iSCSI Configuration Manager

User's Guide

Version 2.0

iSCSI Configuration Manager

User's Guide

Version 2.0

Note
Before using this information and the product it supports, read the @server information in "Notices," on page 29.

First Edition (May 2006)

This edition applies to Version 1, Release 1, of IBM iSCSI Configuration Manager (product number 0000-000) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Figures

Tables

Preface

The iSCSI Configuration Manager (ICM) is a standalone JAVA™ application used to configure initiators on supported blades in an IBM® BladeCenter® chassis.

About this guide

The purpose of this guide is to provide end users of the iSCSI Configuration Manager:

- An overview of the tool's features and components.
- Directions for its installation and usage.

Who should read this guide

This guide is for system programmers and end users working in an IBM® BladeCenter® environment and using iSCSI Configuration Manager to configure initiators on supported blades in an IBM® BladeCenter® chassis. It is a good starting point for a basic understanding of the product.

Chapter 1. Overview

The iSCSI Configuration Manager (ICM) is a standalone Java™ application you can use to configure initiators on supported blades in an IBM® BladeCenter® chassis. The configuration manager can optionally communicate with the iSCSI target enclosure, DS300, to retrieve the configuration of the target logical unit numbers (LUNs). You can then map target LUNs to initiators using the configuration manager's GUI. If the target device is not available or not supported by the configuration manager, then you can manually enter the target's parameters using the configuration manager's GUI and then map the manually entered targets to initiators.

Once you have mapped targets to initiators, the configuration manager will format the parameters into the basic input/output system (BIOS) layout and send the commands to the BladeCenter management module (MM) that is necessary for enabling the MM to write the parameters into the nonvolatile random access memory (NVRAM) of the initiator blades. The configuration manager can then save the parameters to a XML file for subsequent downloads.

Figure 1 shows the configuration manager running on a management station.

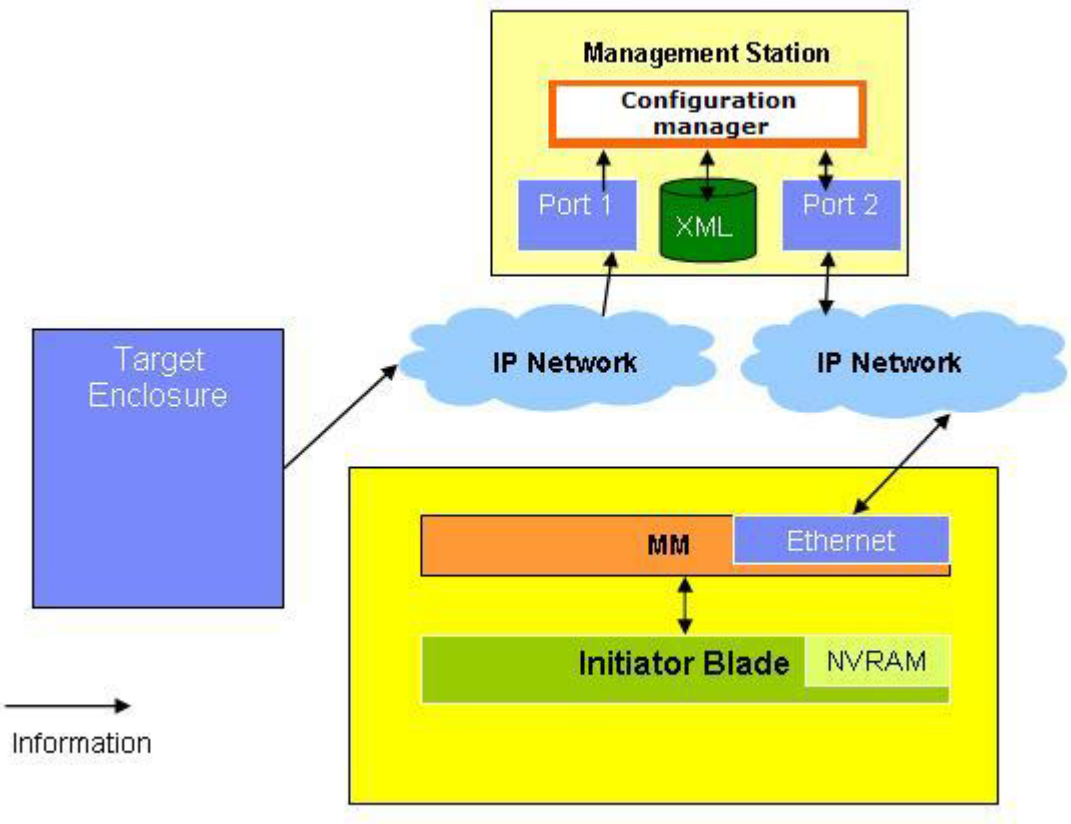

Figure 1. Initiator configuration manager overview

This management station can be a PC or other system running one of the supported operating systems and connected to the IP network connected to the management module. Optionally, the management station can connect to the IP network of the target device (which may be the same network connected to the management module).

Chapter 2. Supported platforms and requirements

This section details the supported targets and initiators as well as the requirements for the management station.

Management station requirements

The management station minimum requirements are the superset of the requirements for the Java Virtual Machine (JVM) and the requirements necessary for the management station to communicate with the BladeCenter MM. In some environments, you may want to also communicate with the target device. However, communicating with the target device is an optional convenience and not required.

Supported management station operating system requirements

- Microsoft® Windows® XP
- Red Hat Enterprise Linux™ 4 AS Update 1 for IA32

Requirements for communicating with MM

- Ethernet Network Interface Card (NIC)
- Internet Protocol (IP) connectivity to the BladeCenter MM

JVM requirements

- Version 1.4.2
- The requirements for the JVM are listed at http://java.com/en/download/help/sysreq.xml.

Supported iSCSI target platforms

Currently, the only supported target platform for automatic retrieval of target parameter information by the iSCSI Configuration Manager is DS300. However, you can manually enter parameters for any target supported by the initiator, so use of the iSCSI Configuration Manager is not limited to environments, where DS300 is the target device.

Supported iSCSI initiator platforms

IBM BladeCenter HS20 Model 8843 with appropriate firmware levels.

Chapter 3. iSCSI Configuration Manager installation

The following section outlines the steps necessary to install the iSCSI Configuration Manager on the management station.

1. Install Java Run-time Environment version 1.4.2 on the management station.
2. Change the PATH system environment variable to include the JVM executable **java**.
3. Unzip the zip file downloaded containing the configuration manager components into the directory from which you want to run the configuration manager or install it under Microsoft Windows using `iSCSI_Configuration_Mgr_V2.0.msi` (a Microsoft installer file).
4. To run the configuration manager on windows:
   a. Run the file: `iSCSI_Configuration_Mgr_V2.0.msi`.
   b. Run the `wizard.bat` file that installs to the **C:\Program Files\IBM\iSCSI** configuration manager directory. The BAT file takes the directory where the configurations should be stored as its only parameter:

      ```
      wizard.bat <configuration directory>
      ```
5. To run the configuration manager on Linux™:
   a. Open a shell window and change the directory to the directory where you stored the contents of the zip file.
   b. Run the shell file, `setup.sh`. The shell file takes the default location for the XML files, which is also the where the setup will place the `wizard.sh` shell file to launch the configuration manager, as its only parameter:

      ```
      setup.sh <prefix directory>

      For example:

       setup.sh /usr

      will install the main script wizard.sh under: /usr/bin
      and the configuration manager's .jar files under:  /usr/lib/iscsiwiz
      ```
   c. Run the newly created shell file, `wizard.sh`, from the default location entered in step 5b. The shell file takes the path where the configurations should be stored as its only parameter:

      ```
      wizard.sh <configuration directory>
      ```
6. The configuration manager GUI will launch.

Chapter 4. iSCSI Configuration Manager usage

This section details the function and usage of the various configuration manager panels.

XML configuration file selection panel

The Configuration file selection panel (Figure 2) allows you to select the configuration file to read. The configuration manager uses the parameter values read from the configuration file as the initial values in the fields on the subsequent panels. You can enter a file name or use the pull-down box to select a file. After you select the desired file, pressing the **Next** button reads the parameter values and directs you to the environment panel.

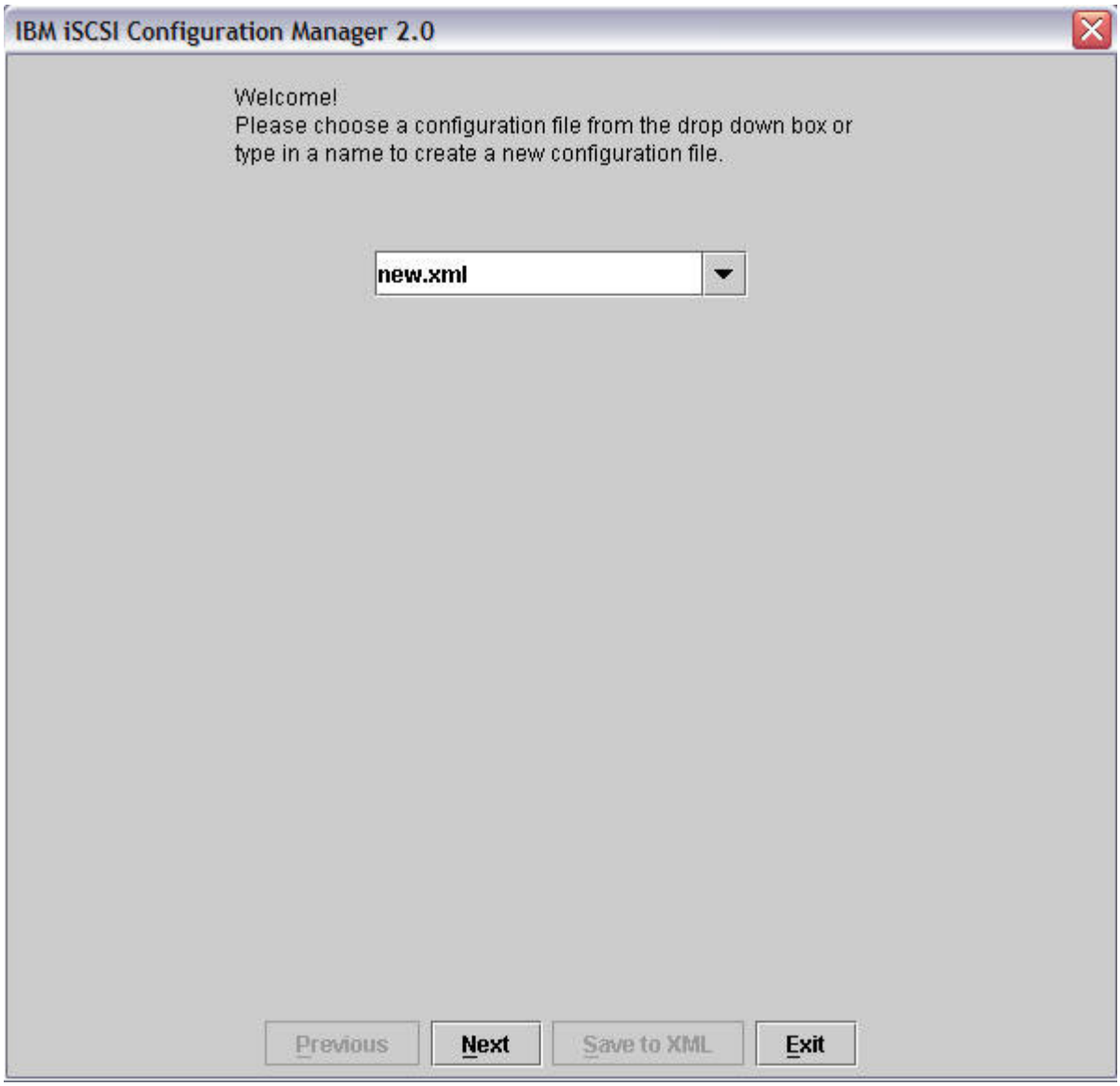

Figure 2. Configuration file selection panel

Environment panel

The Environment panel (Figure 3) allows configuration of the parameters needed to communicate with the BladeCenter MM and the iSCSI target. Communication with the BladeCenter MM is required to write the initiator's parameters to the supported blades. The configuration manager communicates with supported targets to extract target LUN information that will later be assigned to initiators. The parameters and their descriptions are contained in Table 1 on page 10 and Table 2 on page 10. Pressing the **Next** button retrieves the information from the BladeCenter and iSCSI target, and directs you to the target data panel.

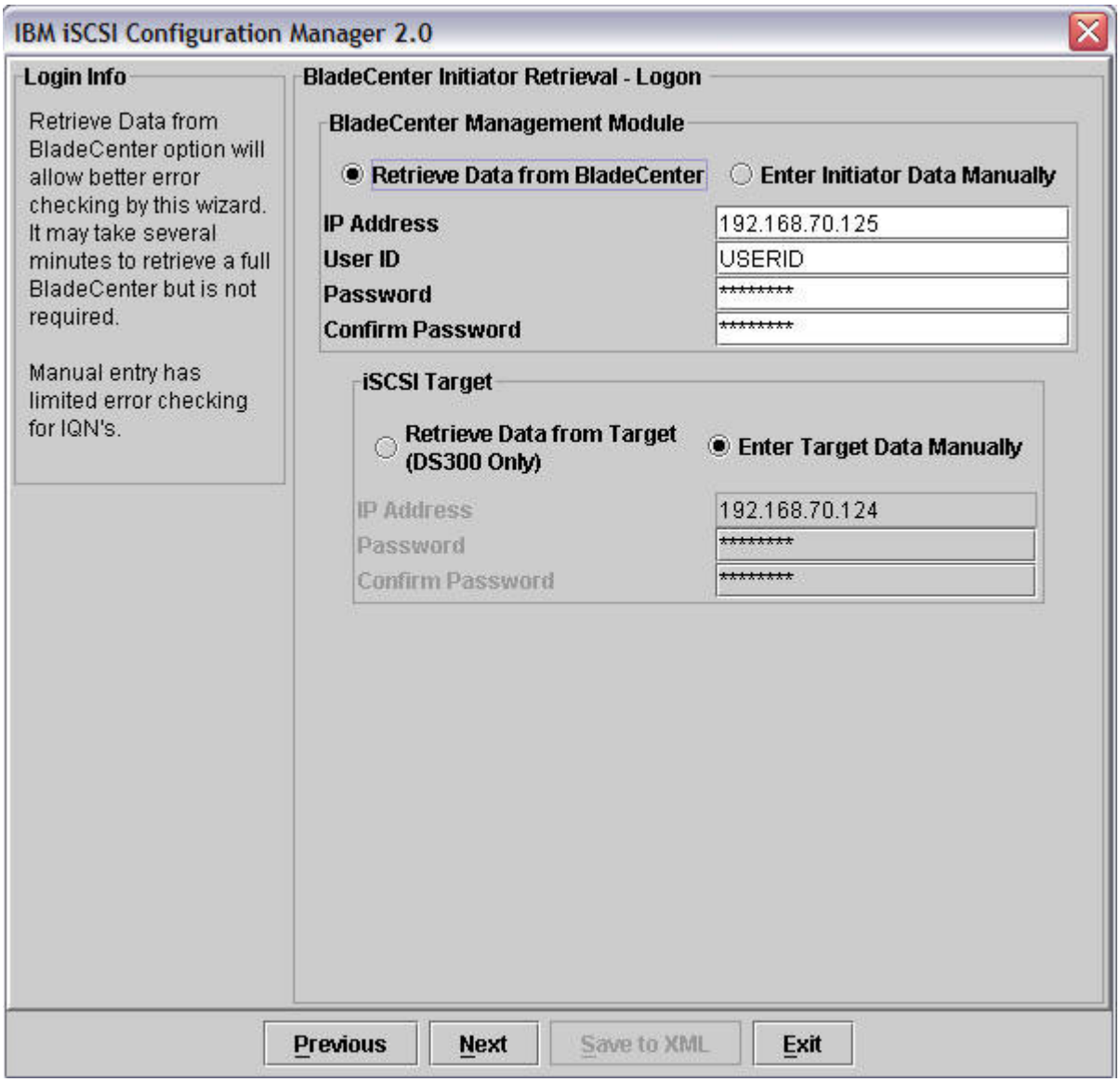

Figure 3. Environment panel

Table 1. Environment panel BladeCenter parameters

Parameter	Description
Retrieve Data From BladeCenter	When you select this radio button, the configuration manager reads the BIOS settings from supported blades and displays those settings as the initial parameter values on the configuration manager's GUIs. This may take several minutes.
Enter Initiator Data Manually	When you select this radio button, the initial parameter values displayed by the configuration manager's GUI will be those contained in the specified configuration file or the default values.
IP Address	The IP address of the BladeCenter MM reachable from the management station running the configuration manager.
User ID	The user ID you use to log into the MM. This is the same ID used by the MM's web and command line interfaces.
Password	The password you use to log into the MM. This is the same password used by the MM's web and command line interfaces.
Confirm Password	Same as Password.

Table 2. Environement panel iSCSI target parameters

Parameter	Description
Retrieve Data From Target (DS300 only)	When you select this radio button, the configuration manager reads the LUN settings from DS300 target devices and displays those settings as the initial parameter values on the configuration manager's GUIs.
Enter Target Data Manually	When you select this radio button, the initial parameter values displayed by the configuration manager's GUI will be those contained in the specified configuration file or the default values.
IP Address	The IP address of the supported target device reachable from the management station running the configuration manager. This field is only active when you select **Retrieve Data From Target**.
Password	The password you use to log into the supported target device. This field is only active when you select **Retrieve Data From Target**.
Confirm Password	The same as Password. This field is only active when you select **Retrieve Data From Target**.

Target data panel

You use the Target data panel (Figure 4) to enter and display target parameters that are relevant to the initiators. If you selected the **Retrieve Data from Target** option on the environment panel, then the configuration manager will display the retrieved data on this panel. If you selected the **Enter Target Data Manually** option on the environment panel, then you must enter target parameters on this panel. In both cases, target parameters entered on this panel will not be sent back to the target. The parameters and their descriptions are contained in Table 3 on page 12, Table 4 on page 12, and Table 5 on page 13.

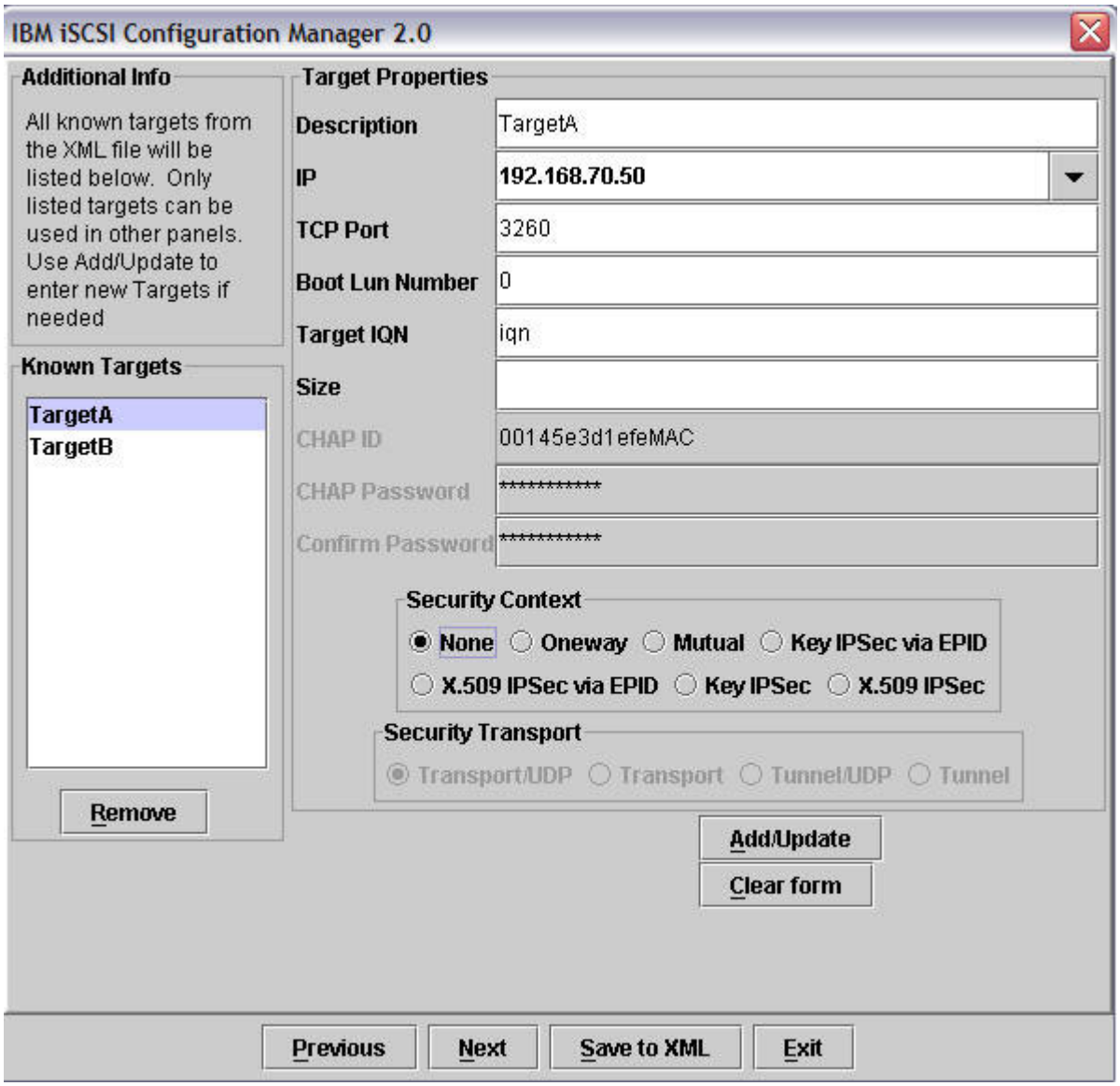

Figure 4. Target data panel

You can enter and display target parameters for multiple targets using the **Add/Update**, **Clear form** and **Remove** buttons. The **Known Targets** selection box on the left displays the available targets. You can add targets by entering the desired parameters in the **Target Properties** box and pressing the **Add/Update** button. The new target will then display in the **Known Targets** selection box. You

can modify target parameters (in the configuration manager's GUI only) by selecting the target in the **Known Targets** selection box, modifying the desired parameters in the **Target Properties** box, and pressing the **Add/Update** button. You can set the values in the **Target Properties** box to their defaults by pressing the **Clear form** button. You can remove a target by selecting the target in the target selection box then pressing **Remove**.

When you finish entering all the target data, press the **Next** button to move to the initiator configuration panel.

Table 3. Target panel target parameters

Parameter	Description
Description	A text description of the target.
IP	iSCSI target IP address of storage.
TCP Port	iSCSI TCP port on target IP address.
Boot LUN Number	Boot LUN.
Target IQN	iSCSI qualified name of target.
Size	Optional size of storage.
Chap ID	CHAP ID or 1st half of security key.
Chap Password	CHAP PW or 2nd half of security key.
Confirm Password	Confirmation of CHAP Password.

Table 4. Target panel target security context

Parameter	Description
None	No security context to be used.
Oneway	One way security to be used in logging into target (target authenticates initiator) CHAP only.
Mutual	Mutual security to be used in logging into target CHAP only (target authenticates initiator or initiator authenticates target).
Key IPSec through EPID	Pre-shared key based IPSec authentication. The distinguished name is supplied through the EPID.
X.509 IPSec through EPID	X.509 certificate based IPSec authentication. The distinguished name is supplied via the EPID.
Key IPSec	Pre-shared key based IPSec authentication.
X.509 IPSec	X.509 certificate based IPSec authentication.

Security transport

This is an optional field indicating the security transport mode you use when you select IPSec security context. If you specify CHAP authentication, then these fields are inactive.

Table 5. Target panel target security transport

Parameter	Description
Transport/UDP	Target security transport is transport mode or UDP encapsulation. This field is only active when one of the IPSec options in **Security Context** is selected.
Transport	Target security transport is transport mode. This field is only active when one of the IPSec options in **Security Context** is selected.
Tunnel/UDP	Target security transport is Tunnel Mode/UDP encapsulation. This field is only active when one of the IPSec options in **Security Context** is selected.
Tunnel	Target security transport is tunnel mode. This field is only active when one of the IPSec options in **Security Context** is selected.

Initiator configuration panel

You use the Initiator configuration panel (Figure 5) to enter and display initiator parameters. If you selected the **Retrieve Data from BladeCenter** option on the environment panel, then the configuration manager displays the retrieved data on this panel. If the **Enter BladeCenter Data Manually** option was selected on the environment panel, then you must manually enter initiator parameters on this panel. The parameters and their descriptions are contained in Table 6 on page 15 - Table 9 on page 19.

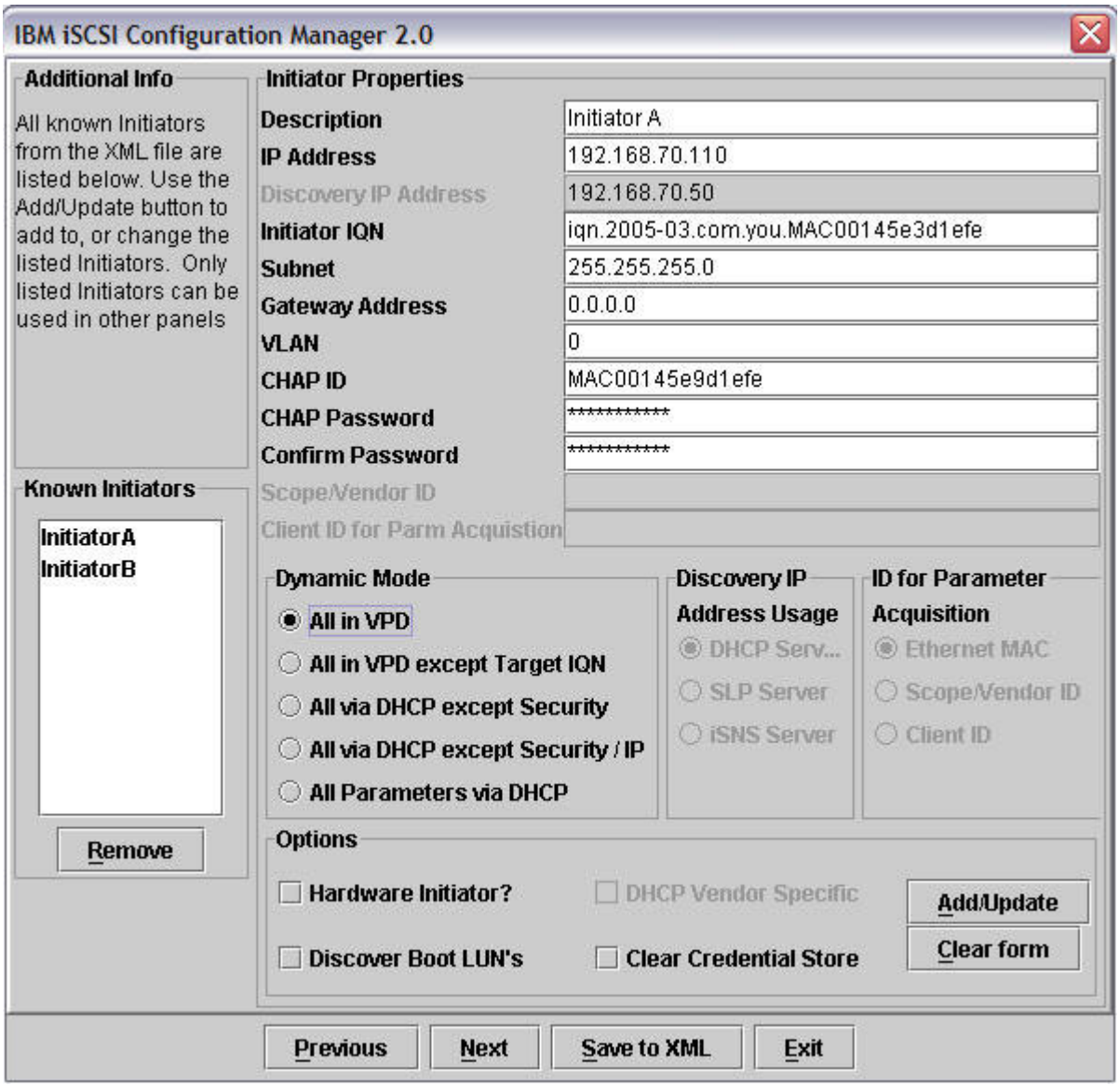

Figure 5. Initiator configuration panel

You can enter and display initiator parameters for multiple initiators using the **Add/Update**, **Clear form** and **Remove** buttons. The **Known Initiators** selection box on the left displays the available initiators. You can add initiators by entering the desired parameters in the **Initiator Properties** box and pressing the **Add/Update** button. The new initiator will then display in the **Known Initiators** selection box. You can modify initiator parameters by selecting the initiator in the **Known**

Initiators selection box, modifying the desired parameters in the **Initiator Properties** box, then pressing the **Add/Update** button. You can set the values in the **Initiator Properties** box to their defaults by pressing the **Clear form** button. You can remove an initiator by selecting the initiator in the **Known Initiators** selection box then pressing **Remove**.

When you finish entering all the initiator data, press the **Next** button to move to the blade configuration panel.

Table 6. Initiator configuration panel initiator parameters

Parameter	Description
Description	A text description of the initiator.
IP Address	iSCSI initiator IP address. This field is inactive when you select either **All Parameters via DHCP** or **All via DHCP except Security** under Dynamic Mode.
Discovery IP Address	The discovery IP address is an optional address the initiator uses in cases where you define the initiator IP address through the static or parameter push approach. This option aids in the dynamic or parameter acquisition approach where, for a variety of reasons, the initiator must access a specific IP address to acquire the parameters. The initiator uses the discovery IP address (with the appropriate Discovery IP Address Usage set to use DHCP option) to identify and to unicast to a specific DHCP server to acquire some or all of the iSCSI parameters. With the unicast support, you can eliminate DHCP broadcast storms. In the future, solutions using SLP or iSNS discovery services will use this discovery IP address for identifying the SLP or iSNS server in the network. This field is only active when you select **All via DHCP except Security/IP** under **Dynamic Mode**.
Initiator IQN	The iSCSI qualified name of initiator. This field is inactive when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode**.
Subnet	The network subnet mask is an optional mask the initiator uses in cases where the subnet mask is defined through static or parameter push approach. The mask defines the local network scope of all the IP addresses on this particular subnet. Specifically, this mask defines the local network containing stations that you may access directly from this station (for example, no router or gateways involved). This field is inactive when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode**.

Table 6. Initiator configuration panel initiator parameters (continued)

Parameter	Description
Gateway Address	The network gateway or router IP address is an optional address the initiator uses in cases where the subnet mask is defined using static or parameter push approach. Note that this address defines either the gateway or the router to reach outside the current subnet and it is IETF compliant. This field is inactive when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode**.
VLAN	The VLAN tag defines the VLAN virtual LAN to use for the iSCSI traffic within the subnet. A value of zero in this field means the initiator NIC should not insert a VLAN tag. This field is inactive when you select **All Parameters via DHCP** under **Dynamic Mode**.
CHAP ID	CHAP ID or 1st half of security key. This field is inactive when you select **All Parameters via DHCP** under **Dynamic Mode**.
CHAP Password	CHAP PW or 2nd half of security key. This field is inactive when you select **All Parameters via DHCP** under **Dynamic Mode**.
Scope/Vendor ID	The scope or vendor ID is an optional address the initiator uses in cases where the initiator acquires parameters from a DHCP service and needs some scope or vendor casting to aid the DHCP service in determining the parameters to return to the DHCP client. For example, the initiator can use this field to identify that the DHCPREQUEST or DHCPINFORM transaction is within the scope of iSCSI parameter acquisition. This field is only active when you select **DHCP Vendor Specific** under **Options**. **Note:** Since this field is per instance and per initiator, finer levels of scoping are possible.

Table 6. Initiator configuration panel initiator parameters (continued)

Parameter	Description
Client ID for Parm Acquisition	This client alternate ID is an optional address the initiator uses in cases where the initiator acquires parameters from a DHCP service and a client ID different from EN MAC address or the initiator needs scope or vendor casting to aid the DHCP service in determining the parameters to return to the DHCP client. For example, the initiator can use this field to identify that the DHCPREQUEST or DHCPINFORM transaction is within the scope of IP parameter or iSCSI parameter acquisition. This field is only active when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode** **Note:** Since this field is per instance and per initiator, finer levels of scoping are possible. Also, the initiator may use this ID for either IP or iSCSI and use Scope/Vendor for iSCSI or IP to segment the context of acquisition.
Hardware Initiator?	This is a hardware initiator versus a software initiator.
DHCP Vendor Specific	This option defines the appropriate DHCP options to use to acquire iSCSI parameters. Namely, whether to use the internet draft using DHCP Option 17 to acquire iSCSI path information or whether to use customer or site specific options defined in this document. The initiator and DHCP functionality may supersede this option. Specifically, the initiator can choose to ignore this option and ask DHCP for both Option 17 and site or user specific options. In turn, the DHCP server may respond with the valid options leaving the initiator to interrogate the DHCP server response to determine which options are valid. This field is only active when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode**.
Discover Boot LUNs	This option indicates whether to use the target boot LUN field on the target page or to ignore that value and discover from external sources. If the initiator is to determine the boot LUN through other means such as intelligence or discovery, then you should check this option. If an initiator is to use the defined LUN number in the boot LUN fields on the target page, then you should leave this option unchecked. This field is inactive when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode**.

Table 6. Initiator configuration panel initiator parameters (continued)

Parameter	Description
Clear Credential Store	The initiator uses this option to indicate to iSCSI service (iSCSI HBA based services namely) whether to clear IPSec certificates if they are in persistent storage.

Discovery IP address usage

The **Discovery IP Address Usage** field indicates whether the initiator should use the discovery IP address to access a DHCP server or an SLP server (DA). The options under this field are only active when you select **All via DHCP except Security/IP** under **Dynamic Mode**.

Table 7. Initiator configuration panel discovery IP address usage

Parameter	Description
DHCP Server	The discovery IP address points to a DHCP server.
SLP Server	The discovery IP address points to an SLP server.
iSNS Server	The discovery IP address points to an iSNS server.

ID for parameter acquisition

The **ID for Parameter Acquisition** field indicates what to use as the client ID for iSCSI parameter acquisition when querying a DHCP server for iSCSI parameters. If not present, then the initiator must acquire parameters from DHCP. The options under this field are only active when you select either **All Parameters via DHCP**, **All via DHCP except Security** or **All via DHCP except Security/IP** under **Dynamic Mode**.

Note: Usage of **Scope/Vendor ID** as an additional usage scope tool is independent of this option.

Table 8. Initiator configuration panel ID for parameter acquisition

Parameter	Description
Ethernet MAC	Use ethernet MAC address of current port as ID.
Scope/Vendor ID	Use scope or vendor ID as ID.
Client ID	Use client alternate ID as ID.

Dynamic mode

BIOS uses the **Dynamic Mode** field to determine if the iSCSI parameters are located in VPD space, for static mode, or should be acquired by a discovery service, in dynamic mode.

Table 9. Initiator configuration dynamic mode

Parameter	Description
All in VPD	All parameters are present in the data structure
All in VPD except Target IQN	All parameters are present in data structure except: • Target name parameters
All via DHCP except Security	Initiator acquires all parameters through DHCP except: • Security parameters
All via DHCP except Security/IP	Initiator acquires all parameters through DHCP except: • Security parameters • Initiator IP address and discovery IP address
All Parameters via DHCP	Initiator acquires all parameters through DHCP acquisition.

Blade configuration panel

You use the Blade configuration panel (Figure 6) to enter and display blade parameters. If you selected the **Retrieve Data from BladeCenter** option on the environment panel, then the configuration manager displays the retrieved data on this panel. If you selected the **Enter BladeCenter Data Manually** option on the environment panel, then you must manually enter initiator parameters on this panel. The parameters and their descriptions are contained in Table 10 on page 21.

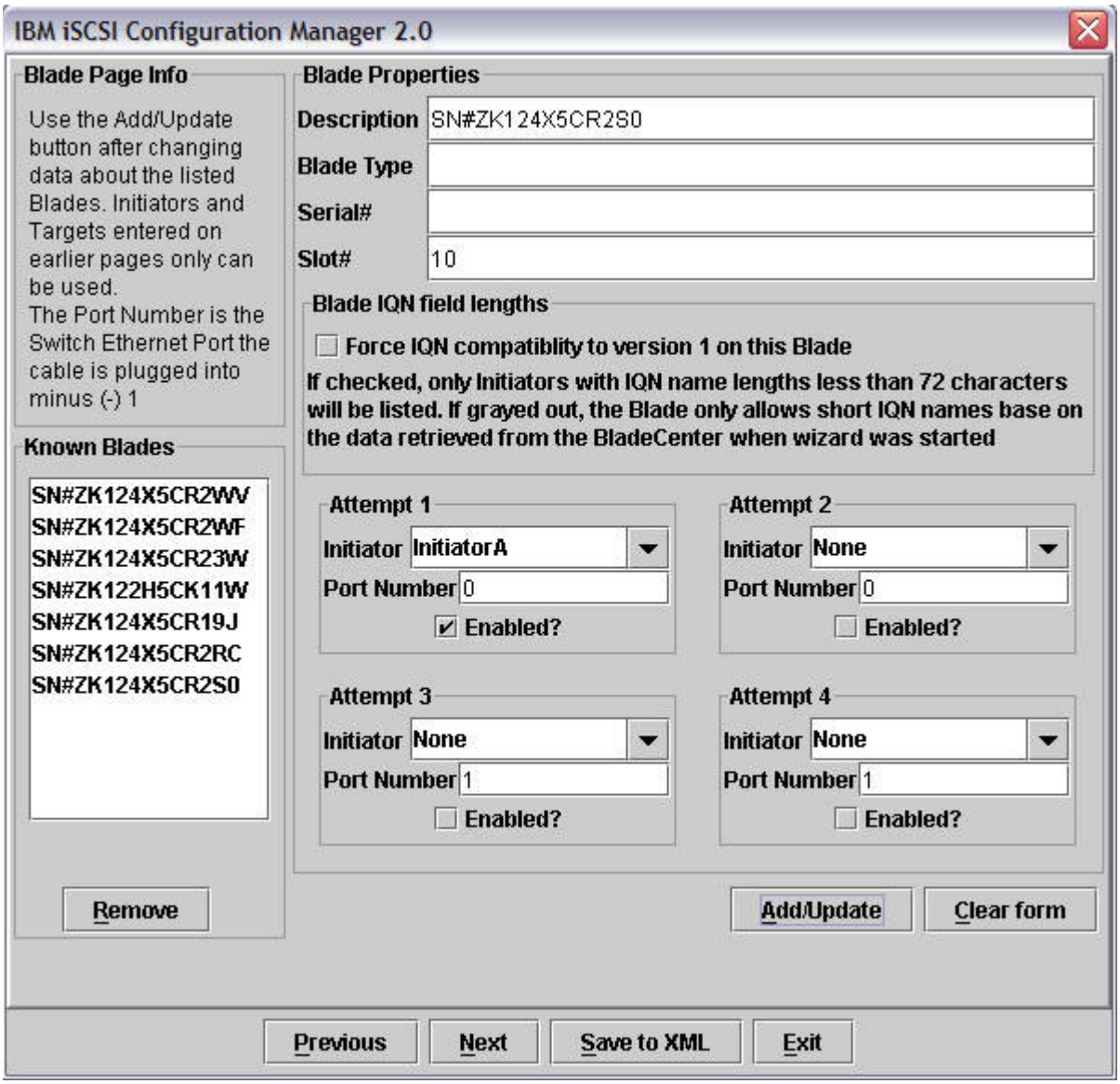

Figure 6. Blade configuration panel

You can enter and display blade parameters for multiple blades using the **Add/Update**, **Clear form** and **Remove** buttons. The **Known Blades** selection box on the left displays the available blades. You can add blades by entering the desired parameters in the **Blade Properties** box and pressing the **Add/Update** button. The new blade will then display in the **Known Blades** selection box. You can modify blade parameters by selecting the blade in the **Known Blades** selection box, modifying the desired parameters in the **Blade Properties** box, then pressing

the **Add/Update** button. The user can set the values in the **Blade Properties** box to their defaults by pressing the **Clear form** button. The user can remove a blade by selecting the blade in the Known Blades selection box then pressing **Remove**.

When you finish entering all the blade data, press the **Next** button to move to the initiator/target mapping panel or the blade configuration download panel depending on whether the configuration needs to map initiators to targets.

Table 10. Blade configuration panel blade properties

Parameter	Description
Description	A text description of the blade.
Blade Type	An optional field describing the type of blade.
Serial#	An optional field containing the serial number of the blade.
Slot#	The slot in BladeCenter where the blade resides. If the blade occupies more than one slot, then this is the slot number of the slot containing the LEDs and power button.

Force IQN compatibility to version 1 on this blade

Checking this option will limit the selections of initiators to those that have IQN values with less than 72 characters. This option is per blade. If you chose the **Retrieve Data from BladeCenter** option on the environment panel and the BIOS level requires this limitation, this option will be grayed out and checked. If you chose the **Enter BladeCenter Data Manually** option on the environment panel, the configuration manager checks this box based on the XML file and it will not be grayed out; unchecking the box, in this case, may result in assigning an IQN that will not work.

Attempt n

Each blade can have up to four initiator attempts. They are attempted one at a time until a target is contacted. Attempt one is first, and attempt four last. The parameters for the four attempts are identical and described in Table 11.

Table 11. Blade configuration panel attempt

Parameters	Description
Initiator	The description of the initiator configured on the initiator configuration panel to use for this attempt. This field is only active when you select **Enabled** and **Use Full DHCP** is set to **No**.
Port Number	The switch bay on your chassis where you have connected the iSCSI SAN. This is 0 based, so the first switch bay jack is 0, the second is 1, and so on. This field is only active when you select **Enabled**.
Use Full DHCP	If this is set to **Yes**, then the configuration manager ignores all configured initiator parameters for this attempt and retrieves them from a DHCP server. This field is only active when you select **Enabled**.

Table 11. Blade configuration panel attempt (continued)

Parameters	Description
Enabled	Indicates whether or not this attempt is enabled.

Initiator or target mapping panel

You use the Initiator or target mapping panel (Figure 7) to assign targets to initiators.

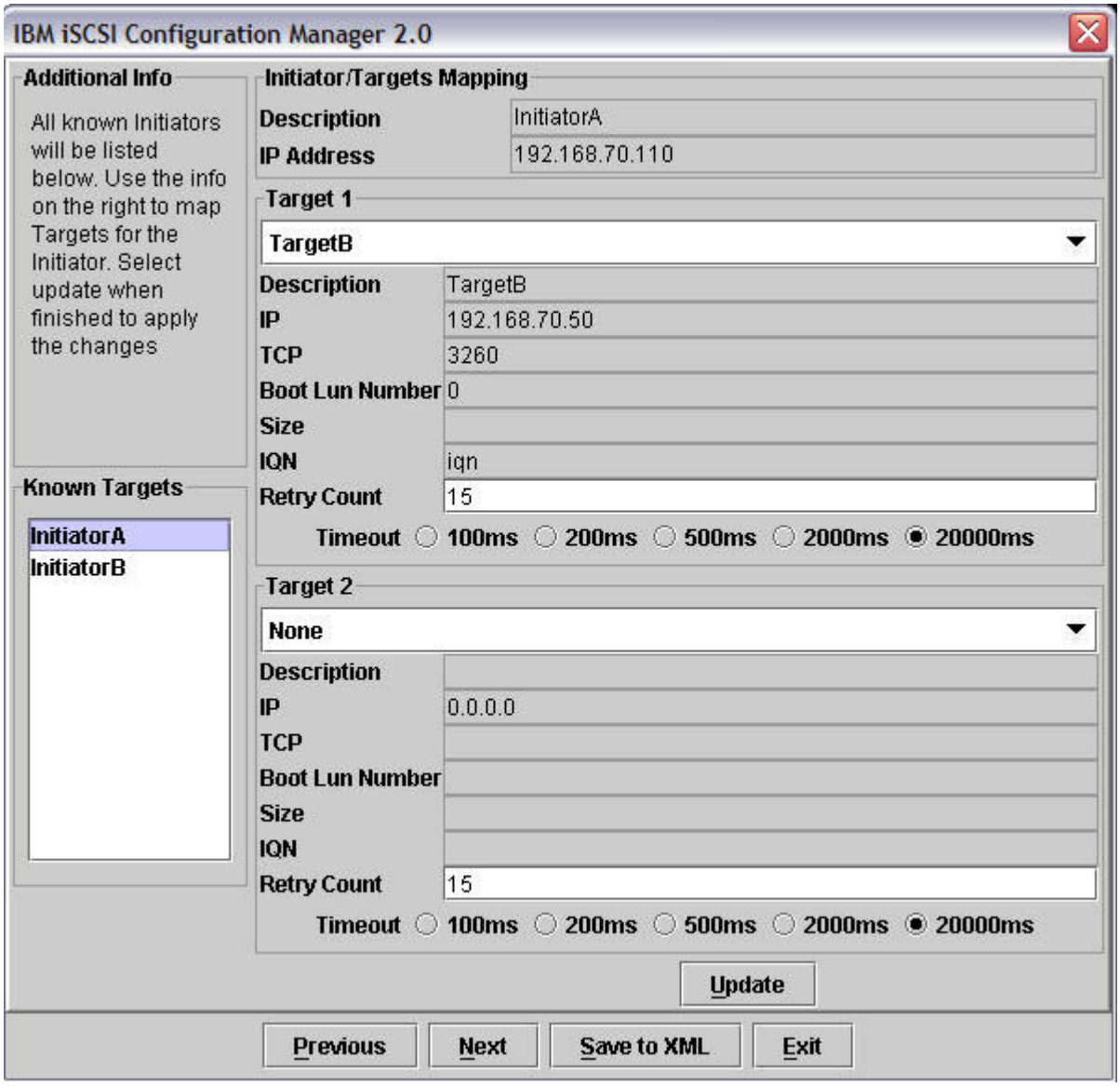

Figure 7. Initiator or target mapping panel

You can assign up to two targets to each initiator. The initiators configured on the previous panels are displayed in the **Known Targets** selection box. The configured targets are contained in the pull downs in the boxes marked **Target 1** and **Target 2**. You can assign a target only once to an initiator. When an initiator is configured in a blade's attempt on the blade configuration panel, the targets assigned to the initiator will be contacted when that attempt is activated during the boot process.

The **Retry Count** and **Timeout** fields are only active when you select either **All in VPD** or **All in VPD except Target IQN** in the **Dynamic Mode** box of the initiator configuration panel.

Press the **Next** button to move to the blade configuration download panel.

Blade configuration download panel

After you complete configuration of targets, initiators, and blades, the configuration manager can write the configuration into non-volatile storage on the blades. On the blade configuration download panel, you select the blades that should accept configuration from the configuration manager. After you select the desired blades, you press the Flash NVS on Blade(s) button to cause the configuration manager to download the configuration to the blades. The configuration manager uses the management module IP address, user ID, and password from the environment panel to communicate with the blade through the management module. This is the last configuration manager panel.

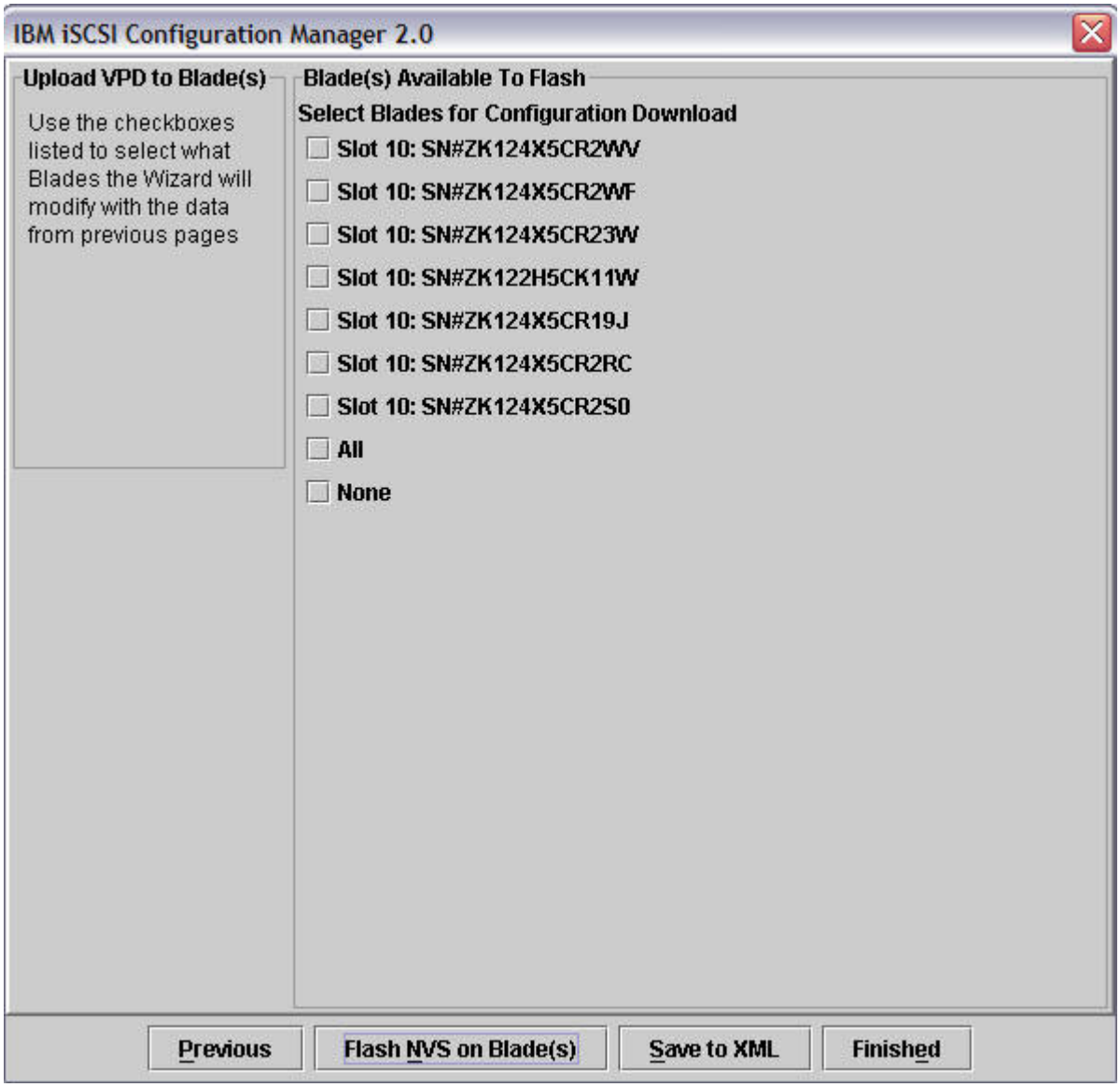

Figure 8. Blade configuration download panel

Save initiator configuration panel

After downloading the configuration to the blades, or at anytime during the configuration process, you can save the parameters entered on the configuration manager's GUI. To do so, press the **Save** button on any of the panels. The **Save Initiator Configuration** pop-up will appear. You can save the configuration in an existing file by selecting a file from the pull down list or enter a new file name in the blank.

The configuration manager will save the parameters when you press the **Save** button and when you press the **Finished** button on the blade configuration download panel.

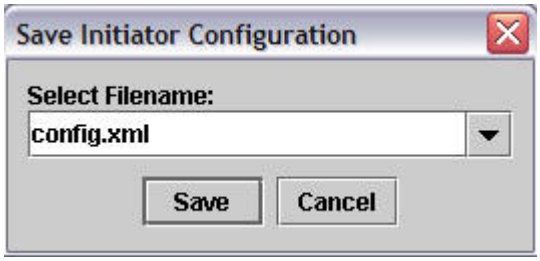

Figure 9. Save initiator configuration pop-up

Chapter 5. CLI usage of iSCSI Configuration Manager

In addition to its use as a GUI, you can use the configuration manager from a command line interface (CLI). In that case, the configuration manager reads an XML file containing the parameters and destination blades, builds the BIOS data structures, and sends the data structures to the destination blades. A document type definition (DTD) is available to validate the XML file produced by an application other than the initiator configuration manager.

Verifying the XML file

A XML DTD file is available for the configuration manager's configuration file. The configuration manager should produce a valid configuration file that you can use in CLI mode. However, there may be environments, where you may need to modify the XML file produced by the configuration manager. For example, you may want to replicate one base configuration file to many initiators changing the IP address of each initiator. In this case, you may individually download the configuration to each initiator using the CLI mode. You can then verify the modified XML file by using a tool such as **xmllint** (http://xmlsoft.org/xmllint.html - available as part of the libxml2 library from http://xmlsoft.org/downloads.html) with the example command below in a DOS prompt or Linux shell window.

```
xmllint --dtdvalid wizard.dtd <filename>.xml
```

Running the iSCSI Configuration Manager in CLI mode

The following command executes the configuration manager in CLI mode. All the parameters are supplied on the command line or in the configuration file. There is no user prompt. If all the parameters are valid the configuration manager downloads the configuration to the blades specified in the configuration file on the chassis containing the management module with the IP address <MM IP address>. The configuration file is required. The IP address is optional. The user ID is optional, but if the user ID is given, then the IP address and password are required. When an optional parameter is not present, its value is retrieved from the configuration file.

Command to run Configuration Manager in CLI mode

Note: The command is line wrapped for clarity. In actual CLI mode, you should type the command as one line.

```
java -cp wizard.jar;asmlibrary.jar;xercesImpl.jar
com.ibm.iSCSIWiz.initiatorwizard.InitiatorWizardGenerator –CLI
<configuration file> [<MM IP address> [<MM user ID> <MM Password>]]
```

CLI mode examples

Note: The following examples are line wrapped for clarity. In actual CLI mode, you should type the examples as one line.

```
java -cp wizard.jar;asmlibrary.jar;xercesImpl.jar
com.ibm.iSCSIWiz.initiatorwizard.InitiatorWizardGenerator –CLI
config\chassis1.xml

java -cp wizard.jar;asmlibrary.jar;xercesImpl.jar
 com.ibm.iSCSIWiz.initiatorwizard.InitiatorWizardGenerator –CLI
config\chassis1.xml 192.168.70.125

java -cp wizard.jar;asmlibrary.jar;xercesImpl.jar
com.ibm.iSCSIWiz.initiatorwizard.InitiatorWizardGenerator –CLI
config\chassis1.xml 192.168.70.125 USERID PASSW0RD
```

Figure 10. CLI mode examples

Appendix. Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Software Interoperability Coordinator, Department 49XA
3605 Highway 52 N
Rochester, MN 55901
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this information and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM the IBM logo, and BladeCenter are registered trademarks of IBM in the United States.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Glossary

Terms

This glossary defines technical terms and abbreviations used in this iSCSI configuration manager document. If you do not find the term you are looking for, view the IBM Glossary of Computing Terms, located at: http://www.ibm.com/ibm/terminology.

Selection of Terms: A term is a word or group of words to be defined. In this glossary, the singular form of the noun and the infinitive form of the verb are the terms most often selected to be defined. If the term may be abbreviated, the abbreviation is indicated. The abbreviation is also defined in its proper place in the glossary.

A

ASYNC
See **asynchronous**. See also **synchronous**.

asynchronous
Pertaining to events that are not synchronized in time or do not occur in regular or predictable time intervals. See also. See also **synchronous**.

B

Basic Input/Output System (BIOS)
The code that controls basic hardware operations, such as interactions with diskette drives, hard disk drives, and the keyboard.

baud The number of changes in signal levels, frequency, or phase per second on a communication channel. If each baud represents 1 bit of data, baud is the same as bits per second. However, it is possible for one signal change (1 baud) to equal more than 1 bit of data.

BIOS See **Basic Input/Output System**.

bits per second (bps)
In serial transmission, the instantaneous bit speed with which a device or channel transmits a character.

bps See **bits per second**.

C

cache Memory used to improve access times to instructions, data, or both. Data that resides in cache memory is normally a copy of data that resides elsewhere in slower, less expensive storage, such as on a disk or on another network node.

Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
A class of medium access procedures that allows multiple stations to access the medium at will, without explicit prior coordination, and avoids contention by way of carrier sense and deference. Contention is resolved by way of collision detection and transmission.

CHAP See **Challenge Handshake Authentication Protocol**.

Challenge Handshake Authentication Protocol (CHAP)
An authentication protocol that protects against eavesdropping by encrypting the user name and password.

chassis
The metal frame in which various electronic components are mounted.

client/server
Pertaining to the model of interaction in distributed data processing in which a program on one computer sends a request to a program on another computer and awaits a response. The requesting program is called a client; the answering program is called a server.

collision avoidance
In carrier sense multiple access with collision avoidance (CSMA/CA), the process of sending a jam signal and waiting for a variable time before transmitting data. The process is designed to avoid two or more simultaneous transmissions.

CRU See customer-replaceable unit.

CSMA/CD
See **Carrier Sense Multiple Access with Collision Detection**.

customer-replaceable unit (CRU)
An assembly or part that a customer can replace.

D

device parity protection
A function that protects data stored on a disk-unit subsystem from being lost because of the failure of a single disk unit in the subsystem. When a disk-unit subsystem has device parity protection and one of the disk units in the subsystem fails, the subsystem continues to run. The disk-unit subsystem reconstructs the data after the disk unit is repaired or replaced. See also Redundant Array of Independent Disks.

DHCP See **Dynamic Host Configuration Protocol**.

DIMM
See **dual inline memory module**.

document type definition (DTD)
The rules that specify the structure for a particular class of SGML or XML documents. The DTD defines the structure with elements, attributes, and notations, and it establishes constraints for how each element, attribute, and notation can be used within the particular class of documents.

drive bay
A receptacle in an appliance for a hard-disk-drive module. The drive bays are in storage units that can be located in a different rack from the appliance.

DTD See **document type definition**.

Dynamic Host Configuration Protocol (DHCP)
A communications protocol that is used to centrally manage configuration information. For example, DHCP automatically assigns IP addresses to computers in a network.

dual inline memory module (DIMM)
A small circuit board with memory-integrated circuits containing signal and power pins on both sides of the board.

E

EISA See Extended Industry Standard Architecture.

electrostatic discharge
An undesirable discharge of static electricity that can damage equipment and degrade electrical circuitry.

engine
The unit that contains the processors that respond to requests for data from clients. The operating software for the IBM TotalStorage appliance resides in the engine. See also storage port.

Ethernet
A packet-based networking technology for local area networks (LANs) that allows multiple access and handles contention by using Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the access method. Ethernet is standardized in the IEEE 802.3 specification.

expansion slot
In personal-computer systems, one of several receptacles in the rear panel of the system unit into which a user can install an adapter.

Extended Industry Standard Architecture (EISA)
The PC bus standard that extends the AT bus (ISA bus) to 32 bits and provides support for bus master. It was announced in 1988 as a 32-bit alternative to the Micro Channel that would preserve investment in existing boards. PC and AT adapters (ISA adapters) can plug into an EISA bus.

extensible markup language (XML)
A standard metalanguage for defining markup languages that is based on Standard Generalized Markup Language (SGML).

F

File Transfer Protocol (FTP)
In the Internet suite of protocols, an application layer protocol that uses TCP and Telnet services to transfer bulk-data files between machines or hosts.

FTP See **File Transfer Protocol**.

G

GBIC See gigabit interface converter.

gigabit interface converer (GBIC)
An encoding/decoding device that is a class-1 laser component assembly with transmitting and receiving receptacles that connect to fiber-optic cables. GBICs perform a serial optical-to-electrical and electrical-to-optical conversion of the signal. The GBICs in the switch can be hot-swapped.

H

host In TCP/IP, any system that has at least one Internet address associated with it.

I

iLUN See iSCSI client logical-unit number.

initiator
In Small Computer System Interface (SCSI) technology, the part of a host computer that communicates with its attached targets.

Internet Protocol (IP)
A protocol that routes data through a network or interconnected networks. This protocol acts as an intermediary between the higher protocol layers and the physical network.

interrupt request (IRQ)
An input found on a processor that causes it to suspend normal instruction execution temporarily and to start executing an interrupt handler routine.

IP See **Internet Protocol**.

IRQ See **interrupt request**.

iSCSI client logical-unit number (iLUN).
A unique number that is assigned to each virtual logical unit number (VLUN). The iLUN for a single client starts at zero and increments sequentially.

iSCSI configuration manager
A standalone Java application you can use to configure initiators on supported blades in an IBM BladeCenter chassis.

J

Java An object-oriented programming language for portable interpretive code that supports interaction among remote objects. Java was developed and specified by Sun Microsystems, Incorporated.

Java virtual machine (JVM)
A software implementation of a processor that runs compiled Java code (applets and applications).

jumper
A connector between two pins on a network adapter that enables or disables an adapter option, feature, or parameter value.

JVM See **Java virtual machine**.

L

LAN See **local area network**.

local area network (LAN)
A network that connects several devices in a limited area (such as a single building or campus) and that can be connected to a larger network.

logical drive
A unit of virtual storage that is made available to the network through virtual logical unit numbers (VLUNs) and iSCSI client logical-unit number (iLUNs). A logical drive consists of one or more physical disks that are combined using Redundant Array of Independent Disks (RAID) technology.

logical unit (LU)
An access point through which a user or application program accesses the SNA network to communicate with another user or application program.

logical unit number (LUN)
In the Small Computer System Interface (SCSI) standard, a unique identifier used to differentiate devices, each of which is a logical unit (LU).

LU See **logical unit**.

LUN See **logical unit number**.

M

megahertz (MHz)
A unit measure of frequency.

MHz See **megahertz**.

modulation
(1) The process by which a characteristic of a carrier is varied in accordance with a characteristic of an information-bearing signal. (2) The process by which a message signal is impressed upon a carrier signal so that the carrier is altered to represent the message signal.

multicast address
A type of IP address that identifies a group of interfaces and permits all of the systems that are in that group to receive the same packet of information.

N

N See **newton**.

network interface controller (NIC)
Hardware that provides the interface control between system main storage and external high-speed link (HSL) ports.

newton (N)
The unit of force required to impart an acceleration of one meter per second per second to a mass of one kilogram.

NIC See **network interface controller**

Nonvolatile Random Access Memory (NVRAM)
Random access memory (storage) that retains its contents after the electrical power to the machine is shut off.

NVRAM
See **Nonvolatile Random Access Memory**.

P

path (1) In a network environment, the route between any two nodes. (2) The route through a file system to a specific file. (3) In VSAM, a named logical entity that is composed of one or more clusters and provides access to the records of a base cluster either directly or through an alternate index.

path group
A collection of equivalent paths. Storage devices may have one - n path groups.

PCI See **Peripheral Component Interconnect**.

Peripheral Component Interconnect (PCI)
A local bus that provides a high-speed data path between the processor and attached devices.

R

RAID See **Redundant Array of Independent Disks**. See also **device parity protection**.

Redundant Array of Independent Disks (RAID)
A collection of two or more disk physical drives that present to the host an image of one or more logical disk drives. In the event of a single physical device failure, the data can be read or regenerated from the other disk drives in the array due to data redundancy. See also **device parity protection**.

S

SAN See **storage area network**.

SCSI See **Small Computer System Interface**.

Service Location Protocol (SLP)
An Internet protocol that identifies and uses network hosts without having to designate a specific network host name.

Simple Network Management Protocol (SNMP)
A set of protocols for monitoring systems and devices in complex networks. Information about managed devices is defined and stored in a Management Information Base (MIB).

SLP See Service Location Protocol.

Small Computer System Interface (SCSI)
An ANSI-standard electronic interface that allows personal computers to communicate with peripheral hardware, such as disk drives, tape drives, CD-ROM drives, printers, and scanners faster and more flexibly than previous interfaces.

SNMP
See **Simple Network Management Protocol**.

storage area network (SAN)
A dedicated storage network tailored to a specific environment, combining servers, storage products, networking products, software, and services.

storage client network
A classic, interconnected, fibre-channel fabric with a single, fibre-channel, fabric name.

storage controller
A device, such as a Redundant Array of Independent Disks (RAID) controller, that creates and manages other storage devices.

storage network
An arrangement that provides shared access to a set of logical unit numbers (LUNs) across one - n storage client networks.

storage port
An engine's connection point to a storage client network. A storage port is a member of a single fabric. See also engine.

storage unit
Hardware that contains one or more drive bays, power supplies, and a network interface. Some storage units contain Redundant Array of Independent Disks

(RAID) controllers; in this case, the storage unit is accessed by the appliance.

synchronous
Pertaining to two or more processes that depend upon the occurrences of specific events, such as a common timing signal. See also asynchronous.

T

Target A collection of logical units (LUs) that are directly addressable on the network. The target corresponds to the server in a client-server model.

Telnet In TCP/IP, a protocol that provides remote-terminal connection service. It allows users of one host to log on to a remote host and interact as if they were directly attached terminal users of that host.

U

UDP See **User Datagram Protocol**.

Universal Serial Bus (USB)
A serial-interface standard for telephony and multimedia connections to personal computers.

USB See **Universal Serial Bus**.

UFiT See **User Friendly Instance Tag**.

User Datagram Protocol (UDP)
An Internet protocol that provides unreliable, connectionless datagram service. It enables an application program on one machine or process to send a datagram to an application program on another machine or process.

V

virtual local area network (VLAN)
A logical association of switch ports based upon a set of rules or criteria, such as Medium Access Control (MAC) addresses, protocols, network address, or multicast address. This concept permits the LAN to be segmented again without requiring physical rearrangement.

vital product data (VPD)
A structured description of a device or program. For devices, it is recorded in the device at manufacture and includes at least the type, model, serial number, and installed features. It may include the manufacturer's ID and other fields. For programs, it is compiled as a data area accompanying the program and includes the name of the licensed program or Licensed Internal Code group, the release and modification, the program module names, the national language or languages selected, and possibly other fields. Vital product data is transferred from the device to the system and stored for display. Vital product data is also visible on the device name plate or a similar tag.

virtual logical unit number (VLUN)
A subset of a logical drive.

VLAN See **virtual local area network**.

VLUN See **virtual logical unit number**.

VPD See **vital product data**.

X

XML See **Extensible Markup Language**.

Index

Part Number: xxxxxxx

Printed in USA

(1P) P/N: xxxxxxx