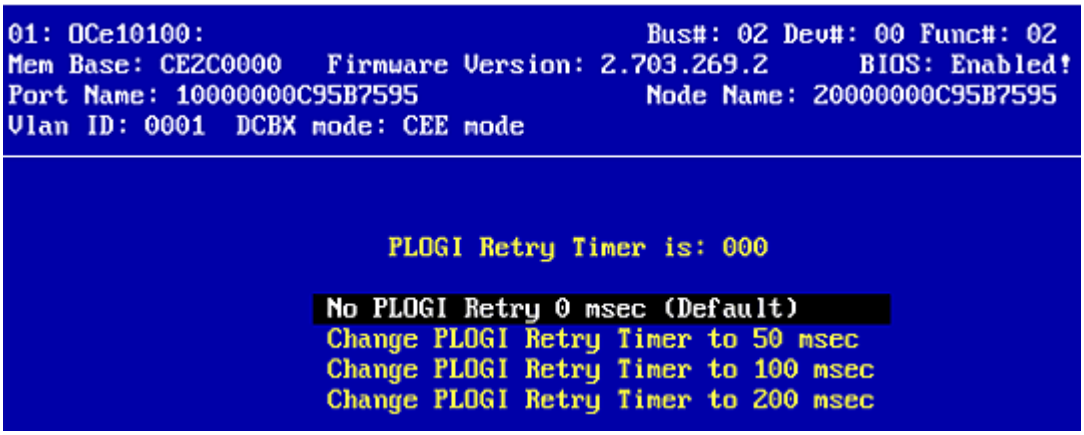

Figure 5-20 Change the PLOGI Retry Timer Screen

3. Select the retry timer interval.
4. Press **<Enter>** to accept the new interval.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Enabling or Disabling the Spinup Delay

This option allows you to enable or disable the disk spinup delay. The factory default setting is disabled.

If at least one boot device has been defined, and the spinup delay is enabled, the boot BIOS searches for the first available boot device.

- If a boot device is present, the boot BIOS boots from it immediately.
- If a boot device is not ready, the boot BIOS waits for the spinup delay and, for up to three additional minutes, continues the boot scanning algorithm to find another multi-boot device.

If boot devices have not been defined, and auto scan is enabled, then the boot BIOS waits for five minutes before scanning for devices.

- In a private loop, the boot BIOS attempts to boot from the lowest target AL_PA it finds.
- In an attached fabric, the boot BIOS attempts to boot from the first target found in the NameServer data.

To enable or disable the spinup delay:

1. On the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Enable or Disable Spinup Delay** and press **<Enter>**. Information similar to Figure 5-21 is displayed.

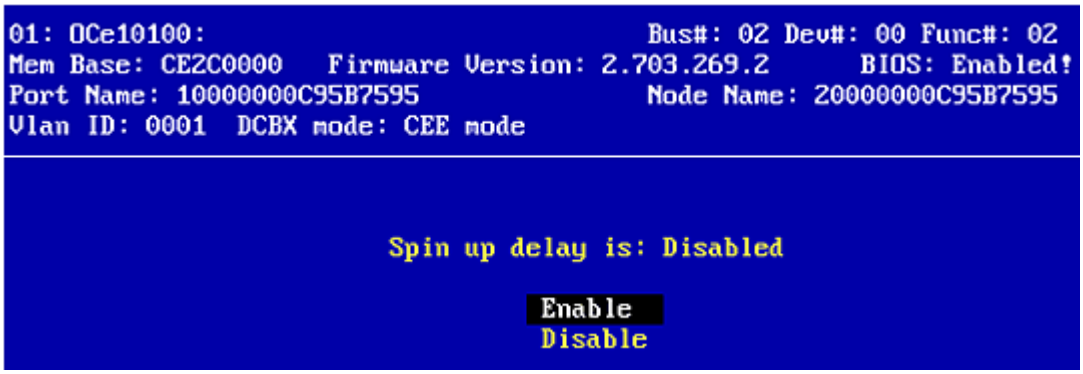

Figure 5-21 Enable or Disable Spinup Delay Screen

3. Select whether to enable or disable spinup delay.
4. Press **<Enter>** to accept the new value.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Setting Auto Scan

This option allows you to set auto scan and enable the first device in the boot entry list to issue a Name Server Inquiry. Auto scan is available only if none of the eight boot entries is configured to boot from DID or WWPN. The factory default is disabled. If there is more than one adapter with the same PCI Bus number in the system, and each has a boot drive attached, the first PCI-scanned adapter is the boot adapter. The first adapter is usually in the lowest PCI slot in the system.

Use the Boot Devices menu (Figure 5-9) to configure up to eight boot entries for fabric point-to-point, public loop or private loop configurations. The first adapter is usually in the lowest PCI slot in the system. This device is the only boot device and it is the only device exported to the multi-boot menu.

Auto scan options:

- Autoscan disabled – default.
- Any first device – The first adapter issues a Name Server Inquiry and the first D_ID from the inquiry becomes the boot device. The adapter attempts to log in to a public loop first. If it fails, it logs in to a private loop. The first successfully scanned device becomes the boot device. This device only is exported to the multi-boot menu.
- First LUN 0 device
- First NOT LUN 0 device (a device other than LUN 0)

To set auto scan:

1. From the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Auto Scan Setting** and press **<Enter>**. Figure 5-22 is displayed.

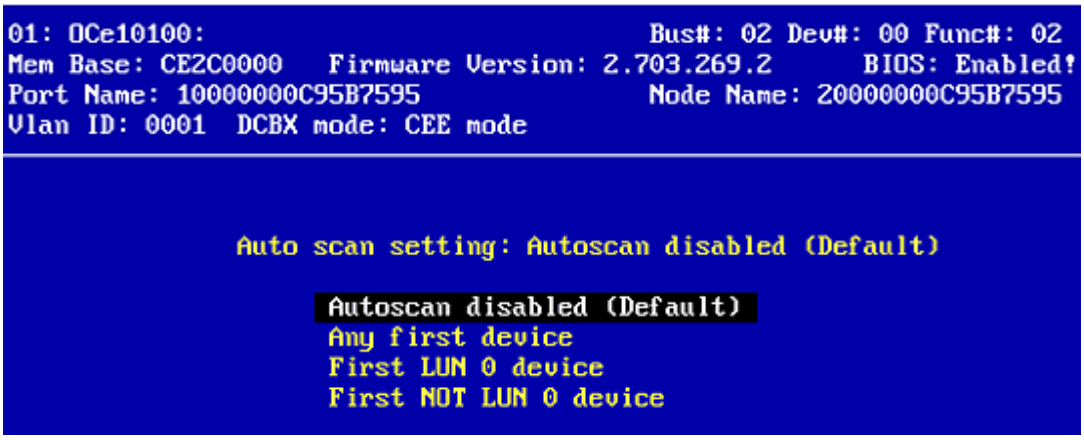

Figure 5-22 Set Auto Scan Menu

3. Select the appropriate auto scan option.
4. Press **<Enter>** to accept the new scan option.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Enabling or Disabling EDD 3.0

EDD 3.0 provides additional data to the operating system boot loader during an INT-13h function 48h call (get device parameters). This information includes the path to the boot device and the disk size. The default setting for EDD 3.0 is disabled (EDD 2.1).

To enable or disable EDD 3.0:

1. From the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Enable or Disable EDD 3.0** and press **<Enter>**. The EDD 3.0 configuration screen is displayed.

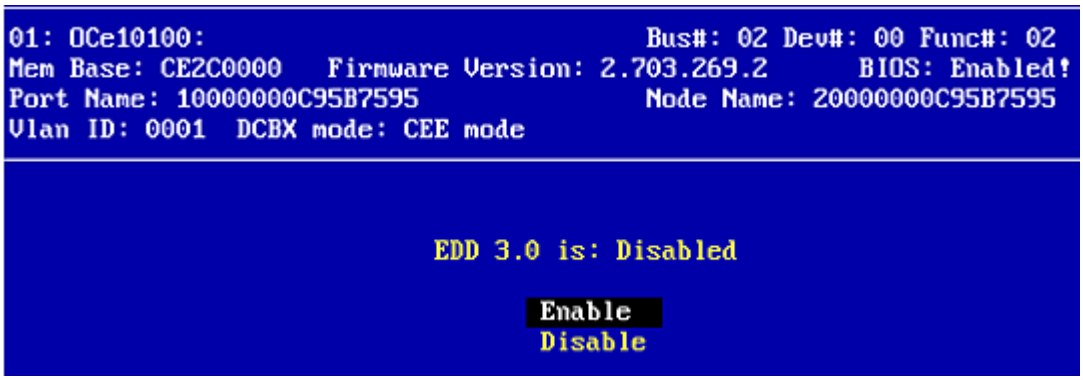

Figure 5-23 Enable or Disable EDD 3.0 Screen

3. Select whether to enable or disable EDD 3.0.
4. Press **<Enter>** to accept the change.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Enabling or Disabling the Start Unit Command

You must know the specific LUN to issue the SCSI start unit command. The default setting is disabled.

To enable or disable the start unit command:

1. From the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Enable or Disable Start Unit Command** and press **<Enter>**. The Start Unit Command configuration screen is displayed.

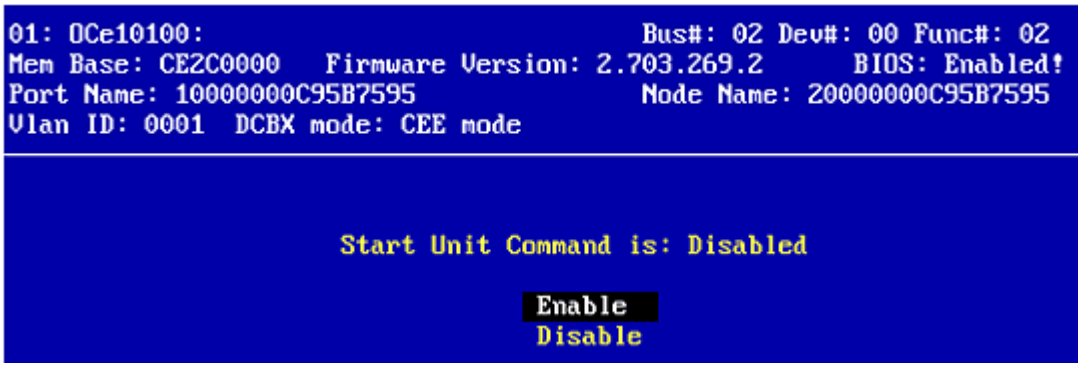

Figure 5-24 Enable or Disable Start Unit Command Screen

3. Select whether to enable or disable the start unit command.
4. Press **<Enter>** to select the change.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Enabling or Disabling the Environment Variable

Sets the boot controller order if the system supports the environment variable. The default setting is disabled.

To enable or disable the environment variable:

1. From the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Enable or Disable Environment Variable** and press **<Enter>**. The Environment Variable configuration screen is displayed.

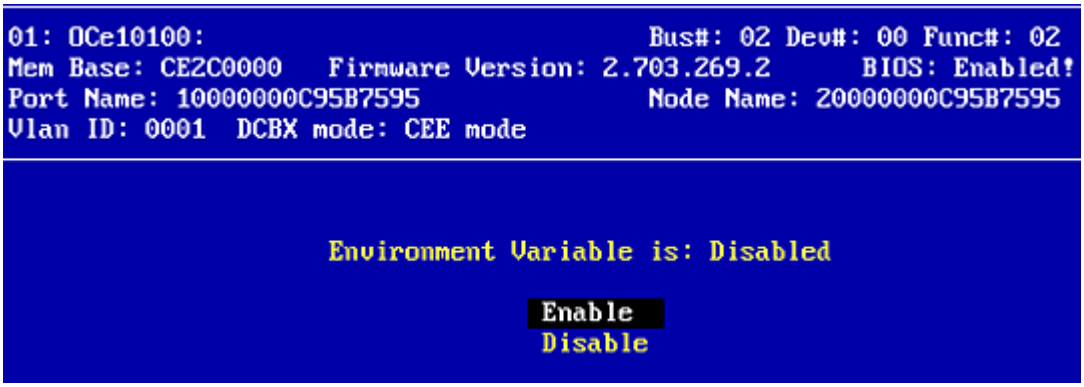

Figure 5-25 Enable or Disable Environment Variable Screen

3. Select whether to enable or disable the environment variable.
4. Press **<Enter>** to select the change.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Enabling or Disabling Auto Boot Sector

This option automatically defines the boot sector of the target disk for the migration boot process, which applies only to HP MSA1000 arrays. If there is no partition on the target, the default boot sector format is 63 sectors. The default setting is disabled.

To enable or disable the auto boot sector format:

1. From the main configuration menu (Figure 5-2), select **Configure Advanced Adapter Parameters** and press **<Enter>**. The adapter configuration menu is displayed (Figure 5-18).
2. Select **Enable or Disable Auto Boot Sector** and press **<Enter>**. The Auto Boot Sector configuration screen is displayed.

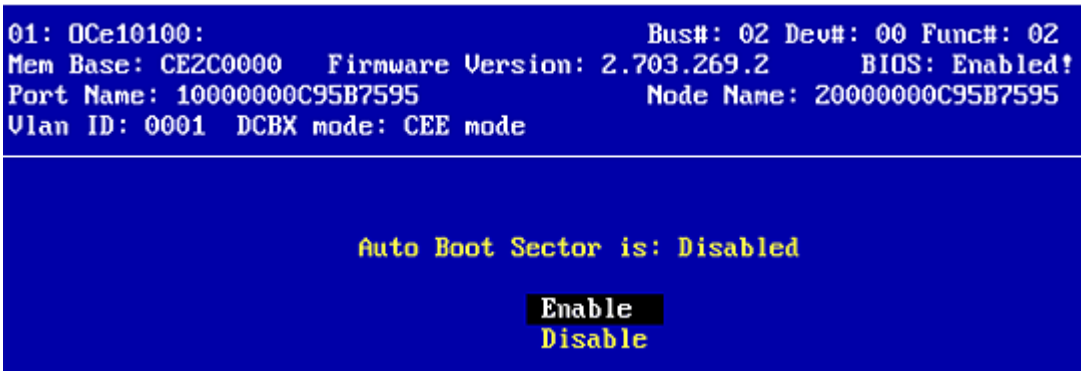

Figure 5-26 Enable or Disable Auto Boot Sector Format Screen

3. Select whether to enable or disable the auto boot sector.
4. Press **<Enter>** to accept the new value.
5. Press **<Esc>** to return to the advanced adapter configuration menu.
6. For changes to take effect, reboot the system.

Using Multi-Path Boot from SAN

Multi-boot BIOS is in compliance with BIOS Boot Specification (BBS). The system must have a Multi-boot system BIOS in order to take advantage of this option. The Multi-boot BIOS allows you to select any boot disk in the system BIOS setup menu. The boot disk can be an FC drive, a SCSI drive, an IDE drive, a USB device, or a floppy drive. The Emulex BIOS supplies the first eight drives to the system BIOS menu. The Multi-boot BIOS can override the FC drive that is selected in the BIOS utility.

For example, the system has eight FC disks only. The boot disk has AL_PA 02. However, you can select AL_PA 23 in the system BIOS setup menu. The boot device is the FC disk with AL_PA 23 instead of AL_PA 02, as is set in the BIOS utility.

If your system supports Multi-boot BBS, the local boot disk (drive C) is the first entry in Multi-boot on the system BIOS setup menu. The list of entries is determined by the list of configured boot entries in the BIOS utility. For example:

```
Adapter 1: boot_entry0, boot_entry1
Adapter 2: boot_entry2, boot_entry3
```

The order of boot entries exported to Multi-boot (BBS) is

```
boot_entry0, boot_entry1, boot_entry2, and boot_entry3.
```

However, Multi-boot allows changing the boot order in the server BIOS, which allows any disk to become the C drive.

Resetting to Default Values

The BIOS utility enables you to reset BIOS boot parameters to their factory default settings. These defaults are listed in Table 5-2.

Table 5-2 Default Adapter Boot Parameter Values

Parameter	Default Value	Valid Values
Boot from SAN	Disabled	Enabled Disabled
AL_PA Value	0x00 Fibre	See Table 5-1, Valid AL_PA Values.
EDD 3.0	Disabled (EDD 2.1)	Enabled (EDD 3.0) Disabled (EDD 2.1)
PLOGI Retry Timer	Disabled	Disabled 50 msec 100 msec 200 msec
Spinup Delay	Disabled	Enabled Disabled
Auto Scan	Disabled	Enabled Disabled
Start Unit	Disabled	Enabled Disabled
Environmental Variable	Disabled	Enabled Disabled
Auto Boot Sector	Disabled	Enabled Disabled

Note: DCBX mode settings are firmware (UCNA) parameters and are not altered when setting the BIOS boot parameters to their defaults.

To reset parameters to their factory default settings:

1. On the main configuration menu (Figure 5-2) select **Reset Adapter Defaults** and press **<Enter>**. A screen is displayed that asks if you want to reset to the defaults.

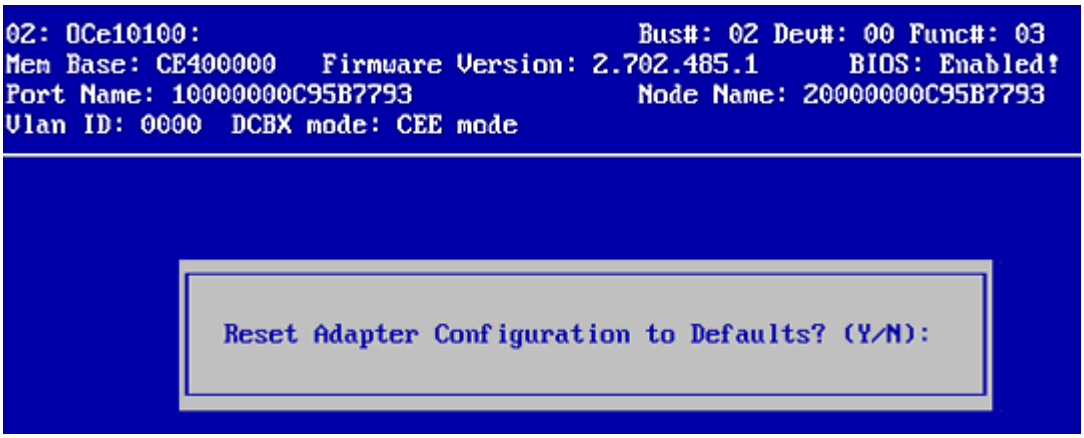

Figure 5-27 Reset Adapter Configuration to Defaults Screen

2. Press **<Y>**. All settings revert to their factory default values.
3. Press **<Esc>** to go to the previous menu.

6. Installing, Updating, and Enabling Boot Code

Emulex provides utilities to install, update, and enable boot code. The utility that you use depends on the operating system and, in some cases, the driver type or system architecture. Table 6-1 indicates the utilities that are currently available for each operating system.

Table 6-1 Utilities that Install, Update, and Enable Boot Code

Operating System	OneCommand Manager Application	HBAcmd Utility	Offline Utilities
Windows	✓	✓	✓
Linux	✓	✓	✓
Citrix	✓	✓	✓
VMware	✓	✓	✓

Note: For the Citrix and VMware operating systems, the OneCommand Manager application GUI is not supported locally, but can be managed through the GUI from a remote system.

After you decide which utility to use, see the appropriate documentation for the proper procedures:

- OneCommand Manager application: see the *OneCommand Manager Application User Manual*.
- HBAcmd utility: see the *OneCommand Manager Application CLI User Manual*.
- Offline utility: see the *Offline Utilities User Manual*.

7. Configuring iSCSI Boot Support with the iSCSISelect Utility

This section provides quick installation instructions for setting up a basic boot configuration. For more information on setting up an iSCSI initiator and adding an iSCSI target, see chapter 8., "Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility," on page 76 and chapter 9., "Configuring and Managing iSCSI Targets with the iSCSISelect Utility," on page 82.

Navigating the iSCSISelect Utility

Use the following methods to navigate the iSCSISelect utility:

- Press the up/down arrows on your keyboard to move through and select menu options or configuration fields. When multiple adapters are listed, use the up/down arrows to scroll to the additional adapters.
- Press **<Tab>** to move to the next field, and **<Shift> <Tab>** to move to the previous field.
- Press **<Enter>** to accept a selection, select a menu option, to select a row in a configuration screen, or to change a configuration default.
- Press **<Esc>** to return to the previous menu or page, cancel a selection or dialog box, or exit the utility.

Setting Up a Basic iSCSI Boot Configuration

By setting up a basic iSCSI boot configuration, you can configure your initiator, contact network devices, and set up an iSCSI boot target. With iSCSI boot capability, the iSCSISelect utility can quickly and easily provide the target LUN disk to the operating system through the BIOS. After setting up a basic iSCSI boot configuration, you can continue to use the iSCSISelect utility to manage your OneConnect Server iSCSI SAN environment.

When setting up a basic iSCSI boot configuration you must do the following:

- Configure the iSCSI initiator name and enable boot support
- Configure the network properties
- Add an iSCSI target and enable it as a boot target
- Set your boot LUN
- Reboot your system

To set up a basic iSCSI Boot configuration:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. From the iSCSI Initiator Configuration menu, set the initiator name.

3. Select **Save** and press **<Enter>** to save your initiator name.

Figure 7-1 iSCSI Initiator Configuration Menu

4. Select **Controller Configuration** and press **<Enter>**. If you are running a single controller, the Controller Configuration menu is displayed (Figure 7-3). If you are running multiple controllers, the Controller Selection menu is displayed (Figure 7-2).

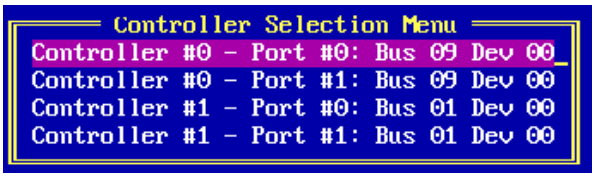

Figure 7-2 Controller Selection Menu

5. From the Controller Selection menu, select your controller and port then press **<Enter>**. For more information, see "Selecting a Controller" on page 77.
6. After you have selected your controller, the Controller Configuration menu appears.

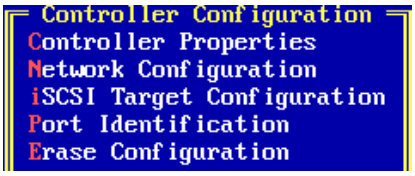

Figure 7-3 Controller Configuration Menu

7. From this menu, select **Controller Properties** and press **<Enter>**.
8. Ensure Boot Support is set to Enabled.
9. Select **Save** and press **<Enter>**.
10. From the Controller Configuration menu, select **Network Configuration** and press **<Enter>**.
11. Configure a network IP address. From the Network Configuration menu, do one of the following:
    - Enable DHCP. For more information, see "Enabling DHCP" on page 78.
    - Set up a static IP address. For more information, see "Configuring a Static IP Address" on page 79.
12. If desired, configure a VLAN ID. For more information, see "Configuring VLAN ID/Priority" on page 80.
13. Add a SCSI target. From the Controller Configuration menu, select **iSCSI Target Configuration**, then select **Add a New iSCSI Target**. For more information, see "Adding iSCSI Targets" on page 82.
14. After you have successfully configured the iSCSI initiator and target, reboot the system.

Booting the System

After you have successfully set up your basic boot configuration, exit the iSCSISelect utility and the system automatically reboots. During the next boot up, the iSCSI BIOS logs into the configured iSCSI boot target and display its target/LUN information in the BIOS sign-on banner. For example:

```
Controller#0 Port#0 Base 0xFCE60000 at Bus:01 Dev:00 Fun:02
Controller#0 Port#1 Base 0xFCEA0000 at Bus:01 Dev:00 Fun:03

<<< Press <Ctrl><S> for iSCSISelect(TM) Utility >>>

Initiator iSCSI Name:  iqn.2004-05.com.emulex
Initiator IP Address:  172. 40.  1.41
Initiator IP Address:  172. 40.  1.62

Drive #0 NETAPP   LUN 0  2048 MB
Drive Geometry    105    3FFF
BIOS Installed Successfully!
```

8. Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility

The iSCSI initiator or host (also known as the iSCSI client) is a system such as a server, which attaches to an IP network and initiates requests and receives responses from an iSCSI target. Each iSCSI host is identified by a unique iSCSI qualified name (IQN).

Once you have an initiator host system running, you must configure the initiator to allow access to the iSCSI SAN. To do this, you must:

1. Configure the iSCSI initiator name.
2. Select a controller. For additional information, see "Selecting a Controller" on page 77.
3. Configure network properties. For additional information, see "Configuring Network Properties" on page 78.
4. Verify network settings. For additional information, see "Confirming Network Settings" on page 81.

Configuring the iSCSI Initiator Name

The iSCSI initiator name is a unique identifier for the initiator on the network and configures target access. It must be unique to that system on the network and is identified by an IQN. The iSCSI initiator name is global to the entire system. The iSCSI initiator name must also match the target's Access Control List (ACL). After you log into the iSCSISelect utility, you can configure the iSCSI initiator name from the iSCSI Initiator Configuration screen.

Note: When installing Microsoft software iSCSI initiator service, the iSCSI initiator name for OneConnect will change and any IQN name previously configured through the iSCSISelect utility will be overridden. Though this will not affect existing boot sessions and persistent sessions, new target logins may fail because the new IQN name may not match the incoming initiator IQN names configured on the target. To avoid this situation, after installing Microsoft software, you must rename the IQN name to the previous IQN name you had configured.

To configure the iSCSI initiator name:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted. After the BIOS initializes, the iSCSI Initiator Configuration screen appears.
2. Set or change the iSCSI initiator name from this screen.

Figure 8-1 iSCSI Initiator Configuration Screen

Note: If there are multiple controllers in your system, your iSCSI Initiator name may be different for each controller. If this happens, an error message

indicates an Initiator iSCSI Name mismatch. You must save a new initiator name on this menu so that the iSCSI Initiator Name on all the controllers match. If there were pre-existing sessions before the iSCSI Initiator Name change, the pre-existing sessions use the original name that was used to login the very first time. The new name is used for any sessions added after the name change.

3. Select **Save** and press **<Enter>** to save the iSCSI initiator name. If you select **Controller Configuration** without saving the changes, a warning message will appear stating that your settings will be lost and asking whether you want to cancel or not. Press **<Y>** and you will lose your changes. Press **<N>** and you will return to the iSCSI Initiator Configuration screen.

Selecting a Controller

After you configure an ISCSI initiator name, select a controller to configure the iSCSI target. If you are running the iSCSISelect utility with multiple controllers, all the controllers are listed in the Controller Selection menu. The OneConnect is a dual-port chip; therefore, the Controller Selection menu always shows two controllers (dual-ports) for each physical controller. Figure 8-2 is an example of the Controller Selection menu showing two physical controllers with two controllers (dual-port) each.

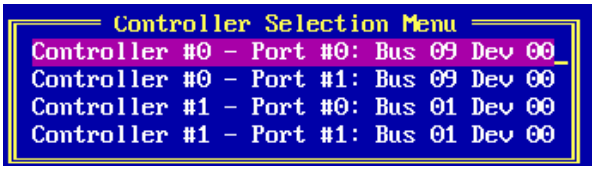

Figure 8-2 Controller Selection Menu

After you select the controller, the Controller Configuration menu appears. From this menu, you can configure and manage the iSCSI initiator and target(s).

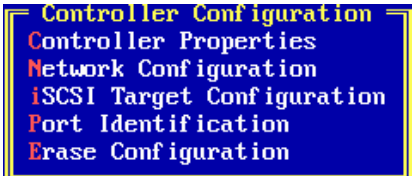

Figure 8-3 Controller Configuration Menu

If you are not sure that you are configuring the correct port, you can check by either:

- Performing port identification. For additional information, see “Identifying a Port” on page 80.
- Checking the link status in the Network Configuration menu. Connect the controller port to a 10 Gb/s switch port and check the link status in the Network Configuration menu. If the status is Link Up, it is the correct controller port.

  Note: Make sure you back out of the Network Configuration menu to the Controller Configuration menu before checking the Network

Configuration menu. This allows the Link Status field to refresh when you insert or remove the cable from the controller.

Configuring Network Properties

Use the Network Configuration menu to configure a network IP address for the controller. The IP address is a logical address for the controller and uniquely identifies the system on a TCP/IP network. The IP address can be determined statically (manually assigned) or dynamically (with the DHCP server to obtain an IP address). The method that you choose depends on your network configuration. If your network uses a DHCP configuration, then you can enable DHCP and obtain an IP address from the DHCP server. If a DHCP server is not available, you must configure a static IP address. You can also set a VLAN ID and/or priority from the Network Configuration dialog box.

Note: For all Linux-based operating systems, Emulex recommends that you enable DHCP when attempting to assign an IP address to an iSCSI port. This should be done as the iSCSI firmware will not detect it as a duplicate IP address if one already exists on a Linux server. Otherwise, you must manually ensure there are no duplicate IP addresses before assigning an IP address.

Note: If you are using target discovery through DHCP, you must add the root path to the DHCP server and enable DHCP discovery through the iSCSISelect utility.

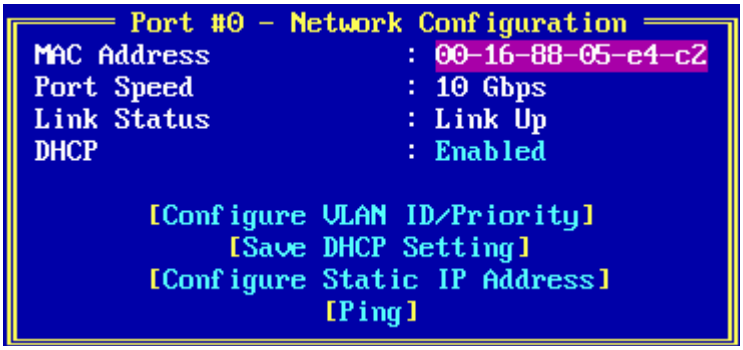

Figure 8-4 Network Configuration Dialog Box

Enabling DHCP

Enabling DHCP provides the initiator with an IP address.

Note: If you are using the DHCP server to obtain an IP address for your iSCSI initiator, set up a reservation. A reservation assigns a specific IP address based on the MAC address of your iSCSI function. If you do not reserve an IP address through DHCP, then you must set the lease length for the iSCSI initiator IP address to unlimited. This prevents the IP address lease from expiring.

To enable DHCP:

1. From the Controller Configuration menu, select **Network Configuration** and press **<Enter>** (Figure 8-4).

2. Select **Enabled** from the DHCP drop-down menu and press **<Enter>**.
3. Select **Save DHCP Settings** and press **<Enter>**. The DHCP IP Address dialog box appears. For example:

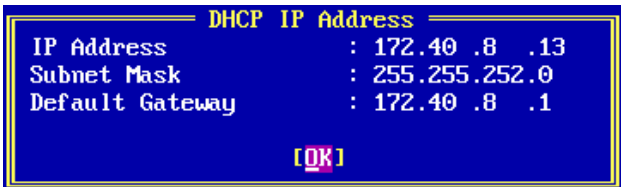

Figure 8-5 DHCP IP Address Dialog Box

Note: If you have set a static IP address, a message warns that the static IP address will be lost. Press **<Y>** to continue with enabling DHCP.

Configuring a Static IP Address

If a DHCP server is not available, you must manually configure a static IP address.

To configure a static IP address:

1. From the Network Configuration menu, select **Configure Static IP Address** and press **<Enter>**.

   Note: If you have DHCP enabled, a message warns that the DHCP IP Address will be lost. Press **<Y>** to continue to configure a static IP address.

   The Static IP Address dialog box is displayed.

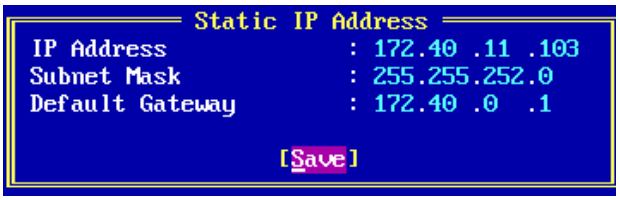

Figure 8-6 Static IP Address Dialog Box

2. Enter the IP address. This is a unique 32-bit address that specifies the location of each device or workstation in the network. This address is required for communication to the iSCSI SAN. For an initiator with its own network interface, you must assign an IP address in the same range as the iSCSI SAN.
3. Enter the subnet mask. The subnet mask provides a way to segment networks. All hosts (iSCSI initiators or targets) on the same physical network usually have the same subnet mask. For example, Figure 8-6 shows the initiator in the subnet 255.255.xxx.xxx. All the hosts (initiators or targets) in a sub-network will have the same subnet mask.
4. Enter the default gateway information, if necessary. A gateway is a router on a computer network that serves as an access point to another network and that an initiator uses by default. Any data to addresses not on the initiator's subnet are sent through the default gateway.
5. Select **Save** and press **<Enter>** to save the settings.

6. You are prompted to save the changes, type **<Y>**.
7. Press **<Esc>** to return to the Network Configuration menu.

Configuring VLAN ID/Priority

A Virtual Local Area Network (VLAN) is a way of partitioning the network. If the LAN is made up of all devices within a broadcast domain, a VLAN is a broadcast domain made up of switches. You first create a VLAN and then assign ports to a VLAN. All ports in a single VLAN are in a single broadcast domain.

You do not have to configure VLANs unless your network is already using them. Some reasons why VLANs are used include:

- A LAN increases in size with several devices
- A LAN has increased broadcast traffic on it
- Groups of users on a LAN need more security

A VLAN ID, like an IP address or initiator name, is assigned a value to uniquely identify it on a network. A VLAN priority is set to determine what packet gets priority order within a VLAN.

To configure a VLAN ID/priority:

1. On the Network Configuration menu, select **Configure VLAN ID/Priority** and press **<Enter>**. The Configure VLAN ID/Priority dialog box appears.

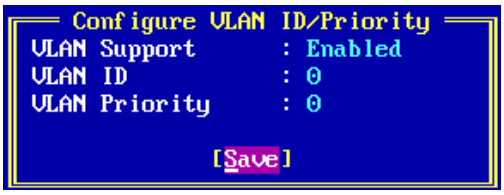

Figure 8-7 Configure VLAN/ID Priority Dialog Box

2. Select the VLAN Support drop-down menu and select **Enabled**.
3. Set a VLAN ID number. This is a unique value you assign to each VLAN on a single device. There are a maximum of 4095 possible values ranging from 0-4094.
4. Set a VLAN Priority, if necessary. This unique value assigns a priority to outbound packets containing a specified VLAN ID. Valid values range from 0 -7, with 0 the highest priority level.
5. Select **Save** and press **<Enter>**.
6. Press **<Esc>** to return to the Network Configuration menu.

Identifying a Port

Port identification, or beaconing, helps you physically determine which port you are configuring by blinking both the link and the activity LEDS of that port.

LEDs blink on the back of the server so that there is no confusion as to which physical port you are configuring with the iSCSISelect utility. Port identification allows you to correlate the iSCSI software configuration with the hardware port.

Note: Not all controllers have LEDs that are externally visible. If you are using an add-in card in a blade server environment, the port identification or beaconing capability does not work.

To identify a port, from the Controller Configuration menu, select **Port Identification** and press **<Enter>**. The LED status indicators for the selected port blink on the controller until you select **Done** and press **<Enter>** on the Port Identification screen.

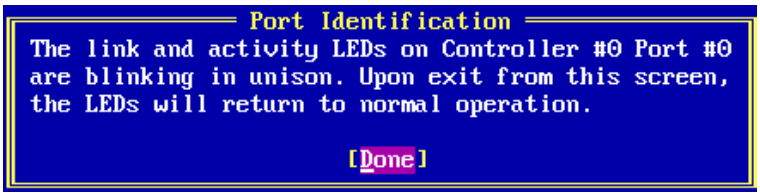

Figure 8-8 Port Identification Screen

Confirming Network Settings

After you configure the iSCSI initiator, confirm your network settings by pinging the network. The ping option checks whether the IP address is on the network. If there is another IP entity on that network when you ping, you receive a ping reply back to confirm the network settings. Ping can be a diagnostic tool but it is also a validation that your network is set up properly prior to target login.

To verify that a target is accessible and that you are connected to the network:

1. From the Network Configuration menu, select **Ping** and press **<Enter>**.
2. In the Ping Target dialog box, enter the IP address of the iSCSI device you want to ping. You are notified that the ping is successful. If the ping is unsuccessful you receive a failed message. For more information, see "Troubleshooting for the iSCSI Protocol" on page 157. Figure 8-9 is an example of a successful ping.

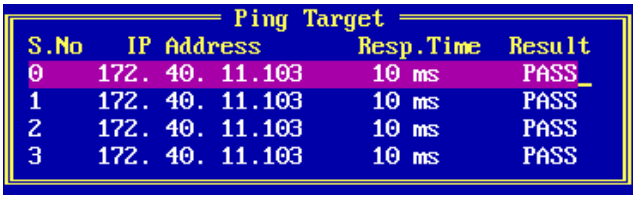

Figure 8-9 Successful Ping Screen

Note: The Ping works for any IP address that supports ICMP (Echo).

If you cannot verify the network interface, there may be a number of reasons why. For more information, see "Troubleshooting for the iSCSI Protocol" on page 157.

9. Configuring and Managing iSCSI Targets with the iSCSISelect Utility

An iSCSI target is any device that receives iSCSI commands. The device can be an end node, such as a storage device, or it can be an intermediate device, such as a bridge between IP and FC devices. Each iSCSI target is identified by a unique IQN, and each port on the controller (or on a bridge) is identified by one or more IP addresses.

As the client system, the initiator initiates disk I/O. It communicates with the target and the target serves the initiator by providing resources to the initiator.

Once you configure your iSCSI initiator and verified that your network interface is working, you can log into your target to establish your connection. To do this, you must:

- Perform a login to the target (adding a target)
- Ping a target and verify that you can connect to it
- Reboot the system

Adding iSCSI Targets

Once the initiator has been configured you need a process that shows you how to make an iSCSI target available to that initiator host. The discovery process presents an initiator with a list of available targets. The discovery methods used for discovering targets are:

- SendTargets discovery
- Manually configuring targets

With the iSCSISelect utility, you can easily configure an iSCSI target by selecting and enabling values on the Add/Ping iSCSI Target menu. From this menu, you can configure the target and perform a login to the target to establish an iSCSI network connection.

Before you begin the login session, gather the following information:

- iSCSI target name (only for manual configuration) – The target name that you are adding. The iSCSI target name is not required if you are using SendTargets discovery. It is required only for manually configured targets. This name should be known to you based on how you configured your iSCSI target. For more information, see “Using SendTargets Discovery to Add an iSCSI Target” on page 83.
- iSCSI target IP address – The IP address of the target into which you are logging.
- TCP port number – The TCP port number of the target portal. Typically this is 3260, which is the well-known port number defined for use by iSCSI.

Using SendTargets Discovery to Add an iSCSI Target

SendTargets discovery asks an iSCSI target to provide the list of target names that can be logged into by the initiator. The iSCSI initiator then uses the SendTargets Discovery option to perform the device discovery. Use this method if an iSCSI node has a large number of targets. When adding an iSCSI target, leave the iSCSI target name option blank, you can use the iSCSI SendTargets mechanism to add a target.

To configure an iSCSI target using the SendTargets discovery:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Select **Controller Configuration** and press **<Enter>**. A list of controllers is displayed.
3. Select a controller and press **<Enter>**. The Controller Configuration menu is displayed.

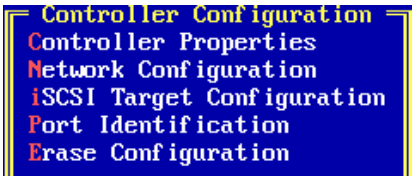

Figure 9-1 Controller Configuration Menu

4. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>**.
5. Select **Add New iSCSI Target** and press **<Enter>**.
6. In the Add/Ping iSCSI Target dialog box, leave the iSCSI Target Name blank for a SendTargets response.

   Note: Only the first 64 sessions are returned during a single discovery session.

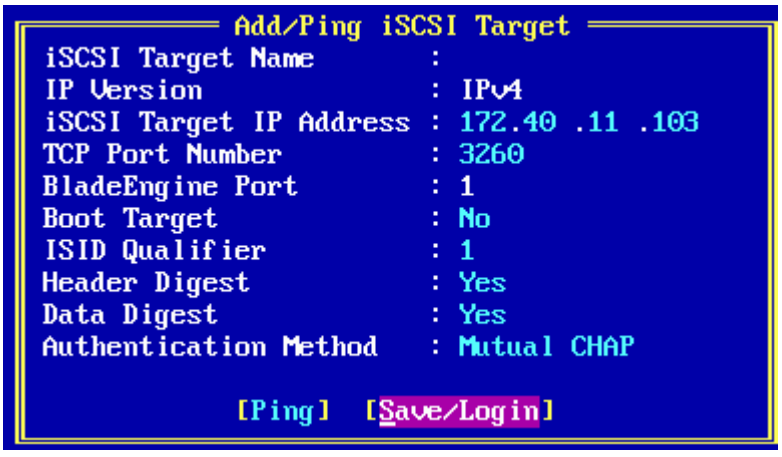

Figure 9-2 Add/Ping iSCSI Target dialog box

7. Enter the iSCSI target IP address.
8. Change the TCP port number value, if necessary. The default target port number is 3260.

9. For a boot target, accept the default (No), even if you want to enable the target as a boot target. For more information about the boot target, see "Setting Up a Basic iSCSI Boot Configuration" on page 73.

   Note: You must enable the Boot Target option after you add the target via SendTargets (see step 16).

10. Change the ISID qualifier value, if necessary. A unique ISID value is necessary if you connect dual sessions to the same target portal group. Enter a number up to 65535. For more information, see "Setting an ISID Value" on page 88.
11. Select **Yes** from the Header Digest drop-down menu if you want to enable header digest. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU's header segment is protected by CRC32C checksum. The default setting is No.
12. Select **Yes** from the Data Digest drop-down menu if you want to enable Data Digest. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU's data segment is protected by CRC32C checksum. The default setting is No.
13. Select an authentication method (optional). If you are enabling an authentication method, you are prompted to enter CHAP configuration. For more information, see "Enabling CHAP Authentication" on page 88.
14. Select **Save/Login**. A message reminds you that you have left the iSCSI Target name blank and that the SendTargets mechanism will be used. If you want to continue, press **<Y>**.
15. If the firmware successfully logs into the target, the Targets Discovered Via SendTargets screen appears. An unsuccessful login produces a failure message. After you send your SendTargets request to the target, the Targets Discovered Via SendTargets screen appears with a list of targets. From this list of targets specify which targets to add.

    To do this, select the target or targets you want to add from the menu and press **<F3>**. After you have selected your targets, you can add these targets to the list of iSCSI targets available for the initiator to login. To do this, select **Add Selected iSCSI Targets** and press **<Enter>** (Figure 9-3). If you enabled CHAP Authentication, you are prompted to enter CHAP configuration for each target, one at a time.For more information, see "Enabling CHAP Authentication" on page 88.

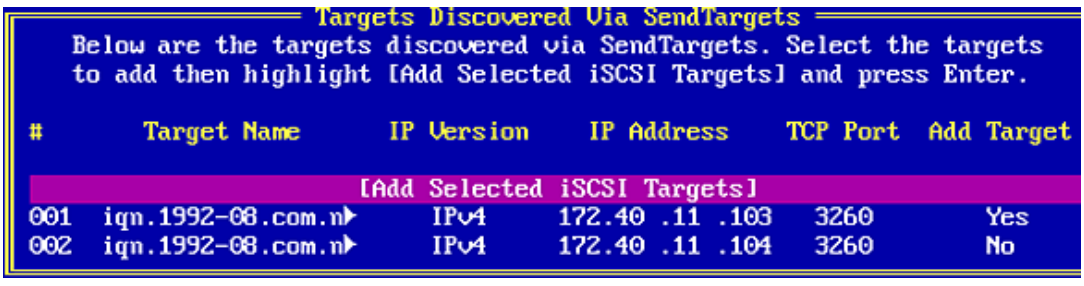

Figure 9-3 Targets Discovered via SendTargets Screen

16. After you have added your targets, from the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>** to view the added target information.

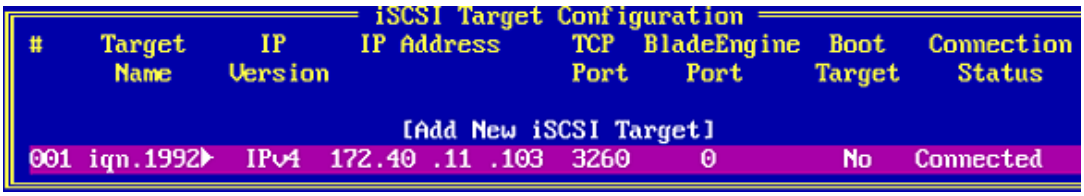

Figure 9-4 iSCSI Target Configuration Screen

Note: If you set the Boot Target option in step 5 before adding the target, the Boot Target displays No on this menu. To enable Boot Target, go to step 17.

17. To enable Boot Target or make any other changes to your target or targets, select the target and press **<Enter>**. The Edit/Ping iSCSI Target menu is displayed. From this menu, you can edit your target.

Manually Adding an iSCSI Target

Use this method if an iSCSI node has a small number of targets, or you want to restrict the targets that an initiator can access. To manually configure a target, you must provide the iSCSI target name.

To configure an iSCSI target manually:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Select **Controller Configuration** and press **<Enter>**. A list of controllers is displayed.
3. Select a controller and press **<Enter>**. The Controller Configuration menu is displayed.
4. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>**.
5. Select **Add New iSCSI Target** and press **<Enter>**. The Add/Ping iSCSI Target dialog-box is displayed (Figure 9-2).
6. Enter the iSCSI target name.
7. Enter the iSCSI target IP address.
8. Enter the TCP port number (the default target port number is 3260).
9. If you want to enable the target as a boot target, select **Yes**.
10. Enter an ISID Qualifier if needed. A unique ISID value is needed if you are connecting dual sessions to the same target portal group. You can enter a number up to 65535. For more information, see “Setting an ISID Value” on page 63.
11. Select **Yes** from the Header Digest drop-down menu if you want to enable Header Digest. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU’s header segment is protected by CRC32C checksum. The default setting is No.
12. Select **Yes** from the Data Digest drop-down menu if you want to enable Data Digest. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an

iSCSI PDU's data segment is protected by CRC32C checksum. The default setting is No.

13. Select the Authentication Method. For more information, see "Enabling CHAP Authentication" on page 88.
14. Select **Save/Login** and press **<Enter>**. If the firmware logs into the target successfully, you receive a successful login message. Press **<Esc>** to go to the iSCSI Target Configuration menu where you can view information about the added target.
15. To enable Boot Target or make any other changes to your target or targets, select the target and press **<Esc>**.

Managing an iSCSI Target

With the iSCSISelect utility you can manage a target by viewing target details or by editing the target configuration.

Viewing Target Information

After you have successfully logged into the target, you can view the details of the newly-added target or manage the target. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>** to view the target information.

Note: The iSCSISelect utility only shows LUN information for the first 128 LUNs.

The following is an example of a target detail.

Figure 9-5 iSCSI Target Configuration Information

In the iSCSI Target Configuration menu, the functions keys located at the bottom of the menu help you manage your target configuration.

- Press **<Enter>** to select the target configuration.
- Press **<Del>** to delete the target.
- Press **<F5>** to log in to the target.
- Press **<F6>** to log out of the target.
- Press **<F7>** to configure the LUN.
- Press **<Esc>** to return to the previous menu.

Editing a Target Configuration

Once you have added a target, you can edit your iSCSI target configuration or apply other management options to the target.

To edit a target configuration:

1. From the iSCSI Target Configuration dialog box, select the target and press **<Enter>**. The Edit/Ping iSCSI Target dialog box is displayed.

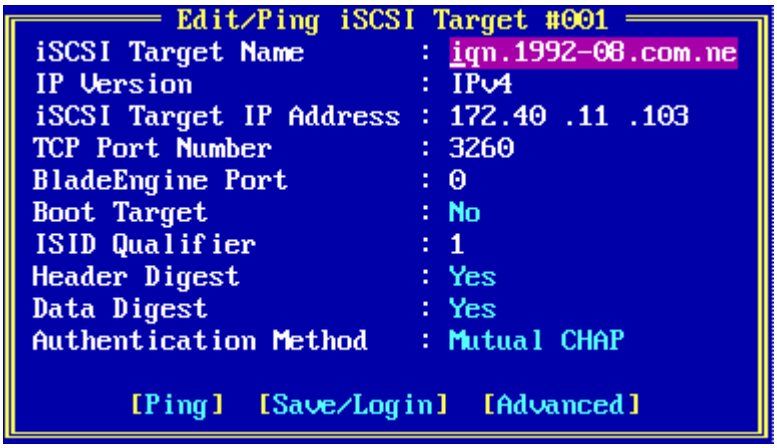

Figure 9-6 Edit/Ping iSCSI Target Dialog Box

2. If you want to enable the target as a boot target, select **Boot Target** and select **Yes** in the Boot Target drop-down menu.
3. You can set the ISID Qualifier on the Edit/Ping iSCSI Target dialog box by selecting **ISID Qualifier** and typing a number value up to 65535. A unique ISID value is required if you if you are connecting dual sessions to the same target portal group. For additional information, see "Setting an ISID Value" on page 88.
4. To enable the Header Digest, select **Yes** in the Header Digest drop-down menu. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU's' header segment is protected by CRC32C checksum. The default setting is No.
5. To enable the Data Digest, select **Yes** in the Data Digest drop-down menu. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU's data segment is protected by CRC32C checksum. The default setting is No.
6. To select an authentication method to use when logging into the target, select an authentication method from the Authentication Method drop-down menu. For more information about authentication methods, see "Enabling CHAP Authentication" on page 88.
7. To verify your target connection, select **Ping** and press **<Enter>**. For more information about ping, see "Adding iSCSI Targets" on page 82.
8. To view more target properties, select **Advanced** and press **<Enter>**. For more information on these properties, see "Viewing Advanced Target Properties" on page 92.
9. To save your changes, select **Save/Login** and press **<Enter>**.

   The iSCSI Target Configuration appears with the revised information.

Setting an ISID Value

The ISID qualifier is a unique ISID value to specify if you are connecting dual sessions to the same target portal group. This value ensures that you do not log into the same session twice. A combination of the initiator name, ISID qualifier, target name, and target portal group defines an iSCSI session. For the ISID qualifier, you can enter a number up to 65535.

To set the ISID Qualifier:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Select **Controller Configuration** and press **<Enter>**. A list of controllers is displayed.
3. Select a controller and press **<Enter>**. The Controller Configuration menu is displayed.
4. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>**.
5. Select **Add New iSCSI Target** and press **<Enter>**.
6. From the Add/Ping iSCSI Target dialog box, select **ISID Qualifier** and type in a numeric value.
7. To save your changes, select **Save/Login** and press **<Enter>**.

   The iSCSI Target Configuration appears with the revised information.

For more information on when an ISID value must be changed, see "Booting from SAN for iSCSI MPIO" on page 49.

Enabling CHAP Authentication

The iSCSISelect utility uses CHAP to authenticate initiators and targets for added network security. By using a challenge/response security mechanism, CHAP periodically verifies the initiator's identity. This authentication method depends on a secret known only to the initiator and the target. Although the authentication can be one-way, you can negotiate CHAP in both directions with the help of the same secret set for mutual authentication. You must make sure however, that what you configure on the target side, matches the initiator side. The iSCSISelect utility supports both one-way and mutual authentication.

Authenticating One-Way CHAP

With one-way CHAP authentication, the target authenticates the initiator. Use one-way CHAP authentication for a one-way challenge/response security method.

To enable one-way CHAP authentication:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.
2. Select **Controller Configuration**. A list of controllers is displayed.
3. Select a controller and press **<Enter>**. The Controller Configuration menu is displayed.
4. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>**.

5. Select **Add New iSCSI Target** and press **<Enter>**.
6. Follow steps 5–11 in the procedure "Using SendTargets Discovery to Add an iSCSI Target" on page 83.
7. In the Add/Ping iSCSI Target dialog box, select **Authentication Method**, select **One-Way Chap**, and press **<Enter>**.

Figure 9-7 One-way Chap Configuration Dialog Box

8. Enter the target CHAP name and target secret, then select **OK** and press **<Enter>**.

   The target CHAP name can be any name or sequence of numbers over 12 and less than 16 characters. However, the name and secret on the target side must match the name and target on the initiator side.

   The target secret can be in string (for example, abcdefg23456) or hexadecimal (for example, 0x0123456789012345678ABCD) format.

   - If using a string format, the secret can be any name or sequence of numbers over 12 and less than 16 bytes long, where each character equals one byte.
   - If using a hexadecimal format, the secret must be at least 12 and less than 16 bytes long, where two characters equal one byte. Hexadecimal formatting restrictions:
     - The 0x representation requires an even number of hexadecimal values excluding the 0x (0-9, A-F). For example, the secret 0x123456789012345678ABCD is not allowed because the character length is odd, with 23 hexadecimal values excluding the 0x. The secret 0x0123456789012345678ABCD is allowed, with 24 hexadecimal values excluding the 0x.
     - The hexadecimal representation of CHAP secrets must only contain hexadecimal values. The 0x representation must only have the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, and F. Any other characters are not allowed.

   When you have successfully enabled the CHAP authentication, the Add/Ping iSCSI Target dialog box appears. For more information, see "Pinging a Target" on page 91.

Authenticating Mutual CHAP

With mutual CHAP authentication, the target authenticates the initiator and the initiator authenticates the target. Use mutual CHAP authentication for a two-way challenge/response security method.

To enable mutual CHAP authentication:

1. Log into the iSCSISelect utility by pressing **<Ctrl+S>** when prompted.

2. Select **Controller Configuration** and press **<Enter>**. A list of controllers is displayed.
3. Select a controller and press **<Enter>**. The Controller Configuration menu is displayed.
4. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>**.
5. Select **Add New iSCSI Target** and press **<Enter>**.
6. From the Add/Ping iSCSI Target dialog box, select **Authentication Method** and select **Mutual Chap**, and press **<Enter>**. The CHAP Configuration dialog box is displayed.

Figure 9-8 Mutual CHAP Configuration Dialog Box

7. Enter the target CHAP name, target secret, initiator CHAP name, and initiator secret. Select **OK** and press **<Enter>**.

   The target/initiator CHAP names can be any name or sequence of numbers over 12 and less than 16 characters. However, the name and secret on the target side must match the name and target on the initiator side.

   The target/initiator secret can be in string (for example, abcdefg23456) or hexadecimal (for example, 0x0123456789012345678 9ABCD) format.

   - If using a string format, the secret can be any name or sequence of numbers over 12 and less than 16 bytes long, where each character equals one byte.
   - If using a hexadecimal format, the secret must be at least 12 and less than 16 bytes long, where two characters equal one byte. Hexadecimal formatting restrictions:
     - The 0x representation requires an even number of hexadecimal values excluding the 0x (0-9, A-F). For example, the secret 0x123456789012345678 9ABCD is not allowed because the character length is odd, with 23 hexadecimal values excluding the 0x. The secret 0x0123456789012345678 9ABCD is allowed, with 24 hexadecimal values excluding the 0x.
     - The hexadecimal representation of CHAP secrets must only contain hexadecimal values. The 0x representation must only have the following characters: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, a, b, c, d, e, f, A, B, C, D, E, and F. Any other characters are not allowed.

   When you have successfully enabled the CHAP authentication, the Add/Ping iSCSI Target dialog box appears.

Pinging a Target

There are different ways to ping a target. For instance, you can ping a target from the Network Configuration menu, or you can ping a target from the Controller Configuration menu.

From the Network Configuration Menu

1. From the Network Configuration menu, select **Ping** and press **<Enter>**. The Ping Target dialog box opens.

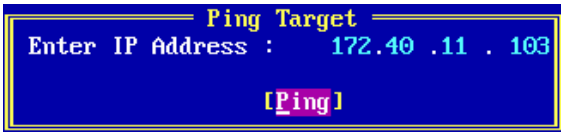

Figure 9-9 Ping Target Dialog Box

2. Enter the IP address of the target you want to ping.
3. Select **Ping** and press **<Enter>**.

From the Controller Configuration Menu

1. From the Controller Configuration menu, select **iSCSI Target Configuration** and press **<Enter>**.
2. Select **Add/Ping iSCSI Target** or **Edit/Ping iSCSI Target** and press **<Enter>**. The "iSCSI Target IP Address" is the address that will be pinged.
3. From the Add/Ping iSCSI Target dialog box (Figure 9-2) or the Edit/Ping iSCSI Target dialog box (Figure 9-6), select **Ping** and press **<Enter>**.

   If the ping is successful, you are notified that the ping is successful. Figure 9-10 is an example of a successful ping.

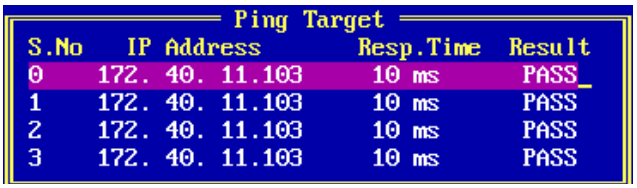

Figure 9-10 Successful Ping Screen

   If the ping is unsuccessful you receive a failed message. There are several reasons for an unsuccessful ping. For more information see "Troubleshooting for the iSCSI Protocol" on page 157.

Viewing Advanced Target Properties

After you have logged into a target, you can view more information about that target.

To view more information about the target, from the Edit/Ping iSCSI Target dialog box, select the **Advanced** option and press **<Enter>**. Advanced information is displayed.

Figure 9-11 Advanced Target Properties Screen

Configuring LUN Settings

A LUN represents an individually addressable logical device that is part of a target. An initiator negotiates with a target to establish connectivity to a LUN.

To configure a LUN:

1. From the iSCSI Target Configuration screen, press **<F7>** to display the LUNs associated with the iSCSI node.

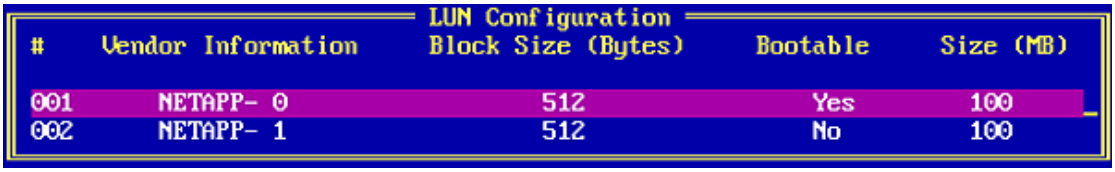

Figure 9-12 LUN Configuration Menu

2. Press **<F3>** to set the boot LUN if the target is a boot target. By setting the LUN to bootable, you can confirm that you have the boot target configured properly and see what LUN you are booting from. By looking at the LUN size, you can also determine which target is which along with the LUN order.

   Note: The LUN order is determined by the target and is in the order listed. The boot LUN must be one of the first eight LUNs on the target.

If there are no LUNs available, the following message is displayed:

```
No LUN available, please check your configuration on the Target.
```

For more information, see “Troubleshooting for the iSCSI Protocol” on page 157.

Removing and Logging Out and In of a Configured Target

If you remove or delete a target, you log out of the target and remove it from the list of targets.

To remove a target, from the iSCSI Target Configuration screen, select the target and press the **<Delete>** key.

If you log out of a target, you log out of the target but the target is listed in the target list with the connection status of disconnected. With a logout, you are only deleting the target session. If you have logged out of a target, you can perform a login.

To log out of a target, from the iSCSI Target Configuration screen, select the target and press **<F6>**.

To log into a target, from the iSCSI Target Configuration screen, select the target and the disconnected target, and then press **<F5>** to establish the target session.

Booting the System

After you have configured the iSCSI initiator and target, you must reboot the system for the configurations to take effect. When you exit the iSCSISelect utility, the system automatically reboots and during system startup, the OneConnect BIOS is displayed. For example:

```
Controller#0 Port#0 Base 0xFCE60000 at Bus:01 Dev:00 Fun:02
Controller#0 Port#1 Base 0xFCEA0000 at Bus:01 Dev:00 Fun:03

<<< Press <Ctrl><S> for iSCSISelect(TM) Utility >>>

Initiator iSCSI Name:  iqn.2004-05.com.emulex
Initiator IP Address:  172. 40.  1.41
Initiator IP Address:  172. 40.  1.62
BIOS Not Installed.
```

Note: The iSCSI BIOS logs into the configured iSCSI boot target and shows its target/LUN information in the BIOS sign-on banner only if you have configured an iSCSI boot target. For more information, see "Setting Up a Basic iSCSI Boot Configuration" on page 73.

Erasing the Configuration

Erase Configuration erases the configuration of a single controller. Configuration data is erased for both ports on the selected controller. The initiator name is global for all OneConnect controllers in the system. If you have more than one controller and you erase the configuration on the first controller, the Erase Configuration option resets the initiator name back to their default values. If you erase the configuration on the second controller, the default values are only reset for the second controller and are not reset globally on both controllers.

Note: You must select **Erase Configuration** to clear out existing IQN data if you purchase a different or subsequent license for the adapter.

To erase a controller configuration:

1. From the Controller Configuration menu, select **Erase Configuration** and press **<Enter>**.
2. A message appears asking if you want to erase the current configuration. Type **<Y>**.
3. You are cautioned that the operation removes any existing configuration permanently. Type **<Y>**.

   When the controller configuration is erased, the Controller Configuration menu is displayed.

Discovering Targets through DHCP for iSCSI

For your target to be discovered by the initiator through DHCP, you must add the root path to the DHCP server:

1. From the DHCP server screen, select **Scope Options**, then right-click and select **Configure Options**.

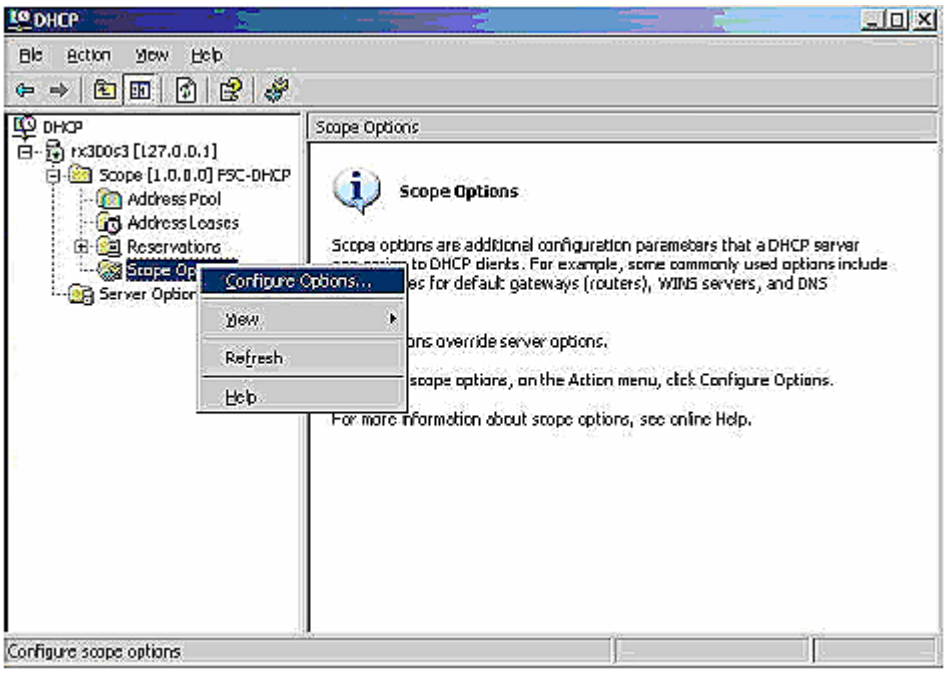

Figure 9-13 DHCP Server Screen

2. From the General tab, scroll down the list of available options and select **017 Root Path**.

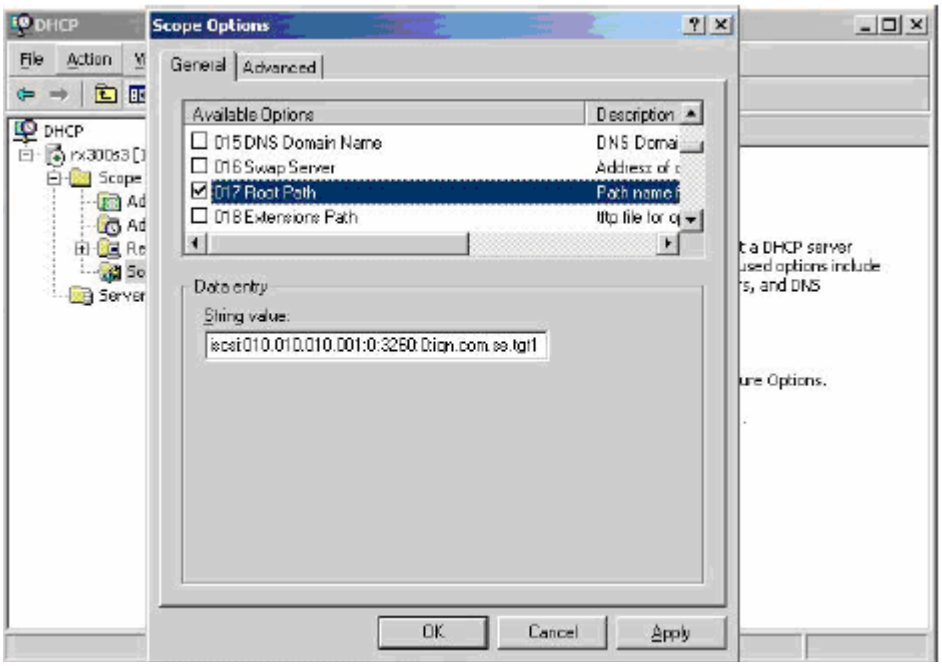

Figure 9-14 DHCP Server Scope Options

3. In the String Value box, add the location of the iSCSI target you want to use for iSCSI boot. Enter the string in the following format:

   ```
   iscsi: <ipaddress>:<protocol>:<iscsi port number>:<luns><target name>
   ```

   For example:

   ```
   iscsi:010.010.010.001:0:3260:0:iqn.1992-08.com.netap:sn.15729740
   ```

4. Click **Apply**. The DHCP server screen is ready to discover boot targets.

Enabling DHCP Discovery Through the iSCSISelect Utility

If your DHCP server supports DHCP discovery and you added the root path to the DHCP server, you can enable Discover Boot Target via DHCP using the iSCSISelect utility. By enabling Discover Boot Target via DHCP, you can use DHCP discovery to provide the boot path from the DHCP server.

Note: If you leave Discover Boot Target via DHCP disabled (default), you must manually configure iSCSI boot.

To enable DHCP discovery through iSCSISelect:

1. After configuring the iSCSI Initiator Name, select **Controller Properties** from the Controller Configuration screen and press **<Enter>**.

2. From the Controller Properties screen, select **Discover Boot Target via DHCP** and press **<Enter>**. Enable the function by selecting **Enabled** from the drop-down menu and press **<Enter>**.
3. Select **Save** and press **<Enter>**.

10. Configuring UEFI for Ethernet

Overview

UEFIBoot supports:

- Multi-topology: Fabric point to-point; FC-AL: private loop and public loop.
- EFI protocols: Configuration, component name, diagnostics and firmware updates are supported.
- Operating systems: Windows Server 2008, Windows Server 2012, Red-Hat Linux 6, SLES 11, and SLES 11 SP1
- Multi-Device path: Fibre/SCSI device path is selectable through the driver configuration protocol.
- Multi-initiators: Up to 128 adapters in a system.
- Multi-boot: Eight targets are selectable through the driver configuration protocol.
- Multi-LUNs: Up to 4096 LUNs
- Multi-mode: Supported.
- Multi-utility: Setup and firmware updates are supported.

This version of UEFIboot is loaded from flash into system memory.

When UEFIBoot is loaded in an EFI Shell, type "`drivers`" and press **<Enter>** to see if the driver is loaded.

Loading UEFIBoot

The UEFI boot code is distributed with the firmware in a .UFI file. This file may be downloaded to a NIC or FCoE adapter through the HII interface in the NIC UEFI code.

Unloading UEFIBoot

To unload UEFIBoot:

1. View Emulex driver handle information by typing "`drivers`" and pressing **<Enter>** at the shell prompt. A list of drivers is displayed.

```
E1 0000000A B - -  2  3 Partition Driver(MBR/GPT/El Torito) FvFile(43B93232-AF
E2 0000000A B - -  1 48 PCI Bus Driver                      FvFile(93B80004-9F
E7 0000000A D - -  1  - SCSI Bus Driver                     FvFile(0167CCC4-D0
E8 0000000A ? - -  -  - Scsi Disk Driver                    FvFile(0A66E322-37
EF 00000001 D - -  1  - Vitesse VSC452 SIO Driver           FvFile(BBA81468-FF
F1 0000000A D - -  4  - Simple Network Protocol Driver      FvFile(A2F436EA-A1
F2 0000000A D - - 16  - UEFI PXE Base Code Driver           FvFile(3B1DEAB5-C7
F4 0000000A D - -  4  - PXE DHCPv4 Driver                   FvFile(A46C3330-BE
F5 0000000A B - -  4 12 MNP Network Service Driver          FvFile(025BBFC7-E6
F6 0000000A B - -  4 28 IP4 Network Service Driver          FvFile(9FB1A1F3-3B
F7 0000000A B - -  4  4 DHCP Protocol Driver                FvFile(94734718-0B
F8 0000000A D - -  4  - IP4 CONFIG Network Service Driver   FvFile(26841BDE-92
F9 0000000A D - -  4  - Tcp Network Service Driver          FvFile(6D6963AB-90
FA 0000000A B - - 24 20 UDP Network Service Driver          FvFile(6D6963AB-90
FB 0000000A D - -  4  - ARP Network Service Driver          FvFile(529D3F93-E8
FC 0000000A B - -  8  4 MTFTP4 Network Service              FvFile(DC3641B8-2F
FD 0000000A ? - -  -  - UEFI PXE Configuration Driver       FvFile(0C086DB5-AA
11C 00050212 B X X  1  1 Broadcom Gigabit Ethernet Driver    Offset(12000,231FF
11E 00050212 B X X  1  1 Broadcom Gigabit Ethernet Driver    Offset(12000,231FF
122 000221A5 B - X  2  2 Emulex 10G NIC                      Offset(8000,169FF)
126 000100AF D - -  2  - Emulex iSCSI Boot Driver            Offset(10000,1A5FF
143 030A0001 D X X  1  - LSI Logic Fusion MPT SAS Driver     Offset(B200,247FF)
147 00000019 ? - -  -  - G200eV Matrox Graphics UEFI Driver  Offset(8000,D1FF)
```

Figure 10-1 Driver Listing

2. Write down the Emulex NIC and iSCSI driver handles. For the above case, the Emulex NIC driver handle is 122 and the Emulex iSCSI driver handle is 126.
3. To unload the Emulex NIC driver in the previous example, type "`unload 122`" and press **<Enter>**.
4. To unload the Emulex iSCSI driver in the previous example, type "`unload 126`" and press **<Enter>**.

Using the Emulex NIC Configuration Utility

Navigating the Utility

Use the following methods to navigate the Emulex NIC configuration utility:

- Press the up/down arrows on your keyboard to move through menu options or fields. When multiple adapters are listed, use the up/down arrows to scroll to the additional adapters.
- Press the **<+>**, **<->**, or **<Enter>** keys to change numeric values.
- Press **<Enter>** to select a menu option, to select a row in a configuration screen, or to change a configuration default.
- Use the navigation entries on the page to move about the utility.
- Press **<Esc>** to exit the current screen and show the previous screen.

Downloading the Latest Firmware and Boot Code

A single firmware image contains the latest version of the firmware and boot code. Depending on the OEM UEFI configuration, the Emulex NIC configuration utility may appear under different setup menus in OEM system firmware or BIOS (such as **System Settings > Network Device List**).

Firmware Components

The ELX UNDI driver implements the PXE UNDI applications programming interface (API) services used by the Simple Network Protocol (SNP) driver during PXE boot and while executing a network bootstrap program (NBP). The boot hardware abstraction layer (HAL) provides the OneConnect input/output control (IOCTL) interface API for the UNDI driver.

The firmware and UEFI NIC/FCoE drivers are contained in one image file with the .UFI extension. This file must be flashed through the NIC interface exposed by the Human Interface Infrastructure (HII).

Viewing the Adapter's Firmware and Boot Code Version

Start the Emulex NIC configuration utility via the HII:

1. Exit the EFI shell.

Figure 10-2 Exiting the EFI Shell

2. The Network screen shows a list of the adapters in the system. Your list may vary depending on the installed adapters. Locate the adapter. Use the up/down arrows on your keyboard to select it, and press **<Enter>**.

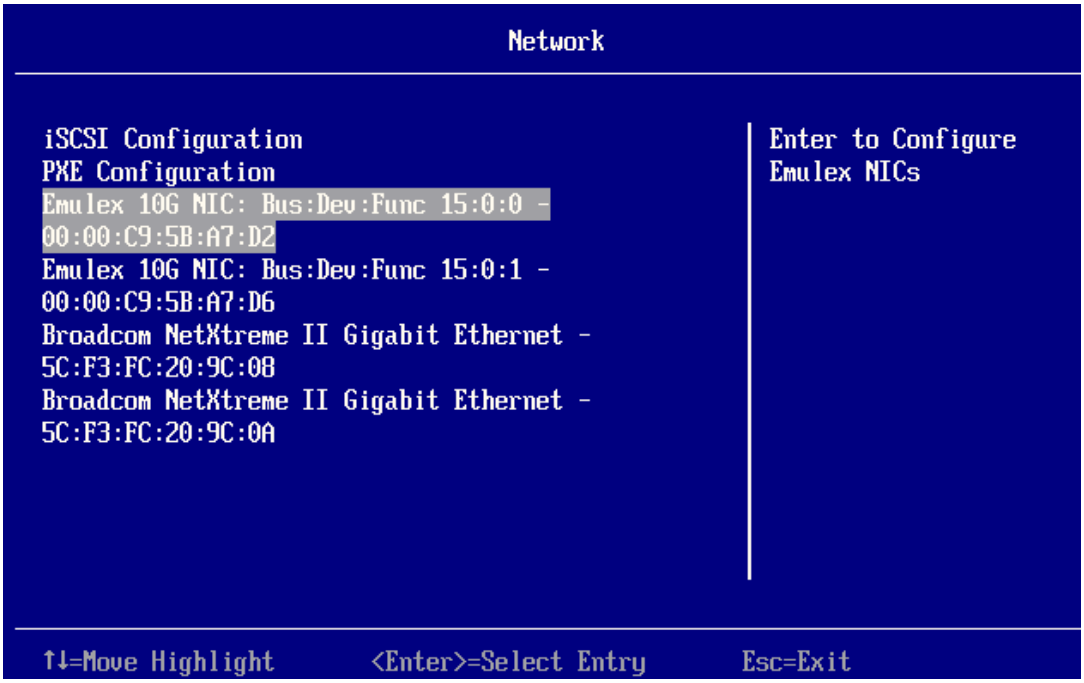

Figure 10-3 Emulex NIC Configuration Utility Network Screen

The Emulex NIC Selection screen shows the current firmware version for the selected adapter. This screen also has a link to the Emulex Flash Update Utility.

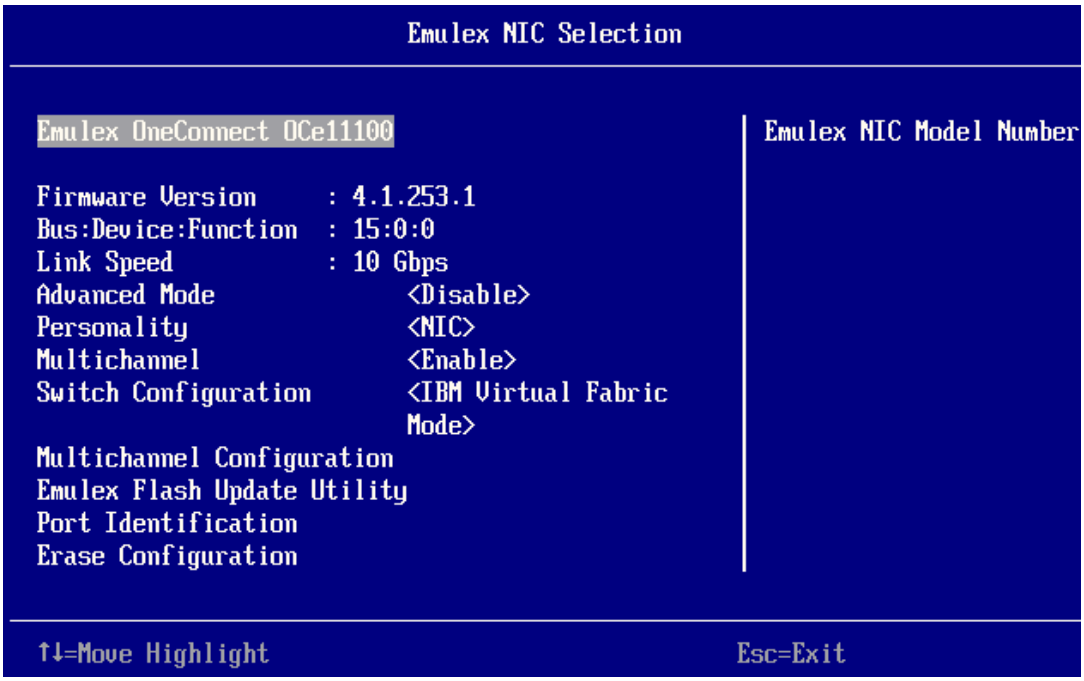

Figure 10-4 Emulex NIC Selection Screen

3. Press **<Esc>** until you exit the utility.

Downloading Firmware and Boot Code

To download firmware and boot code:

1. In an open UEFI shell, copy the firmware and boot code file into a directory on the EFI partition media.

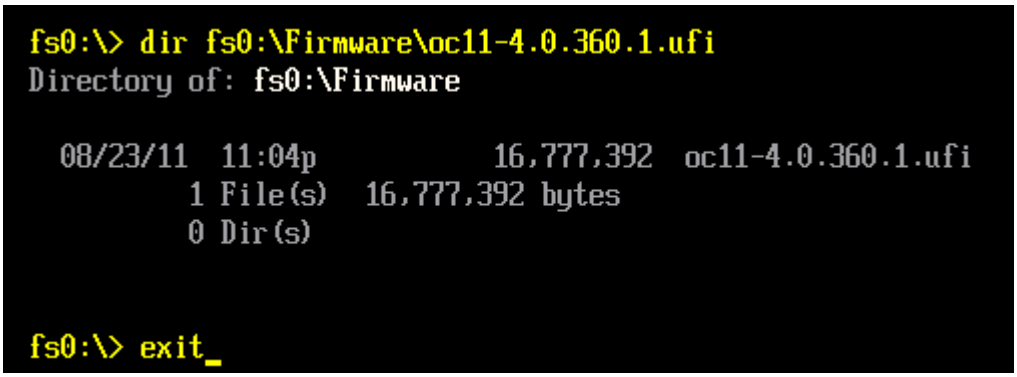

Figure 10-5 EFI Shell with Firmware and Boot Code File

2. Exit the UEFI shell and launch the Emulex NIC configuration utility.
3. From the Network device list, select the NIC adapter you want to modify and press **<Enter>**.
4. The Emulex NIC Selection screen (Figure 10-4) shows information for the selected adapter. Select **Emulex Flash Update Utility** and press **<Enter>**. The Emulex Flash Update Utility screen is displayed. This utility displays all available media and installs the flash file on the adapter.

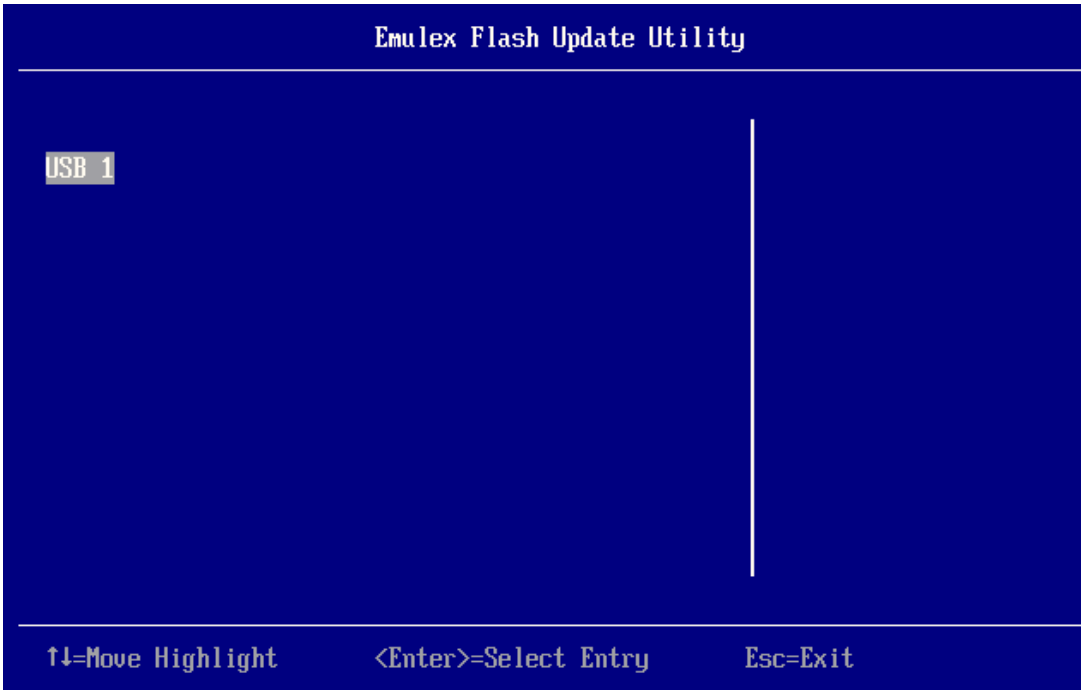

Figure 10-6 Emulex Flash Update Utility

5. Press **<Enter>** to select the media containing the flash file.

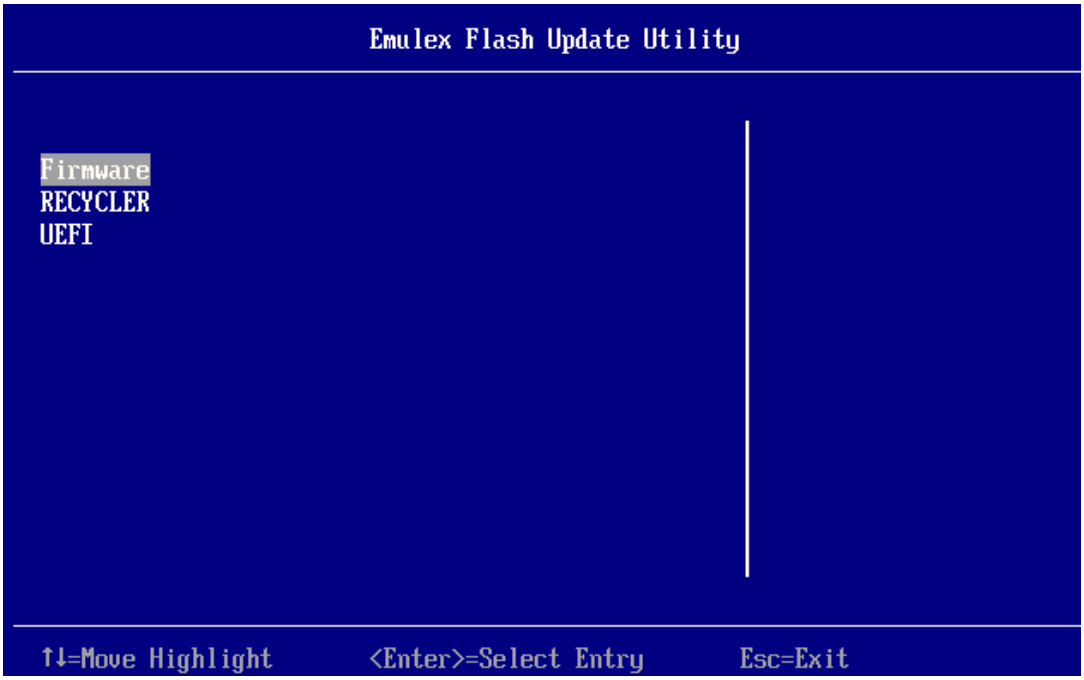

Figure 10-7 Emulex Flash Update Utility with Directory Name Dialog Box

6. Navigate to the directory containing the flash file and press **<Enter>**.

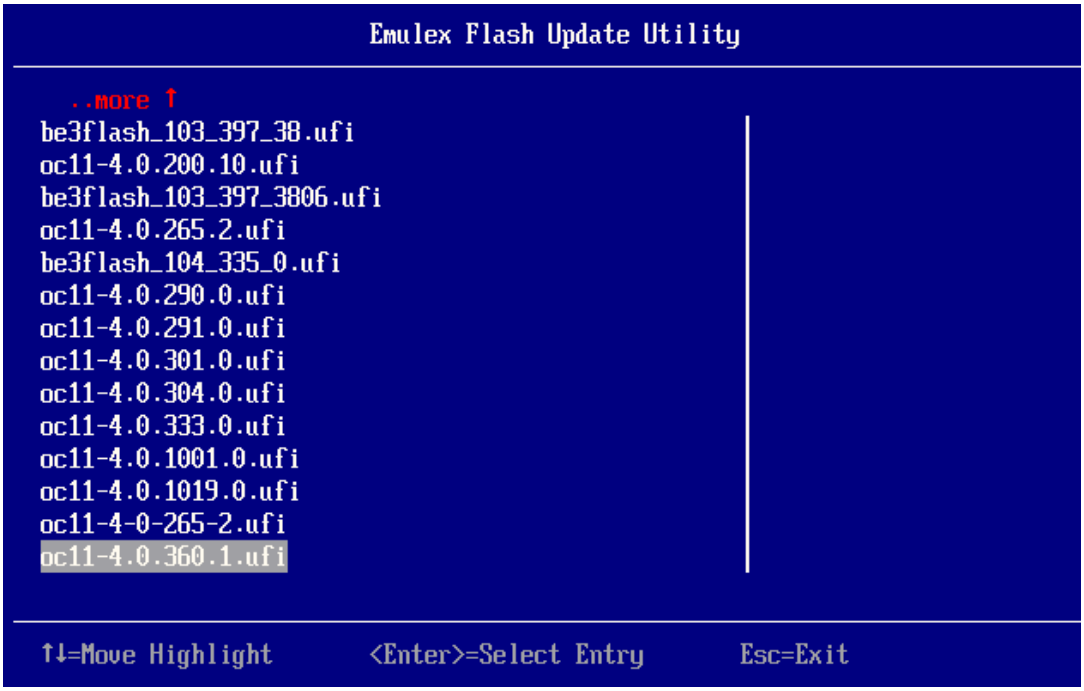

Figure 10-8 Emulex Flash Update Utility with Flash File Name Dialog Box

7. Use the arrow keys to select the flash file and press **<Enter>** to begin the update process. It takes about two minutes to complete.

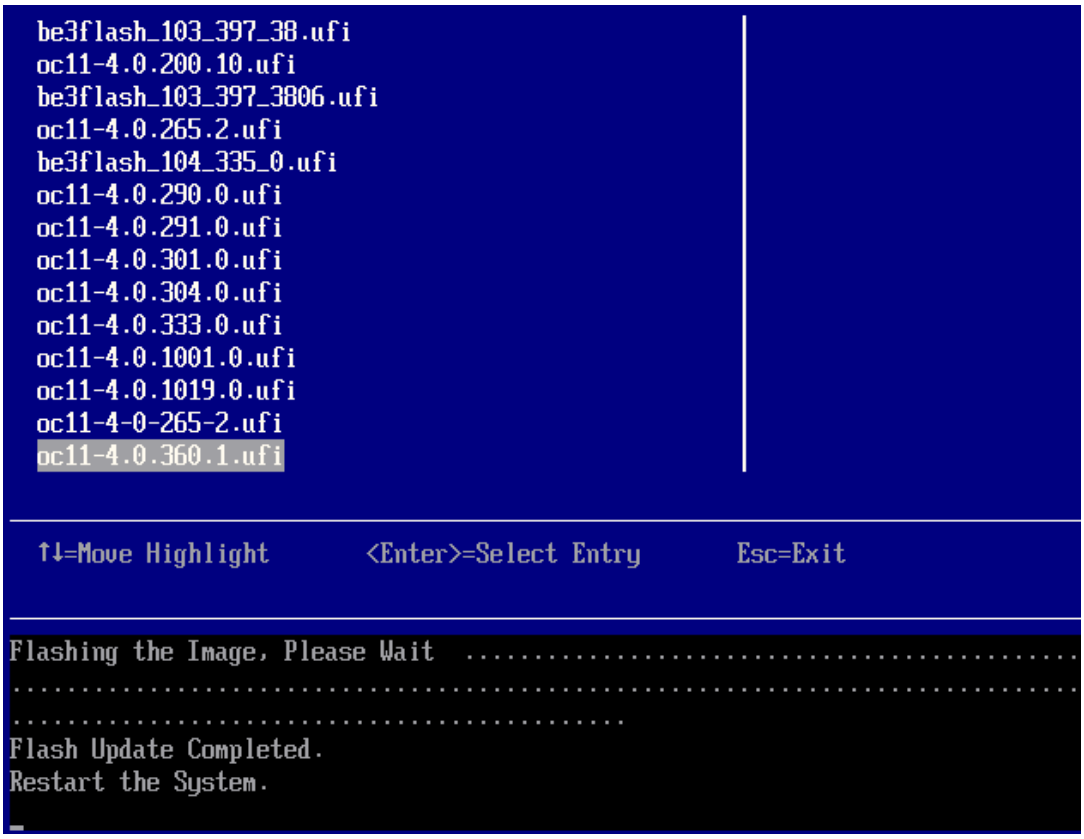

Figure 10-9 Emulex Flash Update Utility, Flash Updating

8. Reset the system. The latest version information for the adapter is displayed in the Emulex NIC Selection screen (Figure 10-4).

Configuring Advanced Mode Support

Advanced Mode is a driver compatibility option. With Advanced Mode enabled, you can run "advanced" drivers that have advanced options, including 4-port support and increased offload and virtualization capabilities. With Advanced mode disabled, you can run older drivers with later versions of the firmware.

Note: Advanced Mode support is available with OCe11100-series 2-port (the default setting is disabled) and 4-port controllers (the default setting is enabled). The Advanced Mode capability is not supported on OCe10100-series controllers (the default setting is disabled). Compatibility with legacy drivers requires that Advanced Mode Support be disabled.

Note: On some 4–port-series LAN on motherboard (LOM) platforms, the Advanced Mode capability is not provided in the HII interface. The Advanced Mode capability on these platforms is implicitly enabled by default and Advanced Mode-aware drivers must be implemented to fully utilize the advanced features of this functionality. Legacy Mode drivers will fail in creating the network interfaces on these platforms.

Table 10-1 Advanced Mode Capabilities (by Operating System)

Operating System	Advanced Mode Enabled	Advanced Mode Disabled (Legacy Mode)
Windows	16 RSS queues **Note:** Only supported on Windows 2008 R2 and Windows Server 2012. Remains four queues for earlier Windows versions.	4 RSS Queues
	VMQ lookahead split **Note:** VMQs are only supported on Windows 2008 R2 and later.	Lookahead split is silently ignored. There may be a small performance penalty for VMQs.
	4-port	2-port
Linux and Citrix	4-port	2-port
	16 RSS Queues	4 RSS Queues
	VFs/PFs can be increased up to 30	
ESX	4-port	2-port
	For both 1500 and 9000 MTU: 16 NQs/PFs in non-VFA 4 NQs/PFs in VFA	1500 MTU – 8 NQ/PF in non-VFA and 4 NQ/PF in VFA. 9000 MTU – 4 NQ/PF in both VFA and non-VFA

For OCe11100-series UCNAs, the overall chip-wide maximum number of VFs is 60 (or 30 per port):

- Legacy Mode TOTAL VF Count = 30 (or 15 per port on 2-port adapters)
- Advanced Mode TOTAL VF Count = 60 (or 30 per port on 2-port adapters)

To enable Advanced Mode support:

1. On the Emulex NIC Selection Screen, select **Advanced Mode** and press **<Enter>**. The Advanced Mode dialog box appears.

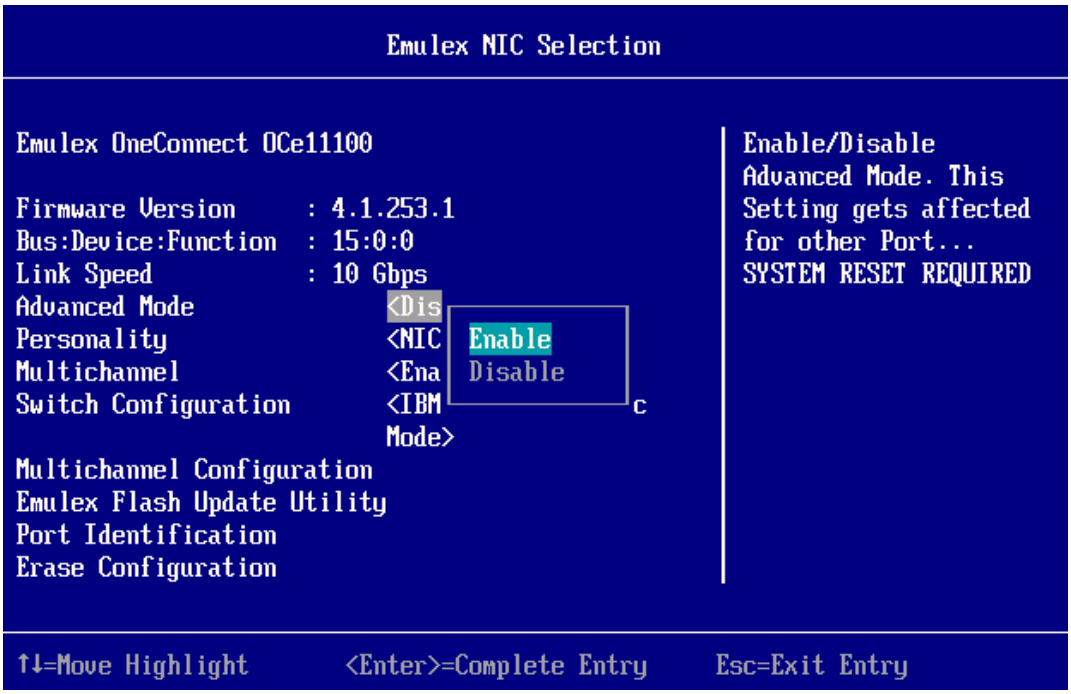

Figure 10-10 Advanced Mode Dialog Box

2. Select **Enable** and press **<Enter>**.
3. Reboot the system.

Note: Changing the Advanced Mode setting requires a reboot.

Configuring Personality

The "personality" reflects the protocol or protocols of the adapter. This option specifies a list of available protocols that can be configured on an adapter. Depending on the personality for which the adapter is licensed, one of the following selections appears:

- NIC (iSCSI and FCoE are not allowed)
- NIC and iSCSI (FCoE is not allowed)
- NIC, iSCSI, and FCoE

The NIC personality implies that all the enabled functions provide NIC/TOE functionality. iSCSI and FCoE personalities are enabled on one function per OneConnect port and include NIC functionality on the other enabled functions.

To view the personalities supported on the adapter, select **Personality** on the Emulex NIC Selection Screen, and then press **<Enter>**. The Personality dialog box appears with a list of available personalities.

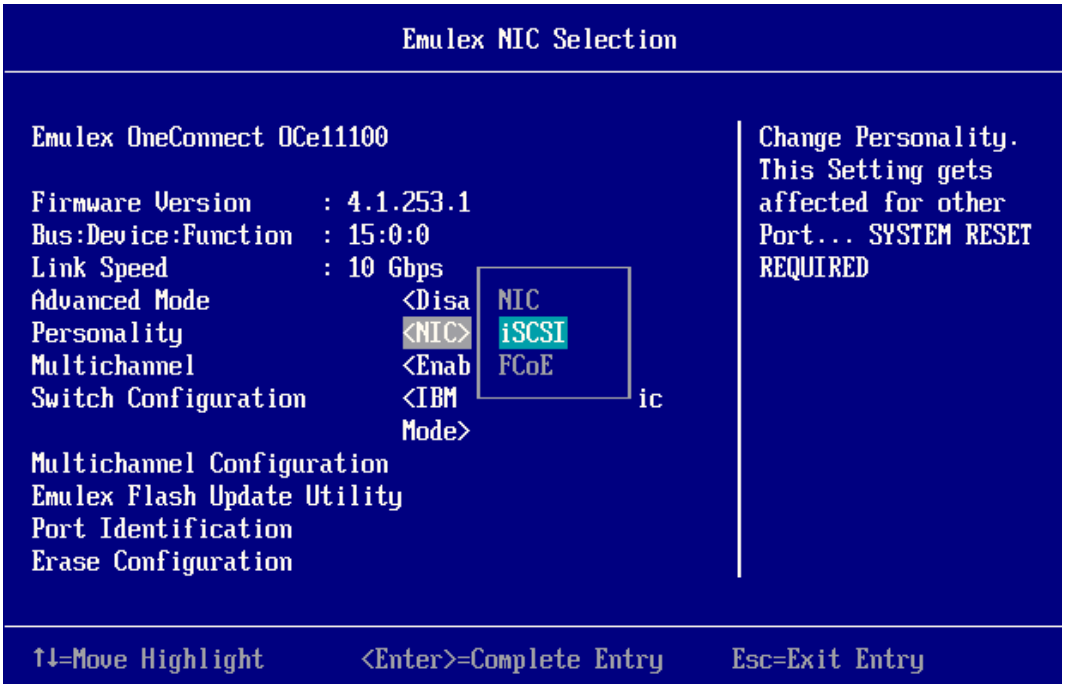

Figure 10-11 Personality Dialog Box

To change the personality of the adapter:

1. On the Emulex NIC Selection Screen, select **Personality** and press **<Enter>**. The Personality dialog box appears.
2. Select the desired personality from the drop-down menu and press **<Enter>**.

Note: Changing the Personality setting requires a reboot. No further configuration changes can be performed on the adapter until the system has been rebooted.

Configuring Multichannel Support

Note: This option is only available on Emulex OneConnect OCe11100-series UCNAs.

Multichannel, also known as universal multichannel (UMC), provides the ability to configure multiple PCI functions or I/O channels for each OneConnect port. Setting up multichannel may or may not depend on cooperation with adjacent switches. For additional information on multichannel support, see appendix E., "Multichannel for OneConnect OCe11100-series UCNAs," on page 189.

If multichannel functionality is supported on your system, the Emulex UEFI NIC utility enables you to perform the following tasks:

- Enable or disable multichannel functionality
- Enable or disable each logical link
- Configure the bandwidth and Logical Port VLAN ID (LPVID) for each channel.

Note: Your system may not support all multichannel options.

To enable multichannel support:

1. On the Emulex NIC Selection screen, select **Multichannel** and press **<Enter>**. The Multichannel dialog box appears.

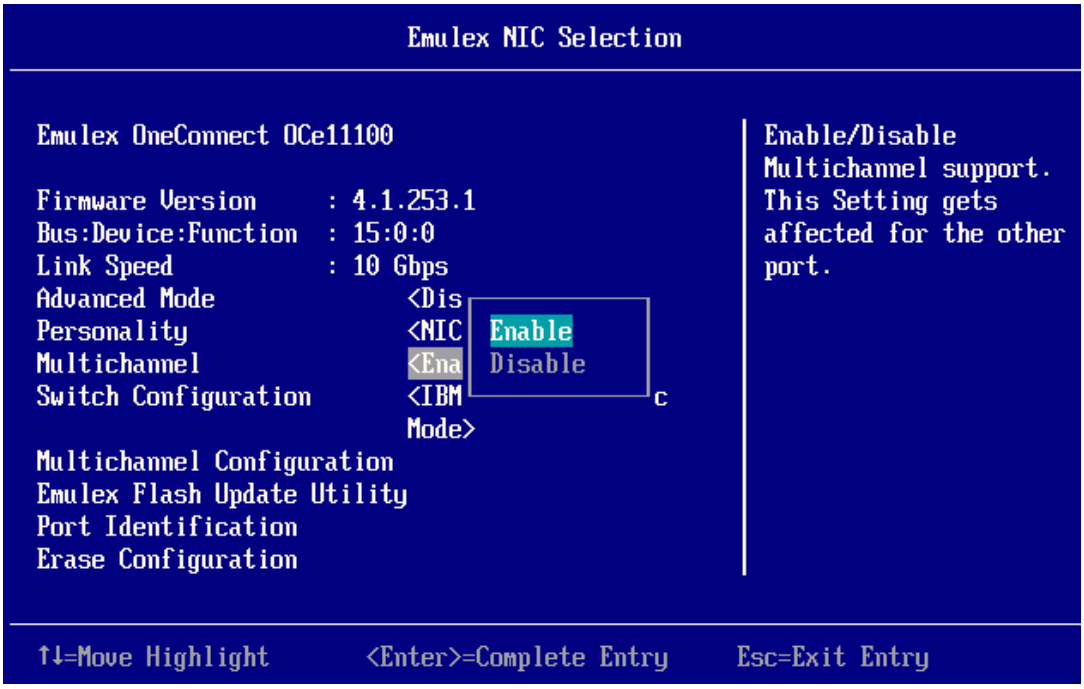

Figure 10-12 Multichannel Dialog Box

2. Select **Enable** to activate multichannel support and press **<Enter>**.

   Note: Additional configuration changes to the adapter cannot be performed until the system has been rebooted.

   Once your system reboots, you can proceed to configure multichannel support.

To configure multichannel support:

1. On the Emulex NIC Selection screen, select **Multichannel Configuration** and press **<Enter>**. A list of functions that are available for configuration is displayed.

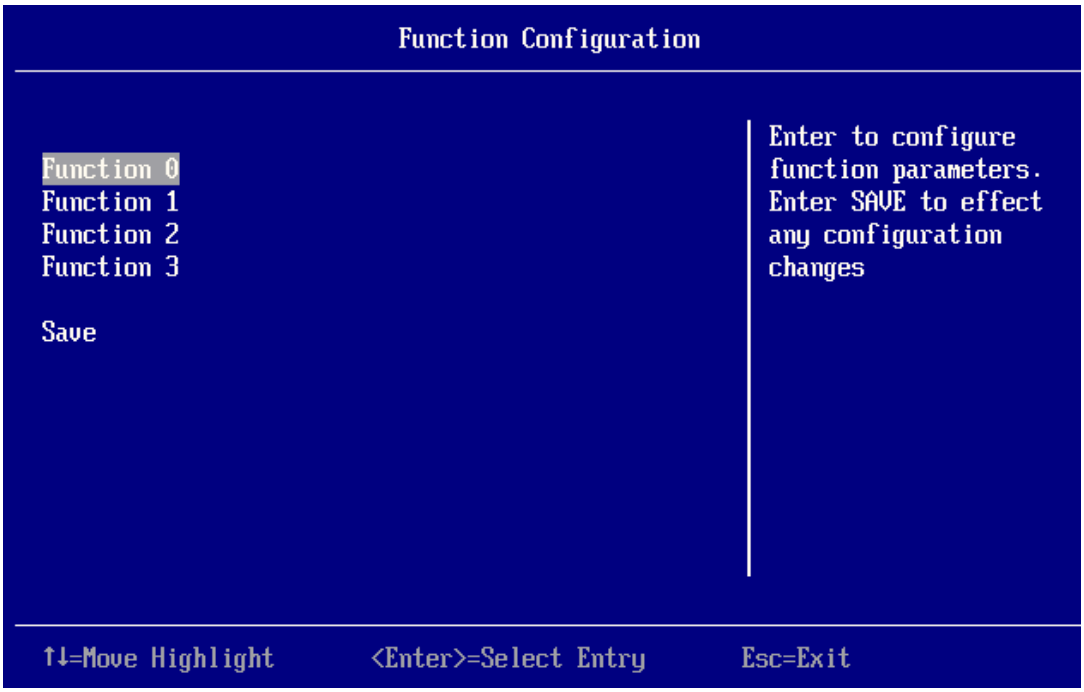

Figure 10-13 Function Configuration Screen

2. Select the function you want to configure and press **<Enter>**. The Multichannel Configuration screen for that specific function appears.

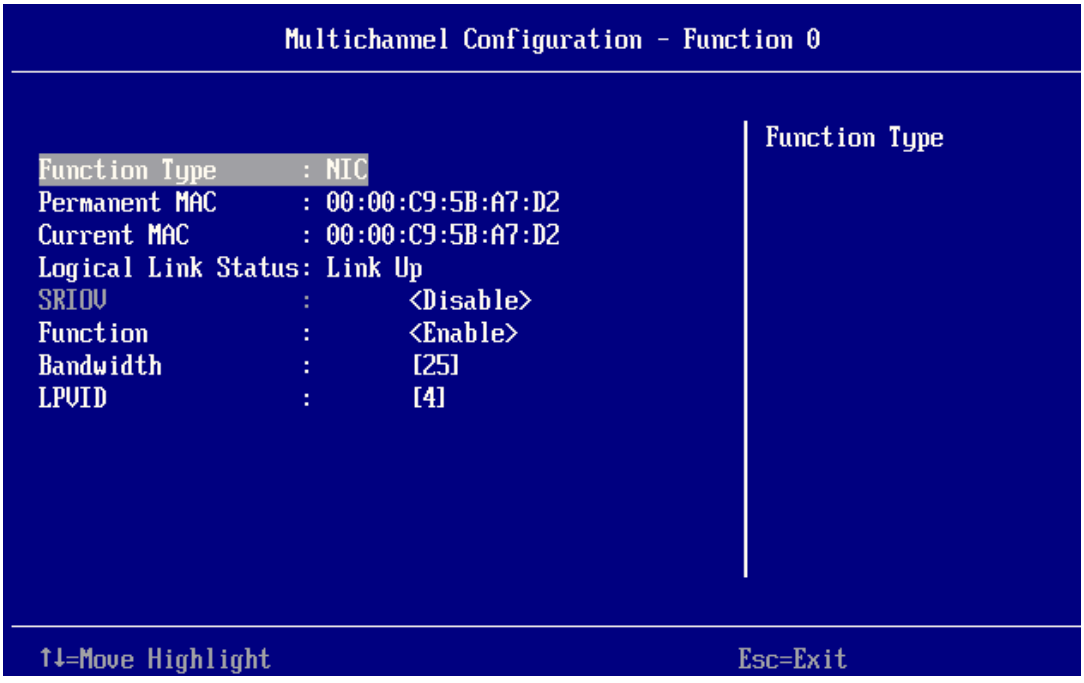

Figure 10-14 Multichannel Configuration for Function 0 Screen

From the Multichannel Configuration screen for that specific function, you can enable or disable a logical link, and configure the bandwidth percentage and LPVID.

To enable or disable a logical link:

a. Select the appropriate option and press **<Enter>**.
b. From the drop-down menu, select **Enable** or **Disable** and press **<Enter>**.

If you are configuring bandwidth, it must total 100% across all the functions on the selected port.

If you are configuring LPVID, set a LPVID number from 2-4094. A value of 0 represents LPVID as disabled.

Note: An LPVID is not required for "IBM Virtual Fabric Mode", but it is required for every function when using "Switch Independent Mode".

For more information on using LPVID, see "Configuring LPVID" on page 28.

Note: SR-IOV support can only be enabled if multichannel support is disabled.

Note: Your system may not support all multichannel options.

3. Press **<Esc>** to return to the list of functions. LPVIDs for other functions can be configured similarly.
4. To save the configurations, select **Save** and press **<Enter>**.

Configuring the Switch

A vNIC switch provides the ability to configure an LPVID for a virtual channel or I/O channel on a OneConnect port. The "IBM Virtual Fabric mode" switch type should be enabled in the Emulex NIC Configuration utility when a OneConnect controller is attached to an IBM vNIC-enabled switch. If you are using a switch other than an IBM vNIC-enabled switch, you must select the "Switch Independent Mode" switch type.

Note: The IBM Virtual Fabric Mode and Switch Independent Mode switch type options are only available on certain systems where multichannel support is enabled.

Note: Multichannel functionality is only supported on OneConnect controllers running in 10Gb mode. The 1Gb mode is not supported for vNIC switches.

If multichannel functionality is supported on your system, the Emulex NIC Configuration utility enables you to perform the following operations:

- Select the "IBM Virtual Fabric Mode" or "Switch Independent Mode" switch type through the Switch Configuration menu, if available.
- Configure the LPVID for each channel.

You can configure LPVIDs using the LPVID option on the Multichannel Configuration menu.

Note: In pre-OS environments, LPVIDs also need to be configured on the switch port.

If the operating system for the PCI function has set up a VLAN ID, then it takes precedence over LPVID. If the operating system has not set up any VLAN IDs, the LPVID can be used for inner VLAN tagging. Outer VLAN tags can only be configured through the network switch.

To configure the switch type:

1. After you have enabled multichannel support, select **Switch Configuration** on the Emulex NIC Selection screen and press **<Enter>**. The Switch Configuration dialog box appears.

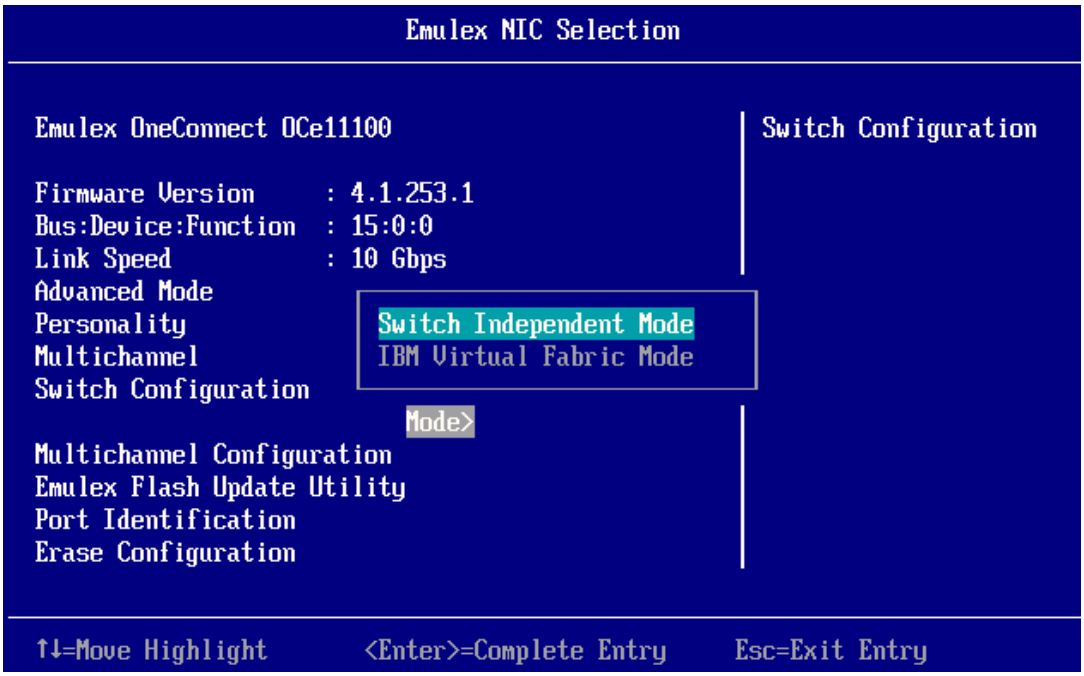

Figure 10-15 Switch Configuration Dialog Box

2. Select **IBM Virtual Fabric Mode** if the OneConnect controller is attached to an IBM Virtual Fabric-enabled switch. Select **Switch Independent Mode** if you are using a switch other than an IBM Virtual Fabric-enabled switch. Press **<Enter>**.

For instructions on how to configure the LPVID, see "Configuring Multichannel Support" on page 107.

Configuring VNTAG Support

VNTAG/Network Interface Virtualization (NIV) allows switching between different virtual network interfaces on the same adapter without the need for a software construct. However, this requires that both the adapter and switch are NIV-capable with certain properties configured on both the switch and the adapter.

Note: The VNTAG/Normal switch type option is only available in systems where multichannel support is enabled. For more information, see "Configuring Multichannel Support" on page 107.

On NIV-capable adapters, the Emulex NIC Configuration utility provides a means to enable or disable the NIV capability in the adapter using the Switch Configuration option. If VNTAG functionality is supported on your system, the Emulex NIC Configuration utility enables you to perform the following tasks:

- Select a VNTAG switch type.
- Attach a Profile Name to each virtual channel.

  There are "port profiles" that must be configured on the switch with certain network properties. The network interfaces on the adapter need to be associated with a profile name so that when the adapter plugs in to the switch, the switch can create and configure a virtual Ethernet interface (veth interface) on the switch. This veth interface matches the properties that were assigned (provisioned) to the port profile. If the switch type is VNTAG, the Emulex NIC Configuration utility allows you to associate profile names with adapter functions.

To enable and configure VNTAG support:

1. After you have enabled multichannel support, select **Switch Configuration** on the Emulex NIC Selection screen and press **<Enter>**. The Switch Configuration dialog box appears.

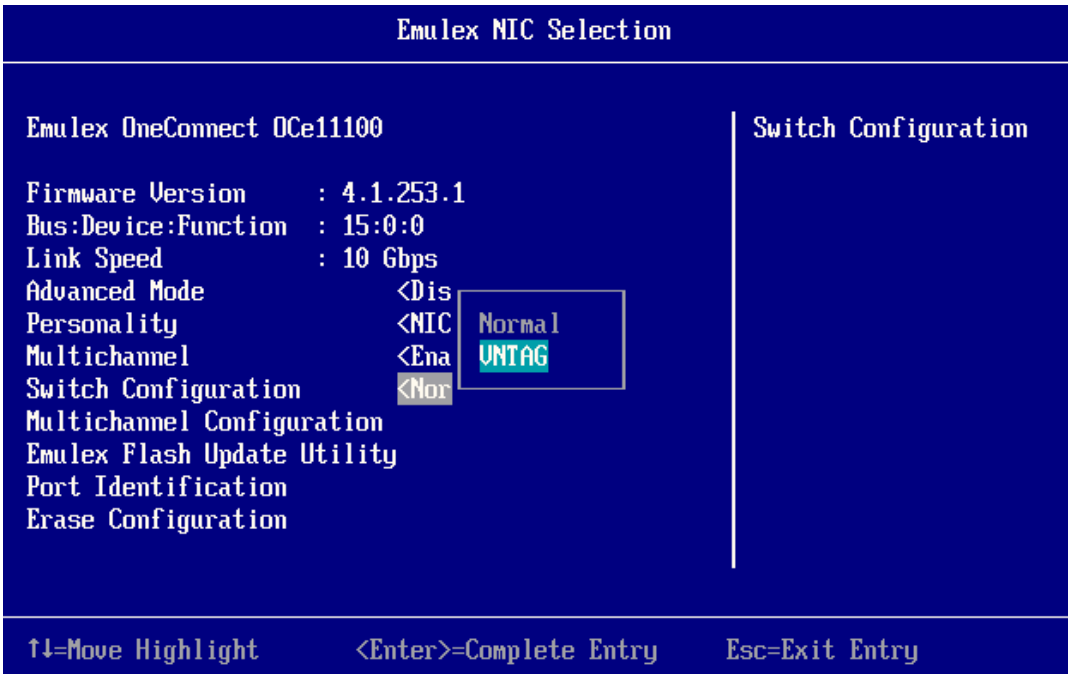

Figure 10-16 VNTAG Switch Configuration Dialog Box

2. Select **VNTAG** from the drop-down menu and press **<Enter>**.
3. From the Emulex NIC Selection screen, select **Multichannel Configuration** and press **<Enter>**. A list of available functions is displayed.

4. Select the function you want to configure and press **<Enter>**.

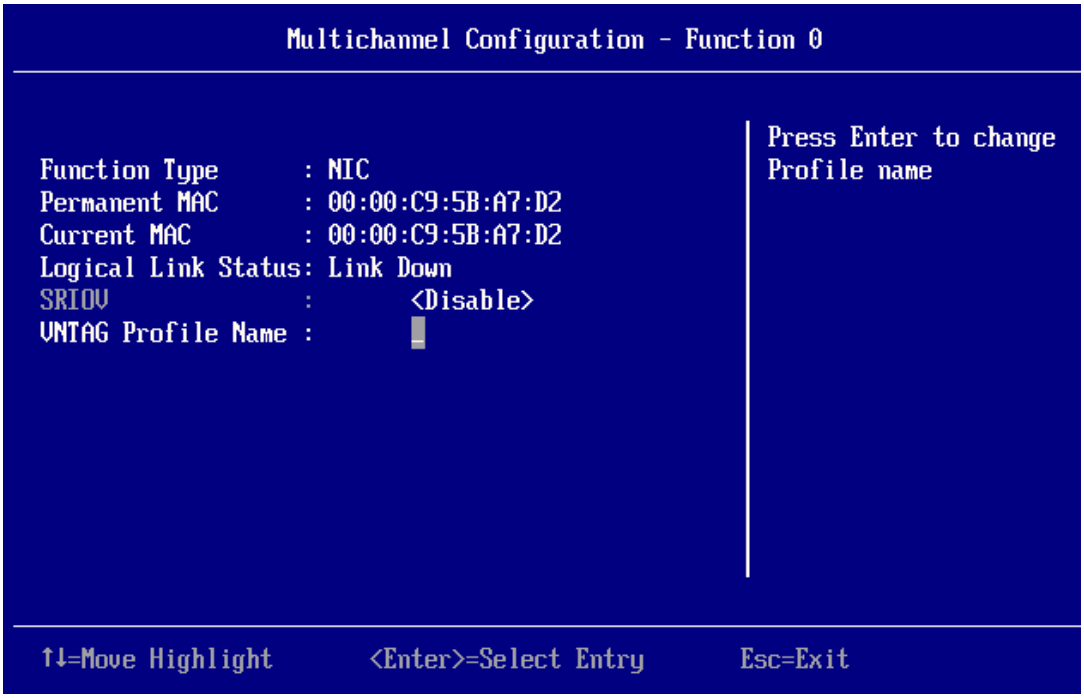

Figure 10-17 VNTAG Configuration Screen

5. Select the **VNTAG Profile Name** option and press **<Enter>**.
6. Type the VNTAG profile name you wish to attach and press **<Enter>**.

   VNTAG profile names are stored on the adapter flash and used during boot to negotiate NIV capabilities with the switch. The Emulex NIC configuration utility reads the on-flash data to display the profile name information.
7. Press **<Esc>** to return to the previous menu.
8. After attaching the profile names for the desired functions, select **Save** and press **<Enter>** to save the configurations.

Identifying a Port

To physically identify a port on the Emulex NIC Selection screen, select **Port Identification** and press **<Enter>**. The LEDs on your controller start blinking indicating the selected port.

Note: Not all controllers have LEDs that are visible externally. If you are using an add-in card in a blade server environment, the port identification or beaconing capability does not work.

Erasing Ports and Controller Configuration

To erase ports and the controller configuration:

1. On the Emulex NIC Selection Screen, select **Erase Configuration** and press **<Enter>**.

   A warning appears asking if you want to erase the configurations for both ports of the controller.

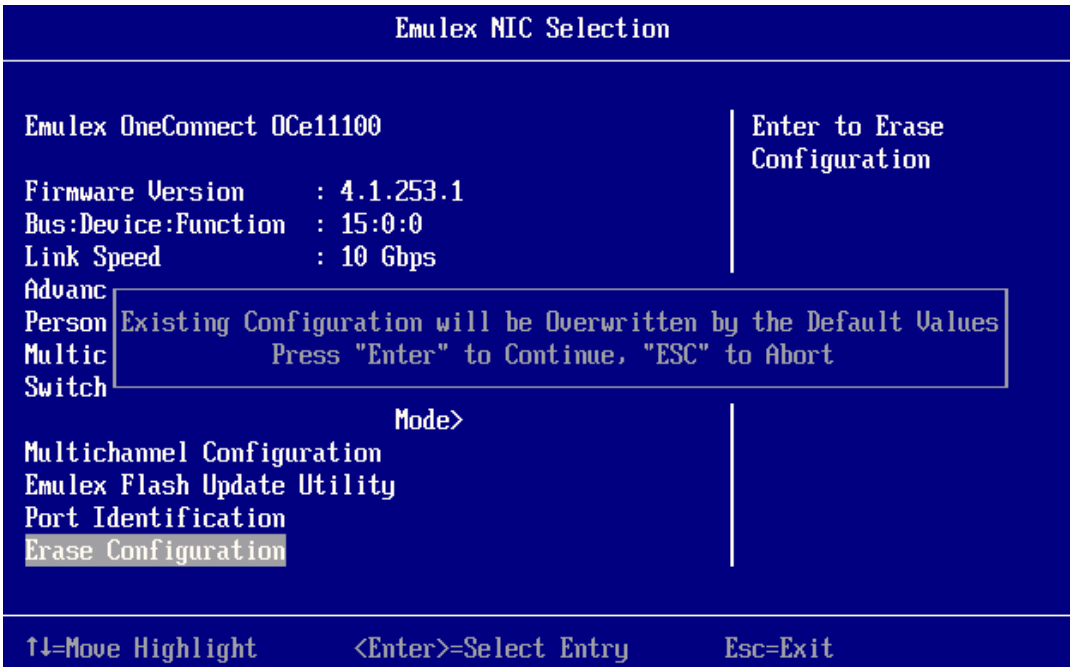

Figure 10-18 Erase Configuration Screen

2. Press **<Enter>** to delete the controller configuration, or press **<Esc>** to abort the operation.

UEFI NIC Diagnostics

The UEFI NIC driver diagnostics protocol can be used to run diagnostic tests on each NIC function of the card. This protocol is used by a platform management utility to allow you to run driver specific diagnostics on a controller.

EFI_DRIVER_DIAGNOSTICS_PROTOCOL

Syntax:

```
drvdiag [-c] [-l XXX] [-s] [-e] [-m] [driverhandle [devicehandle
[childhandle]]]
```

Description:

The UEFI NIC driver diagnostics protocol can be used to run diagnostic tests on each NIC function of the card. Diagnostics can be run in standard mode, extended mode, and manufacturing mode.

Parameters:

`-c`	Diagnose all child devices.
`-l XXX`	Diagnose using the ISO 639-2 language specified by XXX.
`-s`	Run diagnostics in standard mode.
	Diagnostics in standard mode run the LED test, Link test, Get MAC test, and the DMA test (Read, Write, and Read and Write)
`-e`	Run diagnostics in extended mode.
	Diagnostics in extended mode run the ARM Timer test, the MAC Loopback test, and the Physical Loopback test.
`-m`	Run diagnostics in manufacturing mode.
	Diagnostics in manufacturing mode run the Network Loopback test for the OneConnect OCe10100-series adapter and the Low-level Subsystem NLB test for the OneConnect OCE11100-series adapter.
`driverhandle`	Handle of the driver being configured.
`devicehandle`	Handle of a device that the driverhandle is managing.
`childhandle`	Handle of a device that is a child of the devicehandle.

Examples:

The following examples show you a way of using the EFI_DRIVER_DIAGNOSTICS_PROTOCOL.

The `driver` command identifies the handle of the driver:

```
Shell> drivers

   122 Emulex 10G NIC
```

The `drvdiag` command list all the devices available for diagnostics. Each Ctrl [XXX] corresponds to a NIC function, which may be physical or virtual. The command returns handles for NIC functions on both ports.

```
Shell> driverdiag

   Drv[122] Ctrl[121]
   Drv[122] Ctrl[123]
```

To run the standard diagnostic tests on function 0:

```
Shell> drvdiag -s 122 121
```

To run the standard diagnostic tests on all NIC functions:

```
Shell> drvdiag -s 122
```

11. Configuring UEFI for iSCSI

Note: For systems with multiple adapters, the UEFI system firmware or boot code uses the highest version driver installed on any of the adapters. Adapters with older versions of EFIBoot are managed by the more recent version, but only as long as the adapter with the most recent version is in the system. The latest firmware and boot code must be installed on each adapter in the system to ensure that each adapter runs the latest firmware and boot code.

Navigating the Emulex iSCSI Configuration Utility

The Emulex iSCSI configuration utility has menus and configuration screens. Use the following methods to navigate them:

- Press the up/down arrows on your keyboard to navigate menu options or configuration fields. When multiple adapters are listed, use the up/down arrows to scroll to the additional adapters.
- Press the **<+>**, **<->**, or **<Enter>** keys to change numeric values.
- Press **<Enter>** to select an option.
- Press **<Esc>** to exit the current screen and show the previous screen.

Starting the Emulex iSCSI Configuration Utility

Depending on the OEM UEFI configuration, the Emulex iSCSI configuration utility may appear under different setup menus in the OEM system firmware or BIOS (such as **System Settings > Network Device List**).

To start the Emulex iSCSI configuration utility:

1. Select Emulex **iSCSI EFI Configuration Utility** and press **<Enter>**.

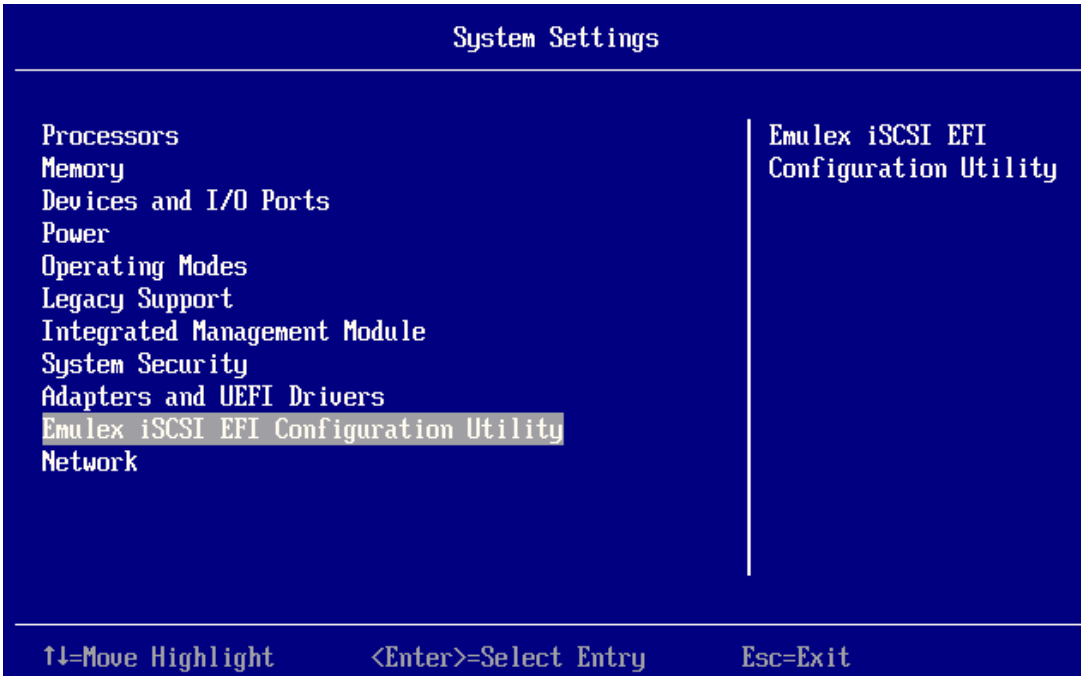

Figure 11-1 System Settings Screen

The iSCSI Initiator Configuration screen is displayed.

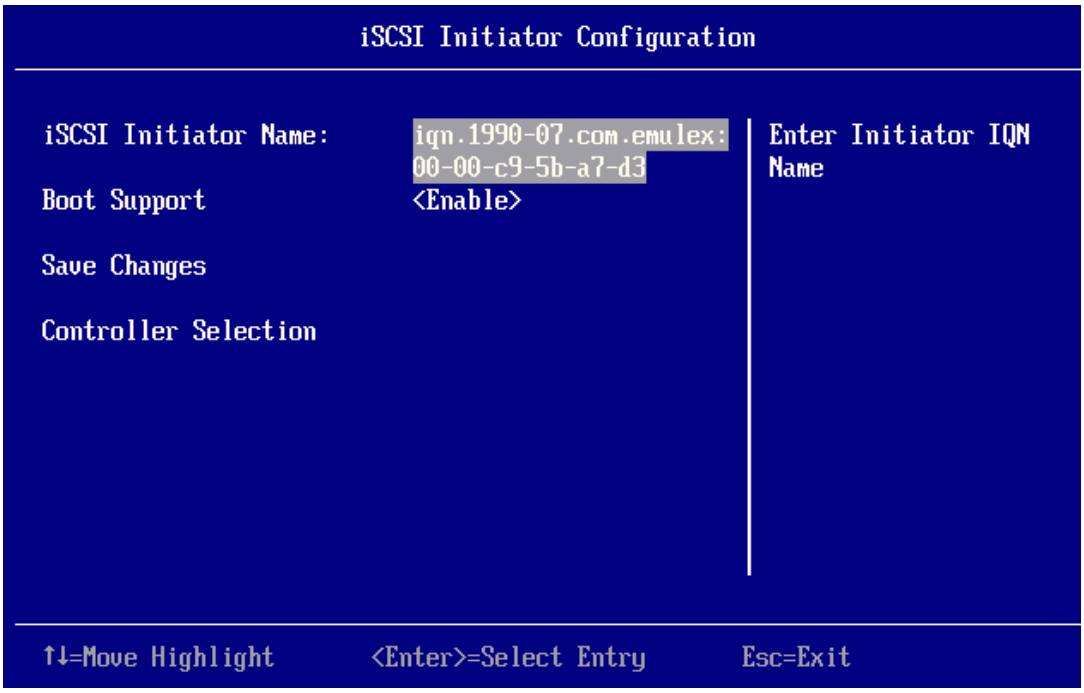

Figure 11-2 iSCSI Initiator Configuration Screen

2. Highlight **iSCSI Initiator Name** and press **<Enter>** to edit the initiator name.

3. Ensure Boot Support is set to **Enable** to support iSCSI boot.
4. To save changes, select **Save Changes** and press **<Enter>**.

Configuring the Controller

To configure the controller:

1. On the iSCSI Initiator Configuration screen, highlight **Controller Selection** and press **<Enter>**. The Controller Selection screen is displayed.

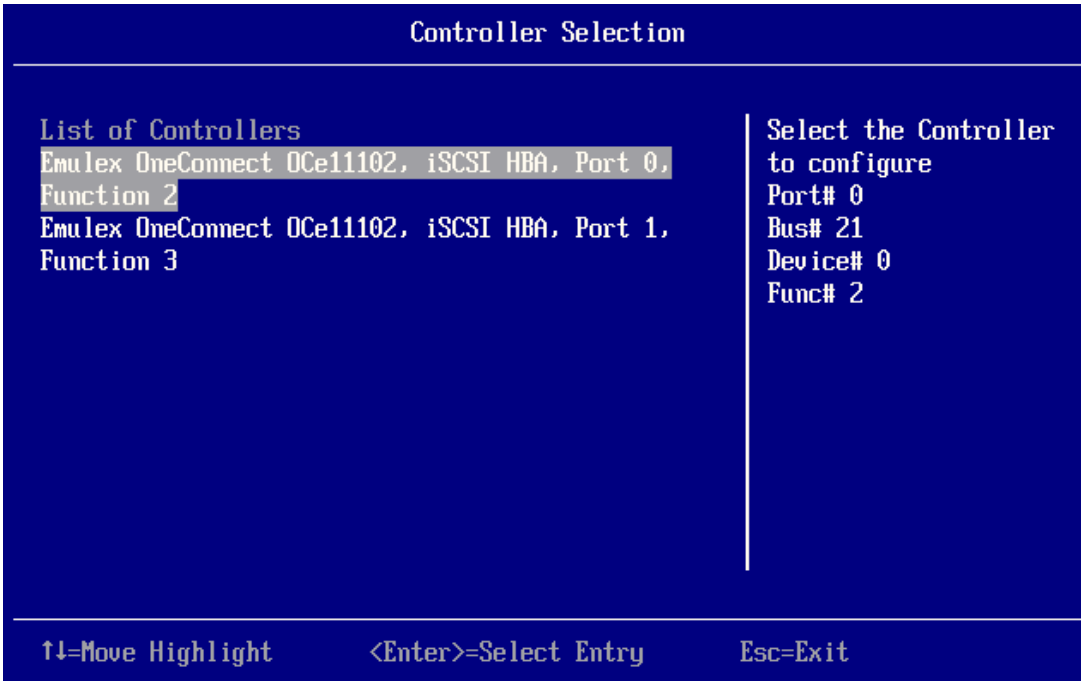

Figure 11-3 Controller Selection Screen

2. Highlight the port you want to configure and press **<Enter>**. The Controller Configuration Menu is displayed.

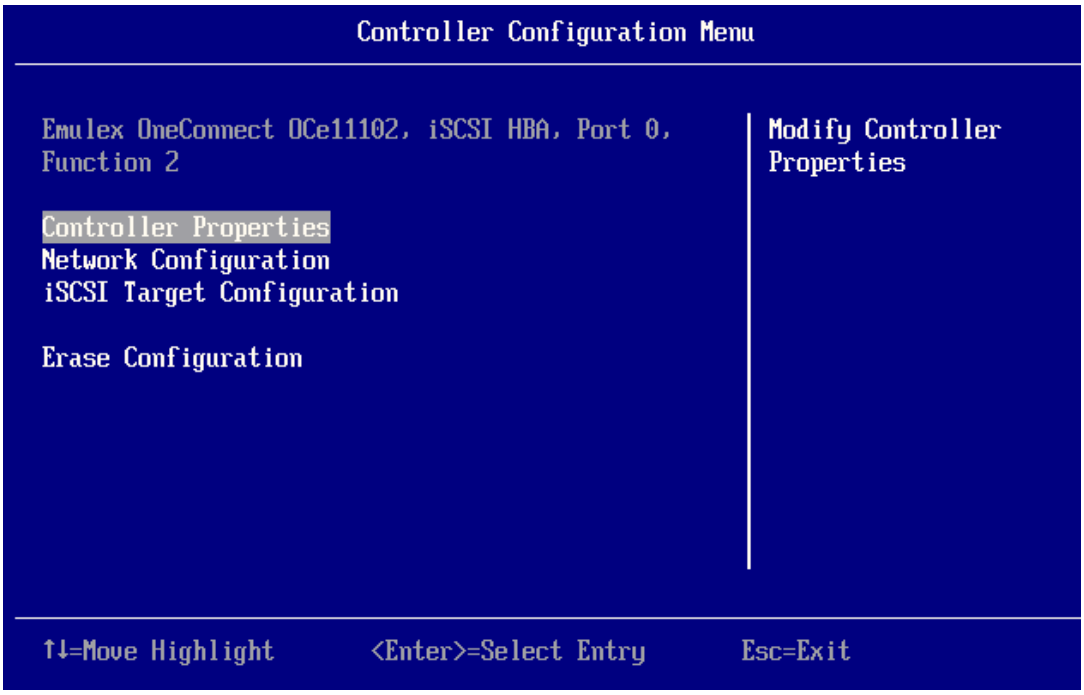

Figure 11-4 Controller Configuration Menu Screen

3. Select **Controller Properties** and press **<Enter>**. The Controller Properties screen is displayed.

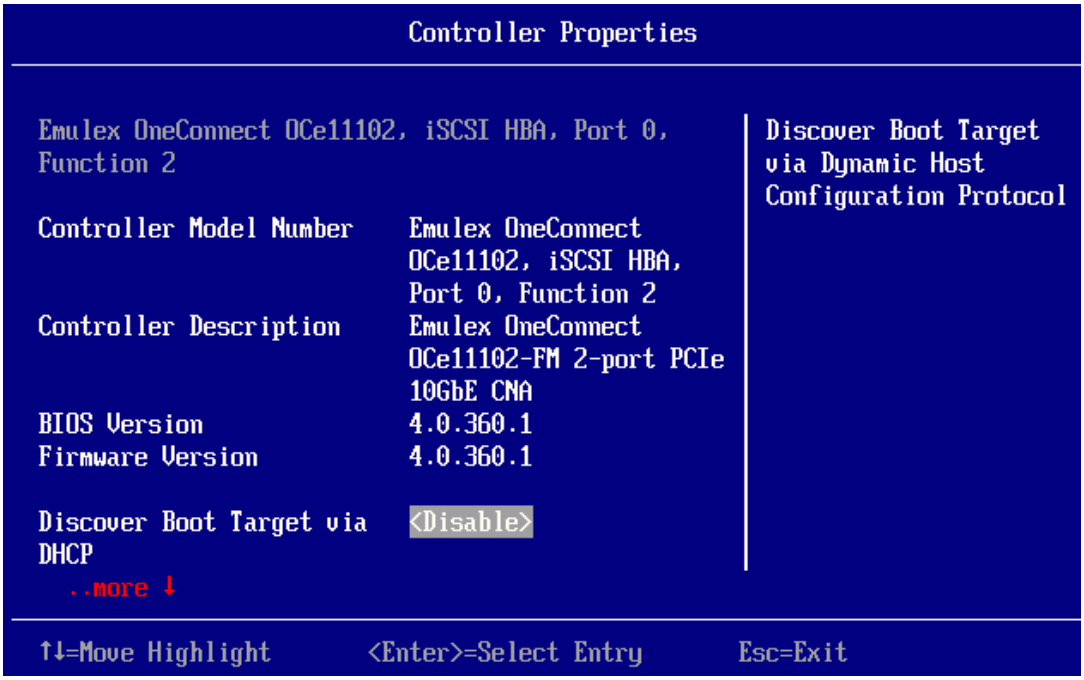

Figure 11-5 Controller Properties Screen

Configuring the Network

Automatically Assigning an IP Address through a DHCP Server

To enable DHCP for automatic assignment of the IP address through a DHCP server:

1. On the Controller Configuration menu (Figure 11-4), select **Network Configuration** and press **<Enter>**. The Network Configuration screen is displayed.

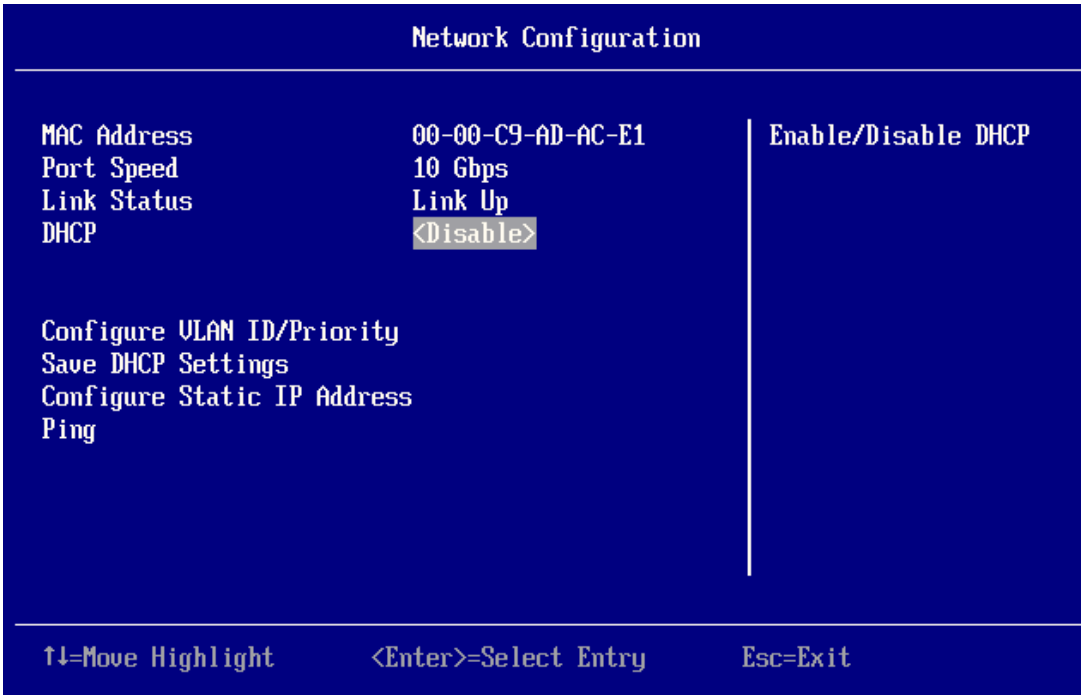

Figure 11-6 Network Configuration Screen

2. DHCP must be set to **<Enable>**. If you change this setting from <Disable> to <Enable>, select **Save DHCP Settings** and press **<Enter>**.

Manually Assigning an IP Address

To manually assign an IP address:

1. On the Controller Configuration menu (Figure 11-4), select **Network Configuration** and press **<Enter>**. The Network Configuration screen is displayed (see Figure 11-6).
2. DHCP must be set to **<Disable>**. If you change this setting from <Enable> to <Disable>, select **Save DHCP Settings** and press **<Enter>**.

3. Select **Configure Static IP Address** and press **<Enter>**. The Configure Static IP Address screen appears.

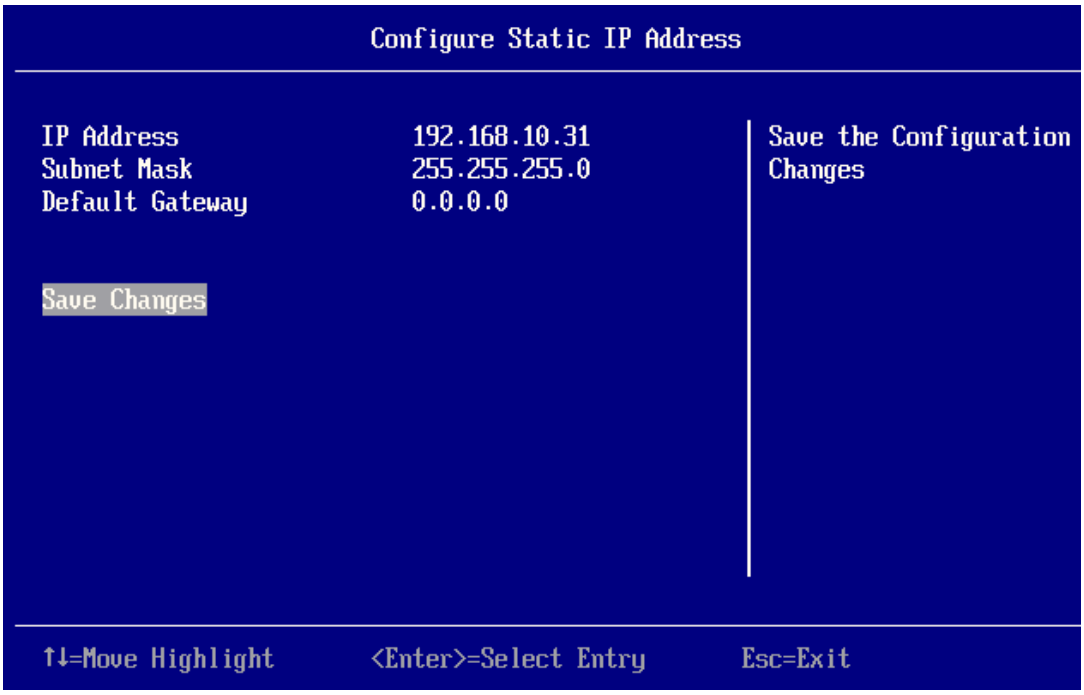

Figure 11-7 Configure Static IP Address Screen

4. Enter the IP address, subnet mask, and default gateway in the corresponding fields.
5. Select **Save Changes** and press **<Enter>**.

Configuring VLAN ID/Priority

A VLAN is a way of partitioning the network. If the LAN is made up of all devices within a broadcast domain, a VLAN is a broadcast domain made up of switches. You first create a VLAN and then assign ports to a VLAN. All ports in a single VLAN are in a single broadcast domain.

You do not have to configure VLANs unless your network is already using them. Some reasons why VLANs are used include:

- A LAN increases in size with numerous devices
- A LAN has extensive broadcast traffic on it
- Groups of users on a LAN need more security

A VLAN ID, like an IP address or initiator name, is assigned a value to uniquely identify it on a network. A VLAN priority is set to determine what packet gets priority order within a VLAN.

To configure a VLAN ID/priority:

1. On the Network Configuration menu, select **Configure VLAN ID/Priority** and press **<Enter>**. The Configure VLAN ID/Priority dialog box appears.

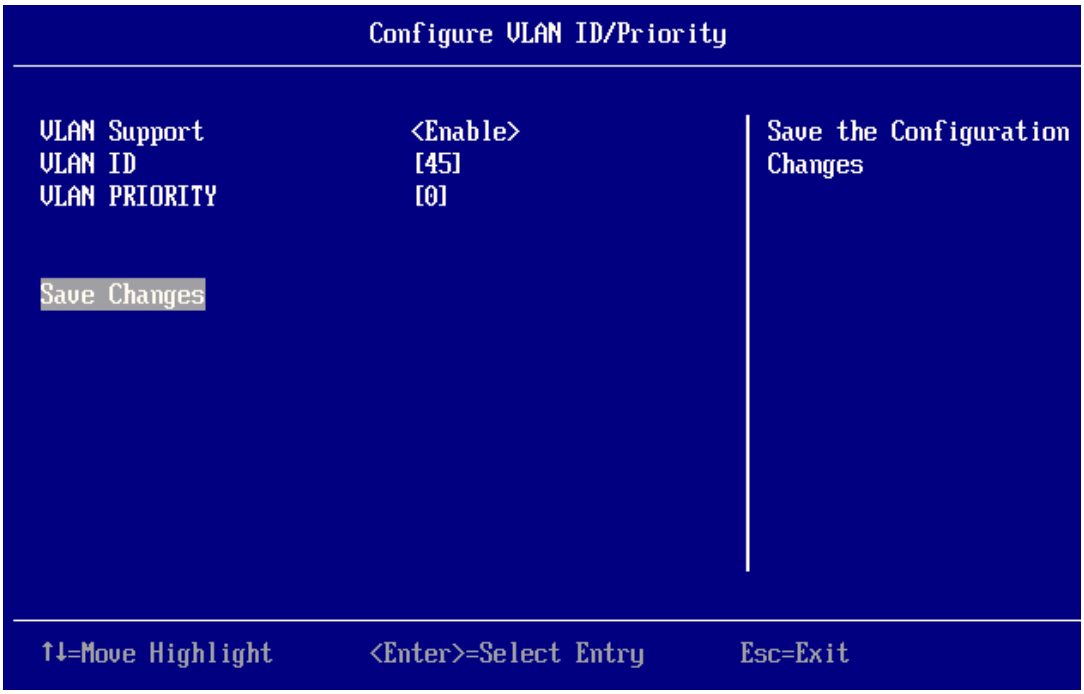

Figure 11-8 Configure VLAN/ID Priority Dialog Box

2. To enable VLAN support:
   a. Select **VLAN Support** and press **<Enter>**.
   b. From the VLAN Support drop-down menu, select **Enable** and press **<Enter>**.
3. To assign a VLAN ID number:
   a. Select **VLAN ID** and press **<Enter>**. This is a unique value you assign to each VLAN on a single device. There are a maximum of 4091 possible values ranging from 4-4094.
   b. Enter a VLAN ID value and press **<Enter>**.
4. To set a VLAN priority, if necessary:
   a. Select **VLAN PRIORITY** and press **<Enter>**. This unique value assigns a priority to outbound packets containing a specified VLAN ID. Valid values range from 0-7, with 0 the highest priority level.
   b. Enter a VLAN priority value and press **<Enter>**.
5. Select **Save Changes** and press **<Enter>**.
6. Press **<Esc>** to return to the Network Configuration menu.

Updating Firmware

To update firmware, you must use the NIC firmware update utility which revises the iSCSI function with a single firmware download image. For more information on downloading firmware, see “Using the Emulex NIC Configuration Utility” on page 99.

Adding and Configuring Targets

Discovering and Adding Boot Targets through DHCP

To automatically discover and add boot targets through DHCP:

1. On the Controller Properties screen (Figure 11-5), set **Discover Boot Target via DHCP** to **<Enable>** and press **<Enter>**.
2. Select **Save Changes** and press **<Enter>**.
3. Reboot the system.
4. On the Controller Configuration menu (Figure 11-4), select **iSCSI Target Configuration** and press **<Enter>**. The iSCSI Target Configuration screen shows the discovered targets.

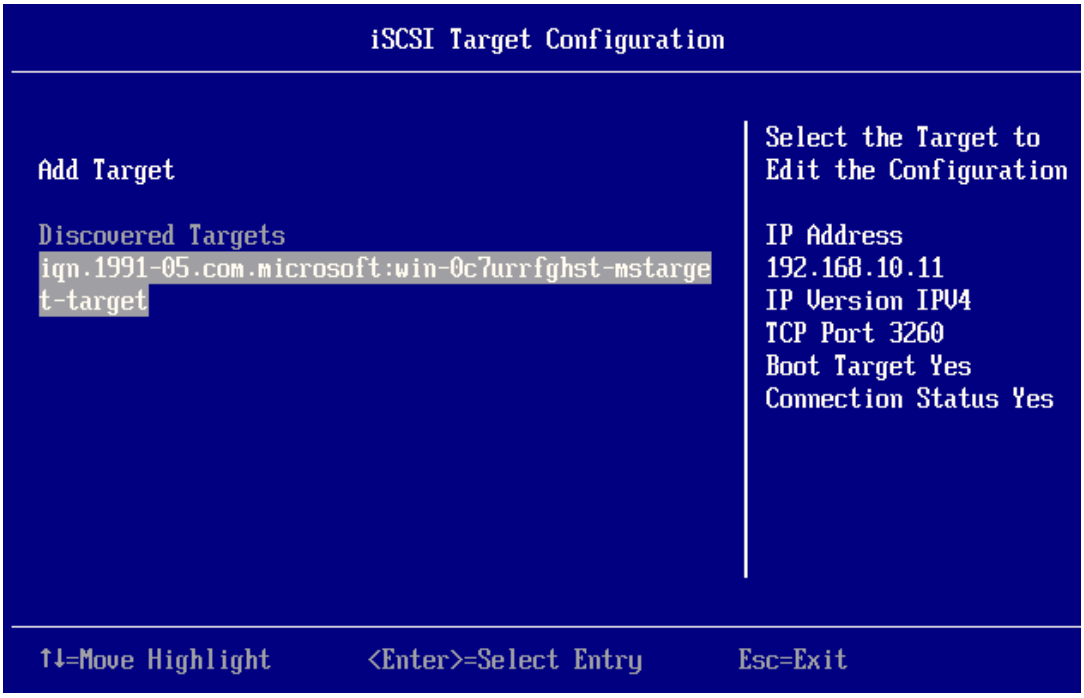

Figure 11-9 iSCSI Target Configuration Screen

Manually Adding, Discovering, and Managing Boot Targets

To manually add and discover boot targets:

1. On the Controller Properties screen (Figure 11-5), set **Discover Boot Target via DHCP** to **<Disable>** and press **<Enter>**.
2. Select **Save Changes** and press **<Enter>**.
3. Reboot the system.
4. On the iSCSI Target Configuration screen, select **Add Targets** and press **<Enter>**. The Add/Ping iSCSI Target screen is displayed.

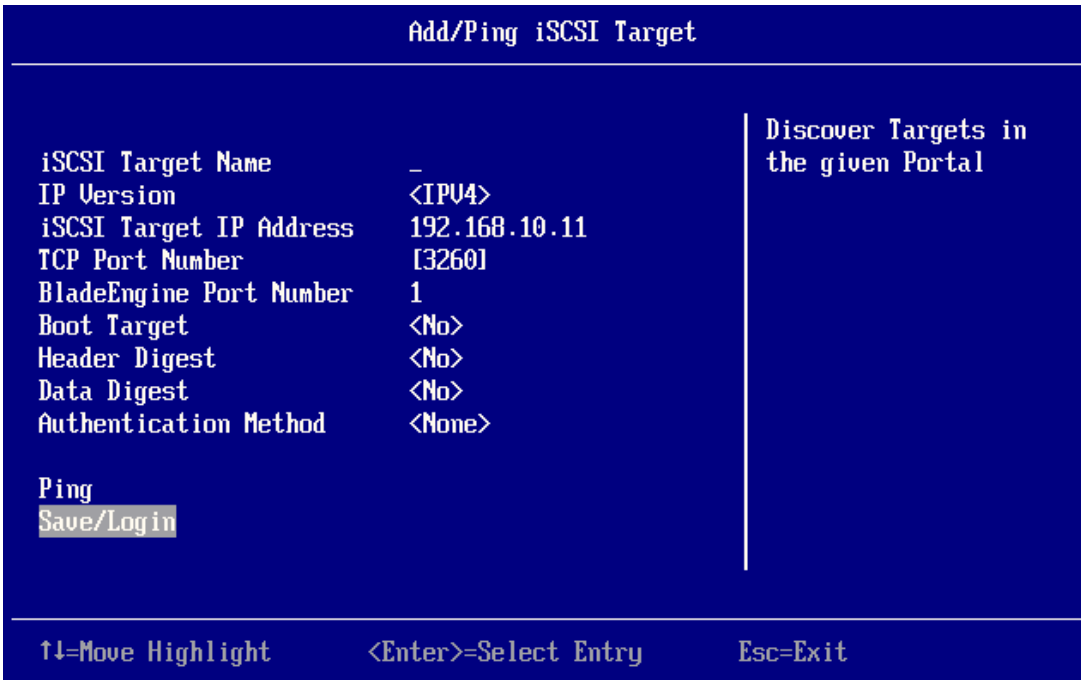

Figure 11-10 Add/Ping iSCSI Target Screen

5. Enter the target IP address and TCP port number (the default target port number is 3260).
6. For a boot target, use the default setting (No), even if you want to enable the target as a boot target. For more information about the boot target, see "Setting Up a Basic iSCSI Boot Configuration" on page 73.

   Note: You must enable the Boot Target option after you add the target via SendTargets.

7. Select **Yes** from the Header Digest drop-down menu if you want to enable header digest. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU's header segment is protected by the CRC32C checksum. The default setting is No.
8. Select **Yes**, from the Data Digest drop-down menu if you want to enable Data Digest. When set to Yes, and the iSCSI initiator is set accordingly, the integrity of an iSCSI PDU's data segment is protected by the CRC32C checksum. The default setting is No.

9. Select an authentication method (optional). If you are enabling an Authentication method, you are prompted to enter CHAP configuration.
10. Select **Save/Login** and press **<Enter>** to discover targets.

Setting a Boot Target

The discovered target must be set as a boot target to enable iSCSI boot.

To set a boot target:

1. On the iSCSI Target Configuration screen, select the target name and press **<Enter>**. The Edit/Ping Target screen is displayed.

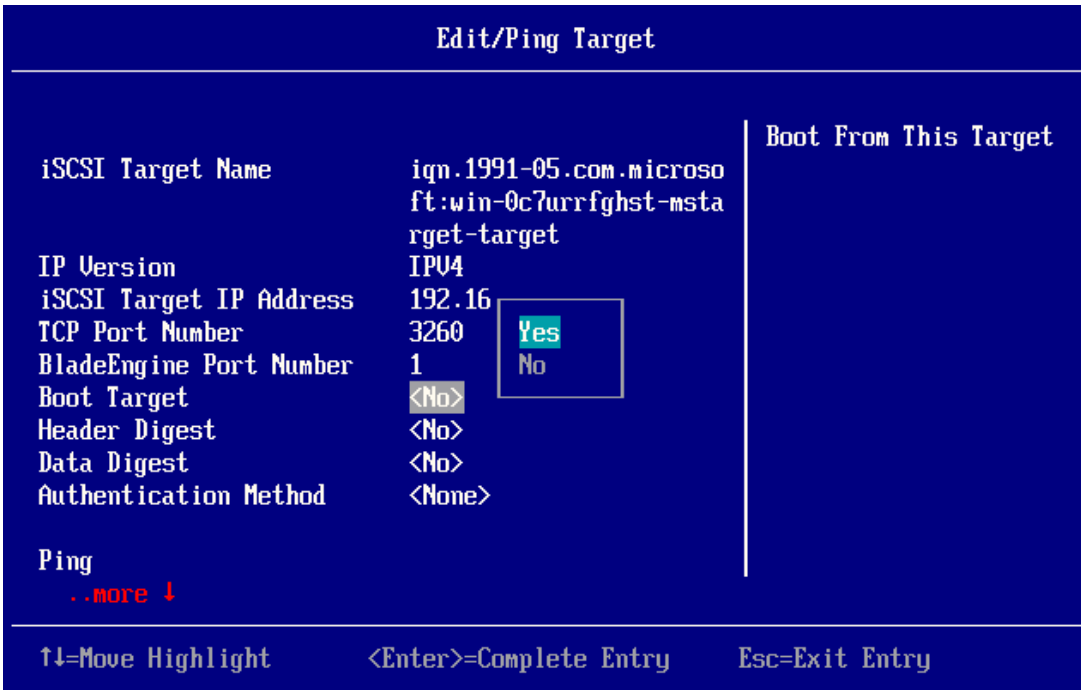

Figure 11-11 Boot Target Option on the Edit/Ping Target Screen

2. Select the **Boot Target** option and press **<Enter>**.
3. Select **Yes** from the drop-down menu and press **<Enter>**.
4. Select **Save/Login** and press **<Enter>**.

Pinging a Target

Note: If you want to verify that you can connect to a target before you log in, you must ping the target before you configure the target on the Edit/Ping Target screen.

To ping a target:

1. On the iSCSI Target Configuration screen, select the target name and press **<Enter>**. The Edit/Ping Target screen is displayed.

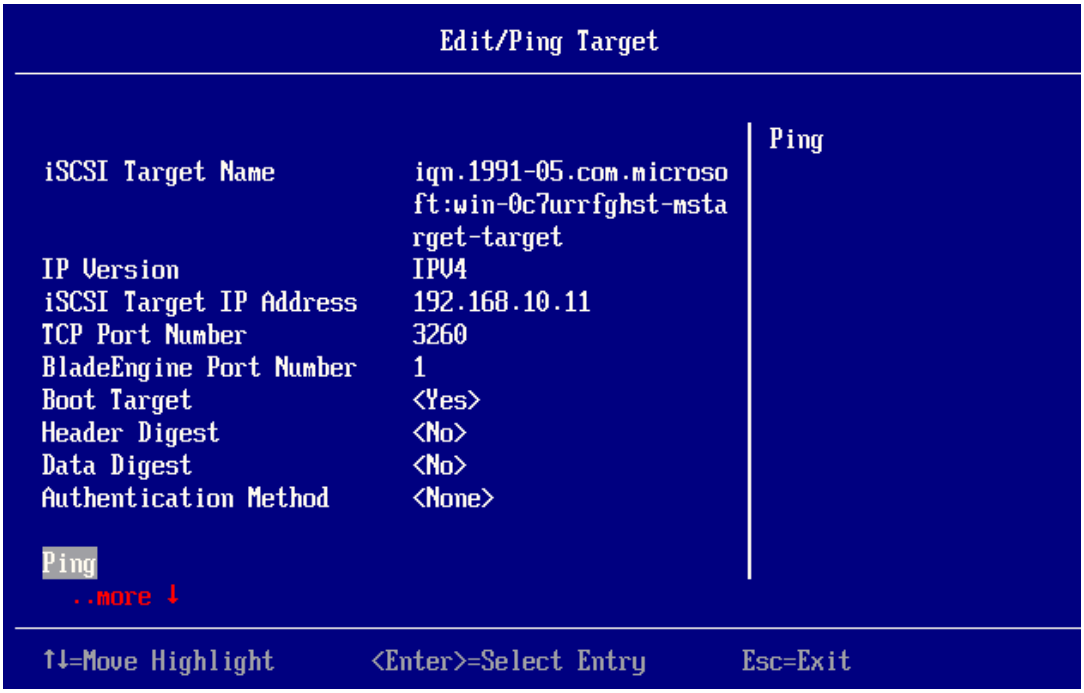

Figure 11-12 Edit/Ping Target Screen

2. From the Add/Ping iSCSI Target screen or the Edit/Ping Target screen, select **Ping** and press **<Enter>**. If the ping is successful, a screen similar to the following is displayed.

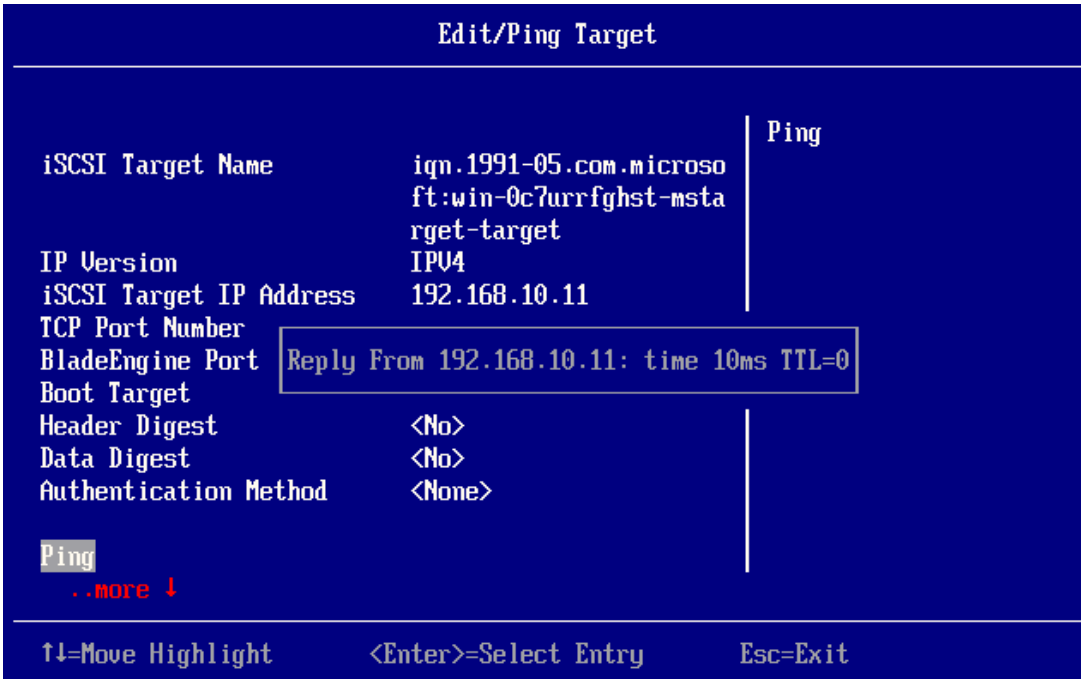

Figure 11-13 Successful Target Ping

If the ping is not successful, a failure message is displayed.

Viewing Advanced Properties

To view advanced properties:

1. On the Edit/Ping Target screen, select **..more** to display additional configuration options.

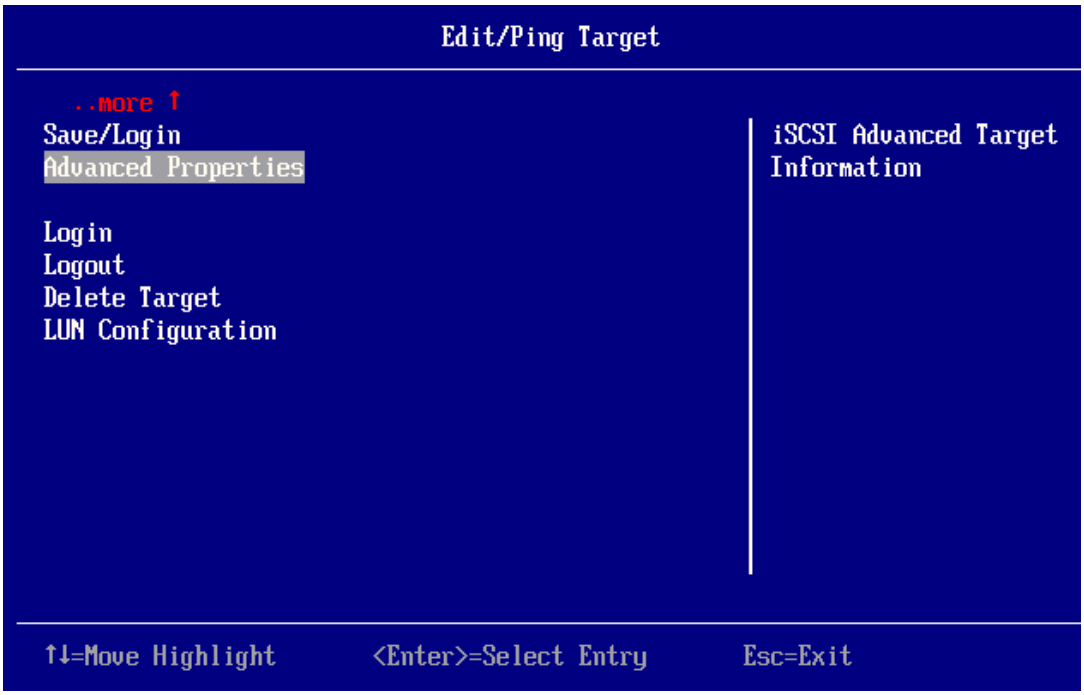

Figure 11-14 Edit/Ping Target Screen with Additional Configuration Options

2. Select **Advanced Properties** and press **<Enter>**. The Advanced iSCSI Target Information screen is displayed.

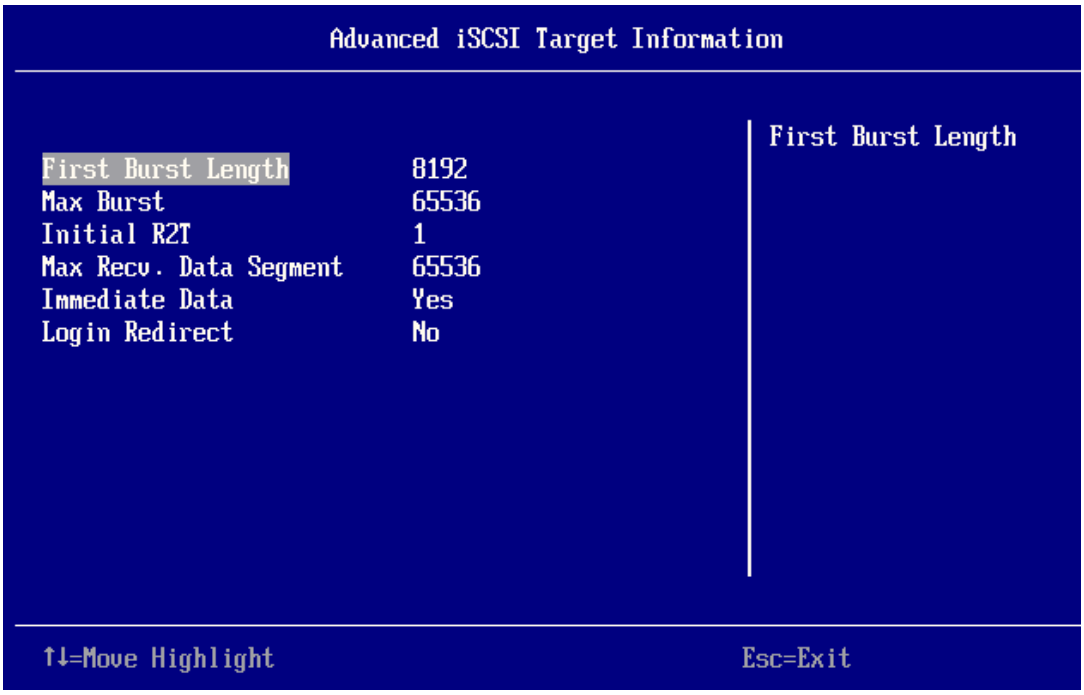

Figure 11-15 Advanced iSCSI Target Information Screen

Logging In or Logging Out of a Target

To log in or out of a target:

1. On the Edit/Ping Target screen, select **..more** to display additional configuration options.

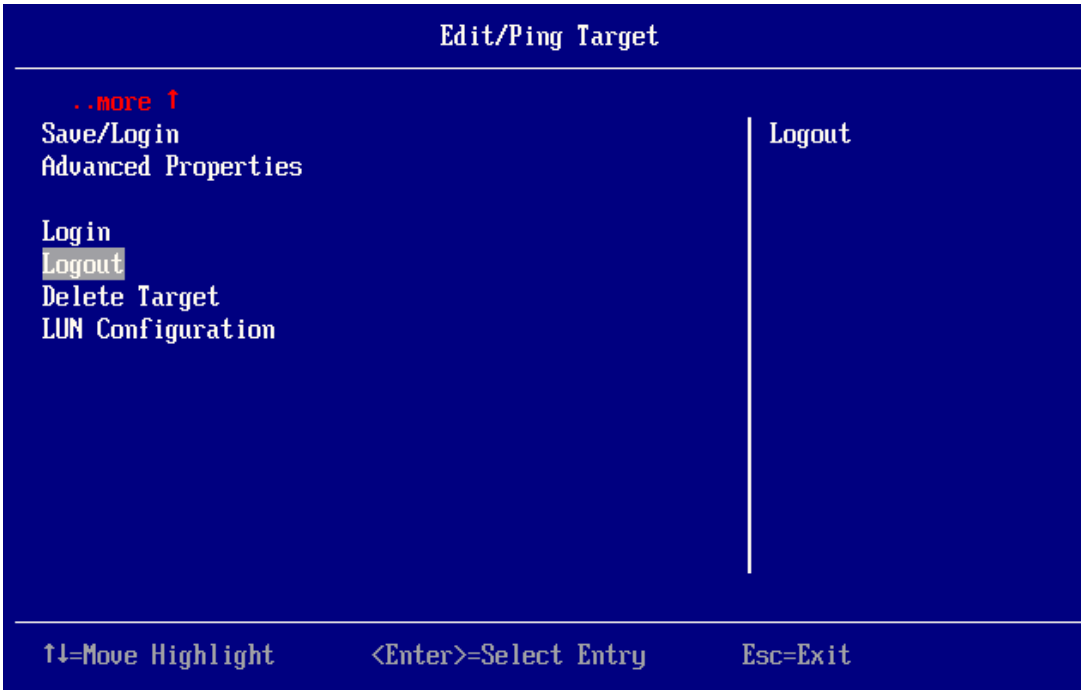

Figure 11-16 Edit/Ping Target Screen with Login and Logout Options

2. To explicitly log in or log out of a target, select **Login** or **Logout** and press **<Enter>**.

Deleting a Target

A target can be deleted only if it is not a boot target.

If a target is set as a boot target:

1. On the Edit/Ping Target screen, select **Boot Target** and press **<Enter>**.
2. From the drop-down menu, select **No** and press **<Enter>**.
3. Select **Save/Login** and press **<Enter>**.

To delete the target:

1. On the Edit/Ping Target screen, select **..more** to display additional configuration options.
2. Select **Delete Target** and press **<Enter>**.

Configuring LUNs

To configure LUNs:

1. On the Edit/Ping Target screen, select **..more** to display additional configuration options.
2. Select **LUN Configuration** and press **<Enter>**. The LUN Configuration screen is displayed.

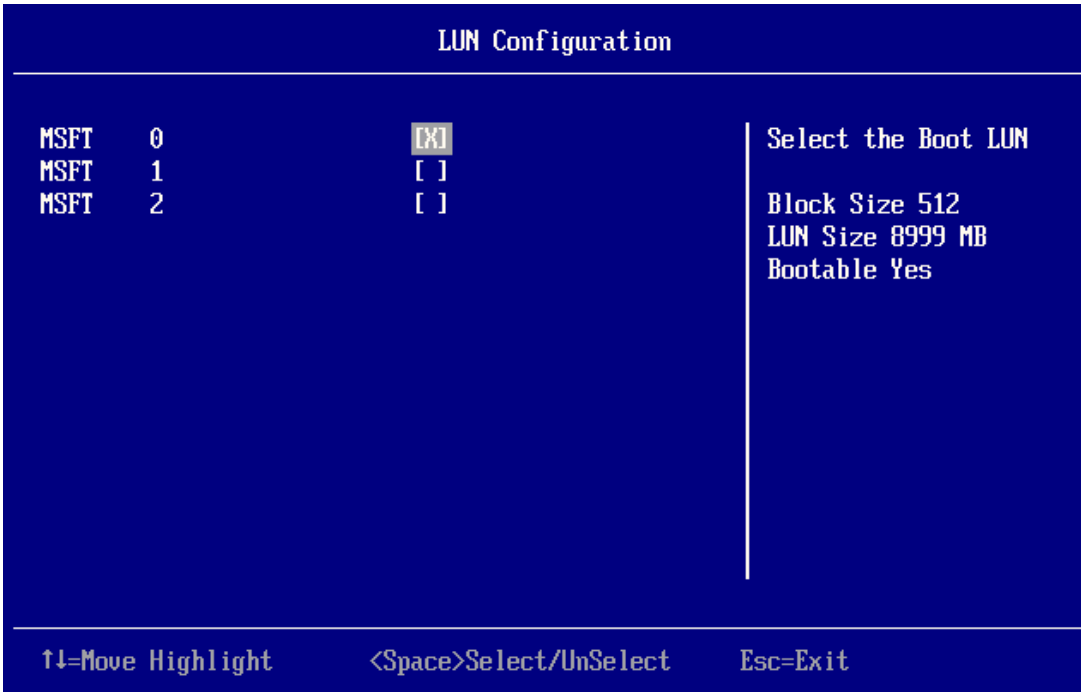

Figure 11-17 LUN Configuration Screen

3. If the target is a boot target, select any single LUN as a boot LUN using the **<Space>** bar.

   Note: If the target is not a boot target, you cannot select any LUNs.

Erasing the Configuration

Erase Configuration erases the configuration of a single controller. Configuration data is erased for both ports on the selected controller. The initiator name and boot support are global for all OneConnect controllers in the system. If you have more than one controller and you erase the configuration on the first controller, the erase configuration option resets the initiator name and boot support back to their default values. If you perform an erase configuration on the second controller, the default values are only reset for the second controller and are not reset globally on both controllers.

Note: You must select **Erase Configuration** to clear out existing IQN data if you purchase a different or subsequent license for the adapter.

To erase a controller configuration:

1. From the Controller Configuration menu, select **Erase Configuration** and press **<Enter>**.

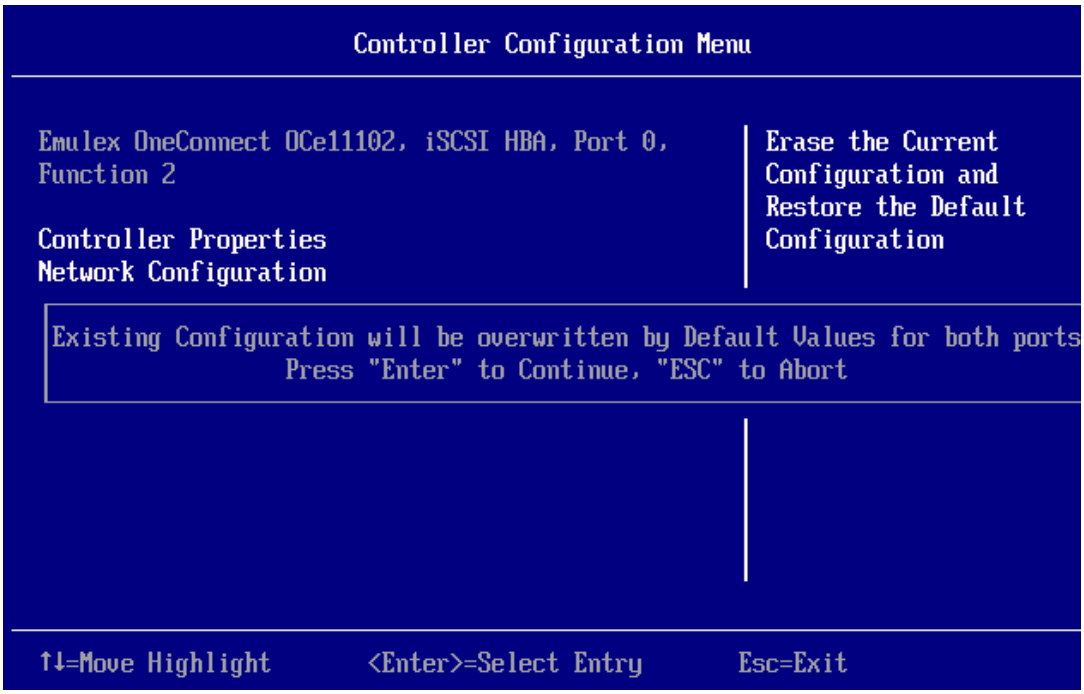

Figure 11-18 Erase Configuration Screen

A warning message appears asking for confirmation.

2. Press **<Enter>** to erase the configuration, or press **<Esc>** to abort the operation.

When the controller configuration is erased, the Controller Configuration menu is displayed.

12. Configuring UEFI for FCoE

Note: If you have several adapters in your system, the UEFI system firmware or boot code uses the highest version driver installed on any of the adapters. Adapters with older versions of EFIBoot are managed by the more recent version, but only as long as the adapter with the most recent version is in the system. The latest firmware and boot code must be installed on each adapter in the system to ensure that each adapter runs the latest firmware and boot code.

Navigating the Emulex FCoE Configuration Utility

The Emulex FCoE configuration utility has menus and configuration screens. Use the following methods to navigate them:

- Press the up/down arrows on your keyboard to move through and select menu options or configuration fields. When multiple adapters are listed, use the up/down arrows to scroll to the additional adapters.
- Press the **<+>**, **<->**, or **<Enter>** keys to change numeric values.
- Press **<Enter>** to select a menu option, to select a row in a configuration screen, or to change a configuration default.
- Use the navigation entries on the page to move about the utility.
- Press **<Esc>** to exit the current screen and show the previous screen.
- Select **Commit** to save changes. Select **Discard** to not save changes.
- Select **Back to Display Adapters and RECONNECT DEVICES** from the Emulex Adapter Configuration Main Menu when you are finished to ensure the changes are made active; otherwise, a system restart is required to make your changes active.You are then returned to the adapter list.

Starting the Emulex FCoE Configuration Utility

Depending on the OEM UEFI configuration, the Emulex FCoE configuration utility may appear under different setup menus in the OEM system firmware or BIOS (such as **System Settings > Network**). This description applies to systems where the Emulex utility is found in the Device Manager.

To start the Emulex FCoE configuration utility using HII:

1. Exit the EFI shell.

Figure 12-1 Exiting the EFI Shell

2. A front page is displayed. Launch the Device Manager.

3. Select **Emulex Configuration Utility Ver:X.XXXXX** and press **<Enter>**.

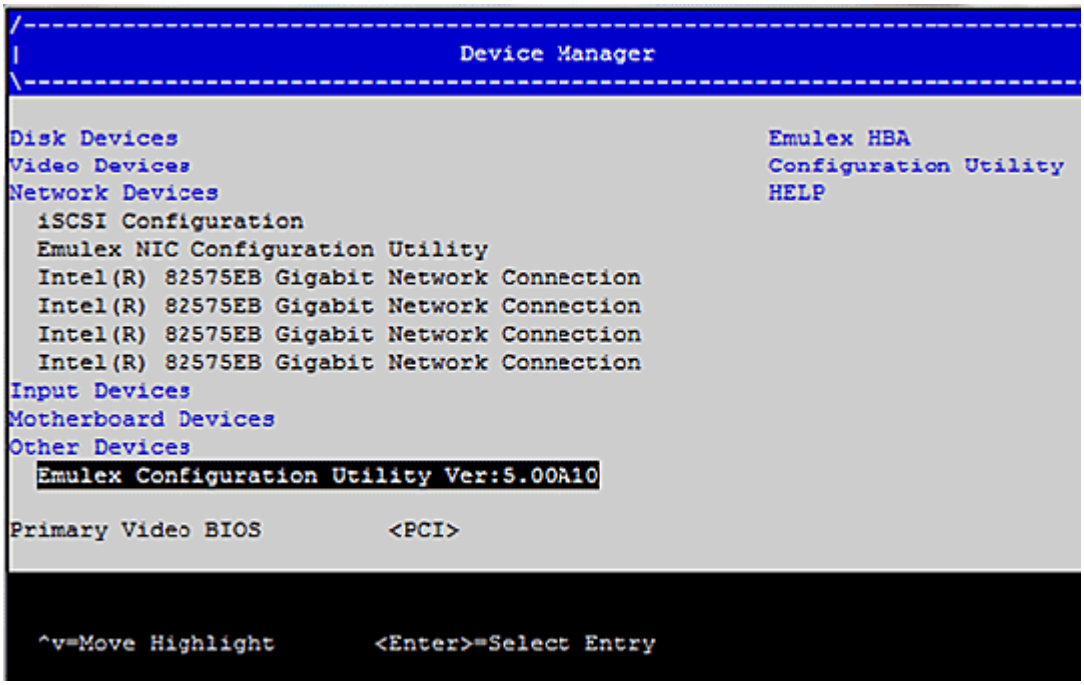

Figure 12-2 Device Manager - Emulex Configuration Utility Selected

4. The Emulex Configuration Utility screen is displayed with Emulex Configuration Setup Utility selected. Press **<Enter>**.

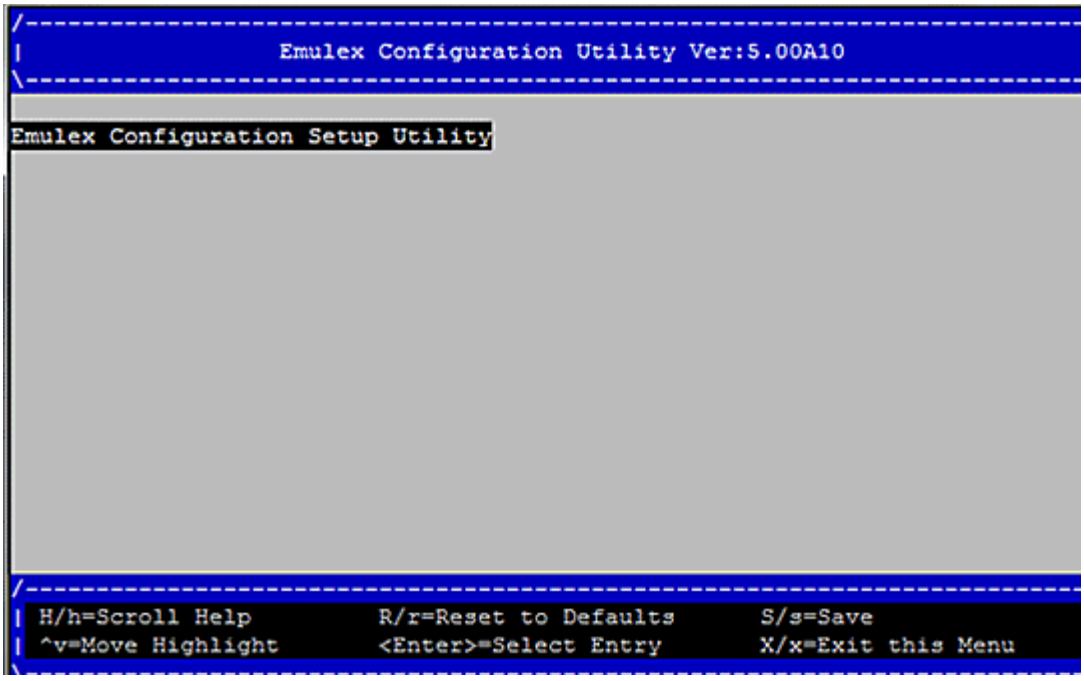

Figure 12-3 Emulex Configuration Utility Screen

A list of all the adapters in the system is displayed. Your list may vary depending on the installed adapters. Locate the adapter you want to configure. Use the up/down arrows on your keyboard to select it, and press **<Enter>**.

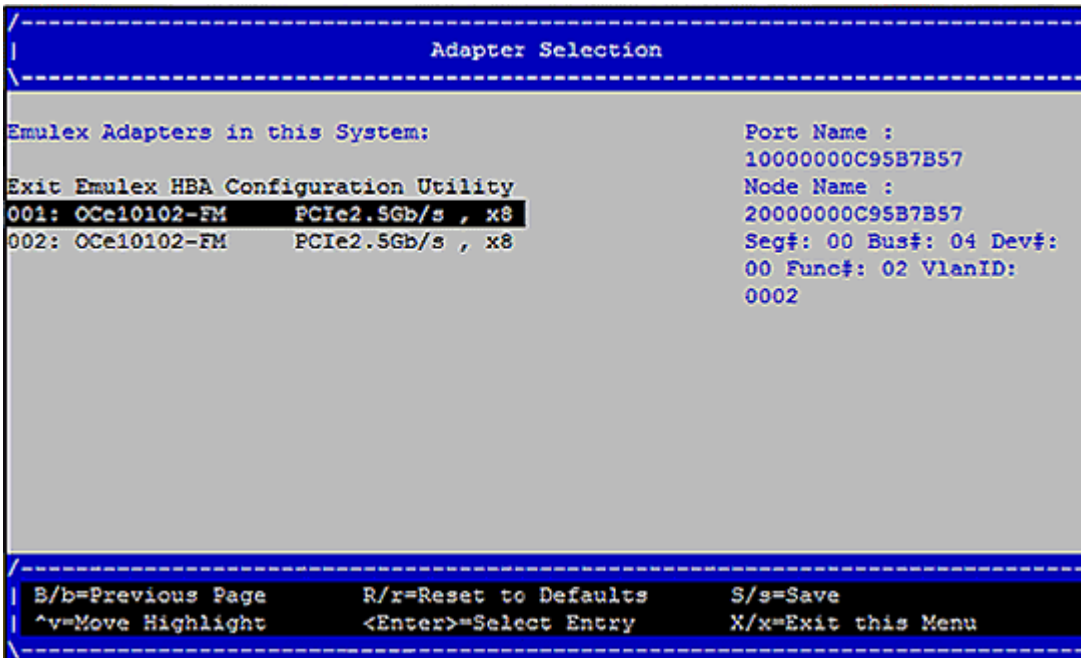

Figure 12-4 Adapter Selection Screen

The Emulex Adapter Configuration Main Menu is displayed.

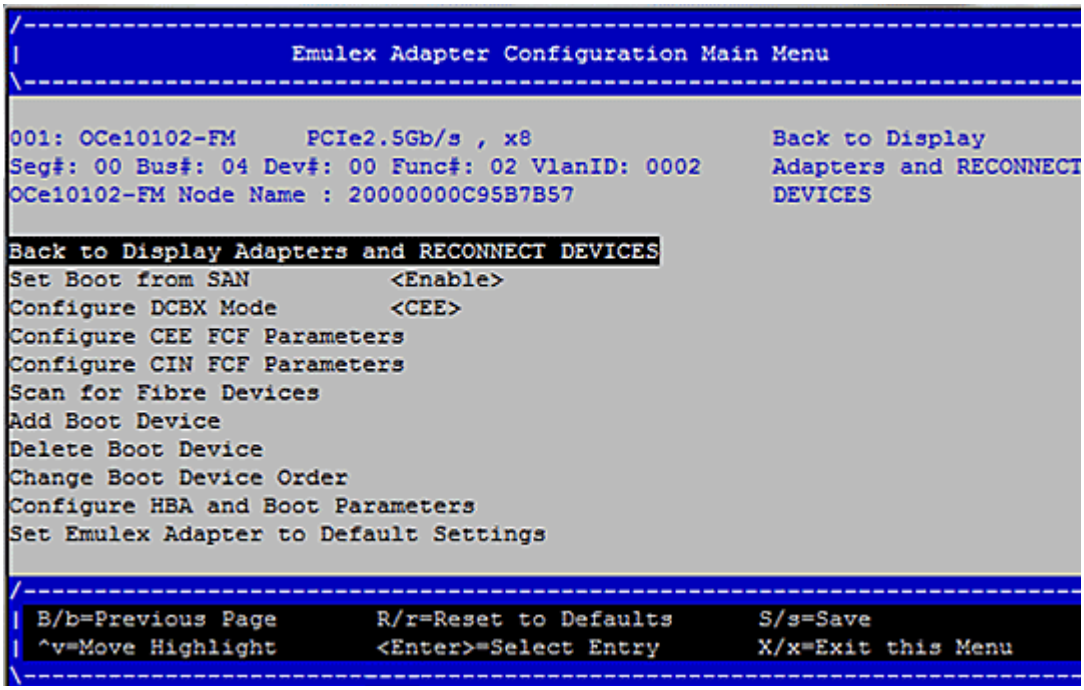

Figure 12-5 Emulex Adapter Configuration Main Menu

Updating Firmware and Boot Code

To update the firmware and boot code to the latest versions, you must use the NIC firmware update utility, which revises the FCoE function with a single firmware and boot code image. For more information on revising firmware versions, see chapter 10., “Configuring UEFI for Ethernet,” on page 97.

Enabling an Adapter to Boot from SAN

To enable an adapter to boot from SAN:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose network boot setting you want to change and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Set Boot from SAN**. The current setting is displayed. A Disable/Enable menu is displayed. Press **<Enter>**.
3. Select **Enable** and press **<Enter>**.The selection is changed to NVRAM and the current setting is displayed.

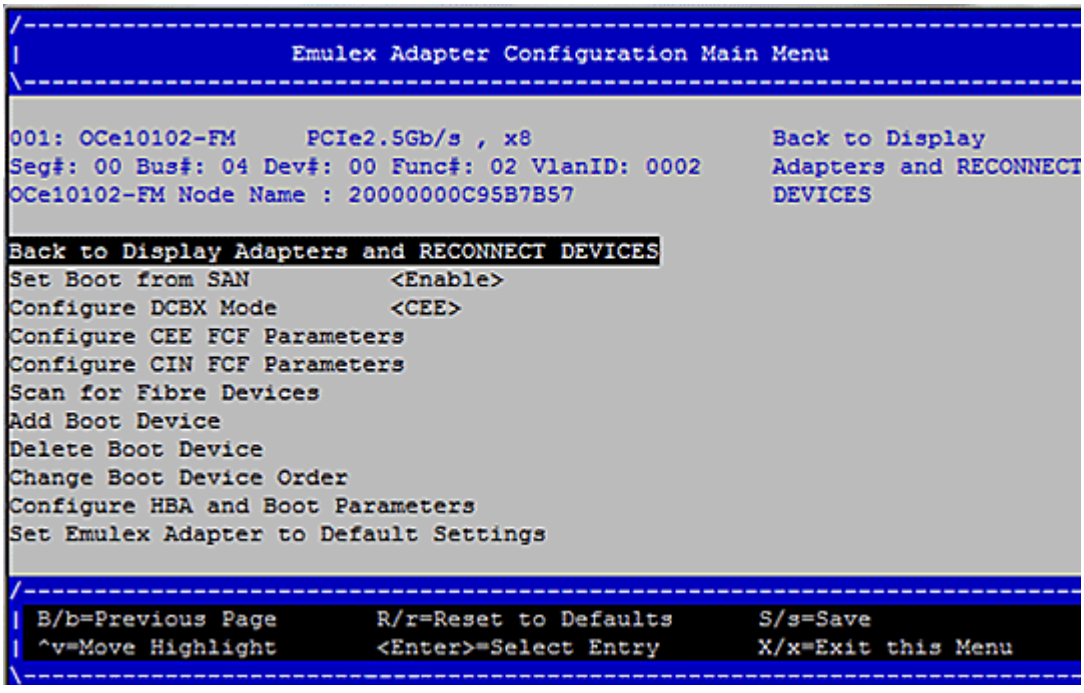

Figure 12-6 Emulex Adapter Configuration Main Menu – Network Boot Options Menu

Configuring DCBX Mode

To configure DCBX mode for the FCoE initialization protocol:

1. From the Adapter Selection screen (Figure 12-4), select the adapter to configure and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure DCBX Mode** and press **<Enter>**. The current setting is displayed.
3. Select **CEE** if the attached switch is CEE compatible, or select **CIN** if the attached switch is CIN compatible. (For more information, see the switch documentation.) Press **<Enter>**.

   The selection is changed to NVRAM and the current setting is displayed.

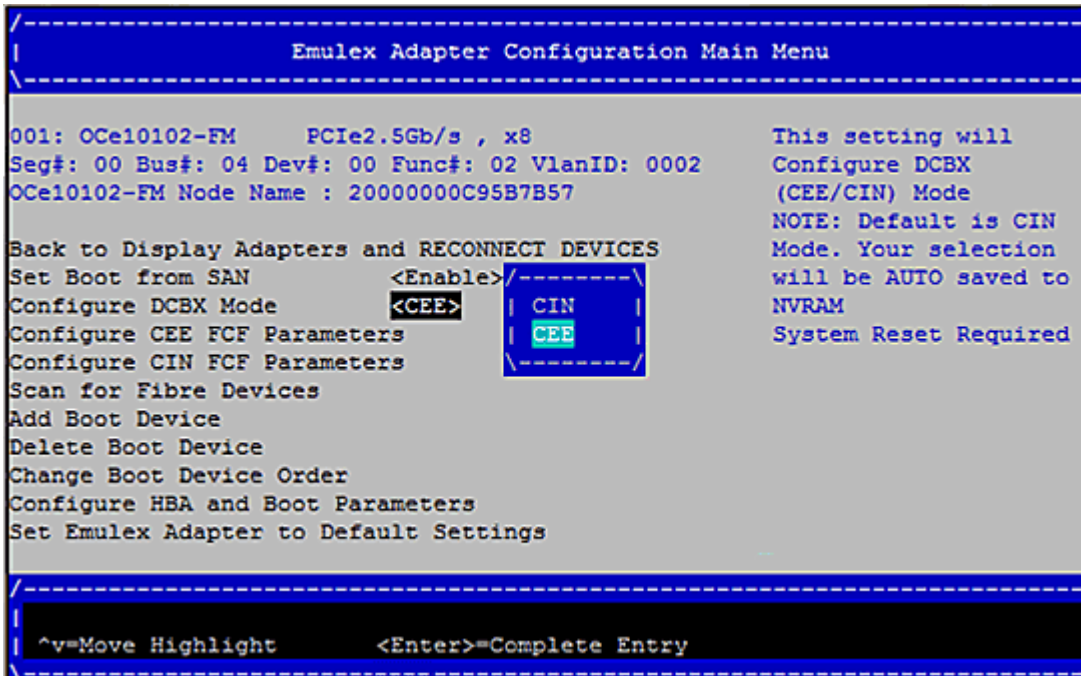

Figure 12-7 Emulex Adapter Configuration Main Menu – DCBX Menu

Configuring CEE FCF Parameters

To configure CEE FCF parameters:

1. From the Adapter Selection screen (Figure 12-4), select the adapter to configure and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure CEE FCF Parameters** and press **<Enter>**. A listing of current CEE FCF record information is displayed.

Figure 12-8 CEE Record Selection List

3. Select the CEE FCF record to modify and press **<Enter>**. The current record information is displayed.

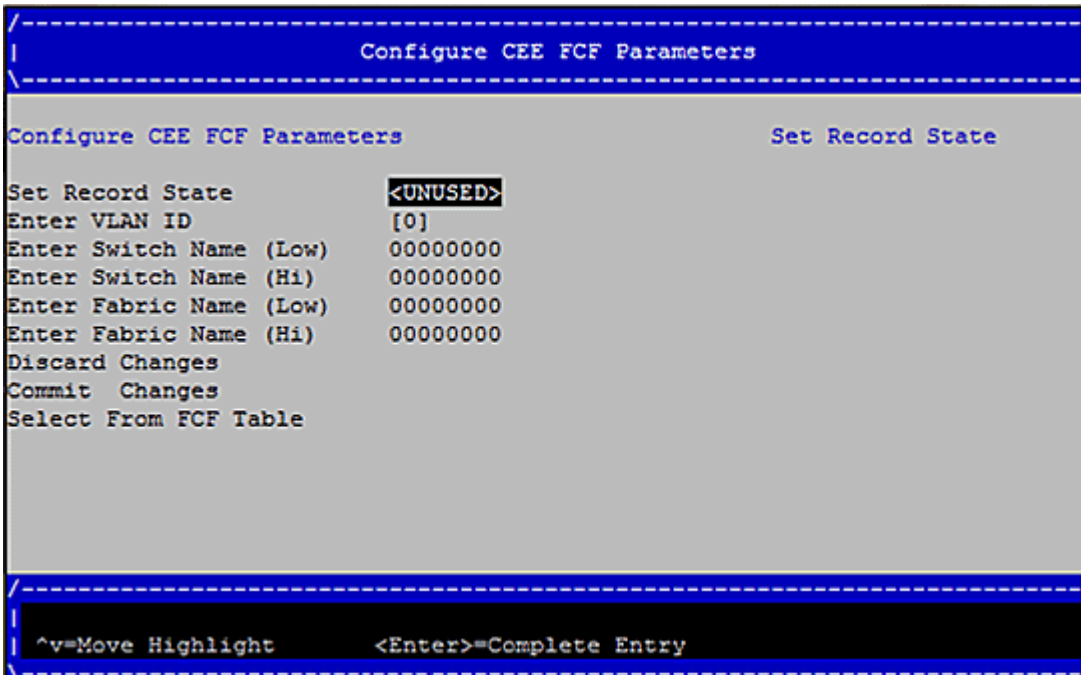

Figure 12-9 CEE FCF Record Information

4. Change the record information as needed.
   - Set Record State can be set to unused, active, or boot.
   - VLAN ID must be a three digit hexadecimal number.
   - Switch Name (Low). Enter the low bits of the FC switch's WWN to which to connect. This must be an 8-digit hexadecimal number.
   - Switch Name (Hi). Enter the high bits of the FC switch's WWN to which to connect. This must be an 8-digit hexadecimal number.
   - Fabric Name (Low). Enter the low bits of the FC fabric's WWN to which to connect. This must be an 8-digit hexadecimal number.
   - Fabric Name (Hi). Enter the high bits of the FC fabric's WWN to which to connect. This must be an 8-digit hexadecimal number.
5. Do one of the following:
   - To save your changes, select **Commit Changes** and press **<Enter>**. The changed CEE FCF record information is displayed.
   - To discard all changes, select **Discard Changes** and press **<Enter>**. The CEE record selection list is displayed (Figure 12-8).
   - To discard your changes and use the CEE parameters from the FCF table, select **Select From FCF Table** and press **<Enter>**. The FCF table parameters are displayed.
6. Press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

Configuring CIN FCF Parameters

To configure CIN FCF parameters:

1. From the Adapter Selection screen (Figure 12-4), select the adapter to configure and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure CIN FCF Parameters** and press **<Enter>**. A listing of current CIN FCF record information is displayed.
3. Select the CIN FCF record to modify and press **<Enter>**. Current record information is displayed.

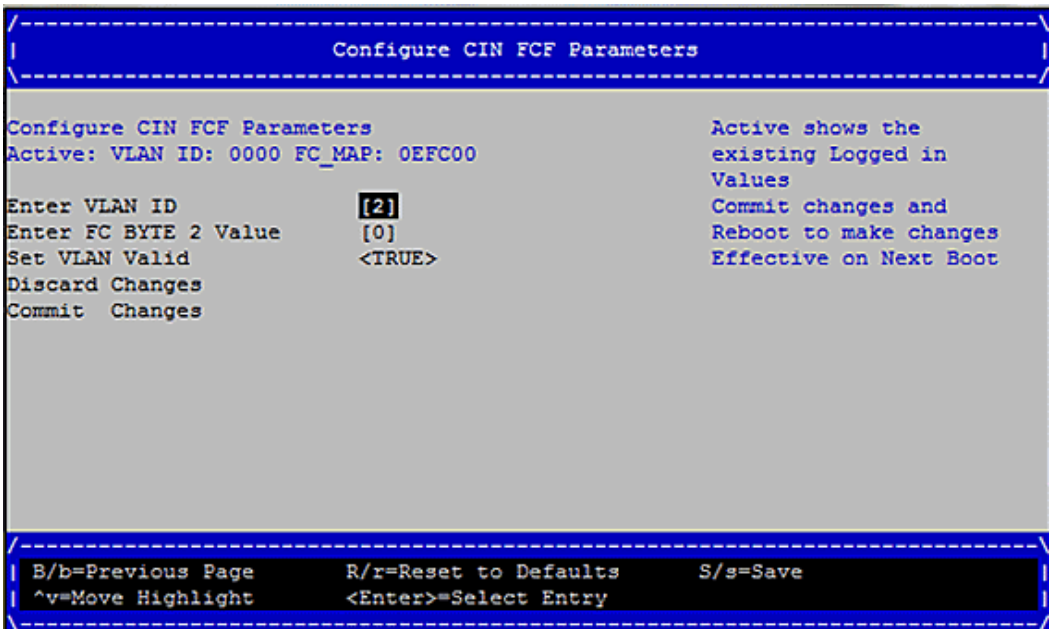

Figure 12-10 CIN FCF Record Information

4. Change the record information as needed.
   - VLAN ID. Enter the VLAN on which the adapter FCoE services are available. This must be a 3-digit hexadecimal number.
   - FC Byte 2. Enter the bit value that completes the fabric-provided MAC ADDRESS.Value can be incremented or decremented with the <+> and <-> keys. FC BYTE 0 and 1 are predefined (unchangeable) to “0E”, “FC” and only the second byte is selectable.
   - Set VLAN Valid. Select TRUE to enable VLAN or FALSE to disable it.
5. Select **Commit Changes** and press **<Enter>**.

Scanning for Fibre Devices

When LUNs are set up on the SAN before POST has completed (that is, before the boot driver has been started), you can select 'Scan for Fibre Devices' or 'Add Boot Device' to discover all available LUNs. Although this procedure does not perform a complete HBA initialization, it executes faster than selecting “Reconnect Devices”.

Note: If you dynamically add LUNs after POST has completed and the driver has been started, you must select **Reconnect Devices** to perform a complete HBA initialization and discovery. If this step is not performed, all LUNs may not be properly discovered.

You should also select **Reconnect Devices** after adding any discovered LUNs to the NVRAM list.

To scan for Fibre devices:

1. From the Adapter Selection screen (Figure 12-4), select the adapter that you want to scan for Fibre devices and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu, select **Scan for Fibre Devices** and press **<Enter>**. A list of discovered targets is displayed. This is only a list of discovered target devices to quickly determine SAN connectivity and provide you with a mechanism to have the port logged in for zoning.

Adding Boot Devices

To add a boot device:

1. From the Adapter Selection screen (Figure 12-4), select the adapter to which you want to add a boot device and press **<Enter>**.

2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Add Boot Device** and press **<Enter>**. Discovered targets are displayed.

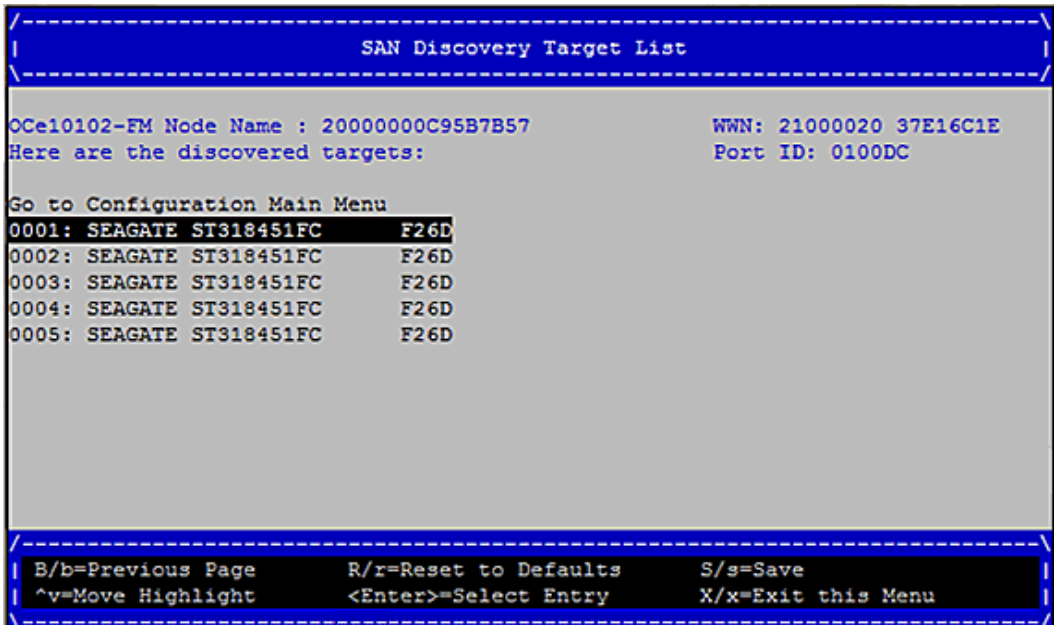

Figure 12-11 SAN Discovery Targets List

3. Select a target and press **<Enter>**.
4. Select a LUN from the list and press **<Enter>**. The target list is displayed.

Figure 12-12 LUN Listing

5. Select **Commit Changes** and press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

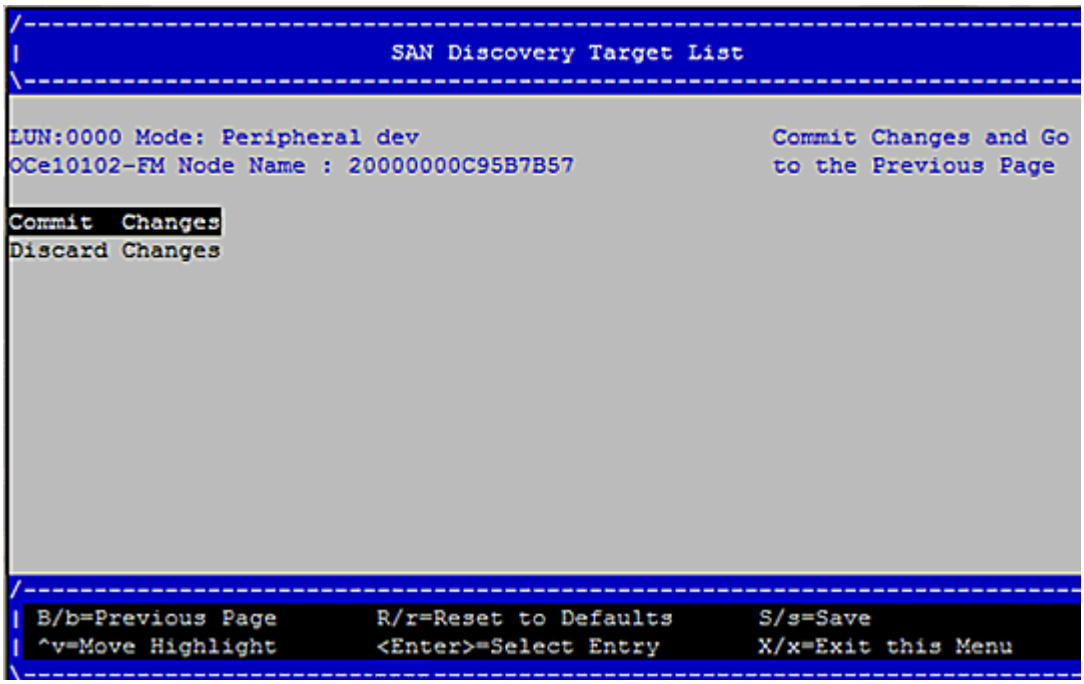

Figure 12-13 Commit/Discard Change

Deleting Boot Devices

To delete boot devices:

1. From the Adapter Selection screen (Figure 12-4), select the adapter from which you want to delete a boot device and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Delete Boot Device** and press **<Enter>**. A list of eight boot devices is displayed.

3. Select the device and press the spacebar to mark it. The device is displayed with an "X" beside it.

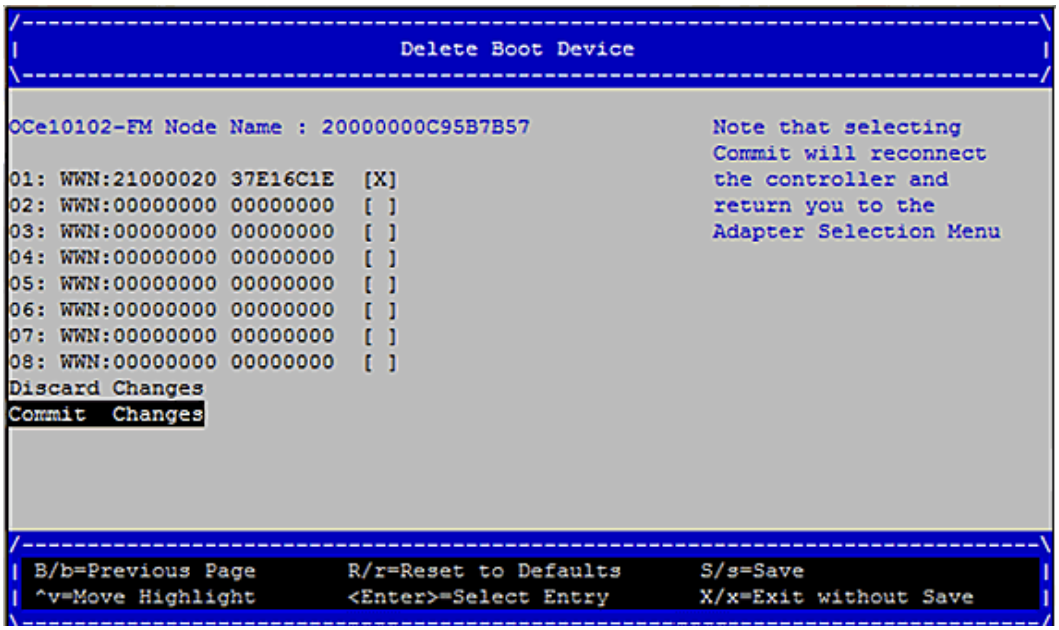

Figure 12-14 Delete Boot Device Screen

4. Select **Commit Changes** and press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

Changing Boot Device Order

Note: The boot device order has no relationship to the system BIOS boot device order. Changing the boot device order with this procedure will only change the order that the devices are discovered by UEFIBoot.

To change boot device order:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose boot device order you want to change and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Change Boot Device Order** and press **<Enter>**. The Change Boot Device Order screen is displayed.

3. Select **Boot Device Order** and press **<Enter>**.

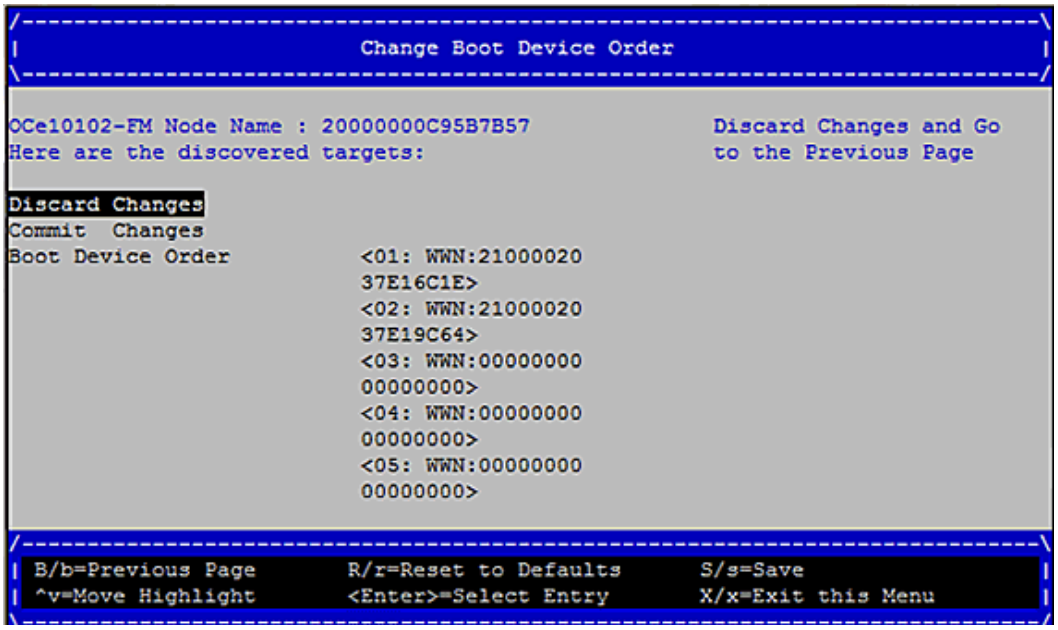

Figure 12-15 Change Boot Device Order Screen

4. Select a device from the list of eight boot devices and press **<Enter>**.

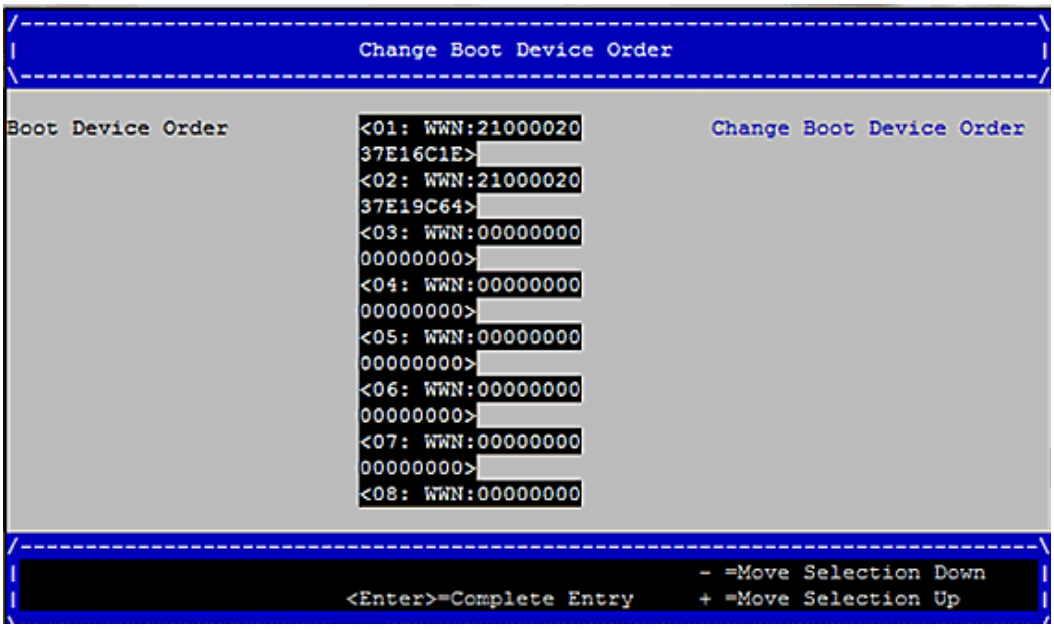

Figure 12-16 Boot Device Order Screen

5. Use the <+> or <-> keys to change the order of the selected device on the dialog box and press **<Enter>**. A screen shows the new boot device order.

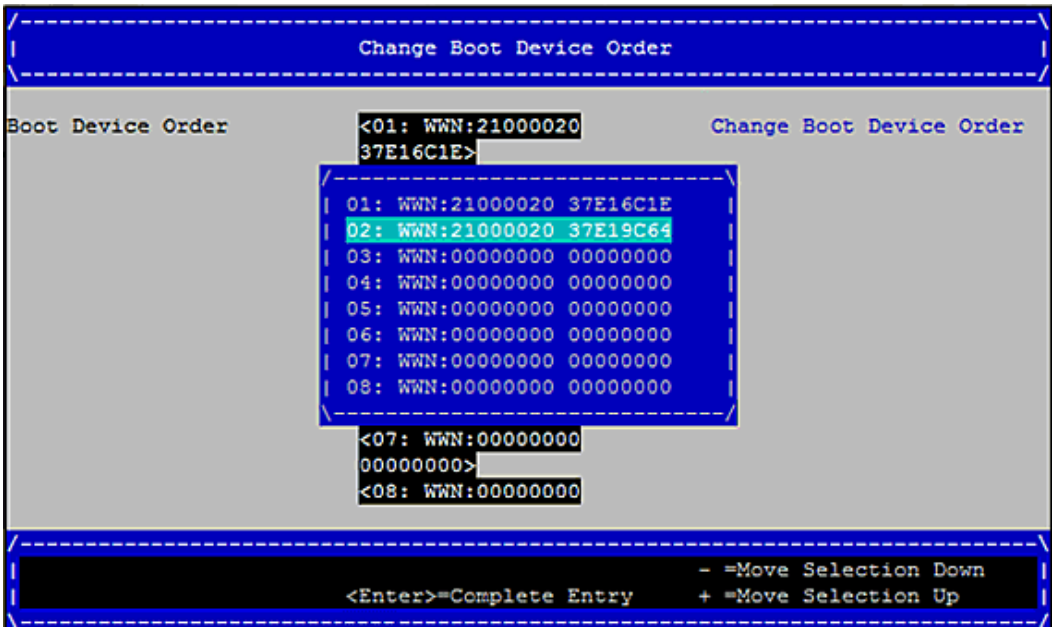

Figure 12-17 Change Boot Device Order Screen

6. Verify that the boot device list order is correct. Press **<Enter>**.

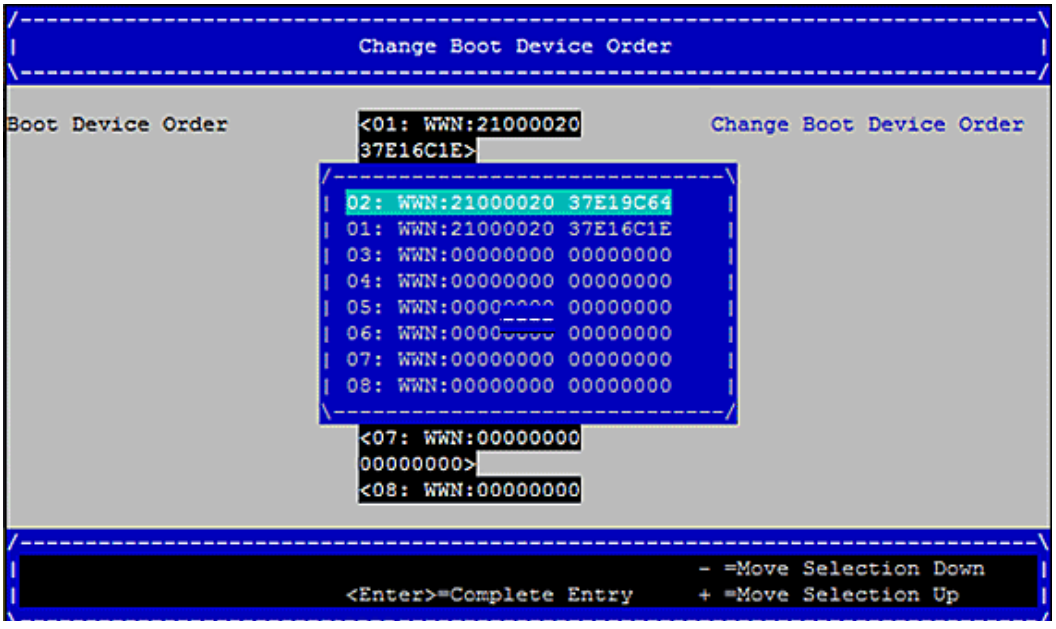

Figure 12-18 Change Boot Device Order Screen with Revised Boot Order

7. Select **Commit Changes** and press **<Enter>**. The revised order is saved to the NVRAM. The Emulex Adapter Configuration Main Menu is displayed.

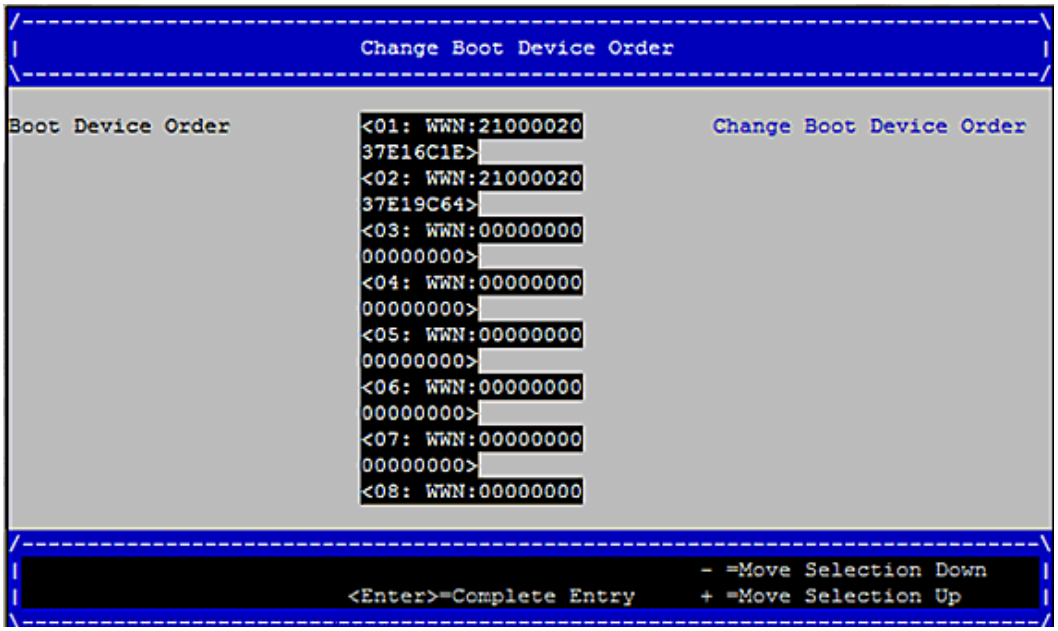

Figure 12-19 Change Boot Device Order

8. From the Emulex Adapter Configuration Main Menu, select **Back to Display Adapters and RECONNECT DEVICES** to complete configuration or select another configuration option.

Configuring Adapter Parameters

Changing the PLOGI Retry Timer

This option allows you to set the interval for the PLOGI retry timer. This option is especially useful for Tachyon-based RAID arrays. Under very rare occasions, a Tachyon-based RAID array resets itself and the port goes offline temporarily in the loop. When the port comes to life, the PLOGI retry interval scans the loop to discover this device.

You can choose:

- Disable – Default
- 50 Msec
- 100 Msec
- 200 Msec

To change timer values:

1. From the Adapter Selection screen (Figure 12-4), select the adapter to configure and press **<Enter>**.

2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure HBA Parameters** and press **<Enter>**. The Configure HBA Parameters screen is displayed.
3. From the Configure HBA Parameters screen, select **PLOGI Retry Timer** and press **<Enter>**. The PLOGI Retry Timer menu is displayed.

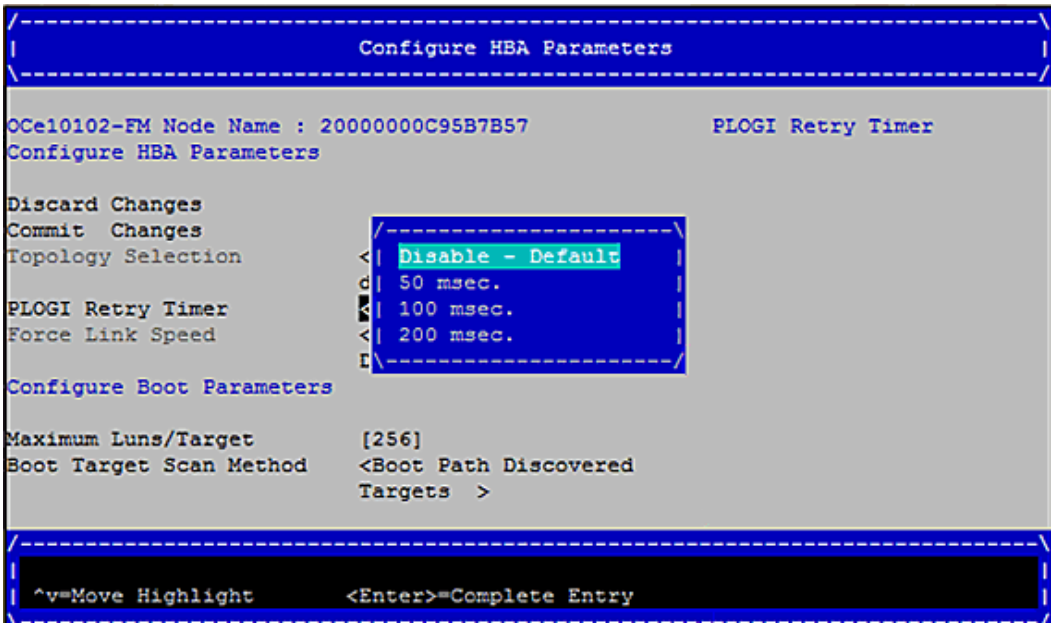

Figure 12-20 PLOGI Retry Timer

4. Select a retry timer option and press **<Enter>**. The screen is refreshed with the modified value.

   Note: Press **<Esc>** to return to the EFI utility menu.

5. Select **Commit Changes** and press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

Changing the Maximum LUNs per Target

The maximum number of LUNs represents the maximum number of LUNs that are polled during device discovery. The minimum value is 1, the maximum value is 4096. The default is 256.

To change the maximum number of LUNs:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose LUNs per target information you want to change and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure HBA Parameters** and press **<Enter>**. The Configure HBA Parameters screen is displayed.

3. From the Configure HBA Parameters screen, select **Maximum LUNs/Target** and press **<Enter>**.

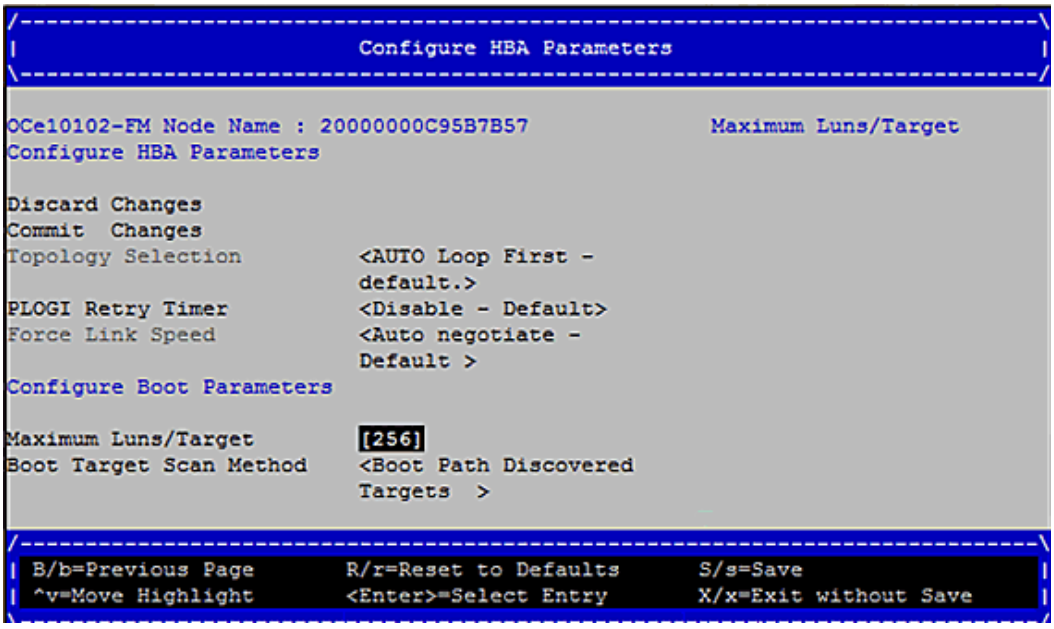

Figure 12-21 Configure HBA Parameters - Maximum LUNs/Target Field

4. Type a decimal value between 1 and 4096 and press **<Enter>**. The screen is refreshed with the modified value.

   Note: The default and typical maximum number of LUNs in a target device is 256. A higher number of maximum LUNs causes the discovery to take more time.

5. Select **Commit Changes** and press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

Changing Boot Target Scan Method

This option is only available if none of the eight boot entries is configured to boot from the DID or WWPN. The Emulex Adapter Configuration Main Menu is used to configure up to eight boot entries. With boot scan enabled, the first device issues a Name Server Inquiry.

The boot scan options are:

- Boot Path from NVRAM Targets – Boot scan discovers only LUNs that are saved to the adapter's NVRAM. Select up to eight attached devices to use as potential boot devices. Limiting discovery to a set of eight selected targets can greatly reduce the time it takes for the EFIBoot driver to complete discovery.
- Boot Path from Discovered Targets – Boot scan discovers all devices that are attached to the FC port. Discovery can take a long time on large SANs if this option is used.
- Do not create boot path.

- EFIFCScanLevel: NVRAM Targets – Boot scan sets the EFIFCScanLevel environment variable to inform the driver to configure only targets in the NVRAM boot table.
- EFIFCScanLevel - Discovered Targets – Boot scan sets the EFIScanLevel environment variable to inform the driver to configure all available targets on the SAN.

To change the boot target scan method:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose boot target scan method you want to change and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure HBA Parameters** and press **<Enter>**. The Configure HBA Parameters is displayed.
3. From the Configure HBA Parameters menu, select **Boot Target Scan Method** and press **<Enter>**. The Boot Target Scan Method menu is displayed.

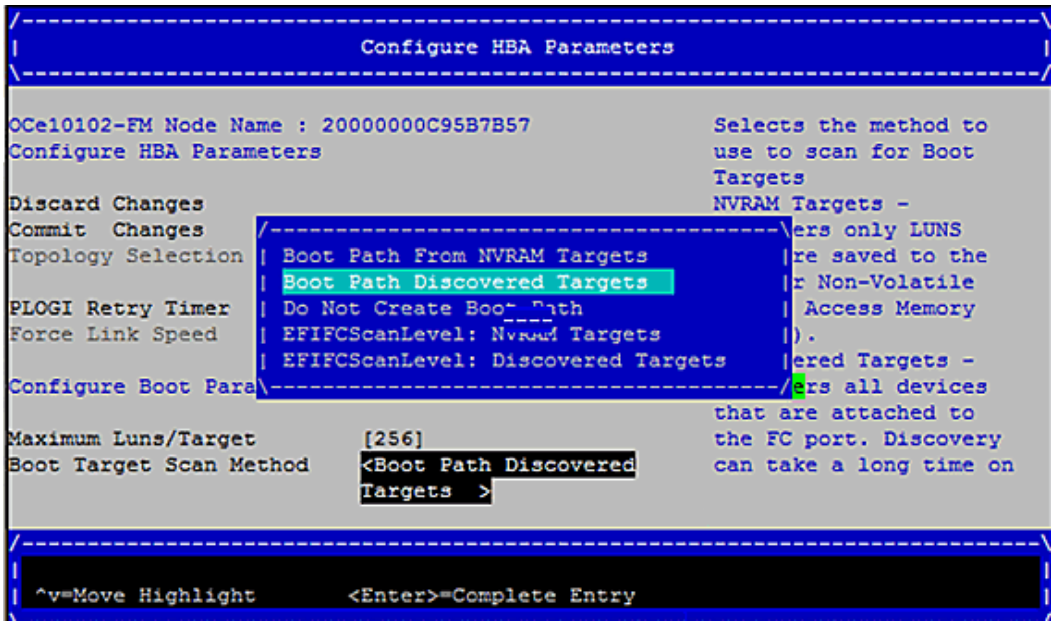

Figure 12-22 Configure HBA Parameters - Boot Target Scan Method Menu

4. Select a boot scan option and press **<Enter>**. The screen is refreshed with the modified value.

   Note: If you have a large SAN and set the boot path to "Boot Path Discovered Targets," discovery takes a long time. Press **<Esc>** to return to the EFI utility menu.

5. Select **Commit Changes** and press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

Changing Device Discovery Delay

This parameter sets a delay to occur after an loop initialization and before a scan is initiated to discover the target. The default is off or 0 seconds. Change the default if you have an HP MSA1000 or HP MSA1500 RAID array and if both of the following conditions exist:

- The MSA array is direct connected or part of an arbitrated loop (for example, daisy chained with a JBOD).
- The boot LUN is not reliably discovered. In this case, a delay may be necessary to allow the array to complete a reset.

Caution: Do not change the delay device discovery time if your MSA array is connected to a fabric switch. Setting it to any other time guarantees that the maximum delay time is seen on every loop initialization.

If both of the above conditions exist, typically set this parameter to 20 seconds. However, the delay should be only long enough for the array to be reliably discovered after a reset. Your value may be different.

To change the delay device discovery value:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose device discovery delay settings you want to change and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Configure HBA Parameters** and press **<Enter>**. The Configure HBA Parameters is displayed.
3. From the Configure HBA Parameters menu, select **Delay Device Discovery** and press **<Enter>**.

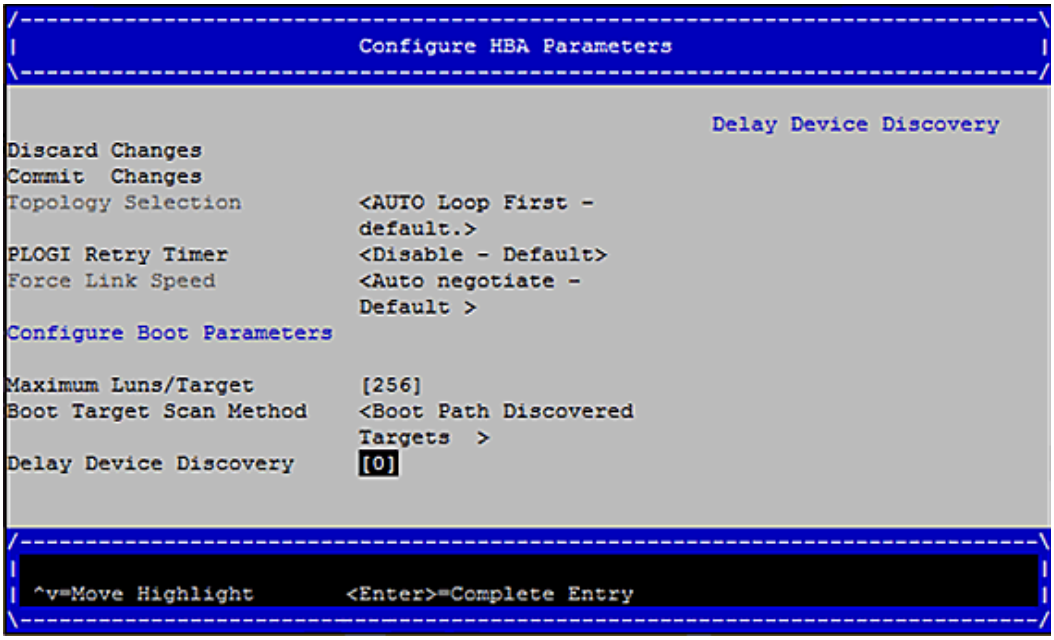

Figure 12-23 Configure HBA Parameters – Delay Device Discovery

4. Use the +/- keys to change the delay device discovery value in increments of 10 seconds and press **<Enter>**. The screen is refreshed with the modified value.
5. Select **Commit Changes** and press **<Enter>**. The Emulex Adapter Configuration Main Menu is displayed.

Resetting Emulex Adapters to Default Values

The EFI utility enables you to clear the NVRAM target list and set all boot device WWNNs back to 0, along with setting the adapter back to the default values. These default values are listed in Table 12-1.

Table 12-1 Adapter Default Values

Parameter	Default Value	Valid Values
Enable/Disable BIOS	Disabled	Enabled Disabled
PLOGI Retry Timer	Disabled	Disabled 50 msec 100 msec 200 msec
Boot Target Scan	Boot path from NVRAM targets	Boot path from NVRAM targets Boot path discovered targets Do not create boot path
Maximum LUNs Setting	0256	0–4096
Delay Device Discovery	0000	0000–0255
Advanced Mode	Enabled (OCe11100-series 4-port controllers) Disabled (OCe11100-series 2-port and OCe10100-series controllers)	Enabled Disabled
PXE Boot Support	The default for this parameter varies depending on the vendor configuration.	Enabled Disabled
SR-IOV	Disabled	Enabled Disabled
VLAN Support	Disabled	Enabled Disabled
VLAN ID	0	0–4094
VLAN Priority	0	0–7
Multichannel Support	The default for this parameter varies depending on the vendor configuration.	Enabled Disabled
Function En/Dis	Disabled	Enabled Disabled

Table 12-1 Adapter Default Values (Continued)

Parameter	Default Value	Valid Values
Bandwidth	0%	Must have a total of 100% across all ports.
LPVID	0	2-4094
Switch Option (IBM Virtual Fabric-capable configuration, if available)	IBM Virtual Fabric Mode	IBM Virtual Fabric Mode Switch Independent Mode
Switch Option (Cisco VNTag-capable configuration)	VNTag	Normal VNTag

Note: The following example sets the default values for FC and FCoE adapters only. To set other adapters to their default settings, you must use the utility for that specific protocol.

To set Emulex adapters to their default settings:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose default settings you want to change and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Set Emulex Adapter to Default Settings** and press **<Enter>**.

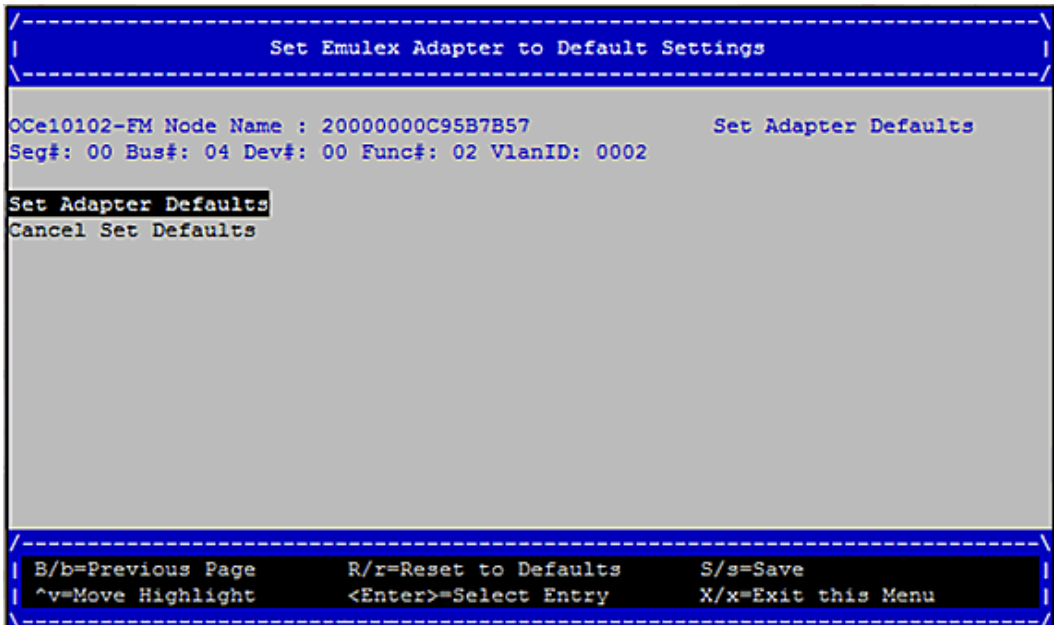

Figure 12-24 Set Adapter Defaults

Note: This will set the adapter to the FCoE driver default settings only.

3. Select **Set Adapter Defaults** and press **<Enter>** to set the adapter back to its default values. The Emulex Adapter Configuration Main Menu is displayed.

4. From the Emulex Adapter Configuration Main Menu, select **Back to Display Adapters and RECONNECT DEVICES** to complete configuration or select another configuration option.

Displaying Adapter Information

The Adapter Information screen shows the following information about the selected adapter:

- Adapter status
- Network boot status
- Link speed
- Topology
- Firmware version – refer to this firmware version if reporting a problem to Emulex Technical Support
- Universal boot version
- EFI Boot version

To display adapter information:

1. From the Adapter Selection screen (Figure 12-4), select the adapter whose information you want to view and press **<Enter>**.
2. From the Emulex Adapter Configuration Main Menu (Figure 12-5), select **Display Adapter Info** and press **<Enter>**. Information about the selected adapter is displayed.

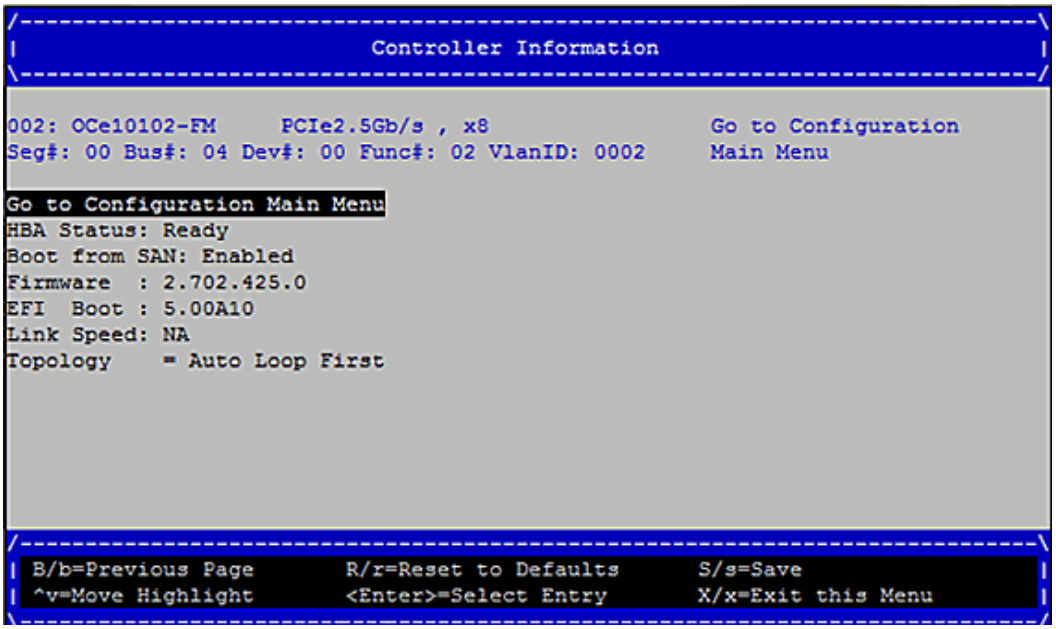

Figure 12-25 Controller Information

13. Troubleshooting

Troubleshooting for the NIC Protocol

Issues During the PXE Boot Process

Situation: If any of the following occur during the boot process:

- The PXE boot ROM sends a DHCP request extended with PXE specific options, but the request is not received.
- The DHCP responses do not contain the DHCP options (DHCPOFFERs) that include the NBP filename and boot server lists.
- The PXE client attempts to download the specified NBP over TFTP from one of the specified boot servers, but fails.
- The PXE client does not execute the downloaded NBP.

Outcome: If any of these issues occur, the boot process continues using the next available device in the boot sequence.

PXE Error Codes

Table 13-1 PXE Error Codes

Error Codes	Possible Reason	Comment/Solution
Init Error Codes		
PXE-E01: PCI Vendor and Device IDs do not match!	The PCI BIOS passes Bus/Device/Function numbers in AX register when it initializes the OptionROM. If the vendor ID & device ID did not match the vendor ID and the device ID in the device's PCI configuration space, with the UNDI device PCI structure defined in UNDI driver initialization code, this error is displayed.	This message should never be seen in the production level BIOS.
PXE-E04: Error reading PCI Configuration space	Any of the PCI BIOS INT 1Ah calls to read the PCI configuration space failed.	This should not happen with any production level motherboard BIOS.
PXE-E07: PXE BIOS calls not supported.	The PCI system BIOS does not support INT 1Ah services.	This should not happen with any PCI BIOS as all PCI BIOS must support these services.

Table 13-1 PXE Error Codes (Continued)

Error Codes	Possible Reason	Comment/Solution
ARP/TFTP Error Codes		
PXE-E11:ARP timeout	An ARP request is tried four times and the client did not receive an ARP reply.	Check the DHCP server settings. If you are connected through a switch, also check the switch settings.
PXE-E32: TFTP Open timeout.	A DHCP address and boot file name has been obtained and attempts to download the file name from a remote server.	• Check that the TFTP is configured properly. • Check that the filename is properly placed in the tftpboot directory. • Check that the PXE server is configured for TFTP not MTFTP.
PXE-E35: TFTP read timeout.	A TFTP server is not able to receive the next packet.	Check that the hardware and TFTP server are functioning properly.
PXE-E36: Error received from TFTP server.	A TFTP server sends an error packet.	Check the TFTP server settings and boot file settings.
PXE-E38: TFTP cannot open connection.	A TFTP client is not able to open a TFTP connection with the TFTP server.	Check that the correct boot file is copied into the default TFTP boot path.
PXE-E3B: TFTP error-File not found	A requested boot file is not found on TFTP server.	Check that the correct boot file is copied into the default TFTP boot path.
PXE-E3C: TFTP error - Access violation.	The TFTP server does not have enough access rights to open or read the file.	Check the TFTP server's file permissions.
PXE-E3F: TFTP packet size is invalid	TFTP packet received is larger than 1456 bytes.	Check the MTU on the Server side NIC interface.
Boot/DHCP Error Codes		
PXE-E51: No DHCP or Proxy DHCP offers were received.	The client did not receive any valid DHCP, BOOTP, or Proxy DHCP offers.	Check that the bootfile name is configured correctly for PXE Clients in the DHCP setup.
PXE-E52: Proxy DHCP offers were received. No DHCP offers were received.	The client did receive at least one valid proxyDHCP offer, but did not receive any valid DHCP or BOOTP offers.	Check that the DHCP server and PXE server are configured properly.
PXE-E53: No boot filename received.	The client did receive a valid BOOTP/DHCP offer, but does not have a boot file name to download in the DHCP offer.	Check that the bootfile name is configured correctly for PXEClients in the DHCP setup.

Table 13-1 PXE Error Codes (Continued)

Error Codes	Possible Reason	Comment/Solution
PXE-E55: Proxy DHCP service did not reply to request on port 4011.	The client issued a proxyDHCP request to the DHCP server on port 4011 but did not receive a reply.	Check that the DHCP server and TFTP server are properly configured on different servers. This issue may happen only when both are configured on separate servers.
UNDI Error Codes		
PXE-E60: Invalid UNDI API function number	The underlying UNDI drivers do not support the UNDI API sent from BaseCode/NBP.	Check with the hardware vendor.
PXE-E61: Media test failed, check cable.	There is no physical link on the PXE client port on which the boot is attempted.	Check the cables on the NIC interface.
PXE-E63: Error while initializing the NIC.	There is an issue in initializing the hardware as part of the UNDI_Initialize API.	Check with the hardware vendor.
BaseCode/UNDI Loader Error Codes		
PXE-EC1: BaseCode ROM ID structure was not found.	The UNDI boot module can not find the BaseCode ROM ID structure. This may be caused by a corrupted BaseCode ROM image.	
PXE-EC3: BaseCode ROM ID structure is invalid.	The BaseCode ROM ID structure is invalid. This may be caused by a corrupted BaseCode image in ROM.	
PXE-EC4: UNDI ROM ID structure was not found.	The BaseCode loader module could not locate the UNDI ROM ID structure. The UNDI ROM image is probably corrupted.	
PXE-EC5: UNDI ROM ID structure is invalid.	The UNDI ROM image is probably corrupted.	
PXE-EC8:!PXE structure was not found in UNDI driver code segment.	The UNDI ROM image is probably corrupted.	
Bootstrap and Discovery Error Codes		
PXE-E74: Bad or missing PXE menu and /or prompt information	PXE tags were detected but the boot menu and/or boot prompt were not found or were invalid.	

Table 13-1 PXE Error Codes (Continued)

Error Codes	Possible Reason	Comment/Solution
PXE-E77: Bad or missing discovery server list.	There are two possible reasons. One is that Multicast and Broadcast discovery are both disabled. The other is that Multicast and Broadcast are enabled, but the server list tag is not found or is invalid.	
PXE-E78: Could not locate boot server.		
PXE-E79: NBP is too big to fit in free base memory.	The NBP file size is larger than the free base memory.	Check the NBP file size.
Miscellaneous Error Codes		
PXE-EA0: Network boot cancelled by keystroke	Pressing **<Ctrl>** and **<C>** during DHCP discovery.	

Troubleshooting for the iSCSI Protocol

The following section includes troubleshooting information for the iSCSISelect utility. Ensure that you also lookup the readme.txt file located on CD1 for the most current troubleshooting issues.

Table 13-2 Troubleshooting the iSCSISelect Utility

Issue	Answer/Solution
iSCSI BIOS banner is not displayed during system post.	• Check the motherboard BIOS configuration and make sure that the Option ROM is enabled and is set for the PCIe slot into which the OneConnect adapter is inserted. • If the Option ROM is enabled and is set for the PCIe slot into which the OneConnect adapter is inserted and the issue persists, erase the Controller Configuration. For more information, see “Erasing the Configuration” on page 93.

Table 13-2 Troubleshooting the iSCSISelect Utility (Continued)

Issue	Answer/Solution
Unable to ping iSCSI target IP address	• Check cable connections and make sure they are securely connected at both ends. Make sure the link light is ON at both ends of the cable. • Verify that you have assigned a valid IP address with the correct subnet mask to the interface(s) that are connected to the network. • Check for duplicate IP addresses. • Make sure you are connected to the correct port. • If the IP address is coming from DHCP, check that the DHCP server is up and available. • Is the target on a different subnet? Check the default gateway and make sure that the IP addresses of both the default gateway and the remote host are correct. • Check link status under Network Configuration. If you try changing the initiator link status, you can back out one screen then go back to Network Configuration to see a view of your current link status.
Login to iSCSI target fails or login succeeds, but no LUNs are available.	• Check initiator IQN name and target IQN name. Verify that they are properly specified. • Check target's ACL settings (if any) to verify that the initiator's IQN name is listed and can be recognized. • Make sure that the target login parameters are compatible with the initiator's. • If this checklist confirms that initiator and target are configured correctly and the issue persists, erase the Controller Configuration. For more information, see “Erasing the Configuration” on page 93.
Login to iSCSI target is successful, but iSCSI I/O causes the system to hang or freeze.	Check the jumbo frame settings on the iSCSI target. If enabled, change the frame size to 1514 and retry. This isolates any issues in the network related to jumbo frames. Jumbo frames, when supported by the entire network, provide increased performance. **Note:** OneConnect adapters support jumbo frames.

Table 13-2 Troubleshooting the iSCSISelect Utility (Continued)

Issue	Answer/Solution
Unable to boot from the iSCSI target.	• Check the target setup. Check the target ACL to verify that the initiator's iSCSI name is listed and can be recognized. • Check the initiator name and make sure it is correct. • If applicable, verify that you have selected the iSCSI LUN as the boot LUN in your system BIOS setting. • Check the system BIOS for boot device priority order. Make sure that the boot device is at the top. If using DHCP: • If Boot Support is not enabled, enable it on the iSCSI Initiator menu. (For more information, see chapter 8., "Configuring and Managing the iSCSI Initiator with the iSCSISelect Utility," on page 76.) If DHCP boot support is enabled, check the DHCP setup and also verify that you have added the root path to the DHCP server. For more information, see "Setting Up a Basic iSCSI Boot Configuration" on page 73. • If this checklist confirms that the initiator and target are configured correctly and the issue persists, erase the Controller Configuration. For more information, see "Erasing the Configuration" on page 93.
BIOS post shows "BIOS Not Installed" message.	• If you *have not* configured an iSCSI boot target, this is proper normal behavior. • If you *have* configured an iSCSI boot target and the BIOS cannot find a bootable LUN, then refer to the solutions provided in the issue *Unable to boot from the iSCSI target*.
If solutions for issues 1-3 and 5-6 all fail.	Use the iSCSISelect utility to erase the controller configuration. To clear controller configuration: 1) From the Controller Configuration menu, select **Erase Configuration** and press **<Enter>**. 2) A message appears asking if you want to erase the current configuration. Press **<Y>**. 3) You are cautioned that the operation removes any existing configuration permanently. Press **<Y>**. **Note:** If you have multiple controllers, you must erase the configuration of each controller separately. For more information, see "Erasing the Configuration" on page 93. After you erase the controller configuration, reboot the system and then reconfigure the OneConnect adapter.

You receive this POST error message:
`Initiator iSCSI Name mismatch, Please use iSCSISelect to set a single name for all controllers.`
`Press <Ctrl><S> to enter iSCSISelect. (Reboot required)`
	In the iSCSI BIOS, the iSCSI initiator name may be different if there is more than one OneConnect controller in the system. If the iSCSI initiator name is different on multiple controllers, you receive a POST error message indicating an iSCSI name mismatch. You must enter the iSCSISelect utility and save a new initiator name on the first iSCSISelect utility menu screen so that the iSCSI initiator name on all controllers match. All logins from the multiple controllers use the new name.

Table 13-2 Troubleshooting the iSCSISelect Utility (Continued)

Issue	Answer/Solution

You receive any of the following POST error messages or warnings:
`Redboot Initialization failed...`
`Firmware Load failed...`
`DDR config failed...`
`DDR callibrate failed...`
`DDR test failed...`
`SEEPROM checksum failed...`
`Secondary firmware image loaded...`
	These POST messages indicate that you must reload the UCNA firmware using OneCommand Manager or one of the Emulex online or offline utilities. If the error(s) persist, contact Technical Support.

You receive this POST error message: `Firmware halted. This firmware does not support this controller.`	The firmware loaded on this UCNA is not supported. Load the appropriate firmware for the controller.

Troubleshooting for the FcoE Protocol

Table 13-3 Troubleshooting the FCoE Protocol

Issue	Answer/Solution
Cisco Nexus switch configuration situations: • Windows creates the NTFS partition properly, but then reports that “The hard disk containing the partition or free space you chose has a LUN greater than 0. Setup cannot continue”. (Dell 1850 server). • Windows reboots successfully, but then gets stuck during the GUI portion of the installation right from the beginning. (HP DL385G2 server).	Ensure that the FCoE switch ports are configured correctly for the UCNA FCoE settings.

Appendix A. Configuring iSCSI through a DHCP Server using Vendor-Specific Option 43

Overview

An iSCSI initiator requires the following parameters to boot from a target:

- Its IP address
- Its unique node name
- The boot iSCSI target's IP address
- The boot target's name. If not available, this may be discovered using the iSCSI discovery protocol.
- The target's non-default TCP port number (if applicable)
- Header and data digest settings to be used with the target
- Authentication parameters, if applicable

All of the above parameters may be configured from a centrally configured DHCP server using vendor-specific option 43. This appendix documents this method of configuration. For this method, the initiator must be configured (using non-DHCP means) with the appropriate DHCP vendor ID. The method and format for specifying the vendor ID is outside the scope of this document. The initiator offers this Vendor ID to the DHCP server to retrieve data in the format described in the following sections.

Two other methods for configuration are not documented in this appendix:

- Manual configuration using iSCSISelect or SMCLP/MILI
- Pre-boot configuration using CLP /BIOS 3.0

Format of Vendor-Specific Option 43

The format for vendor-specific option 43 is as follows:

```
iscsi:<ipaddress>:<protocol>:<iscsi port number>:<lun>:<target name>
```

Fields enclosed in angular brackets (including the angular brackets) should be replaced with their corresponding values. All fields are case insensitive.

See the example at the end of this document.

Description of Parameters

<ipaddress>

Replace this parameter with a valid IPv4 address in dotted decimal notation. This is a mandatory field.

<protocol>

Replace this parameter with a decimal number indicating the TCP port. The default TCP port is 3260.

<iscsi port number>

Replace this parameter with a decimal number ranging from 1 to 65535 (inclusive). It is an optional field.

<lun>

This parameter is a hexadecimal representation of logical unit number of the boot device. It is an optional field. If not provided, LUN 0 is assumed to be the boot LUN. It is an 8-byte number which must be specified as a hexadecimal number consisting of 16 digits, with an appropriate number of 0's padded to the left, if required.

<target name>

Replace this parameter with a valid iSCSI target 'iqn' name of up to 223 characters. This is a mandatory field.

Example

```
iscsi:010.010.010.001:0:3260:0:iqn.1992-08.com.netap:sn.151729740
```

The above example specifies the following:

- Target IP address: 010.010.010.001
- Target protocol: 0
- Target TCP port: 3260
- Target boot LUN: 0
- Target iqn name: iqn.1992-08.com.netap:sn.151729740

Appendix B. Example for Installing and Configuring Linux or Citrix for PXE Boot and UEFI Boot

Linux and Citrix PXE Server Remote Installation Procedure

PXE configuration requires a PXE server and the PXE client.

Setting up a PXE server requires the following configurations:

- NFS server
- TFTP server
- DHCP server
- PXE boot server

The pxelinux functionality occurs in this order:

1. The client machine boots to PXE which requests a DHCP address.
2. The DHCP server responds with an IP address for the client machine along with the address of a TFTP server and a filename to load (pxelinux.0) from that server.
3. The client downloads pxelinux.0 from the specified TFTP server and executes it.
4. The pxelinux.0 file searches the pxelinux.cfg directory on the server for a configuration file that matches the IP address of the machine. If no matches are found, it attempts to load a file called default.
5. The configuration file loaded by pxelinux.0 has instructions on what to do next. Some of the choices include boot to local hard drive, boot to an image file (floppy image), or load vmlinuz and initrd.img.
6. The client searches for a configuration file with the IP address converted to hexadecimal (for example, 192.168.1.60 becomes C0A8013C) or the MAC address of your PXE boot client's Ethernet card with a prefix of "01". The MAC address should be separated with dashes instead of colons.

   In this example, the client looks for the following configuration file names and uses the first one it finds.

   ```
   01-00-00-C9-5B-75-A8
   C0A8013C
   C0A8013
   C0A801
   C0A80
   C0A8
   C0A
   C0
   C
   default
   ```

7. The default file's contents should look similar to the following:

```
prompt 1
default linux
timeout 100

label linux
kernel vmlinuz
append initrd=initrd.img ramdisk_size=9216 noapic acpi=off
```

PXE Server

NFS Server Configuration Script

```
[root@bglinux156 ~]# mkdir /work
[root@bglinux156 ~]# mount 10.192.194.110:/work /mnt
[root@bglinux156 ~]# cd /mnt/
[root@bglinux156 ~]# cp -r rhel5564/ /work/ #copy the entire
 directory to "/work"
[root@bglinux156 ~]# cd /work/rhel5564
[root@bglinux156 ~]# cp -r images/ /tftpboot/linux-install/
[root@bglinux156 ~]# vim /etc/exports###(Add "/work *(rw,sync)")
[root@bglinux156 ~]# exportfs -a (reflect changes in NFS Server)
```

1. Restart NFS Services.

```
[root@bglinux156 ~]# /etc/rc.d/init.d/portmap restart
Stopping portmap: [ OK ]
Starting portmap: [ OK ]
[root@bglinux156 ~]# /etc/rc.d/init.d/nfslock restart
Stopping NFS locking: [ OK ]
Stopping NFS statd: [ OK ]
Starting NFS statd: [ OK ]
[root@bglinux156 ~]# /etc/rc.d/init.d/nfs restart
Shutting down NFS mountd: [ OK ]
Shutting down NFS daemon: [ OK ]
Shutting down NFS quotas: [ OK ]
Shutting down NFS services: [ OK ]
Starting NFS services: [ OK ]
Starting NFS quotas: [ OK ]
Starting NFS daemon: [ OK ]
Starting NFS mountd: [ OK ]
```

2. Check if the NFS services are running.

```
[root@bglinux156 ~]# rpcinfo -p
 program vers proto port
```

```
100000 2 tcp 111 portmapper
100000 2 udp 111 portmapper
100021 1 udp 56782 nlockmgr
100021 3 udp 56782 nlockmgr
100021 4 udp 56782 nlockmgr
100021 1 tcp 44855 nlockmgr
100021 3 tcp 44855 nlockmgr
100021 4 tcp 44855 nlockmgr
100024 1 udp 766 status
100024 1 tcp 769 status
100011 1 udp 815 rquotad
100011 2 udp 815 rquotad
100011 1 tcp 818 rquotad
100011 2 tcp 818 rquotad
100003 2 udp 2049 nfs
100003 3 udp 2049 nfs
100003 4 udp 2049 nfs
100003 2 tcp 2049 nfs
100003 3 tcp 2049 nfs
100003 4 tcp 2049 nfs
100005 1 udp 828 mountd
100005 1 tcp 831 mountd
100005 2 udp 828 mountd
100005 2 tcp 831 mountd
100005 3 udp 828 mountd
```

TFTP Server Setup

```
[root@bglinux156 ~]# vi /etc/xinetd.d/tftp

service tftp
{
 socket_type = dgram
 protocol = udp
 wait = yes
 user = root
 server = /usr/sbin/in.tftpd
 server_args = -s /tftpboot/linux-install #This line specifies
 #path where the pxe boot searches for
 #the images
 disable = no #convert this line from yes to no
 per_source = 11
 cps = 100 2
```

```
 flags = IPv4
}

[root@bglinux156 ~]# /sbin/chkconfig --level 345 xinetd on
[root@bglinux156 ~]# /sbin/chkconfig --level 345 tftp on
[root@bglinux156 ~]# service xinetd restart
```

DHCP Server Configuration

1. Install the following RPMs in the server if not installed:

```
[root@bglinux156 ~]# rpm -qa | grep dhcp
dhcpv6-client-1.0.10-18.el5
dhcp-devel-3.0.5-23.el5
dhcp-3.0.5-23.el5
```

2. Make the following entry in /etc/dhcpd.conf file:

```
#
# DHCP Server Configuration file.
# see /usr/share/doc/dhcp*/dhcpd.conf.sample
#
ddns-update-style interim;
 subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.50 192.168.1.90;
 default-lease-time 3600;
 max-lease-time 4800;
 option subnet-mask 255.255.255.0;
 option domain-name "pxe_text";
 option time-offset -8;
 }

host bglinux45{
 next-server 192.168.1.1;
 hardware ethernet 00:00:C9:5B:75:A8;
 fixed-address 192.168.1.60;
 option host-name "linux-test";

  filename "pxelinux.0";
 }
###This sets up a DNS server that will assign IP Address 192.168.1.60
###to the client machine that has MAC Address "00:00:C9:5B:75:A8"
###assigned to a PXE capable NIC
###The only thing that needs to be changed in the above, is the MAC
###Address to match that of the NIC in the client box
###The IP address that follows the next-server option should be the IP
###address of the tftp server

[root@bglinux156 ~]# service dhcpd restart
Shutting down dhcpd: [ OK ]
```

```
Starting dhcpd: [ OK ]
```

PXE Boot Server Configuration

```
[root@bglinux156 ~]# rpm -qa | grep system-config-netboot
system-config-netboot-cmd-0.1.45.1-1.el5
system-config-netboot-0.1.45.1-1.el5
```

Copying Files to the TFTP Server with the Graphical Version of the Network Booting Tool

Copy the files necessary to start the installation to the TFTP server to enable them to be found when the client requests them. Run the Network Booting Tool on the NFS, FTP, or HTTP server. A separate PXE server is not necessary.

To use the graphical version of the Network Booting Tool, you must be running the X Window System, have root privileges, and have the redhat-config-netboot RPM package installed.

To start the Network Booting Tool from the desktop, do one of the following:

- Go to the Main Menu Button (on the Panel) and select **System Settings >Server Settings >Network Booting Service.**

  -or-

- Type the command system-config-netboot at a shell prompt. (For example, in an XTerm or a GNOME terminal.)

  Note: If you are starting the Network Booting Tool for the first time, select **Network Install from the First Time Druid**.

Copy the files necessary to start the installation to the TFTP server.

1. Select **Configure > Network Installation** from the pull-down menu.

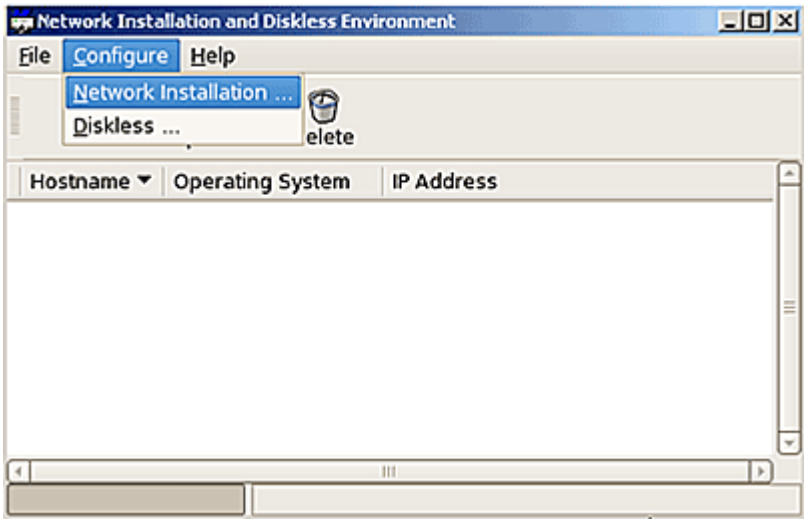

Figure B-1 Network Installation and Diskless Environment Window

2. The Configure Network Installations window is displayed. Click **Add**.

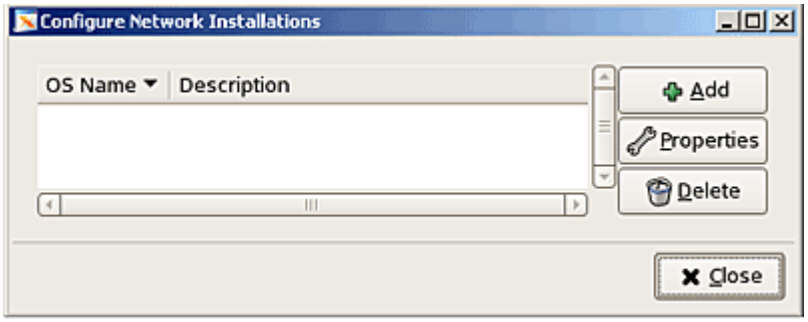

Figure B-2 Configure Network Installations Window

3. The Network Installation Dialog window is displayed.

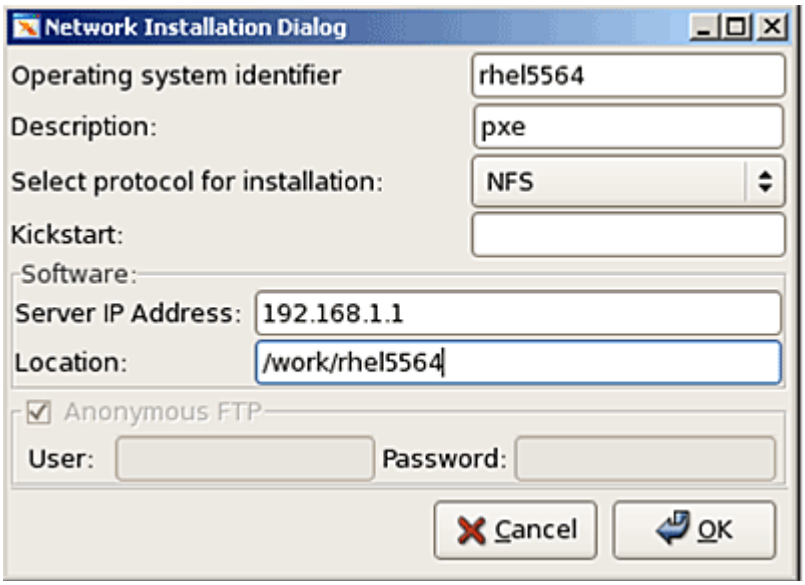

Figure B-3 Network Installation Dialog Window

- Enter the operating system identifier and description.
- Select **pxe** as the protocol for installation.
- Enter the IP address of the TFTP server (as set up in the DHCP server configuration) in the server IP address field.
- Enter a directory location for the server.

The Network Installation and Diskless Environment window shows the IP address of the TFTP server.

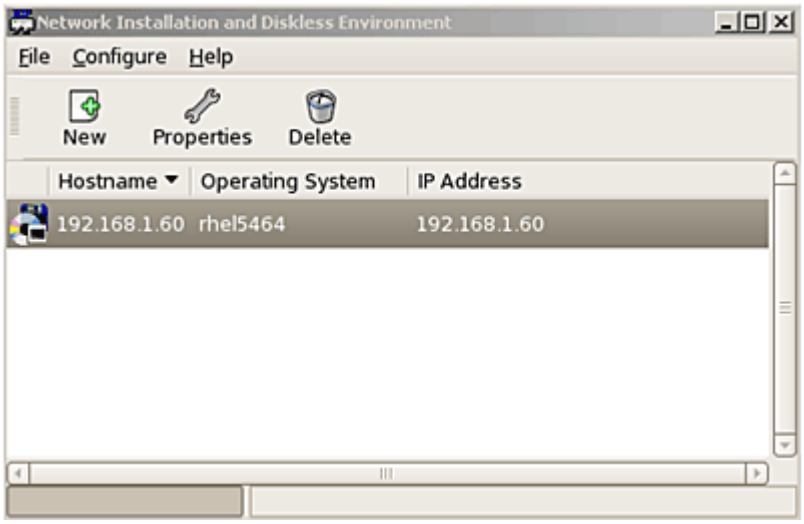

Figure B-4 Network Installation and Diskless Environment Window with IP Address

Configuring the Host

To configure the host:

1. Double-click on the IP address row in the Network Installation and Diskless Environment window (Figure B-4). An edit dialog box is displayed.

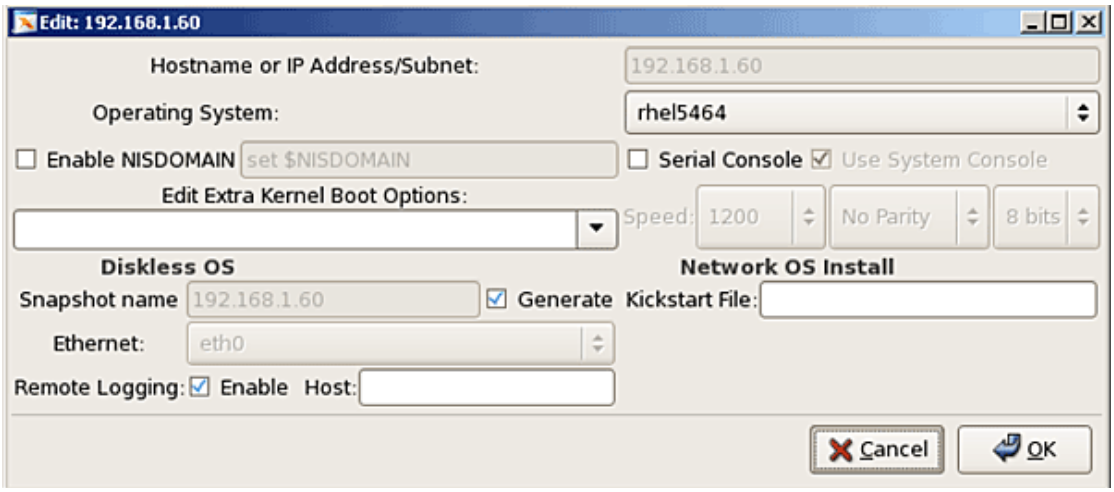

Figure B-5 Edit Dialog Box

2. In the Hostname or IP Address/Subnet field, enter the IP address, fully qualified hostname, or a subnet of systems that should be allowed to connect to the PXE server for installations. In Figure B-5, the Hostname/IP Address is the IP address of the client machine.
3. In the case of a multi-boot environment, select an operating system preference.

4. Select the operating system identifier to install on this client. The list is populated from the network install instances created from the Network Installation dialog box.
5. If you use a serial console, check the **Serial Console** check box.
6. Specify the location of a kickstart file, such as http://server.example.com/kickstart/ks.cfg. This file can be created with the Kickstart Configuration.

   Note: Ignore the Snapshot name and Ethernet options. They are only used for diskless environments.

7. Click **OK**. This closes the dialog box and creates configuration files within:

   `/tftpboot/linux-install and /tftpboot/linux-install/pxelinux.cfg`

8. Go to /tftpboot/pxelinux.cfg and open the file C0A8013C. The C0A8013C file is created when you assign the client IP using "system-config- netboot". This is the hexadecimal address of the IP assigned to the client NIC. It is 192.168.1.60 in the example in Figure B-4.

Enabling the PXE Client with a PXE-enabled Adapter

The PXE client must have a PXE-enabled adapter.

1. Power on the PXE client.
2. Press **<F12>** to enable network boot. Pressing **<F12>** accesses the DHCP server IP and the Boot Linux image.

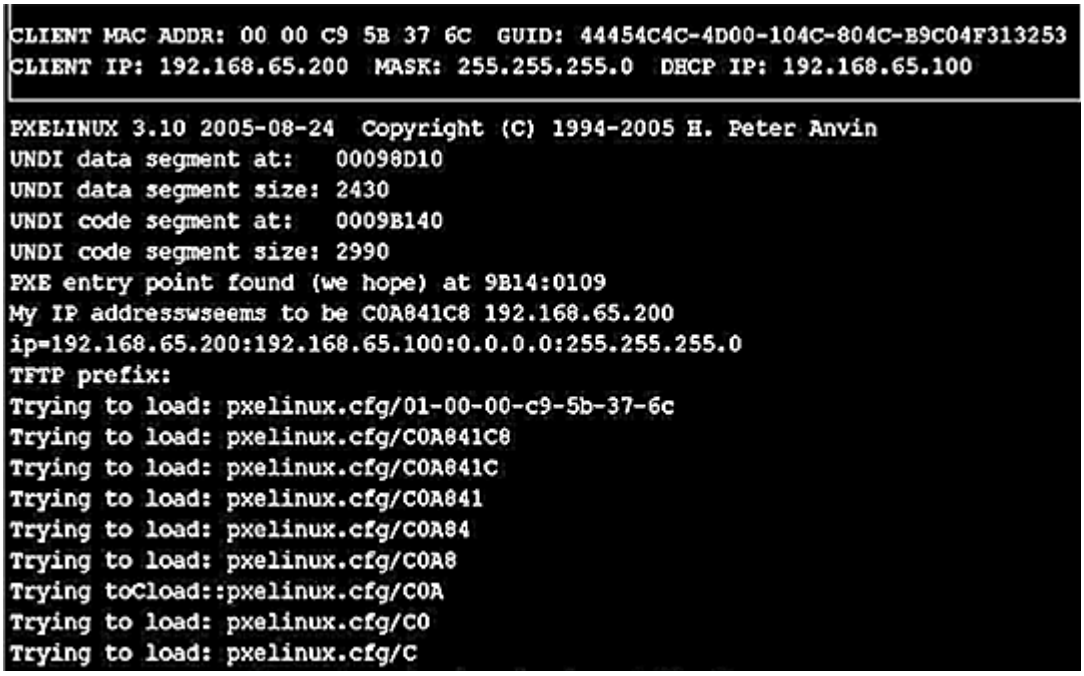

Figure B-6 Enabling Network Boot

Appendix C. Example for Configuring and Booting UEFI NIC

UEFI NIC Server Configuration Script for SLES11 SPx

```
[root@orleansrhel5564 ~]# ls /root/sles11sp164/
SLES-11-SP1-DVD-x86_64-GM-DVD1.iso
[root@orleansrhel5564 ~]# mkdir test1
[root@orleansrhel5564 ~]# mkdir test2
[root@orleansrhel5564 ~]# mount -o loop
sles11sp164/SLES-11-SP1-DVD-x86_64-GM-DVD1.iso test1
[root@orleansrhel5564 ~]# ls test1
ARCHIVES.gz COPYING.degpg-pubkey-3d25d3d9-36e12d04.asc media.1
boot COPYRIGHT gpg-pubkey-7e2e3b05-4be037ca.asc NEWS
ChangeLog COPYRIGHT.degpg-pubkey-9c800aca-4be01999.asc pubring.gpg
content directory.yast gpg-pubkey-a1912208-446a0899.asc README
content.ascdocu gpg-pubkey-b37b98a9-4be01a1a.asc suse
content.keygpg-pubkey-0dfb3188-41ed929b.ascINDEX.gz
control.xmgpg-pubkey-1d061a62-4bd70bfa.asclicense.tar.gz
COPYING gpg-pubkey-307e3d54-4be01a65.ascls-lR.gz
[root@orleansrhel5564 ~]# mount -o loop test1/boot/x86_64/efi test2
[root@orleansrhel5564 ~]# ls -lar test2
total 28
-rwxr-xr-x 1 root root 48 May 20 2010 .packages.boot-efi
drwxr-xr-x 3 root root 2048 May 20 2010 efi
drwxr-x--- 20 root root 4096 Jan 5 14:04 ..
drwxr-xr-x 3 root root 16384 Jan 1 1970 .
[root@orleansrhel5564 ~]# ls -lar test2/efi/boot/
bootx64.efi elilo.conf initrd linux
[root@orleansrhel5564 ~]# ls -lar test2/efi/boot/
total 26838
-rwxr-xr-x 1 root root 3231872 May 20 2010 linux
-rwxr-xr-x 1 root root 23999623 May 20 2010 initrd
-rwxr-xr-x 1 root root 512 May 20 2010 elilo.conf
-rwxr-xr-x 1 root root 241318 May 20 2010 bootx64.efi
drwxr-xr-x 3 root root 2048 May 20 2010 ..
drwxr-xr-x 2 root root 2048 May 20 2010 .
[root@orleansrhel5564 ~]# cp test2/boot/efi/* /tftpboot/linux-install/
```

NFS Server Configuration Script

```
[root@bglinux156 ~]# /etc/rc.d/init.d/portmap restart
Stopping portmap: [ OK ]
Starting portmap: [ OK ]
[root@bglinux156 ~]# /etc/rc.d/init.d/nfslock restart
Stopping NFS locking: [ OK ]
Stopping NFS statd: [ OK ]
Starting NFS statd: [ OK ]
[root@bglinux156 ~]# /etc/rc.d/init.d/nfs restart
Shutting down NFS mountd: [ OK ]
Shutting down NFS daemon: [ OK ]
Shutting down NFS quotas: [ OK ]
Shutting down NFS services: [ OK ]
Starting NFS services:[ OK ]
Starting NFS quotas: [ OK ]
Starting NFS daemon: [ OK ]
Starting NFS mountd: [ OK ]
```

Check if the NFS services are running:

```
[root@bglinux156 ~]# rpcinfo -p
 program vers proto port
 100000 2 tcp 111 portmapper
 100000 2 udp 111 portmapper
 100021 1 udp 56782 nlockmgr
 100021 3 udp 56782 nlockmgr
 100021 4 udp 56782 nlockmgr
 100021 1 tcp 44855 nlockmgr
 100021 3 tcp 44855 nlockmgr
 100021 4 tcp 44855 nlockmgr
 100024 1 udp 766 status
 100024 1 tcp 769 status
 100011 1 udp 815 rquotad
 100011 2 udp 815 rquotad
 100011 1 tcp 818 rquotad
 100011 2 tcp 818 rquotad
 100003 2 udp 2049 nfs
 100003 3 udp 2049 nfs
 100003 4 udp 2049 nfs
 100003 2 tcp 2049 nfs
 100003 3 tcp 2049 nfs
 100003 4 tcp 2049 nfs
 100005 1 udp 828 mountd
```

```
100005 1 tcp 831 mountd
100005 2 udp 828 mountd
100005 2 tcp 831 mountd
100005 3 udp 828 mountd
```

DHCP Server Configuration

```
[root@orleansrhel5564 ~]# cat /etc/dhcpd.conf
```

1. Install the following RPMs in the server if not installed:

```
[root@bglinux156 ~]# rpm -qa | grep dhcp
dhcpv6-client-1.0.10-18.el5
dhcp-devel-3.0.5-23.el5
dhcp-3.0.5-23.el5
```

2. Make the following entry in /etc/dhcpd.conf file:

```
#
# DHCP Server Configuration file.
#      see /usr/share/doc/dhcp*/dhcpd.conf.sample
#

ddns-update-style interim;
#ignore client-updates;
subnet 192.168.47.0 netmask 255.255.255.0 {
range 192.168.47.50 192.168.47.100;
default-lease-time 3600;
max-lease-time-4800;
option subnet-mask 255.255.255.0;
option domain-name "pxe_test";
option time-offset -8; # Eastern Standard Time
}

# we want the nameserver to appear at a fixed address
 host orleansrhel5564 {
 next-server 192.168.47.1;#IP of the NFS Server
 hardware ethernet 00:00:c9:5b:a5:26;#mac address of
 #the client
#machine

 fixed-address 192.168.47.60; #IP assigned to the
 #client machine
 option host-name "linux-test";
 filename "bootx64.efi"; #Used for UEFI boot
 }

###This sets up a DNS server that will assign IP Address 192.168.47.60
###to the client machine that has MAC Address "00:00:c9:5b:a5:26"
###assigned to a PXE(UEFI) capable NIC
###The only thing that needs to be changed in the above, is the MAC
```

```
###Address to match that of the NIC in the client box
###The IP address that follows the next-server option should be the IP
###address of the tftp server
[root@bglinux156 ~]# service dhcpd restart
Shutting down dhcpd: [ OK ]
Starting dhcpd: [ OK ]
```

TFTP Server Setup

```
[root@orleansrhel5564 ~]# cat /etc/xinetd.d/tftp
service tftp
{
 disable = no
 socket_type = dgram
 protocol = udp
 wait= yes
 user = root
 server = /usr/sbin/in.tftpd
 server_args = -s /tftpboot/linux-install
 per_source = 11
 cps = 100 2
 flags = IPv4
```

UEFI NIC Server Configuration Script for RHEL 6.x

Setup Information

PXE client server: Dell R710 with Emulex OneConnect UCNA or Intel X520 card (Test System to do UEFI PXE boot)

PXE server: HP running RHEL 5.5 64 bit

NFS Configuration

```
[root@orleans ~]# mkdir /work
[root@orleans ~]# mount 10.192.194.110:/work /mnt   #### Mounting network drive
[root@orleans ~]# cd /mnt/
[root@orleans ~]# cp -r rhel6364/ /work/  #### Copying rhel6.1-64 bit os to PXE
server mechine
[root@orleans ~]# vim /etc/exports       ####(Add "/work    *(rw,sync)"
[root@orleans ~]#  exportfs -a           ####(reflect changes in NFS Server)


#### Restart NFS services
[root@orleans ~]#/etc/rc.d/init.d/portmap restart
[root@orleans ~]# /etc/rc.d/init.d/nfslock restart
[root@orleans ~]# /etc/rc.d/init.d/nfs restart
```

```
#### Check if NFS is running fine

[root@orleans ~]# rpcinfo -p

   program vers proto   port
    100000    2   tcp    111  portmapper
    100000    2   udp    111  portmapper
    100021    1   udp  56782  nlockmgr
    100021    3   udp  56782  nlockmgr
    100021    4   udp  56782  nlockmgr
    100021    1   tcp  44855  nlockmgr
    100021    3   tcp  44855  nlockmgr
    100021    4   tcp  44855  nlockmgr
    100024    1   udp    766  status
    100024    1   tcp    769  status
    100011    1   udp    815  rquotad
    100011    2   udp    815  rquotad
    100011    1   tcp    818  rquotad
    100011    2   tcp    818  rquotad
    100003    2   udp   2049  nfs
    100003    3   udp   2049  nfs
    100003    4   udp   2049  nfs
    100003    2   tcp   2049  nfs
    100003    3   tcp   2049  nfs
    100003    4   tcp   2049  nfs
    100005    1   udp    828  mountd
    100005    1   tcp    831  mountd
    100005    2   udp    828  mountd
    100005    2   tcp    831  mountd
    100005    3   udp    828  mountd
```

TFTP Configuration

```
[root@orleans ~]# vi /etc/xinted.d/tftp

# default: off
# description: The tftp server serves files using the trivial file transfer \
#       protocol.  The tftp protocol is often used to boot diskless \
#       workstations, download configuration files to network-aware printers, \
#       and to start the installation process for some operating systems.
service tftp
{
        disable                 = no
        socket_type             = dgram
        protocol                = udp
        wait                    = yes
        user                    = root
```

```
        server                  = /usr/sbin/in.tftpd
        server_args             = -s /tftpboot/linux-install
        per_source              = 11
        cps                     = 100 2
        flags                   = IPv4
}


##### Restart TFTP service

[root@orleans ~]# service xinetd restart
Stopping xinetd:                                   [  OK  ]
Starting xinetd:                                   [  OK  ]
[root@orleans ~]# chkconfig tftp on
```

PXE Configuration

```
[root@orleans ~]# cd /work/rhel6364/

[root@orleans RHEL6364]# cd images/pxeboot/

[root@orleans pxeboot]# cp -r * /tftpboot/linux-install/
#### Copy vmlinuz and initrd to TFTP root directory

[root@orleans pxeboot]# mkdir -p /root/test1

[root@orleans images]# cd /work/rhel6364/images/

[root@orleans images]# mount -o loop efiboot.img /root/test1     ###### Extract
efiboot.img to get bootx64.efi and BOOTX64.conf files

[root@orleans images]# cd /root/test1

[root@orleans test1]# cd efi/boot/

[root@orleans boot]# cp -r * /tftpboot/linux-install/   ###### Copy bootx64.efi
and BOOTX64.conf to TFTP root directory

#### Editing efidefault to the following content

[root@orleans boot]# cat /tftpboot/linux-install/efideault
default=0
timeout 10
splashimage=(nd)/splash.xpm.gz
title RHEL6364
        root (nd)
        splashimage /splash.xpm.gz
        kernel /vmlinuz keymap=us lang=en_US  method=nfs:192.168.1.1:/RHEL6364
ip=dhcp noipv6
```

```
        initrd /initrd.im
```

Configuring DHCP

```
[root@orleans ~]# cat  /etc/dhcpd.conf
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.sample
ddns-update-style interim;
ignore client-updates;
#allow booting;
#allow bootp;
subnet 192.168.1.0 netmask 255.255.255.0 {
 range 192.168.1.50 192.168.1.90;
 default-lease-time 3600;
 max-lease-time 4800;
 option subnet-mask 255.255.255.0;
# option router 192.168.1.1;
 option domain-name "pxe_text";
# option name-server 192.168.1.20;
 option time-offset -8;
 }

host bglinux45{
  next-server 192.168.1.1;    #### IP address of PXE server interface connected
back to back to PXE client interface
  hardware ethernet 00:00:C9:BB:C7:8F;  #### MAC address of PXE client interface
  fixed-address 192.168.1.60;  #### IP address to be assigned to PXE client
interface
  option host-name "linux-test";
  filename "bootx64.efi";
 }

#### Restart DHCP service
[root@orleans ~]# service dhcpd restart
Shutting down dhcpd:                                [  OK  ]
Starting dhcpd:                                     [  OK  ]
```

Note: Reboot your system under test and boot from the PXE client interface.

Configuring the IBM HS22 Blade with e-Raptor MEZZ

To install and update the driver, follow these steps:

1. Press **<F1>** during the system boot and log into the System Configuration and Boot Management screen.

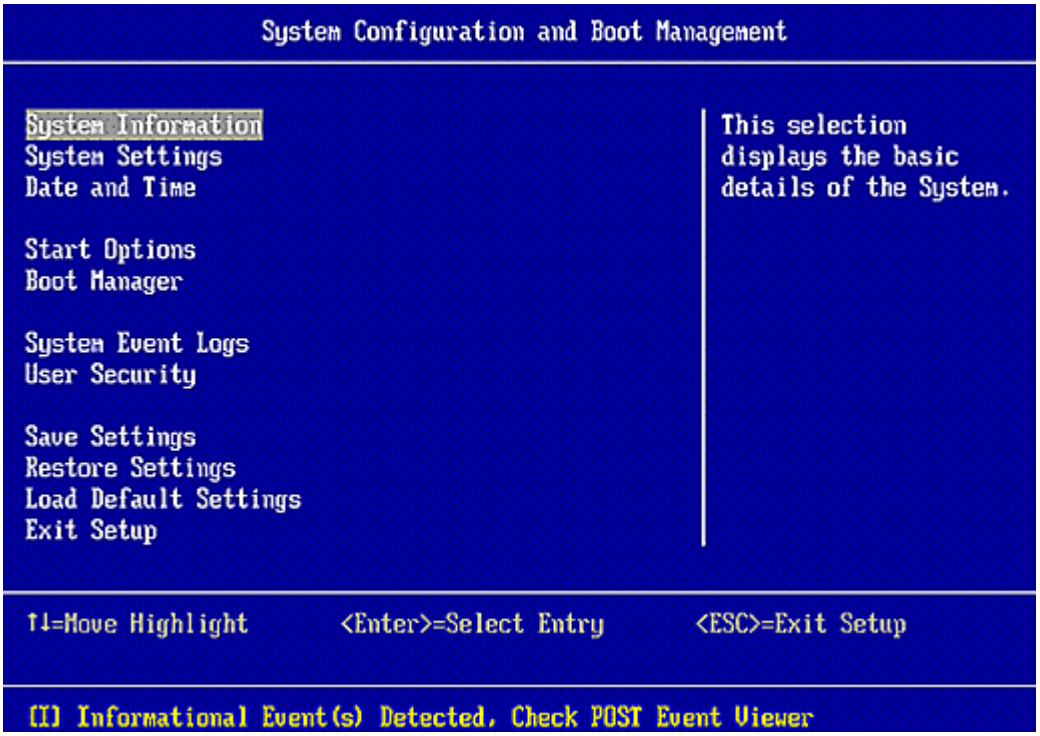

Figure C-1 System Configuration and Boot Management Screen

2. Select **Boot Manager** and press **<Enter>**. The Boot Manager screen is displayed.

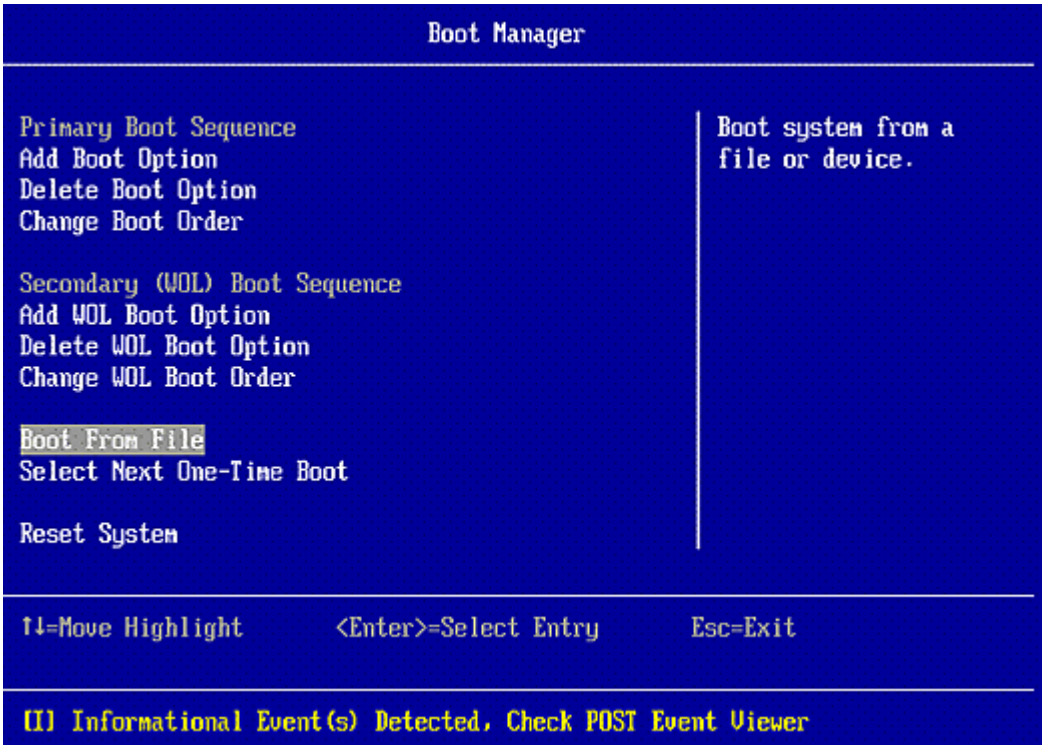

Figure C-2 Boot Manager Screen

3. Select **Boot from File** and press **<Enter>**. The File Explorer screen is displayed.

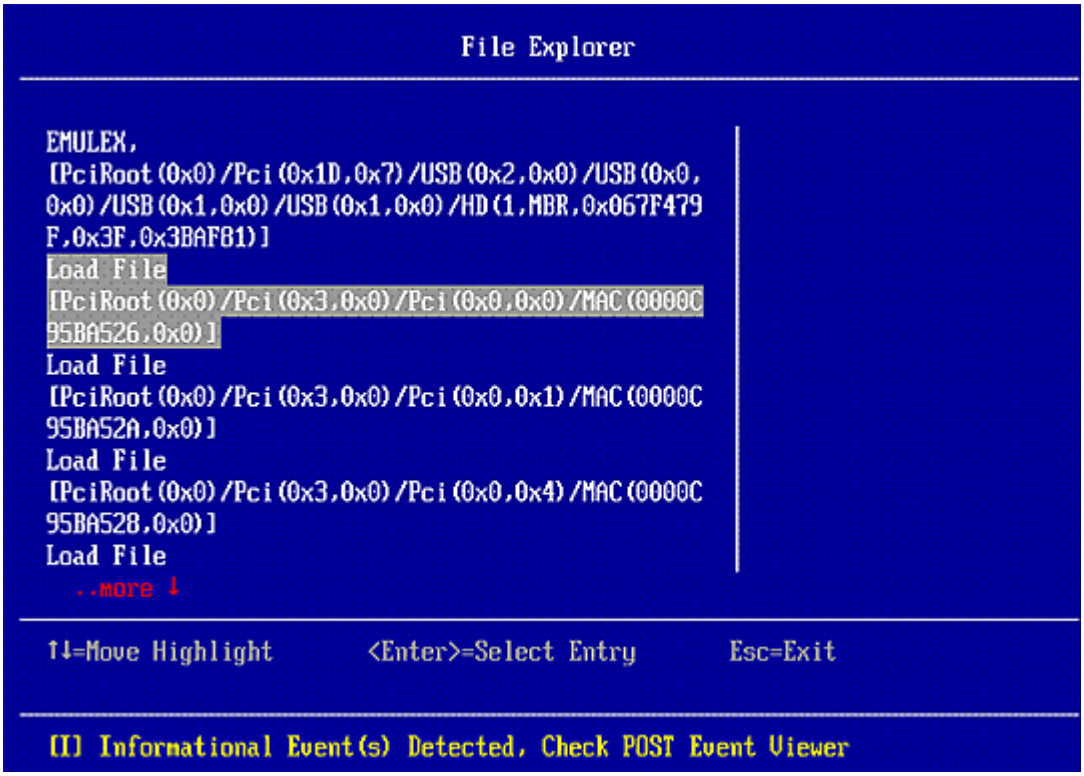

Figure C-3 File Explorer Screen

4. Select the card from which the UEFI NIC boot is to be performed. Press **<Enter>**. A message similar to the following is displayed.

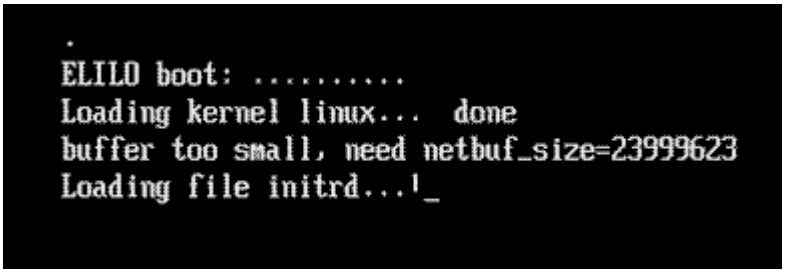

Figure C-4 ELILO Boot Message

5. The Language Selection menu is displayed. Select a language and click **OK**.

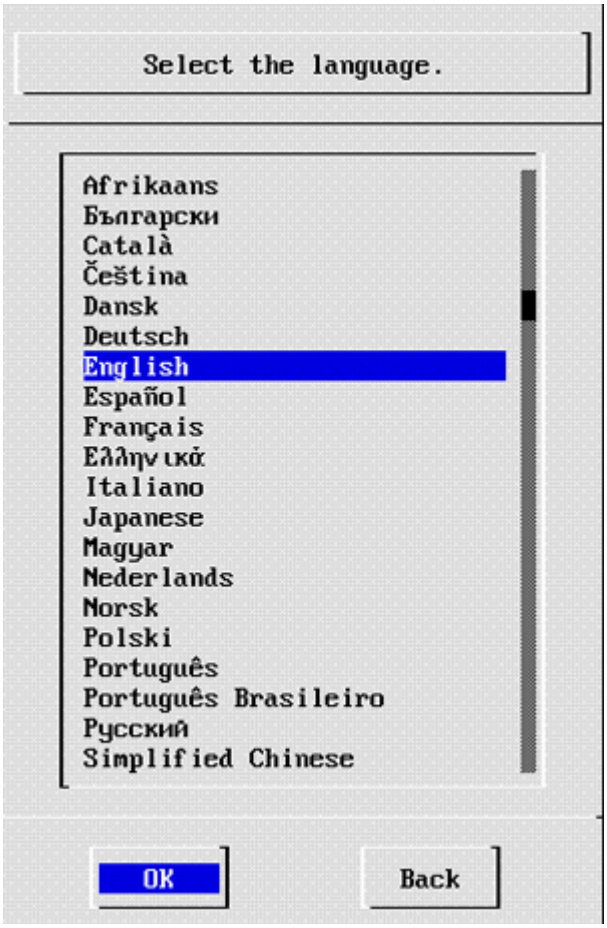

Figure C-5 Language Selection Menu

6. The Main menu is displayed. Select **Expert** and click **OK**.

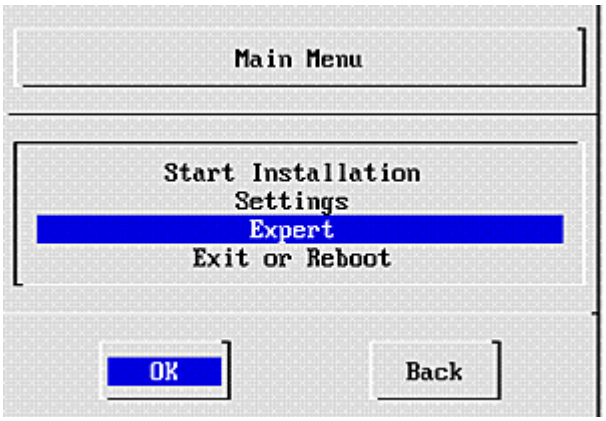

Figure C-6 Main Menu

7. The Expert menu is displayed. Select **Kernel Modules (Hardware Drivers)** and click **OK**.

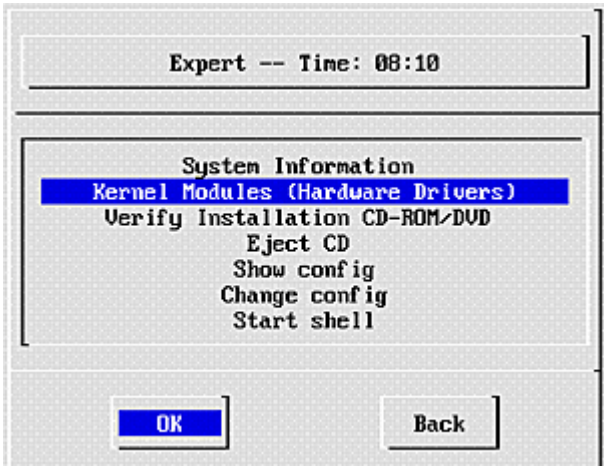

Figure C-7 Expert Menu

8. The Kernel Modules (Hardware Drivers) menu is displayed. Select **Add Driver Update** and click **OK**.

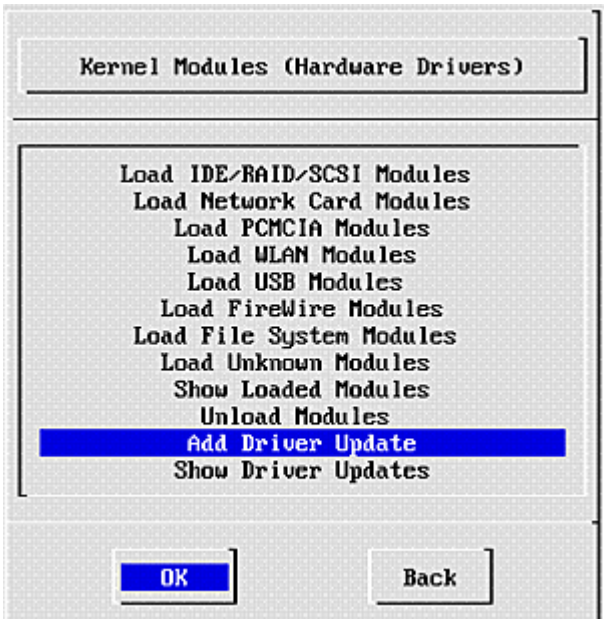

Figure C-8 Kernel Modules (Hardware Drivers) Menu

9. The Driver Update Medium Selection listing is displayed. Select a medium and click **OK**.

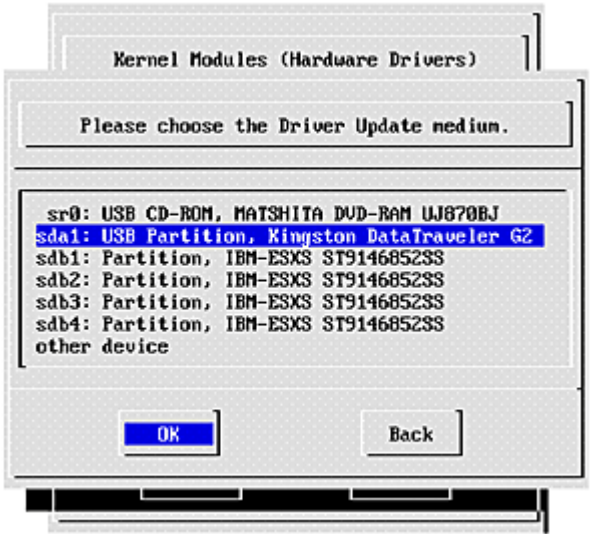

Figure C-9 Driver Update Medium Selection Listing

10. The Driver Update List confirmation dialog box is displayed. Click **OK**.

Figure C-10 Driver Update List Dialog Box

11. The Expert menu (Figure C-7) is displayed. Click **Back**.
12. The Main menu (Figure C-6) is displayed. Select **Start Installation** and click **OK**.
13. The Source Medium Selection menu is displayed. Select **Network** and click **OK**.

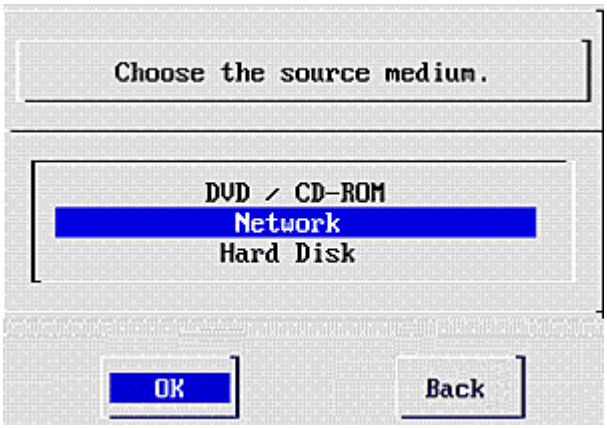

Figure C-11 Source Medium Selection Menu

14. The Network Protocol Selection menu is displayed. Select **NFS** and click **OK**.

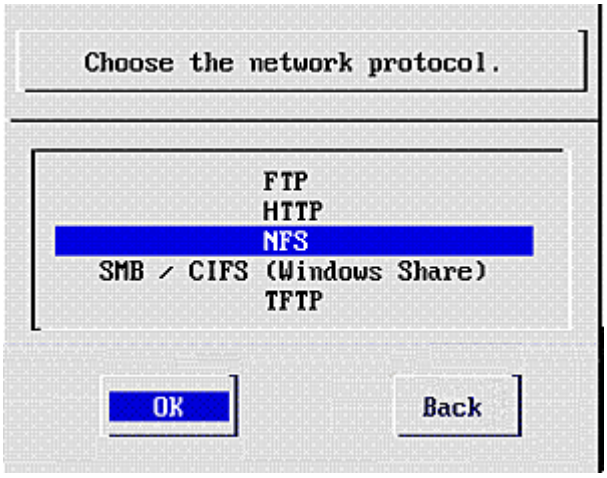

Figure C-12 Network Protocol Selection Menu

15. The Network Device Selection listing is displayed. Select the device and click **OK**.

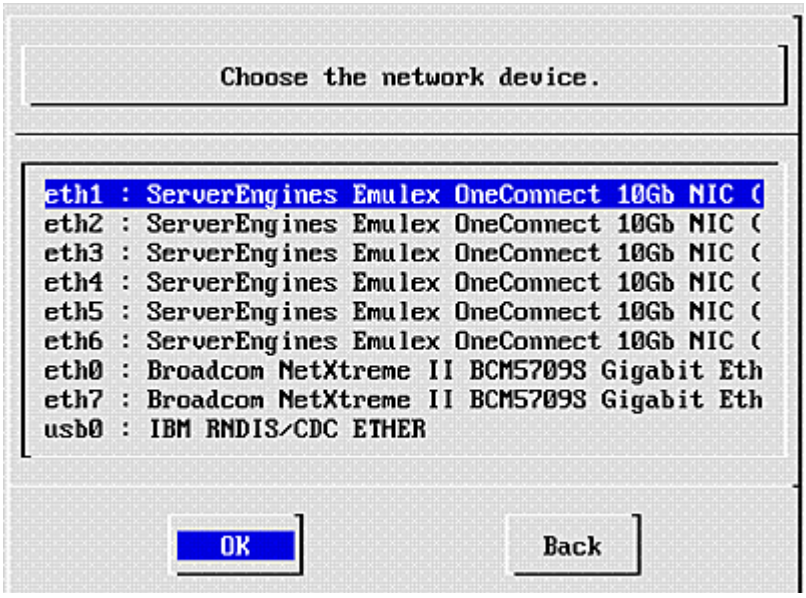

Figure C-13 Network Device Selection Listing

16. The DHCP request is sent. A dialog box prompts you to enter the IP address of the NFS server.

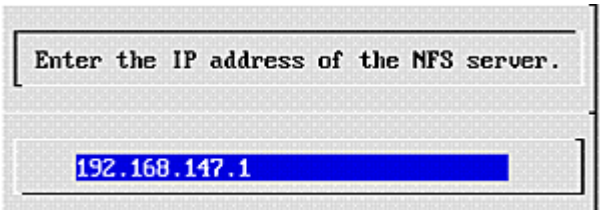

Figure C-14 NFS Server IP Address Dialog Box

17. Enter the IP address and press **<Enter>**. A dialog box prompts you to enter the directory path of the server.

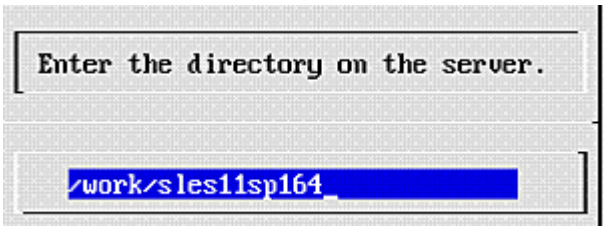

Figure C-15 Server Directory Dialog Box

18. Enter the directory path and press **<Enter>**. Information similar to the following is displayed.

```
starting syslogd (logging to /dev/tty4)... ok
starting klogd... ok
starting yast...
```

Figure C-16 Starting Script

```
SUSE Linux Enterprise Server 11 Installation

- there are shells running on consoles 2, 5, 6, 9
- use 'extend' to load extensions (remove with 'extend -r'); extensions are:
    o bind, gdb, sax2
- network setup: run, e.g. 'dhcpcd eth0'
- sshd: run 'rcsshd start' (don't forget to set a password with 'passwd')

/ # modinfo be2net
filename:       /lib/modules/2.6.32.12-0.7-default/initrd/be2net.ko
supported:      external
license:        GPL
author:         ServerEngines Corporation
description:    ServerEngines BladeEngine 10Gbps NIC Driver 2.103.358.0
version:        2.103.358.0
srcversion:     7382DCFE6EFA5CA10009192
alias:          pci:v000019A2d00000710sv*sd*bc*sc*i*
alias:          pci:v000019A2d00000700sv*sd*bc*sc*i*
alias:          pci:v000019A2d00000221sv*sd*bc*sc*i*
alias:          pci:v000019A2d00000211sv*sd*bc*sc*i*
depends:
supported:      yes
vermagic:       2.6.32.12-0.7-default SMP mod_unload modversions
parm:           rx_frag_size:Size of receive fragment buffer  - 2048 (default), 4096 or 819
parm:           num_vfs:Number of PCI VFs to initialize (max 16) (uint)
parm:           msix:Enable and disable the MSIx (By default MSIx is enabled) (uint)
parm:           multi_rxq:Multi Rx Queue support. Enabled by default (uint)
/ # _
```

Figure C-17 Driver Update Confirmation

Appendix D. Example for Installing and Booting UEFI FCoE

The following steps use the Linux SLES operating system as an example.

1. Boot to UEFI linux from DVD.
2. Select UEFI boot from the BIOS boot manager or boot to shell and execute /efi/boot/elilo.efi from removable media.
3. Follow normal boot instructions from YaST.
4. During the Installation Settings, select **Partitioning**, then select **Custom partitioning (for experts)**.
5. In **SystemViews**, select a hard disk.
6. Select the **Partitions** tab.
7. Delete any old partitions on the disk.
8. To create a GPT disklabel (UEFI does not support booting from disks with an MS-DOS partition table), click **Expert** (above the Accept button).
9. Create a partition table and check GPT (required for UEFI boot).

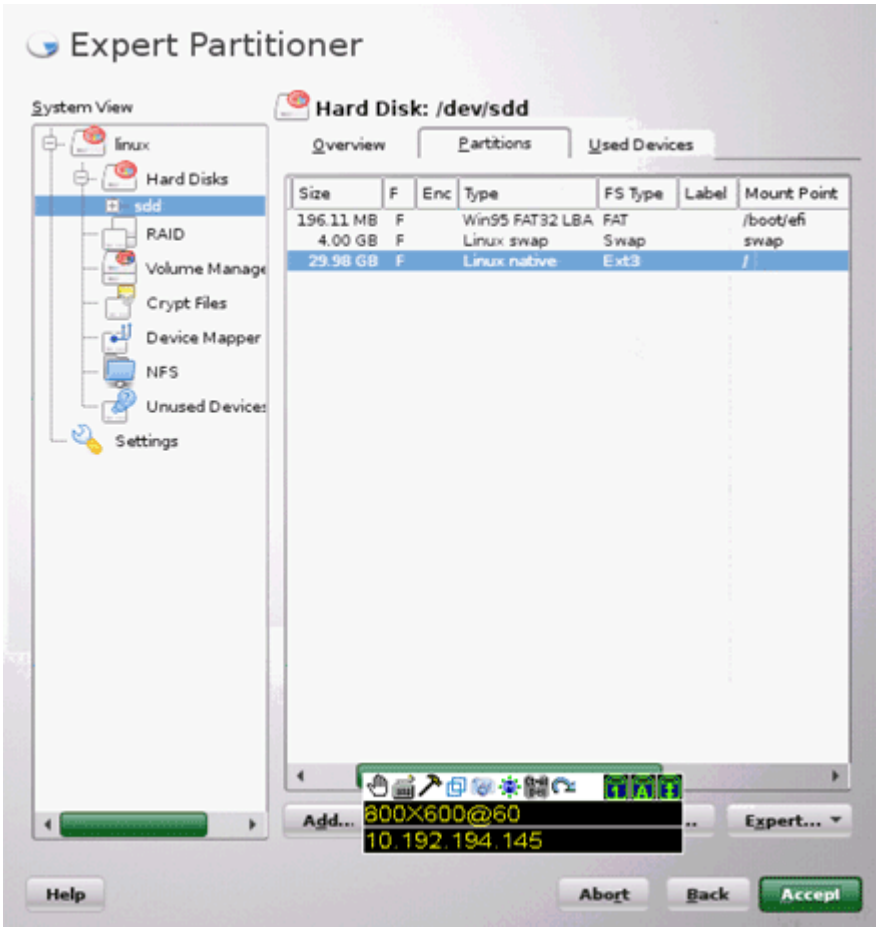

Figure D-1 Partitions Tab

10. To add an UEFI system partition (VFAT or FAT), click **Add**.
11. Select a custom size (100-400MB) depending on what EFI driver and utilities you want to store on the UEFI system partition. In general, using 200 MB is sufficient if the plug-in card detail for UEFI system partition is unknown.
12. In the Formatting options dialog box, select **Format Partition > File system > FAT**.
13. Under Mounting options, select **/boot/efi** and click **Finish**. The boot drive now has a GPT disk label that contains a FAT EFI boot partition.
14. Perform the remainder of the partitioning as with any Linux installation. The remainder of the installation is not unique to UEFI, for example, add a swap partition and an EXT3 partition for root.
15. Once the installation is completed, view the partitions using the `parted -l` command. Information similar to the following is displayed:

```
/ # parted -1
Model : SEAGATE ST336754FC (scsi)
Disk /dev/sdd: 36.7GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Number Start   End     Size   File system Name    Flags
1      17.4kB  206MB   206MB  fat16       primary , , , , , , , , , , , ,
nsftres
2      206MB   4499MB  4294MB linux-swap  primary , , , , , , , , , , , ,
3      4499MB  31.36GB 26.8GB ext3        primary , , , , , , , , , , , ,
```

16. When the system boots, SUSE Linux Enterprise Server 11 SP1 now shows in the system Start Options screen.

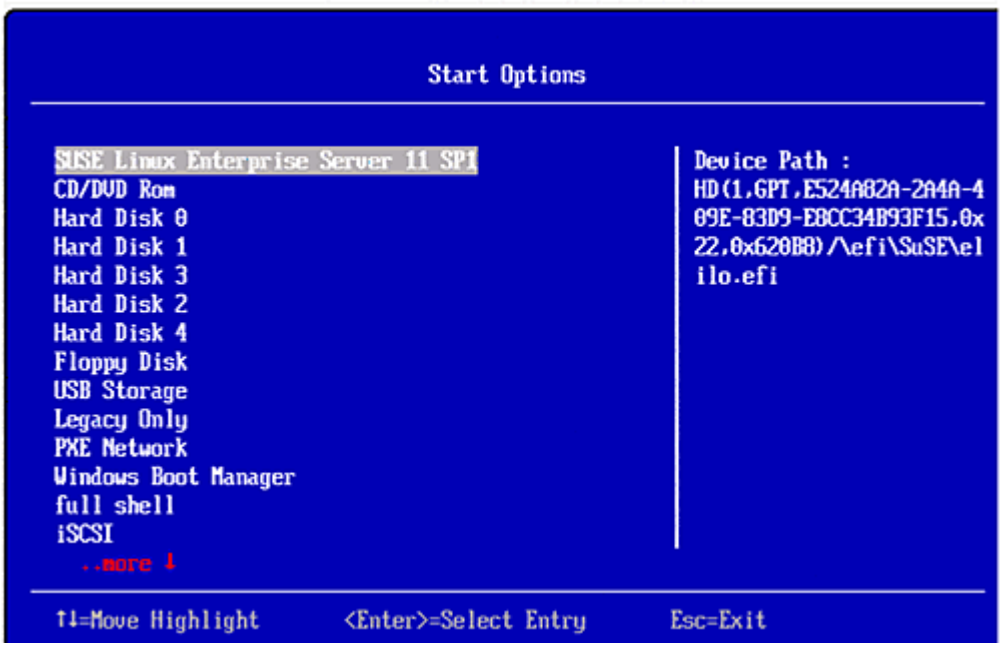

Figure D-2 UEFI FCoE Start Options

Appendix E. Multichannel for OneConnect OCe11100-series UCNAs

Overview

Multichannel (or UMC) for OCe11100-series 10GbE adapters provides powerful port partitioning and traffic management capabilities to optimize bandwidth allocation. With multichannel, system administrators can partition a dual-port OCe11100-series adapter into eight PCIe functions (virtual ports or channels) with assigned bandwidth that can be integrated into both physical and virtual servers. This is particularly beneficial for virtualized servers where individual functions can be assigned for virtual machine (VM) migration, system management, and I/O intensive applications running in VMs.

Multichannel enables four PCIe functions per port for OCe11100-series adapters. Each port can support four virtual channels for OCe11100-series-N Ethernet adapters, or three virtual channels and an iSCSI or FCoE function for OCe11100-series-I and OCe11100-series-F storage adapters. Bandwidths for each function can be specified as a percentage of the full 10 Gb/s for the adapter port.

Most servers are currently deployed with multiple 1GbE physical connections. Typically these additional ports are used to support virtual servers and high availability, and to provide bandwidth needed for I/O-intensive applications. Multichannel provides a similar capability for 10GbE networking using individually configurable partitions of the 10GbE port. With multichannel, data centers can save on costs for cabling, adapters, switches, and power.

Multichannel support includes:

- Switch-agnostic support (works with any 10GbE switch)
- Creation of four physical functions (PFs) per physical port, with the mapping of PFs to physical ports as follows:
  - PF0, PF2, PF4, PF6 > Port0
  - PF1, PF3, PF5, PF7 > Port1
- Separate transmit and receive queues for each channel
- Channel isolation with unique VLAN assignments. Based on the IEEE 802.1Q VLAN standard, each channel has its own independent broadcast and multicast domain.
- Optimized virtual server deployments, which enable allocation of separate PFs for VM migration, console management, iSCSI and NFS storage, and network traffic for individual VMs.
- With UMC enabled, any VLAN IDs to be used by the operating system or applications must also be configured in the UMC NIC driver.
- In Windows, no more than one VLAN can be used with each UMC virtual channel. In other operating systems, up to 63 VLANs can be used.

  Note: You cannot run LACP when UMC is enabled.

Physical Functions

Multichannel is enabled and managed at boot time. When it is enabled on an OCe11002 dual-port network adapter, each 10GbE port is partitioned into four isolated physical functions (PFs). There are a total of eight PFs available on an OCe11100-series dual-port adapter. PFs must be configured as trunk ports on the switch. Switch ports may be configured as access ports or as trunk ports to distribution and/or core switches in the network.

Although multichannel support for virtual channels is switch agnostic, a switch that supports Data Center Bridging (DCB) is required for FCoE and is also required when iSCSI is used with DCB. Multichannel is supported with powerful traffic management and provisioning capabilities such as dynamic rate control, priorities, MAC configuration, and VLAN assignment.

With multichannel, physical functions (PF0–PF7) are presented to an operating system or hypervisor as eight independent adapters. Virtual channels are presented to the operating system or hypervisor as a physical port with a separate MAC address and assigned bandwidth. Port mapping examples are shown in Table E-1 and Table E-2. In Table E-1, all of the physical functions are configured as NICs. In Table E-2, one of the physical functions for each port is configured for storage.

Table E-1 Multichannel Port Mapping – NIC Only

Function Number	Channel Type	Port 0 Physical Function	Port 1 Physical Function
0	NIC	PF0	PF1
1	NIC	PF2	PF3
2	NIC	PF4	PF5
3	NIC	PF6	PF7

Table E-2 Multichannel Port Mapping – NIC and Storage

Function Number	Channel Type	Port 0 Physical Function	Port 1 Physical Function
0	NIC	PF0	PF1
1	Storage (iSCSI or FCoE)	PF2	PF3
2	NIC	PF4	PF5
3	NIC	PF6	PF7

Using VLANs with Multichannel

The term UMC NIC is used to reference a multichannel physical function that is a NIC type. The LPVID for a UMC NIC is initially configured using Emulex boot utilities and is the default VLAN ID (2-4094) that identifies the network channel. An LPVID is not assigned to a multichannel physical function with a storage type (iSCSI or FCoE).

For existing network environments, assign LPVIDs that correspond to VLANs previously configured in your network. The switch ingress port should be set to trunking mode to carry traffic for multiple LPVIDs. The switch ingress port must allow all LPVIDs that are assigned to UMC NICs for the adapter port.

UMC NICs work like physical adapter ports within the network. VLAN membership and trunking-mode between multiple switches are left to the discretion of the system administrator but must include all VLAN IDs in order for traffic to be accepted by other systems in the network.

There are two scenarios that can be used for LPVID assignment: Emulex PXESelect or the System Configuration and Boot Management utility.

An LPVID must be assigned to each UMC NIC when multichannel is enabled with the Emulex PXESelect or System Configuration and Boot Management utility. Each UMC NIC can be configured for a default LPVID and the LPVID value must be unique within the physical port.

The same LPVID can be assigned to UMC NICs on both ports of the adapter for redundancy and high availability as shown in Table E-3.

Table E-3 Multichannel Port Mapping for High Availability

Port 0 Function Number	LPVID	Port 1 Physical Function	LPVID
PF0	2	PF1	2
PF2	5	PF3	5
PF4	9	PF5	9
PF6	12	PF7	12

LPVID values that are assigned at boot time can be overridden using utilities in the operating system or hypervisor. With this option, the same LPVID can be assigned to multiple UMC NICs on the same physical port. In a virtualized server, this allows UMC NICs to be assigned to different VMs and communicate over the same VLAN.

Configuration Options

Bandwidth Assignments

You can assign bandwidth to all logical ports but you cannot assign an LPVID to a logical storage port (iSCSI or FCoE function). The total bandwidth for all logical adapter ports must be 100% and you must configure all logical adapter port fields.

Configurable Parameters

Table E-4 summarizes all configurable parameters with multichannel enabled or disabled.

Table E-4 Multichannel Configurable Parameters

Configurable Parameter	Multichannel Disabled	Multichannel Enabled
Quality of service (QoS)	Based on physical port	Based on channel
TCP Offload, MTU Setting, MSI/VSI-X	Based on physical port	Based on channel
Link State	Mimics physical link state	Based on channel (configurable)
Link speed reported to operating system	Port speed	Based on QoS value
Port speed	1–10 Gb/s	10 Gb/s
Configuration Entity		BIOS, CLP, Switch
PXE/iSCSI/FCoE Boot	Yes	Yes – first primary function per port
Pause (flow control)	Regular – Priority (for storage)	Regular for others – Priority (for storage)
Personality change	NIC, iSCSI+NIC, FCoE+NIC	NIC, iSCSI+NIC, FCoE+NIC

Deploying OneConnect Adapters with Multichannel

Although multichannel is only supported with OCe11100-series adapters, it is possible to use older OCe10100-series adapters with a multichannel-enabled OCe11100-series adapter in the same server. Multichannel also requires a minimum version of driver, firmware, boot code, and management software.

Determine network requirements such as VLANs, bandwidth, trunk ports, and load balance prior to configuring multichannel. Converged traffic such as FCoE or iSCSI over DCB will require specialized network switches. If your configuration requirement is multiple NICs only, you can use a standard 10GbE Layer 2 switch.

High Availability with Multichannel

UMC NICs can be configured for high availability with the same procedures that are used for physical ports. The following sections provides information to configure high availability for Windows, Linux, and VMware.

Windows

Use the OneCommand NIC Teaming and VLAN Manager utility to team UMC NICs with other UMC NICs or other physical adapters. Make sure the selected UMC NICs for teaming are not associated with the same physical port. This will ensure traffic will fail over to the secondary port and switch in the event of a link failure.

Use OneCommand Manager to identify and select the correct physical function, IP address, or MAC for the physical ports. Using the OneCommand NIC Teaming and VLAN Manager utility, select the **Show Config Tab** to view the MAC address of all UMC NICs and other physical NICs in a server. Refer to the *OneCommand Teaming and VLAN Manager User Guide* for more information on NIC teaming with Windows.

Linux

Use the OneCommand Manager CLI or GUI to identify MAC addresses and physical PCIe function numbers, and to manage UMC FCoE and UMC NIC adapters. Use the `ifconfig` command to configure IP addresses for all UMC NICs.

As a best practice, verify the UMC-Adapter Physical Port association, PCIe function, and MAC address prior to bonding UMC NICs. Ensure all bonded UMC NICs are not partitioned from the same physical port. This provides redundancy in the event of a physical link failure.

VMware

From the vSphere Client, use Network Adapters to show the list of UMC NICs that can be provisioned as uplinks for vSphere standard or distributed switches. UMC NICs can be used for individual VMs, VMotion, management, and other network traffic types, such as NAS storage.

VMware recognizes a UMC NIC as an available vmnic that can be configured using a vSwitch to handle network traffic. As a best practice, configure UMC NICs across physical ports using equal bandwidth to ensure consistency across active and standby or aggregated link paths. Also, ensure the vmnics selected for redundant paths are not on the same physical port.