HITACHI
DATA SYSTEMS

Hitachi TagmaStore®
Adaptable Modular Storage
and Workgroup Modular Storage

LUN Manager User's Guide

MK-95DF703-05

Trademarks

Notice of Export Controls

Export of technical data contained in this document may require an export license from the United States government and/or the government of Japan. This technical data may not be used directly or indirectly (without U.S. Government permission), in the design, development, fabrication, production, testing or use of rocket systems, or unmanned air vehicles; or chemical or biological weapons; or nuclear weapons or explosives or operation of facilities or components thereof for chemical processing of irradiated special nuclear or source material, heavy water production, separation of isotopes of source and special nuclear material, or fabrication of nuclear reactor fuel containing plutonium, or in International Atomic Energy Agency (IAEA) un-safeguarded nuclear facilities

Please contact the Hitachi Data Systems Legal Department for any export compliance questions.

Document Revision Level

Revision	Date	Description
MK-95DF703-0P	May 2005	Preliminary draft of documentation for Initial Release
MK-95DF703-00	June 2005	Initial release
MK-95DF703-01	August 2005	Revision 1, supersedes and replaces MK-95DF703-00
MK-95DF703-02	October 2005	Revision 2, supersedes and replaces MK-95DF703-01
MK-95DF703-03	December 2005	Revision 3, supersedes and replaces MK-95DF703-02
MK-95DF703-04	February 2006	Revision 4, supersedes and replaces MK-95DF703-03
MK-95DF703-05	July 2006	Revision 5, supersedes and replaces MK-95DF703-04

Changes in this Revision

- Updated software version to 5.0 and higher
- Updated sections 1.2, 1.3, and 1.4
- Updated section 2.3
- Updated Table 2.5, removing last row concerning queue depth and maximum commands per port
- Updated Figure 5.2, iSCSI Protocol Stack
- Added section 5.3, Network Configuration for iSCSI
- Updated Table 5.1, Requirments and Specifications for iSCSI
- Updated Table 5.2, Combinations of OS and HBA for iSCSI
- Updated Figure 6.1, Figure 6.2, Figure 6.5, Figure 6.6, Figure 6.7, and Figure 6.8
- Updated section 6.2.5, Multiple Host Connections to iSCSI Ports Can Affect Performance
- Updated section 6.4, Assigning Targets and LUs to Hosts
- Updated section 7.1.2, 7.5, and 7.10.1 adding text concerning the iSCSI software initiator
- Updated Appendix B.2.5, Windows NT® / Windows® 2000/2003
- Added Appendix B.2.5.3, Qlogic® QLA2460/QLA2462/QLE2460/QLE2462
- Updated Appendix B.2.5.4, Qlogic® QLA2200F/QLA2300F

Preface

This document describes the LUN Manager software from Hitachi Data Systems. LUN Manager streamlines configuration management processes by enabling you to define, configure, add, delete, revise, and reassign LUNs to specific paths without having to reboot your system. Because LUN Manager can assign multiple paths to a single LUN, you gain the necessary infrastructure to support alternative path failover, path load balancing, and clustered systems.

This document assumes the following:

- The user has a background in data processing and understands direct-access storage device subsystems and their basic functions.
- The user is familiar with the disk array subsystem.
- The user has read and understands the *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711) and/or the *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Command Line Interface (CLI) User's Guide* (MK-95DF712).

For more information about the Adaptable Modular Storage subsystem features and functions, please contact your Hitachi Data Systems account team or visit Hitachi Data Systems online at http://www.hds.com.

Notes:

- The screens shown in this document were captured on a Windows® system with the Internet Explorer web browser. The screens may display differently on other operating systems and browsers. Please refer to the *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-92DF711) for further information on other operating systems and browsers.
- The term "Navigator" refers to the Storage Navigator Modular program.
- The use of Hitachi LVD and all other Hitachi Data Systems products is governed by the terms of your agreement(s) with Hitachi Data Systems.

Notice: The use of Hitachi Resource Manager, the LUN Manager software, and all other Hitachi Data Systems products is governed by the terms of your license agreement(s) with Hitachi Data Systems.

Software Version

This document revision applies to TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage versions 5.0 and higher.

Convention for Storage Capacity Values

Storage capacity values for hard disk drives (HDDs) are calculated based on the following values:

1 KB = 1,000 bytes
1 MB = $1,000^2$ bytes
1 GB = $1,000^3$ bytes
1 TB = $1,000^4$ bytes

Storage capacity values for logical units (LUs) are calculated based on the following values:

1 KB = 1,024 bytes
1 MB = $1,024^2$ bytes
1 GB = $1,024^3$ bytes
1 TB = $1,024^4$ bytes
1 block = 512 bytes

Referenced Documents

- *Hitachi TagmaStore™ Adaptable Modular Storage 200™ User and Reference Guide* (MK-95DF713)
- *Hitachi TagmaStore™ Adaptable Modular Storage 500™ User and Reference Guide* (MK-95DF714)
- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711)
- *Hitachi TagmaStore™ Adaptable Modular Storage and Workgroup Modular Storage, Storage Navigator Modular Command Line Interface (CLI) User's Guide* (MK-95DF712)

Comments

Please send us your comments on this document. Make sure to include the document title, number, and revision. Please refer to specific section(s) and paragraph(s) whenever possible.

- **E-mail:** doc.comments@hds.com
- **Fax:** 858-695-1186
- **Mail:**
  Technical Writing, M/S 35-10
  Hitachi Data Systems
  10277 Scripps Ranch Blvd.
  San Diego, CA 92131

Thank you! (All comments become the property of Hitachi Data Systems Corporation.)

Contents

List of Figures

List of Tables

Chapter 1 Installing and Enabling LUN Manager

This chapter describes LUN Manager installation using the GUI version of Storage Navigator Modular (Navigator). For information about CLI installation, see Appendix A. Each disk array subsystem requires its own set up.

In this chapter:

- System Requirements (section 1.1)
- Installing LUN Manager (section 1.2)
- Uninstalling LUN Manager (section 1.3)
- Enabling and Disabling LUN Manager (section 1.4)

1.1 System Requirements

To be able to use LUN Manager, you need:

- An installed AMS subsystem
- The LUN Manager software enabled

For further information about these requirements, please refer to *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711).

1.2 Installing LUN Manager

The LUN Manager feature is usually unselectable (locked). To make it available, you must first install it and make its functions selectable (unlocked). **To install LUN Manager, you need the key code or key file provided with it.**

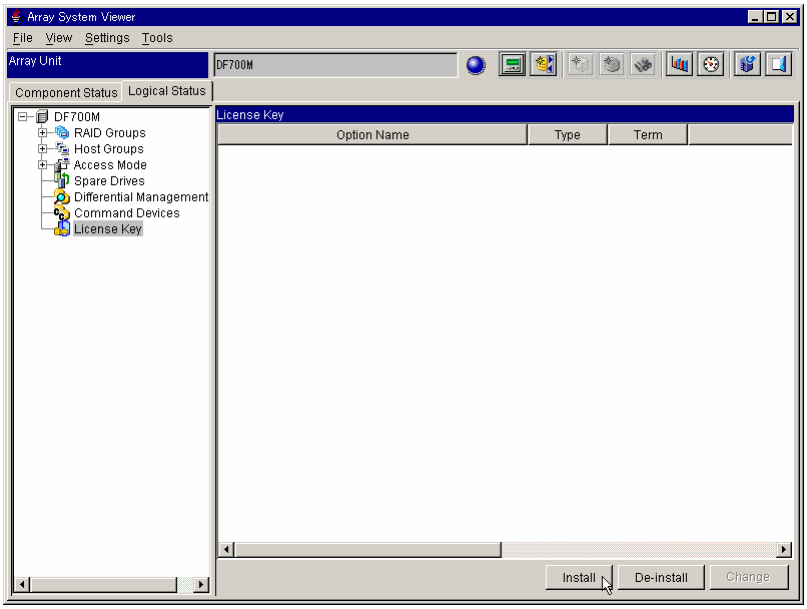
Before installing or uninstalling, make sure that the array unit is in normal operating condition. If a failure such as a controller blockade has occurred, installation and uninstallation operations cannot be performed.

This document describes how to install and uninstall LUN Manager using the GUI version of Storage Navigator Modular (also called Navigator). For more detailed installation instructions using Navigator, refer to the *Hitachi TagmaStore™ Adaptable Modular Storage, Storage Navigator Modular Graphical User Interface (GUI) User's Guide*.

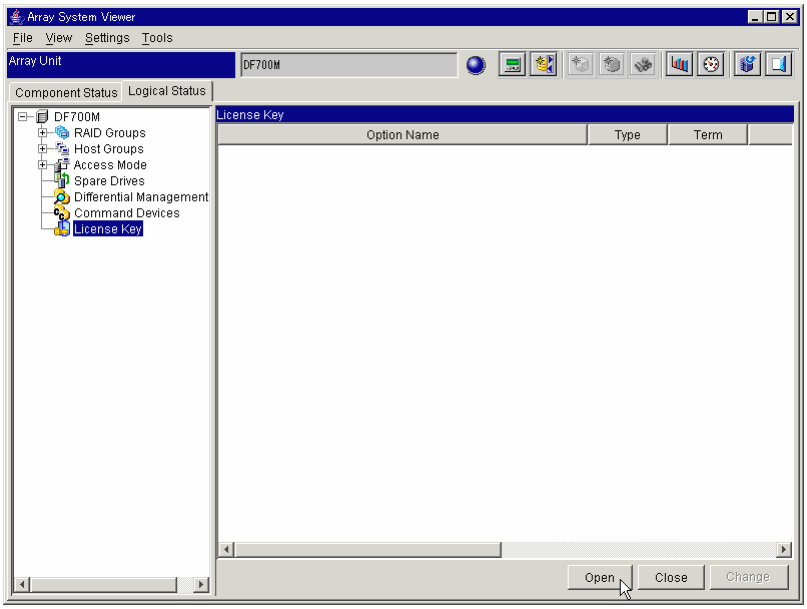
To install the LUN Manager feature using the GUI version of Navigator:

1. Start the Navigator and change the operation mode to **Management Mode**.
2. Register the subsystem (array unit) in which you will install LUN Manager and connect to it.

   The **Array System Viewer** window appears and displays the connected subsystem.



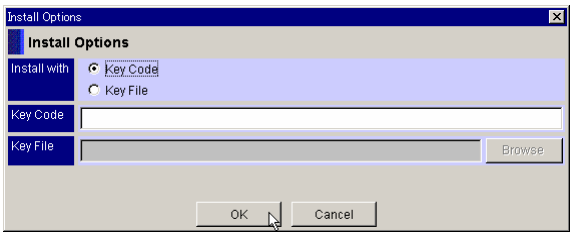
Navigator: Version 5.00 or later



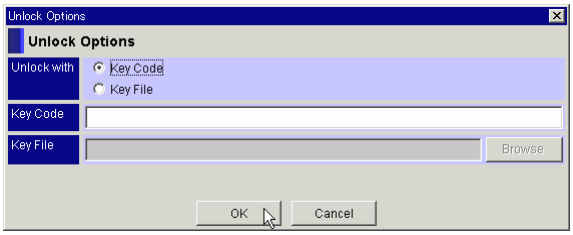
Navigator: Less than 5.00 version

3. Click the **Logical Status** tab.
4. Click the **License Key** icon.
5. Click **Install**. The **Install Options** dialog appears. (Navigator: Version 5.00 or later)

   Click **Open**. The **Unlock Options** dialog appears. (Navigator: Less than 5.00 version)



Navigator: Version 5.00 or later



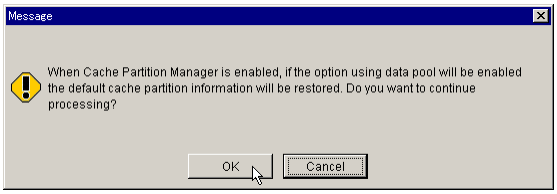
Navigator: Less than 5.00 version

6. Choose an install option:
   - Key Code

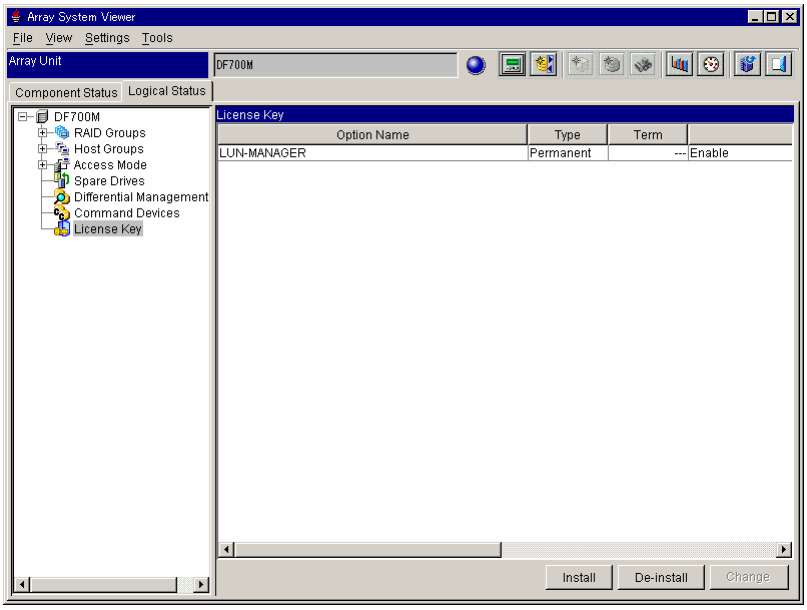
     Select the **Key Code** option. In the Key Code field, enter the key code and click **OK**.
   - Key File

     Select the **Key File** option. In the Key File field, enter the path to the key file and click **OK**. In the **Install/Unlock Options** box that appears, select LUN Manager and click **OK**.
7. In any confirmation screens that appear, click **OK** or **Close** to continue.

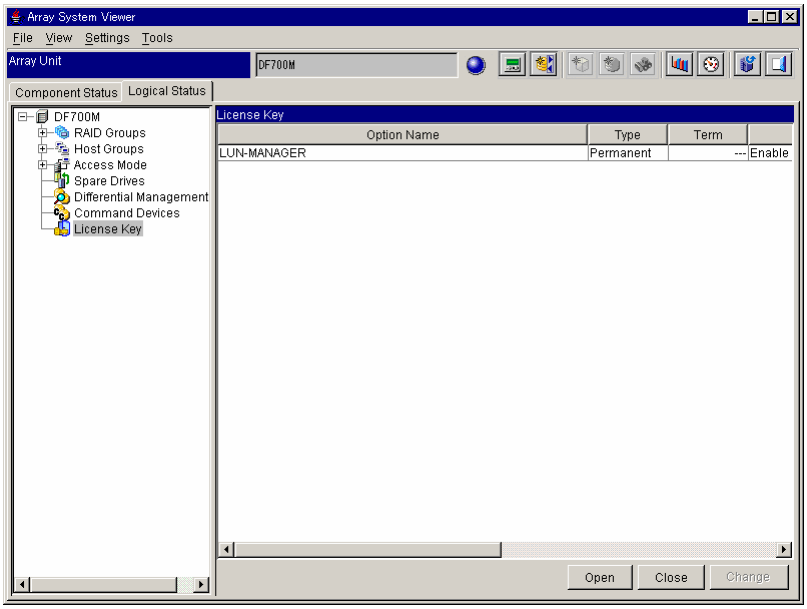
   The window indicates that LUN-MANAGER is enabled and LUN Manager is installed (unlocked).
8. When the Navigator version is 3.00 or later and Cache Partition Manager is enabled, the following message is displayed. Since LUN Manager does not use the data pool, click the **OK** button at this point without doing anything else.



The window indicates that LUN-MANAGER is enabled and LUN Manager is installed.



Navigator: Version 5.00 or later



Navigator: Less than 5.00 version

1.3 Uninstalling LUN Manager

Follow the instructions below to uninstall the LUN Manager. When uninstalled, LUN Manager is uninstalled and not available until it is installed by using the key code or key file.

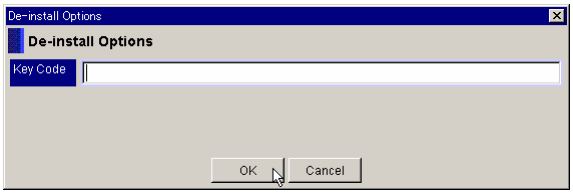
Note: When disabling or uninstalling LUN Manager, you must first disable the host group and/or target security on all ports.

To uninstall LUN Manager:

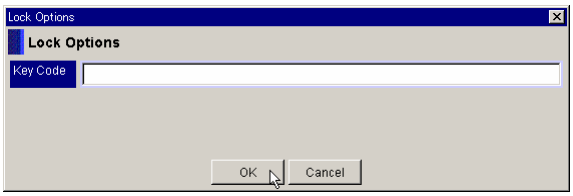
1. Start Navigator and change the operation mode to **Management Mode**.
2. Register the subsystem (array unit) in which you will uninstall LUN Manager. Connect to the subsystem.

   The **Array System Viewer** window appears and displays the connected subsystem.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon.
5. Click **De-install**. The **De-install Options** dialog is displayed. (Navigator: Version 5.00 or later)

   Click **Close**. The **Lock Options** dialog is displayed. (Navigator: Less than 5.00 version



Navigator: Version 5.00 or later



Navigator: Less than 5.00 version

6. Enter a **Key Code** in the text box and click **OK**.
7. In the confirmation screen that appears, click **OK** to continue.

   LUN Manager is uninstalled. To perform other operations, connect to the subsystem again and open the **Array System Viewer** window.

1.4 Enabling and Disabling LUN Manager

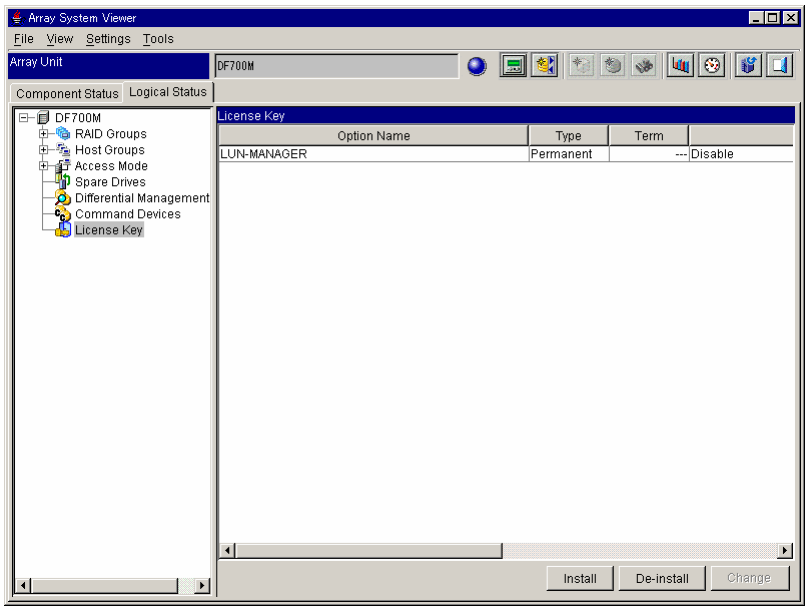
The LUN Manager feature can be set to enable or disable when it is installed.

Note: When disabling or uninstalling LUN Manager, you must first disable the host group and/or target Security on all ports.

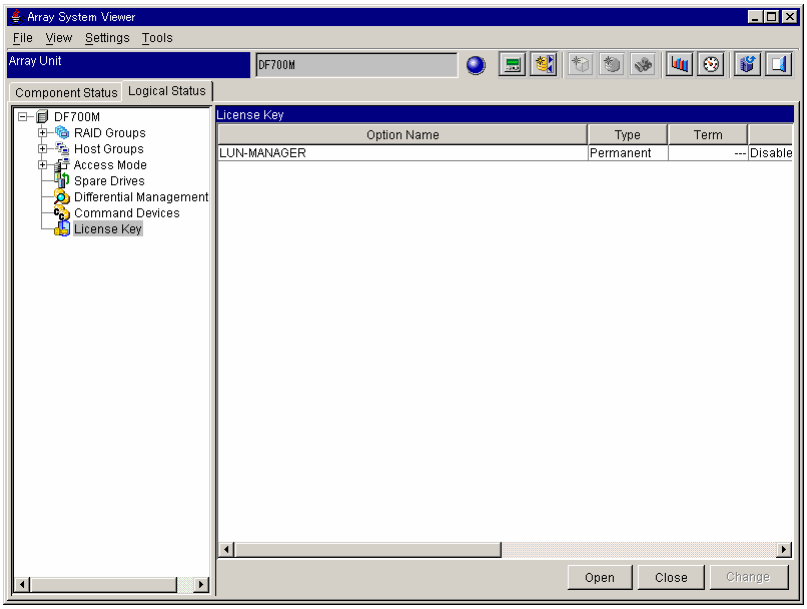
To enable or disable LUN Manager:

1. Start Navigator and change the operation mode to **Management Mode**.
2. Register the subsystem in which you will change the status of LUN Manager. Connect to the subsystem.

   The **Array System Viewer** window appears and displays the connected subsystem.
3. Click the **Logical Status** tab.
4. Click the **License Key** icon.
5. From the **Option Name**, select **LUN-MANAGER** and click **Change**.
6. In the confirmation window that appears, click **OK** to continue.



Navigator: Version 5.00 or later



Navigator: Less than 5.00 version

The status of LUN Manager feature is changed (enabled/disabled). To perform other operations, connect to the subsystem again and open the **Array System Viewer** window.

Chapter 2 Fibre Channel Networks and LUN Manager Overview

The LUN Manager feature enables you to set the option (host connection mode), the Logical Unit (LU), and the WWN (World Wide Name) parameters for each connected host so that multiple hosts may be connected to the same port.

By using LUN Manager, each host may access a LU as if it were a dedicated port to the host, even if that host shares the port with other hosts.

In this chapter:

- LUN Manager Sets Access between Hosts and Logical Units (section 2.1)
- Features (section 2.2)
- Creating a Host Group (section 2.3)
- Setting a Host (section 2.4)
- Setting a Logical Unit (section 2.5)
- Configuration (section 2.6)
- Making Changes After Operation has Started (section 2.7)
- Specifications (section 2.8)
- Overview of Procedures (section 0)

2.1 LUN Manager Sets Access between Hosts and Logical Units

LUN Manager manages access paths between hosts and logical units (LUs) for each port. With LUN Manager, two or more host systems or operating systems (also called host groups) may be connected to one port of a Hitachi Data Systems' AMS/WMS subsystem, and LUs may be freely assigned to each host system.

With LUN Manager, Illegal access to LUs from any host system may be prevented, and each host system may safely use an AMS/WMS subsystem as if it were connected to several storage systems.

Figure 2.1 illustrates a port being shared by multiple host systems.

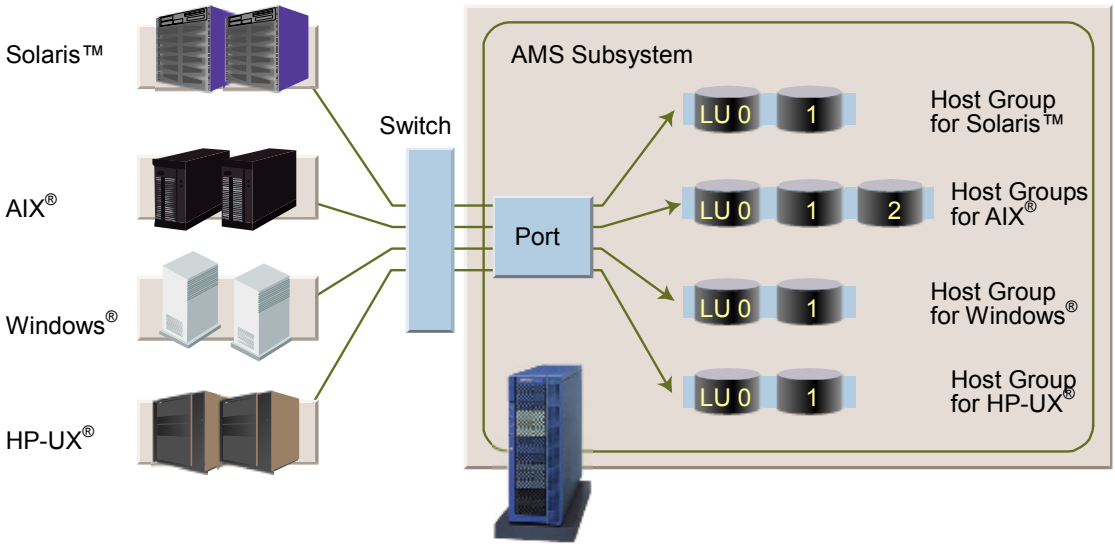


Figure 2.1 Setting Access Paths between Hosts and Logical Units for Fibre Channel

2.2 Features

Table 2.1 lists LUN Manager features for Fibre Channel.

Table 2.1 LUN Manager Features for Fibre Channel

Feature	Description
Prevents illegal access from the other hosts.	LUs are grouped and each group is registered in a port. LUN Manager specifies which host may access which LU by assigning hosts and LUs to each host group.
The host connection mode can be set for each host connected.	The host connection mode can be set for each host group. "HP Connection Mode 2", enables the LU8 and above to be recognized in the HP® connection, may be connected to the same port to which the other hosts are connected.
The LU mapping can be set for each host connected.	LU numbers (H-LUN) recognized by a host can be assigned to each host group. By virtue of this, two or more hosts that require LU0 can be connected to the same port.

Note: Additional hosts may be connected to one port although this increases traffic on the port. When you use LUN Manager, you should design the system configuration appropriately to evenly distribute traffic at the port, controller, and disk drive.

2.3 Creating a Host Group

A system configuration engineer uses LUN Manager to connect a port of a disk array subsystem to a host using a switch, etc., and then sets a data input/output path between the host and the LU. This setting specifies which host may access which LU.

To set a data input/output path, the hosts that are authorized to access the LU are required to be classified as a host group. Then the classified host group is set to the Port.

If a Windows® host and a Linux host are connected to Port A for example, you must create host groups of LUs that can be accessed by both operating systems (see Figure 2.2).

A host group option (host connection mode) may be set for each created host group.

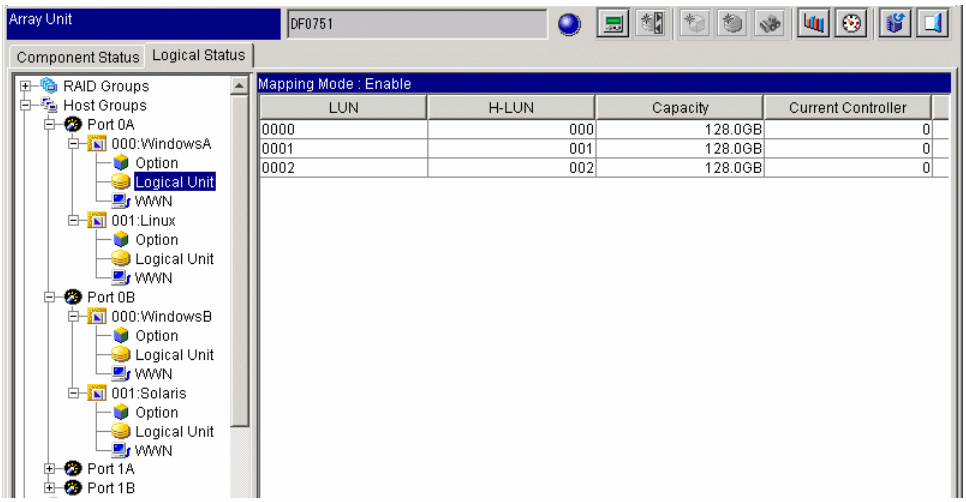
Hosts that are connected to different ports cannot share the same host group.

Even if the LU to be accessed is the same, separate host groups should be created for each port to which the hosts are connected.

2.4 Setting a Host

After creating a host group, the host that has been assigned to the host group is set. This setting is performed by using the World Wide Name (WWN) of the Host Bus Adapter (HBA). The same WWN cannot be set to another host group within the same port.

Figure 2.2 shows an example where the WWN of a Windows® HBA is registered to the Windows® host group in Port A and the WWN of a Linux HBA is also registered to a Linux host group in Port A.



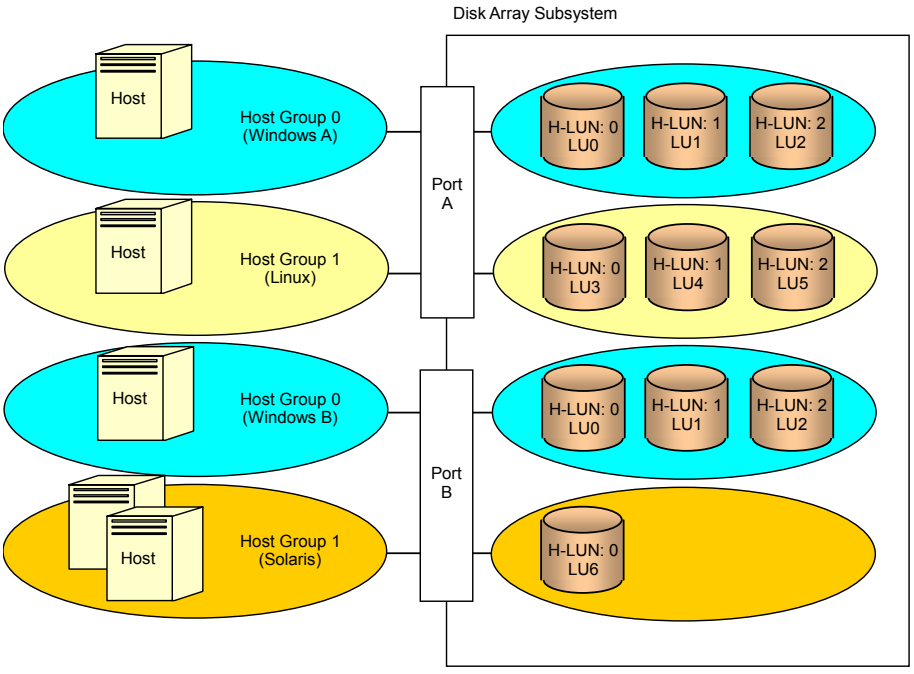


Figure 2.2 Setting Access Paths between Hosts and Logical Units for Fibre Channel

2.5 Setting a Logical Unit

After setting a host to a host group, the LU is connected to that host group by mapping to the host group. A data input/output path is then set between the LU and the host that belongs to the host group so that the host can access the LU.

A host group determines which LU may be accessed from which host. A host can access a LU connected to the host group to which that host belongs, but it cannot access a LU connected to another host group.

A host that belongs to the Windows® host group in Port A, for example, cannot access the LUs in the Linux host group, and a host that belongs to the Linux host group cannot access the LUs in the Windows® host group (refer to Figure 2.2).

LUN Manager can set a host to access multiple LUs. In Figure 2.2, for example, a host in the Windows® host group in Port B may access three LUs.

LUN Manager may also set a LU to be accessed from multiple hosts. In Figure 2.2, for example, two hosts in the Solaris™ host group in Port B may access the same LU.

2.6 Configuration

The subsystem is connected to a host with an optical fibre cable. The end of the cable on the host side is connected to a host bus adapter (HBA) and the end of the cable on the subsystem side is connected to a port on the disk array subsystem.

Using LUN Manager, LUs can be grouped and assigned to a port as a host group. You may specify which HBA can access that group by assigning the WWNs of the HBAs to each host group. Identify which LUs you want to use through which physical port with a particular host, and then define a host group on that port for them.

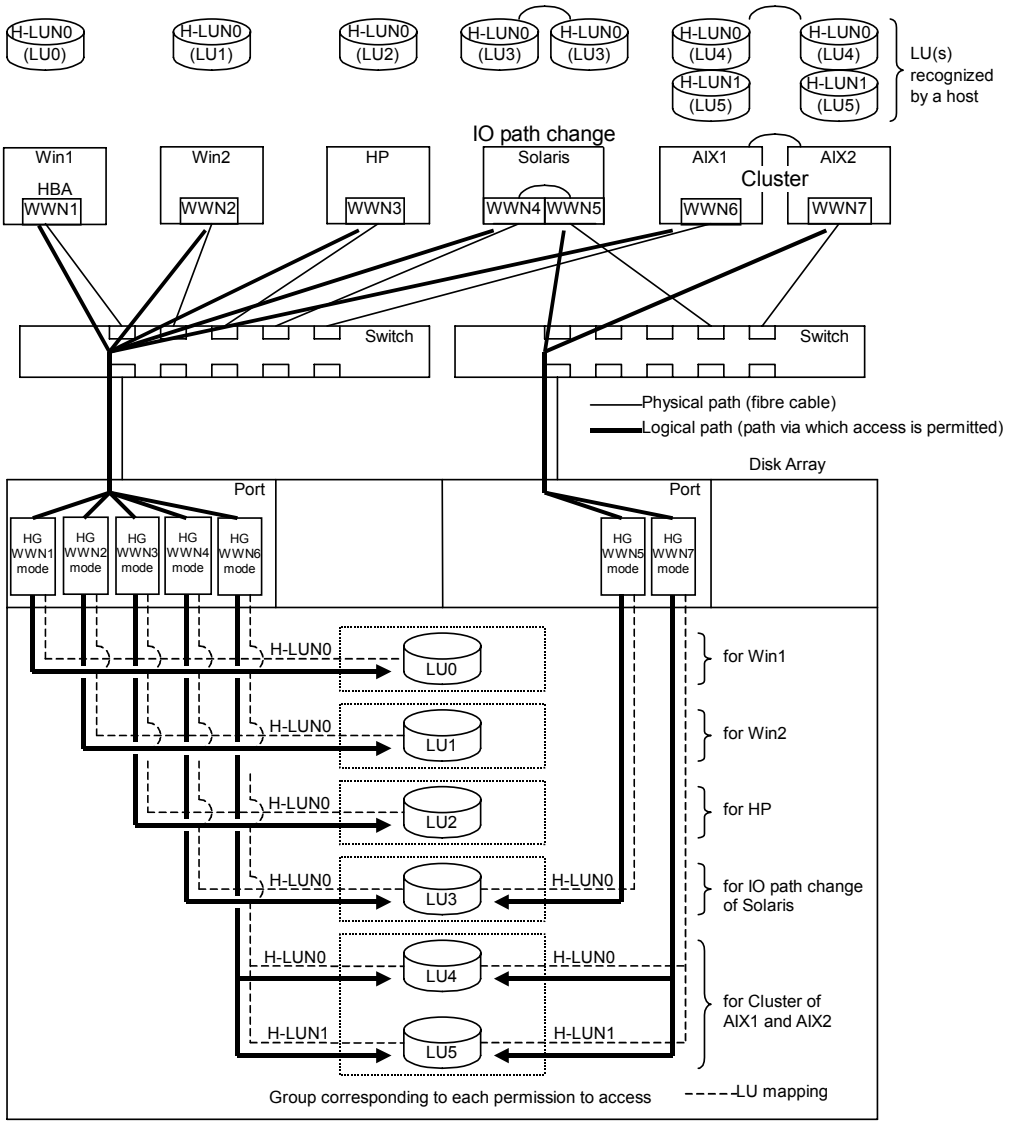


Figure 2.3 Example of System Configuration for Fibre Channel

Figure 2.4 and Figure 2.5 show possible configurations for creating a host group for multipathed and clustered environments.

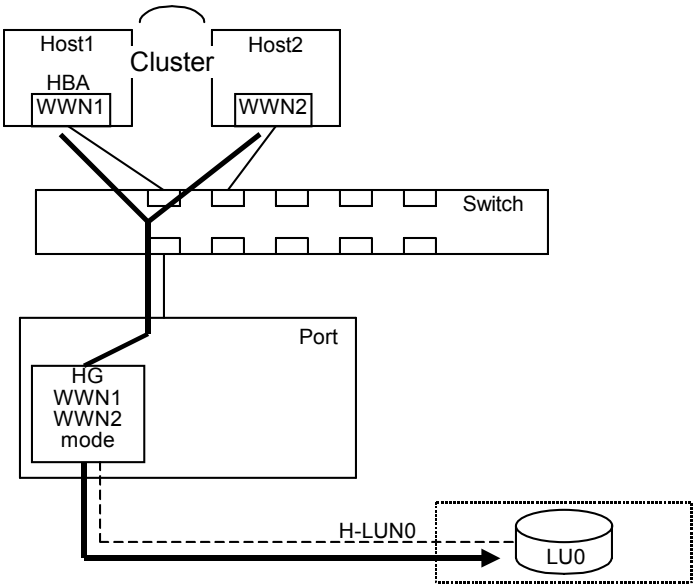


Figure 2.4 Configuration 1 (One Host Group) for Fibre Channel

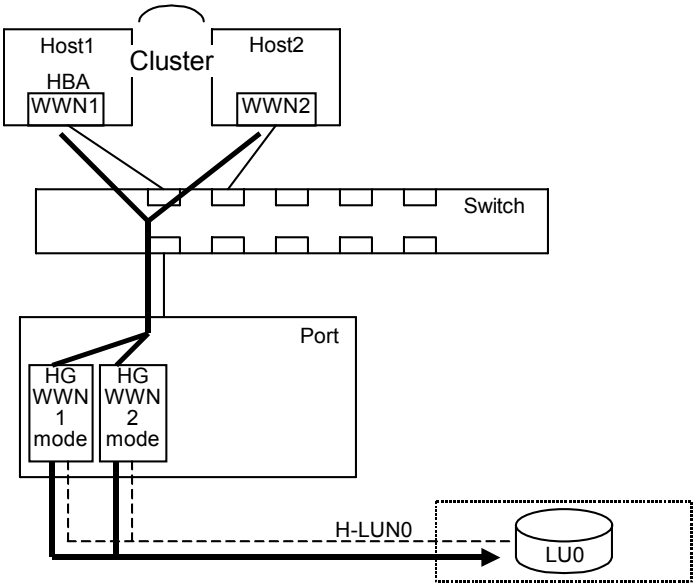


Figure 2.5 Configuration 2 (Two Host Groups) for Fibre Channel

2.7 Making Changes After Operation has Started

LUN Manager can add, modify, or delete a host group after operation of the system has started. For example, when an additional disk is installed or an additional Host is connected, an additional host group can be created. When removing an existing Host, the host group that is connected to the host is deleted first and then the host will be removed.

Note: When adding, modifying, or deleting the settings by LUN Manager, it is not necessary to reboot the Disk Array subsystem.

2.8 Specifications

LUN Manager specifications for Fibre Channel are described in Table 2.2.

Table 2.2 The Specifications of LUN Manager for Fibre Channel

Item	Specifications
Host Group	• Up to 128 host groups may be set for each Port. • Host group 0 (zero) is required.
Setting/Deleting a Host Group	• Host groups 1 through 127 can be set or deleted. • Host group 0 cannot be deleted. To delete the WWN and LU mapping of Host group 0, initialize Host group 0.
Host Group Name	• A name is assigned to a host group when it is created and can be changed.
WWN (Port Name)	• Up to 128 WWNs of HBAs may be set for a host group or port. • The WWN cannot be assigned to another host group on the identical same Port. • A WWN may also be set to the host group by selecting from a Logined WWN of the HBA connected to the port.
Optional WWN	• An optional name may be assigned to a WWN allocated to a host group and then deleted later. • A name assigned to a WWN is valid until the WWN is deleted.
Host Connection Mode	• The host connection mode of a host group can be changed.
LU Mapping	• LU Mapping can be set to the host group. • Up to 256 LU Mappings can be set for a host group. Up to 256X128 LU Mappings can be set for a Port.
Enable/Disable Setting for each Port	• LUN Manager can be set to **enable** or **disable** for each port. • When LUN Manager is disabled, previously set LUN Manager information is kept and is available when it is enabled again.
Online Setting	• When adding, modifying, or deleting settings made with LUN Manager, it is not necessary to reboot the disk array subsystem.

Conditions for using LUN Manager for Fibre Channel are shown in Table 2.3.

Table 2.3 Conditions of Using LUN Manager for Fibre Channel

Item	Conditions
Making Settings	Storage Navigator Modular is required.
Using LUN Manager with other Optional Functions	Optional functions can be used together with LUN Manager.
Queue Depth	Max. 32 commands per LU Max. 512 commands per port

2.8.1 Default Queue Depth Configurations

The default Queue Depth settings for each host operating system is shown in Table 2.4.

Table 2.4 The Queue Depth Configuration for Fibre Channel

Platform	HBA	Queue Depth		Unit of Setting
		Unit of Value	Default	
Solaris™		LU	256	OS
HP-UX		LU	8	LU
AIX®		LU	1	LU
IRIX®		LU	1	LU
Windows®	Emulex® (Port)	LU	8	HBA
	Emulex® (MiniPort)	LU	32	HBA
	Qlogic®	Port	16	HBA

2.8.2 Queue Depth Limits of System Combination

When several host operating systems are connected to a single port of a disk array subsystem, you must set the queue depth value listed in Table 2.5.

See section 3.7 for more information about setting queue depth.

Table 2.5 Queue Depth Limits of System Combination for Fiber Channel

System Combination	Setting Queue Depth
Windows NT®/Windows® 2000 MSCS	Max.16 commands per port (for Qlogic® HBA)
HP-UX MC/ServiceGuard	No limit

2.9 Overview of Procedures

The following are general setup guidelines:

Setting Up a SAN Environment

- Set up connections between hosts and the disk array subsystem.
- Set up switch connections.
- Set up the disk array subsystem offline.

Installing and Setting Up LUN Manager

- Install and set up LUN Manager:
  - Install LUN Manager.
  - Obtain WWNs for each HBA(s) to be set with LUN Manager (see section B.2).
  - Set switch zoning when necessary.
- Verify host connections:
  - Verify that each host can recognize the LU(s) after changing settings with LUN Manager.
  - If necessary, specify the Queue Depth of each host.

Updating LUN Manager Settings if the SAN Environment Changes

- Change LUN Manager settings if hosts connected to the disk array subsystem are added or changed, or if the number of LUs assigned to a host Storage Domain (host group) increases. When adding a host or changing a connected host, the WWN of an HBA of the host must be identified.
- If replacing an HBA, the WWN registered in LUN Management must be changed to that of the new HBA.
- If replacing a switch, the same zoning must be set for the new switch.
- Verify that the LUN Manager settings are correct.

  Note: The LUN Manager function is not available if a host (OS or driver) cannot identify a LUN#0. You must set H-LUN = 0 to the host group.

Table 2.6 Combinations of OS and HBA for Fibre Channel

OS	HBA	Remarks
HP-UX®	HP HBA	When HP-UX Mode = Enable is selected
IRIX®	SGI™ HBA	—
Windows® 2000	Emulex® HBA (with Miniport Driver) Qlogic® HBA	—
Linux®	Emulex® HBA Qlogic® HBA	—

- When you replace an HBA in a host attached to a Disk Array subsystem using host group, be sure to change the setting of the LUN Manager.
- LUN Manager settings (enabling or disabling) are not immediately effective after setting. The host must be rebooted for the settings to take effect.
- When using LUN Manager function on a fabric switch connection:
  - When connecting to the servers (HBA) or changing the HBA, connect the servers (HBA) that can access to Disk Array after the setting (including WWN registration) completes.
  - Set the zoning on Fabric Switch to block the access from HBAs to disk array subsystem as necessary.

Chapter 3 Fibre Channel Configuration

This chapter provides instructions for preparing for LUN Manager operations using the GUI version of Storage Navigator Modular (Navigator).

In this chapter:

- Design Considerations (section 3.1)
- System Design (section 3.2)
- System Configuration (section 3.3)
- Adding and Replacing Equipment (section 3.4)
- Avoiding RAID Group Conflicts (section 3.5)
- Preventing Illegal Access to SAN (section 3.6)
- Queue Depth Setting of SAN (section 3.7)

3.1 Design Considerations

When connecting multiple hosts to one port of the disk array subsystem, the system must be designed to accommodate the following:

- System design
  - Assign LUs to hosts
  - Assign LUs to RAID groups
  - Determine the system configuration
  - Determine the method of illegal access prevention
  - Determine queue depth
- System configuration
  - Set LUN Manager
  - Set switch zoning
- Component addition and replacement
  - Host and HBA addition
  - LU addition
  - HBA replacement
  - Switch replacement

3.2 System Design

System design should incorporate the following:

- Assign LUs to Hosts

  Group logical units (LUs) of the disk array subsystem into host groups with permitted access. Use the host group when making settings for LUN Manager.

- Avoid Contention

  Each LU is defined as belonging to a RAID group. When two LUs (defined as belonging to the same RAID group) are accessed at the same time, operational performance may decrease. When operating two or more hosts at the same time, it is recommended that LUs (assigned to each host) be assigned to separate RAID groups.

- System Configuration

  When connecting more hosts than ports of the disk array subsystem, increase the number of ports to be connected to hosts using the fibre channel switch.

- Prevent Illegal Access

  Determine input/output paths between hosts and LUs according to the assignment mode using LUN Manager. The input/output path is a route through which access from the host is permitted.

  Set switch zoning to prevent interference from the other hosts that share the same switch. When the zoning is set, ports outside the zone do not affect ports within the zone.

- Queue Depth

  Multiple hosts can now be connected to a single port. The queue depth that can be handled by one port is limited and performance drops if that limit is exceeded. You should therefore specify the queue depth so that the sum for all hosts does not exceed the port's limit.

3.3 System Configuration

System configuration incorporates the following:

- Make settings for LUN Manager

  Set the following for each disk array subsystem to specify the input/output paths between hosts and LUs:

  - Host group
  - WWN of HBA
  - LU mapping
  - Host connection mode

  For future reference, keep a detailed record of the settings that have been made for the disk array subsystem. If an HBA is replaced, change the WWN name accordingly so that you can identify the previous WWN name that was set.

- Set Switch Zoning

  Connect hosts and the disk array subsystem to a switch and set a zoning for the switch.

  Create a diagram and record of connections between the switch and hosts, and connections between the switch and disk array subsystem. When the switch is replaced, you can make the same connections as before the replacement by referring to your records.

3.4 Adding and Replacing Equipment

After installing LUN Manager, you may do the following:

- Add a host and an HBA

  When assigning LUs within the disk array subsystem to a host and an HBA, add a host group to the disk array subsystem. When adding a LUN Manager setting, it is not necessary to reboot the disk array subsystem. Execute a host boot or the disk recognition command after making a setting of LUN Manager.

- Add a LU

  When adding a LU to a disk array subsystem and assigning it to a connected host, add a mapping of the LU to the host group to which the host belongs. When adding this setting, it is not necessary to reboot the disk array subsystem. Execute a host boot or the disk recognition command after making a LUN Manager setting.

- Replace an HBA

  When replacing an HBA of a host, the setting for LUN Manager must be modified and the WWN of the HBA must be changed. If you do not make this change, the host will not be able to access the LU after the HBA is replaced.

  Each setting for LUN Manager must be documented when the configuration is created so that the previous setting can be reviewed before making a change to the setting.

- Replace a switch

  When replacing a switch, the same connections and zoning setting used before the replacement must be made for the new switch. If the setting of the port and zoning for the connected switch do not agree with each other, the host will not be able to access the LU.

  For future reference, create a diagram and record of connections between the switch and hosts, and the connections between the switch, zoning, and disk array subsystem. When the switch is replaced, you can make the same connections as before the replacement by referring to your records.

3.5 Avoiding RAID Group Conflicts

When multiple hosts are connected to a disk array subsystem and the LUs assigned to each host belong to the same RAID group, concurrent access to the same disk drive will occur and performance may decrease. LUNs in one RAID group should only be accessed by one host. To avoid a conflict, you should never have more than one host access multiple LUNs in one RAID group.

The number of RAID groups that can be created is determined by the number of mounted disk drives and the RAID level of the RAID groups to be created. If you cannot create as many RAID groups as hosts to be connected, organize the RAID groups according to the operational states of the hosts (see Figure 3.1 and Figure 3.2).

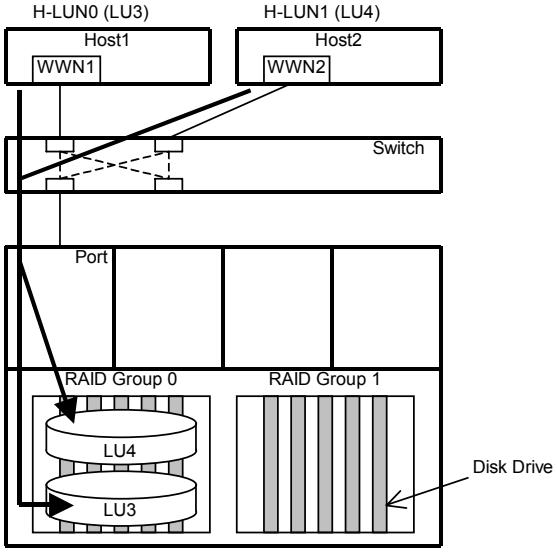


Figure 3.1 Hosts Connected to the Same RAID Group Decreases Performance

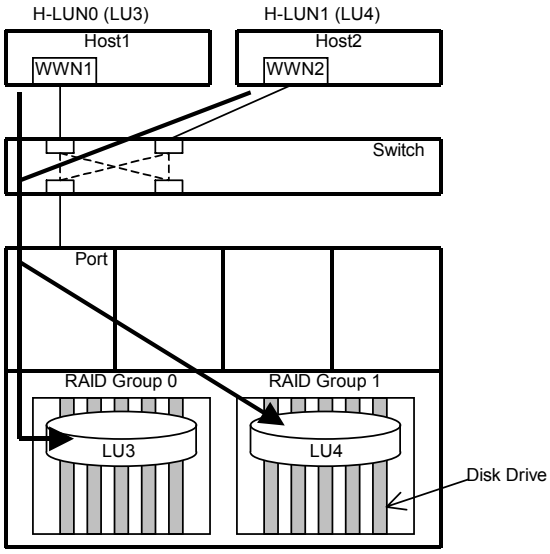


Figure 3.2 Hosts Connected to Different RAID Groups

3.6 Preventing Illegal Access to SAN

When connecting hosts to one port of the disk array subsystem using a switch, you must distinguish an accessible host for each LU.

When assigning LU3 to Host 1 and LU4 to Host 2 as shown in Figure 3.3, both hosts can access the same LU if the LU mapping is set separately.

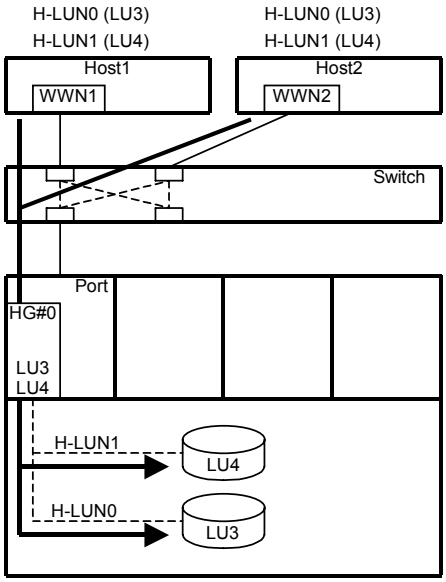


Figure 3.3 LU Mapping that does not Restrict Host Access

With LUN Manager, the host (WWN: World Wide Name) access to each LU can be distinguished even in the same port as shown in Figure 3.3.

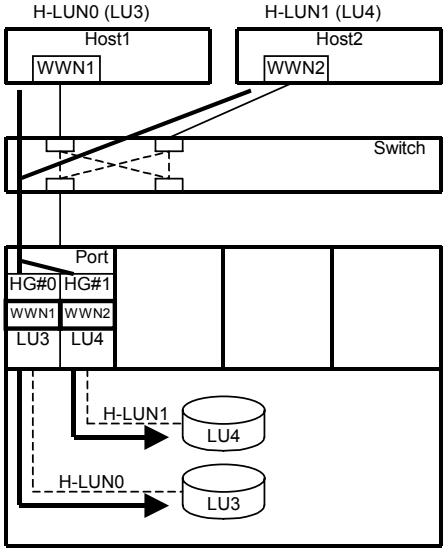


Figure 3.4 Using LUN Manager to Restrict Host Access

To prevent ports of the disk array subsystem from being affected by other hosts even when LUN Manager is used, it is recommended that zoning be set as shown in Figure 3.5.

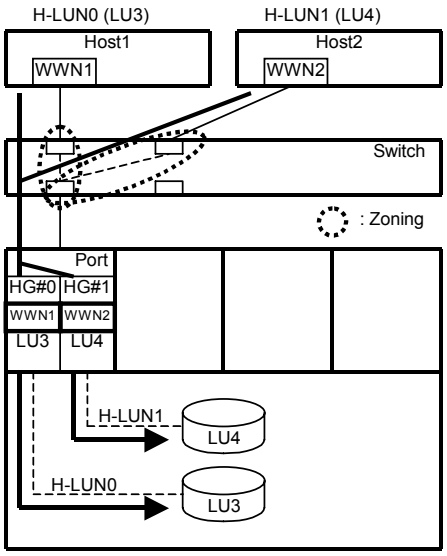


Figure 3.5 Using LUN Manager and Switch Zoning

3.7 Queue Depth Setting of SAN

A host can queue successive commands to the disk array subsystem before execution of a previous command can complete. The number of times successive commands are issued is called Queue Depth. When two or more hosts are connected to a port of a disk array subsystem, the number of queue commands for the port is increased because the host issues commands to each disk array subsystem separately.

Multiple hosts can be connected to a single port. The queue depth for each port is limited and performance drops if that limit is exceeded. You should therefore specify the queue depth so that the sum for all hosts does not exceed the value of the limit per port. The disk array subsystem reports the Queue Full status with commands received after the limit is exceeded. Since the host that has received notice of the Queue Full status stops issuing the multiplex command, a decrease in host performance may occur. To avoid such a situation, queue depth should be carefully determined when designing the system.

Notes:

- If a queue depth setting is increased, traffic on the disk array subsystem also increases. Traffic on the host and switch may also increase. This should also be taken into consideration when changing a queue depth setting.
- The formula for defining Queue Depth on the host side varies depending on the type of operating system or HBA. When determining the overall queue depth settings for hosts, consideration should be given to the port limit.

3.7.1 Increasing Queue Depth Setting and Port Sharing

Figure 3.6 shows how to determine the queue depth when a port is shared.

In this example, Host 1, Host 2, Host 3, and Host 4 are connected to a port that is given a command limit of 512 commands. In this case, the Queue Depth for the port must be specified so that the total numbers of queue depth for Hosts A, B, C, and D does not exceed *X*.

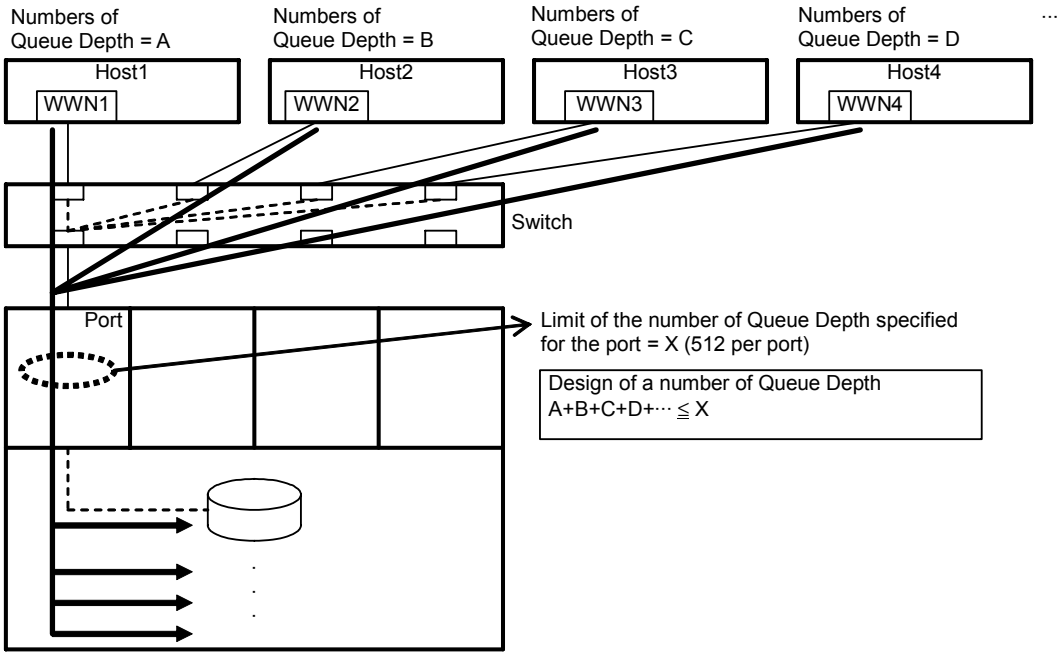


Figure 3.6 Ensuring that Queue Depth does not Exceed the Port Limit

3.7.2 Increasing Queue Depth Through Path Switching

Figure 3.7 shows how to determine queue depth when an alternative path is configured. The system shown has a configuration with an alternative path: the Host 1 and Host 2 sides are assigned to the Primary and Secondary paths, respectively.

Commands are generally issued to a LU via the Primary path on the Host 1 side. In this configuration, commands to be issued via the Primary path are moved to the Secondary path because path switching is done, and the queue depth for a port connected to a host on the Secondary path is increased. You must specify the appropriate queue depth for each host so that the number does not exceed its limit even after the path switching is done.

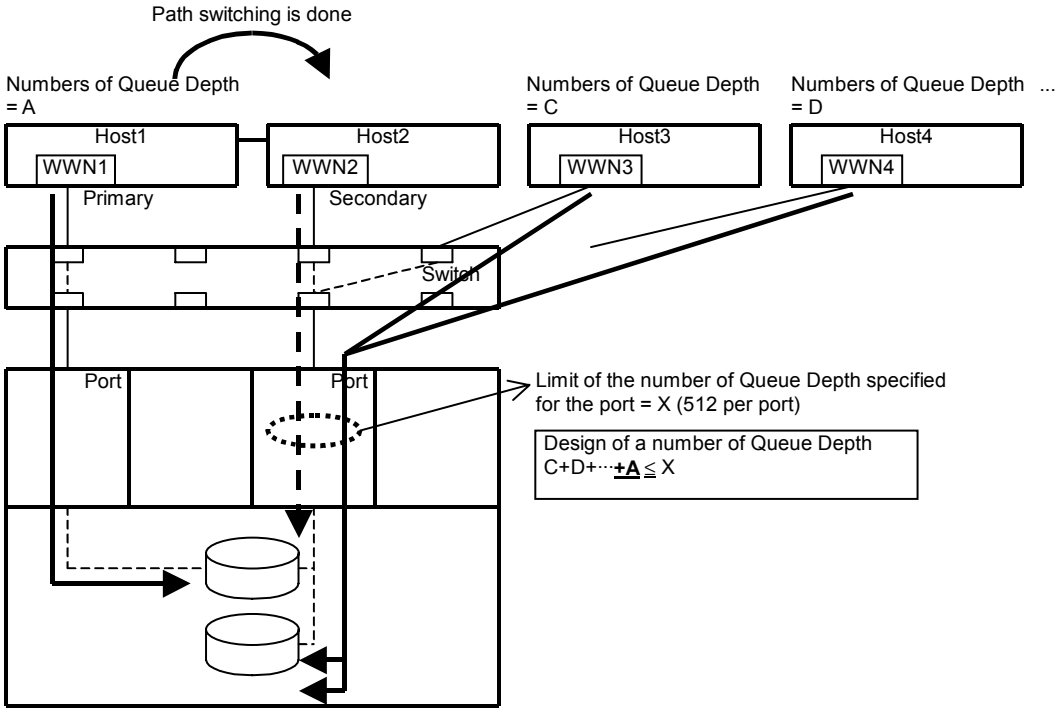


Figure 3.7 Increment of Queue Depth Generated Due to Path Switching

3.7.3 Allocation of Queue Depth According to Priority of Host Job

Figure 3.8 shows how to determine the queue depth when the priority order is given to jobs of connected hosts. To increase the priority of the host job individually, increase the Queue Depth for the host. When a Queue Depth for a certain host is increased, the port concerned must not exceed its limit. If necessary, reduce the numbers for the other hosts connected to the port.

Note: If the disk array subsystem does not have prioritized order control, you must allocate the number of host Queue Depth.

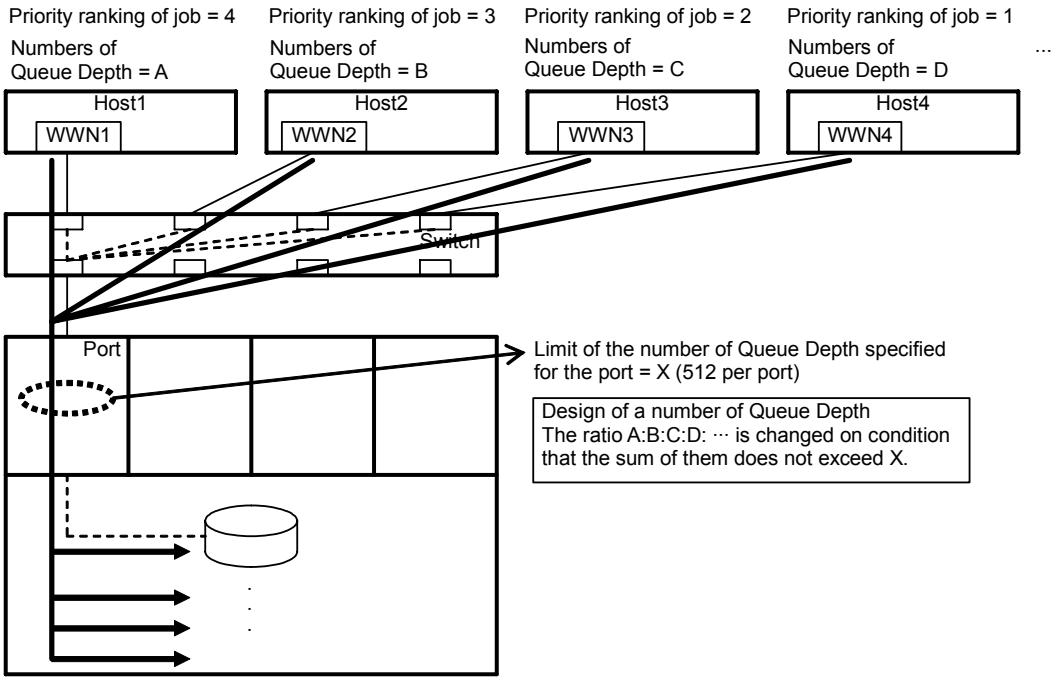


Figure 3.8 When Priority Order is Given to Host Jobs

Chapter 4 Fibre Channel and LUN Manager Software Procedures

This chapter explains how to execute the LUN Manager feature using the GUI version of Navigator. For CLI installation, see Appendix A.

In this chapter:

- Adding a Host Group (section 4.1)
- Setting a Host Group Option (section 4.2)
- Setting Logical Units (section 4.3)
- Adding a WWN (section 4.4)
- Changing a Host Group Name (section 4.5)
- Deleting a Host Group (section 4.6)
- Initializing Host Group 0 (section 4.7)
- Changing a WWN (section 4.8)
- Deleting a WWN (section 4.9)
- Deleting a Logged-In WWN (section 4.10)

4.1 Adding a Host Group

To create a host group for each Port, you must:

- Set the host group Security to enable for each port
- Create a host group

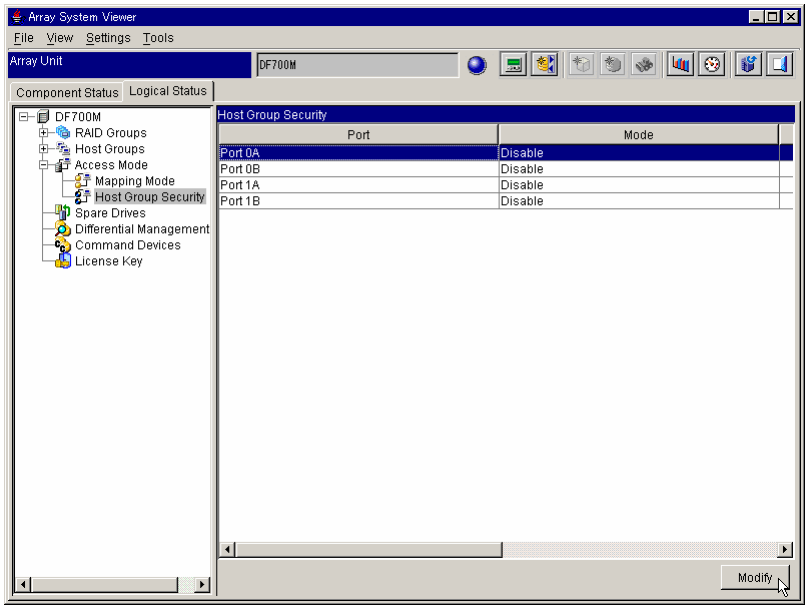
4.1.1 Setting the Host Group Security

The host group Security default setting is **disable** for each port.

To Enable or Disable host group Security for each port:

1. Start Navigator and change the operation mode to **Management Mode**.
2. Register the subsystem in which you will enable or disable host group Security, and connect to the subsystem.

   The **Array System Viewer** window appears and displays the connected subsystem.
3. Select the **Logical Status** tab.
4. Select **host group Security** icon in **Access Mode**.
5. Select the port that you want to set the access mode for enable/disable.
6. Click **Modify**.

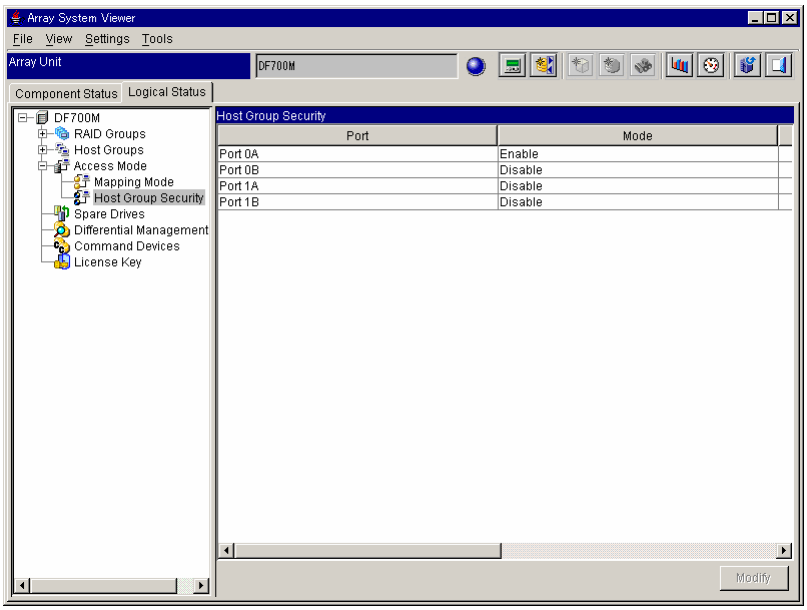


7. Select the **Enable** or **Disable** option and click **OK**.

8. Observe any messages that appear and click **OK** to continue.

   If the host group Security has been set to enable, **Detected WWN (Logined WWN)** is displayed.

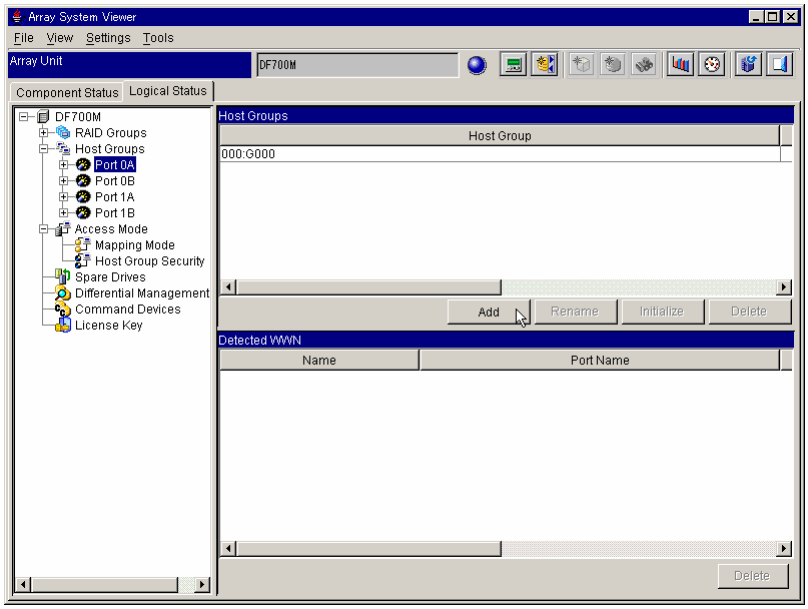
   The WWN of the HBA connected to the selected port is displayed in the **Detected WWN (Logined WWN)** field.



4.1.2 Adding a Host Group

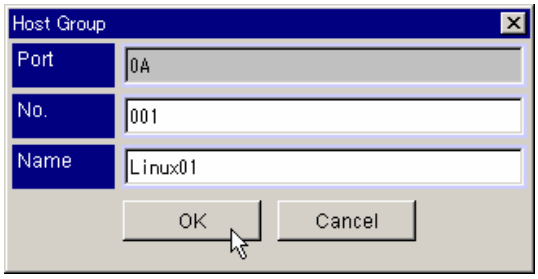
To create host groups for each Port:

1. In the **Logical Status** tab, under host groups, select a port.



2. Click **Add** in the main window.

   The **Host Group** dialog box appears.



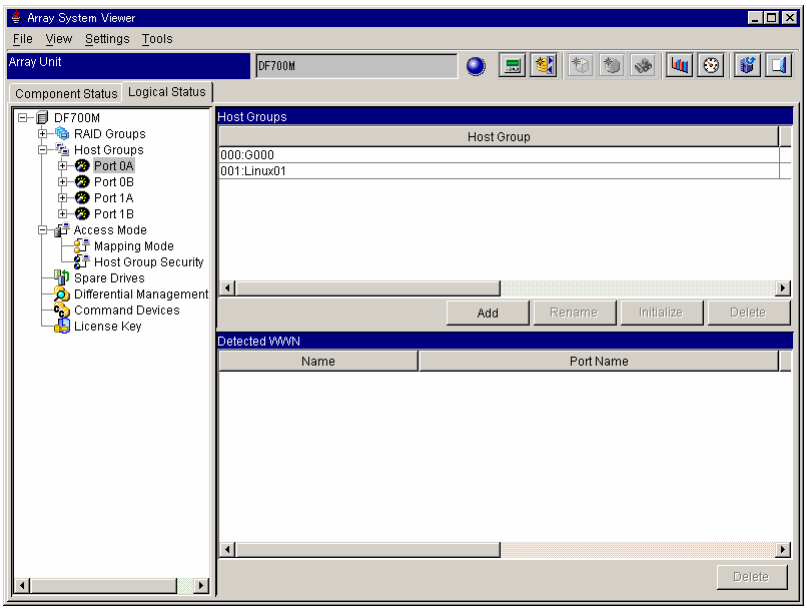
3. Enter the following and click **OK:**
   - **No.**

     Enter a numeral from 1 through 127.
   - **Name**

     Enter the name of the host group with 16 or less alphanumeric characters. (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘

     Spaces at the top or end are ignored. The same name cannot be used in the same port.
4. Observe any messages that appear and click **OK** to continue.

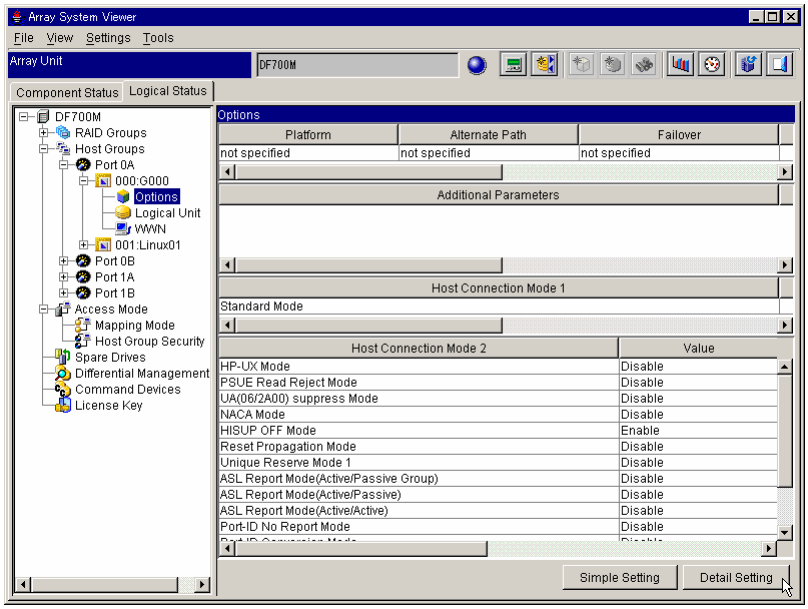
   The **Array System Viewer** window shows the host group information.



4.2 Setting a Host Group Option

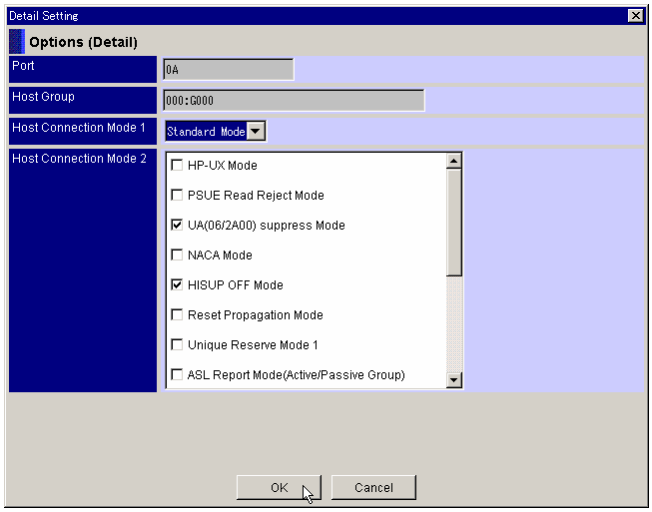
To set a host group Option for each host group:

1. Select an **Options** icon in the host group and click **Detail Setting**.



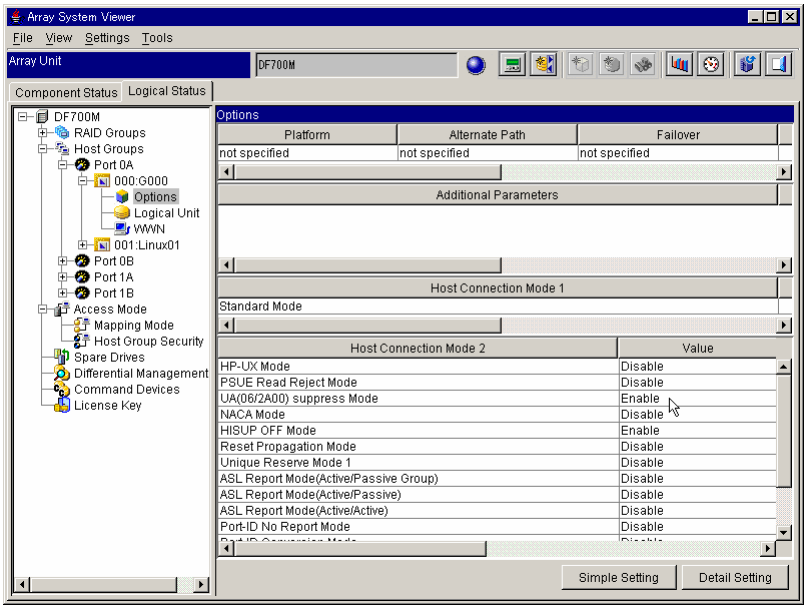
The **Option Property** screen is displayed.

2. Specify **Host Connection Mode 1** and **Host Connection Mode 2**, and click **OK**.



3. Observe any messages that appear and click **OK** to continue.

   The **Array System Viewer** window shows the updated information.

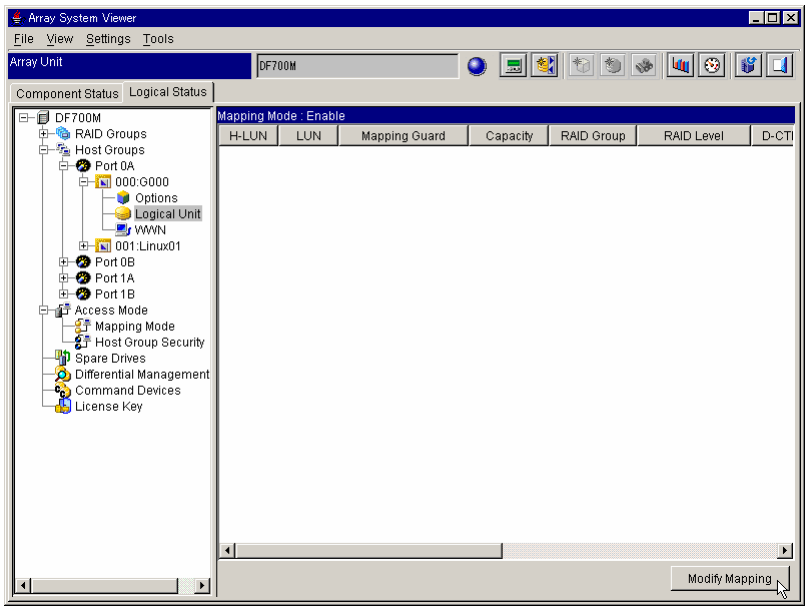


4.3 Setting Logical Units

To set Logical Units to each host group:

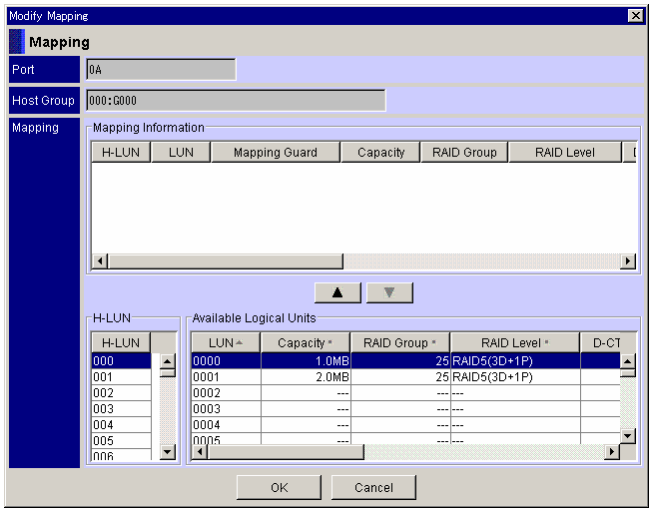
Note: This process is called LU Mapping.

1. Select a **Logical Unit** icon in the host group and then click **Modify Mapping**.



The **Mapping Property** is displayed.

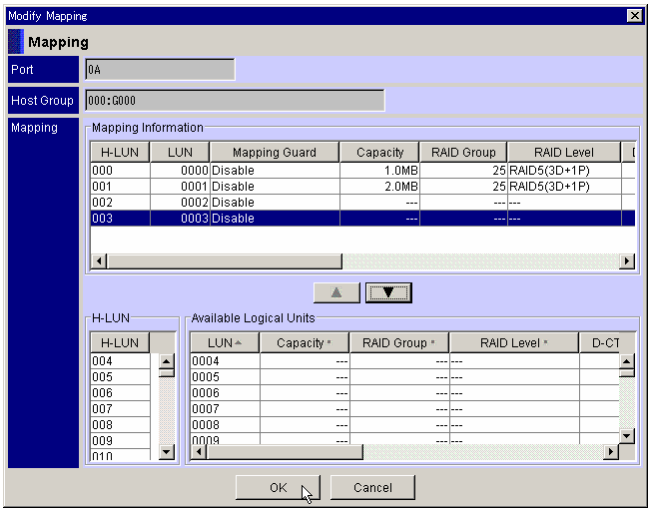
To set LU mapping, you must set **Enable** to **Mapping Mode**.



2. Select an **H-LUN** to be added. Select **LUN**, and click the ▲ button.

   The added contents are displayed in **Mapping Information** list.

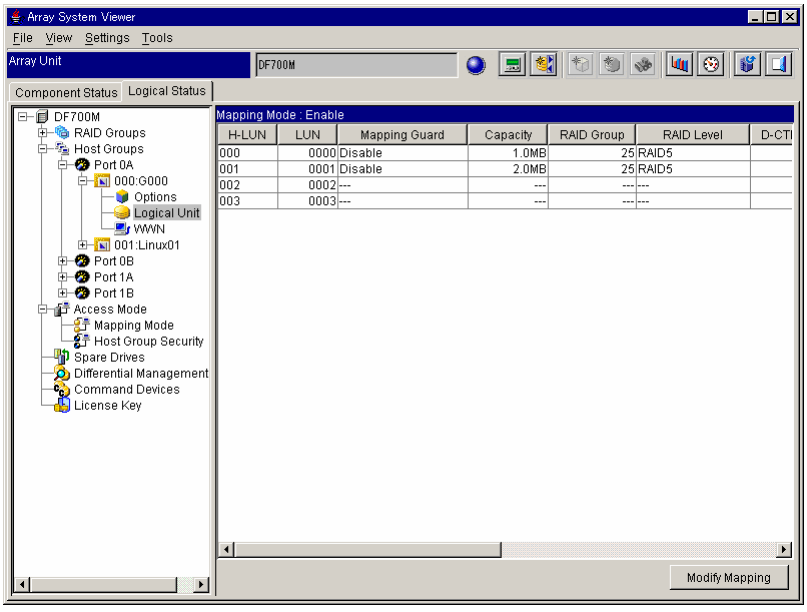
   To delete, click the line to be deleted in the **Mapping Information** list and click the ▼ button. The deleted contents disappears from the display of **Mapping Information** list.



3. Click **OK**.

4. Observe any messages that appear and click **OK** to continue.

   The information that has been set is displayed.



4.4 Adding a WWN

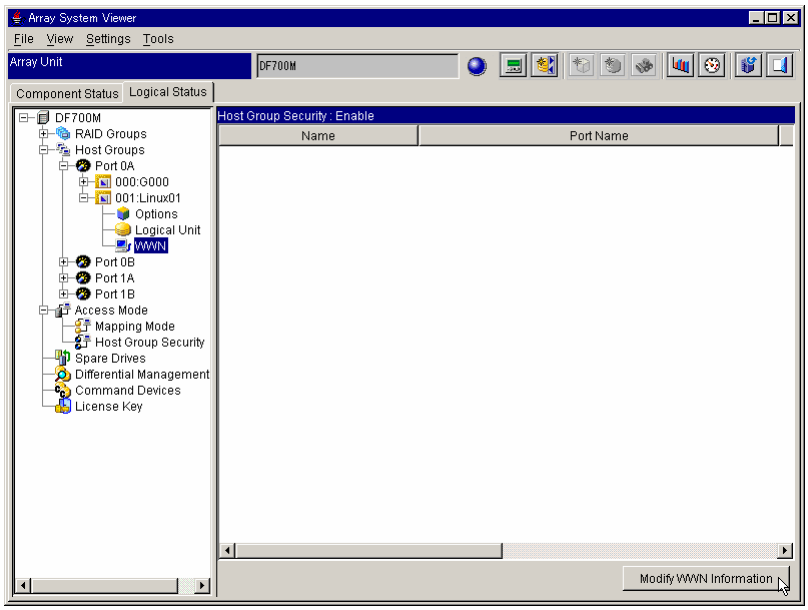
WWNs of an HBA are set to each host group. When a port is connected to a host, WWNs of HBAs are listed in **Logined WWN** and can be selected and added to the host group. WWN is used for identifying hosts.

For information about obtaining WWN information, see Appendix B.

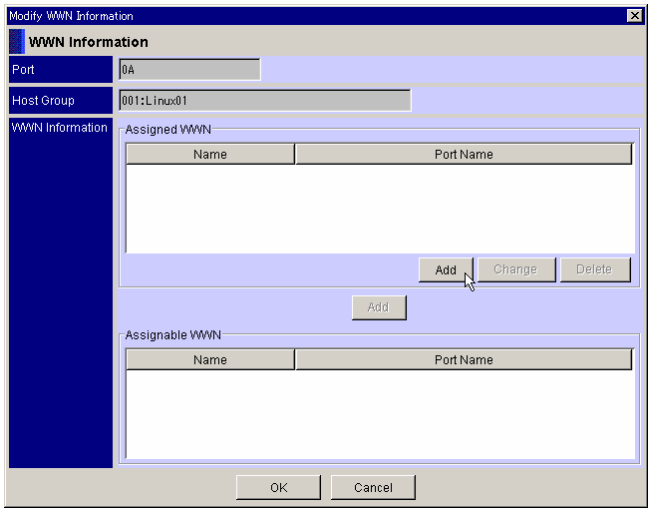
4.4.1 Adding a WWN

To add a WWN by entry:

1. Select a **WWN** icon in the host group and then click **Modify WWN Information**.

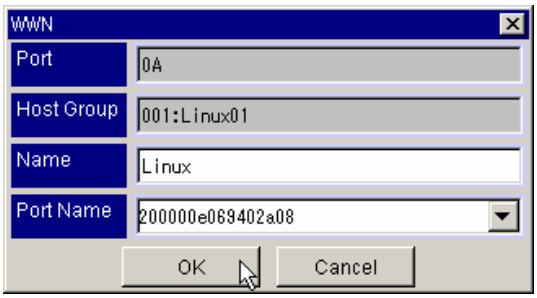


The **WWN Information Property** screen is displayed.



2. In the **WWN Information Property** screen, click **Add**.

   The **WWN** dialog box is displayed.



3. Enter the following and click **OK**:

   – **Name** (optional)

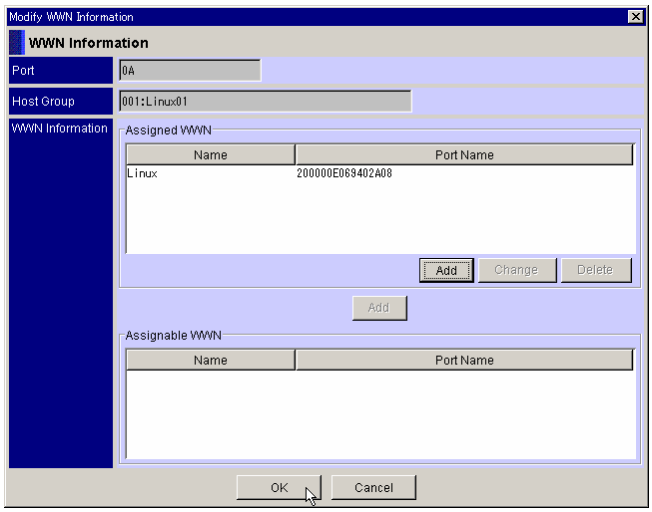
     Enter the name of the host group with 16 or less alphanumeric characters (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

     Spaces at the top or end are ignored. An identical name cannot be used in an identical Port.

   – **Port Name**

     Used to identify the host. Enter the Port Name using sixteen hexadecimal numerals.

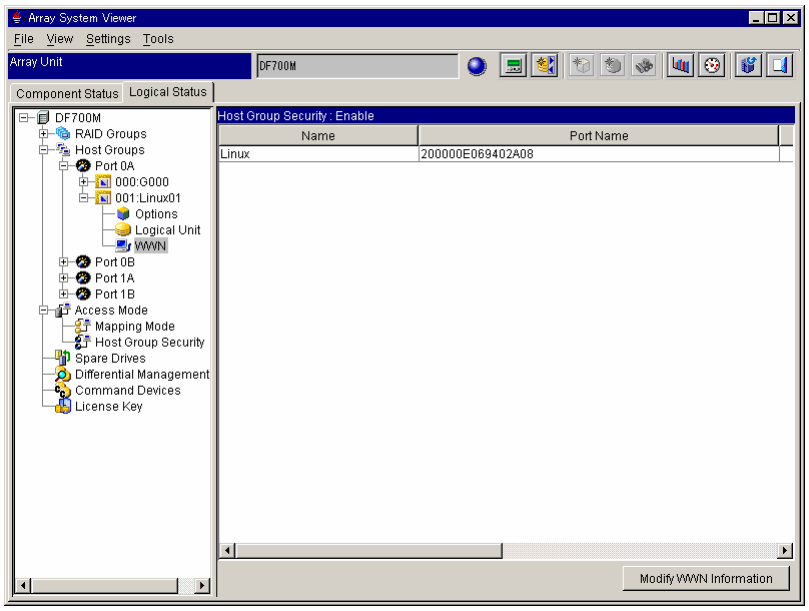
The **WWN Information Property** window shows the updated information.



Note: Up to 128 WWNs can be assigned for a Port. The total number of WWNs that have been assigned (**Assigned WWN**) and the number of WWNs that can be assigned (**Assignable WWN**) is 128 per port. When the number of WWNs assigned to a port exceeds 128 and further input is not possible, delete a **Logined WWN** that is not assigned to a host group.

4. In the **WWN Information Property** screen, click **OK**.
5. The confirmation message is displayed. Click **OK**.

   The **Array System Viewer** window shows the updated information.



4.4.2 Selecting and Adding an Assignable WWN

To select and add an assignable WWN:

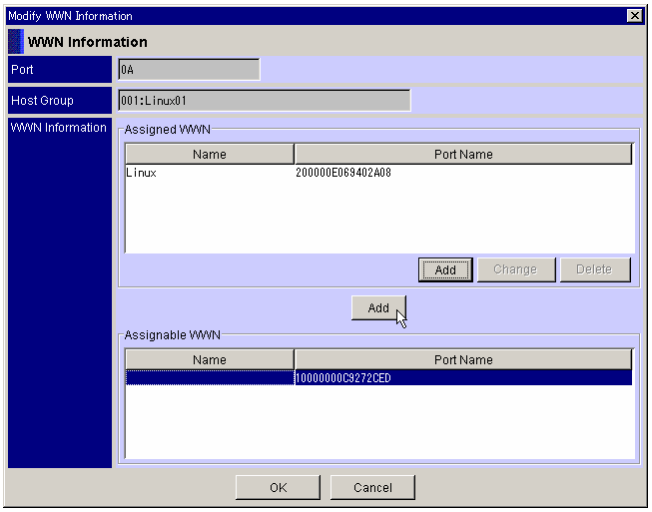
1. Select a **WWN** icon in a host group, and then click **Modify WWN Information**.

   The WWN Information Property screen is displayed.

   The WWNs of HBAs being connected to a port are displayed in **Assignable WWN**. When a WWN of the HBA being connected to the port is already assigned to another host group in the same port, the WWN is not displayed in **Assignable WWN**. When the WWN is deleted from the host group to which the WWN has been assigned, the WWN is displayed in **Assignable WWN**.

2. Select WWN Information in the **Assignable WWN** list and click **Add**.

   The WWN moves from the **Assignable WWN** list to the **Assigned WWN** list.



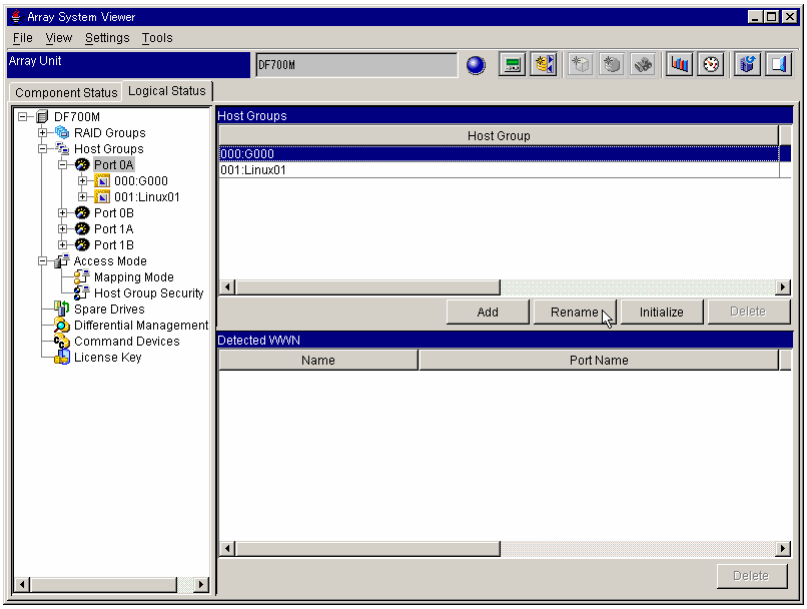
3. In the **WWN Information Property** screen, click **OK**.
4. The confirmation message is displayed. Click **OK**.

Note: The WWN may not be listed in the **Assignable WWN** list even though the port is connected to a host. When the WWN to be assigned to a host group is not listed in the **Assignable WWN** list, input and add it.

4.5 Changing a Host Group Name

To change a host group name:

1. Select the **host group** requiring the host group Name change and click **Rename**.

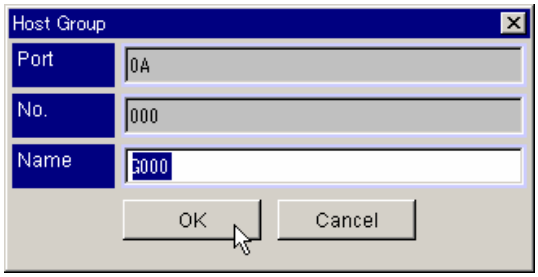


2. Enter a new name for the host group.

   – **Name**

   Enter the name of the host group with 16 or less alphanumeric characters (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

   Spaces at the top or end are ignored. An identical name cannot be used in an identical Port.



3. Click **OK** to confirm the change.

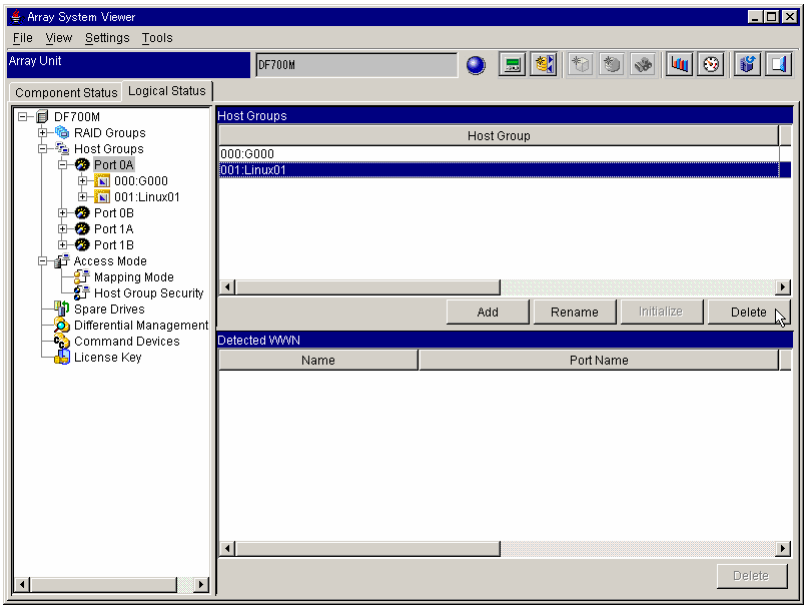
4.6 Deleting a Host Group

Note: Host Group 0 cannot be deleted. When deleting all the WWNs and all LUs in Host Group 0, you must initialize Host Group 0 (see section 4.7).

To delete a host group:

1. Select the **host group** to be deleted, and click **Delete**.

   Observe any warnings that appear, and click **OK** to continue.



4.7 Initializing Host Group 0

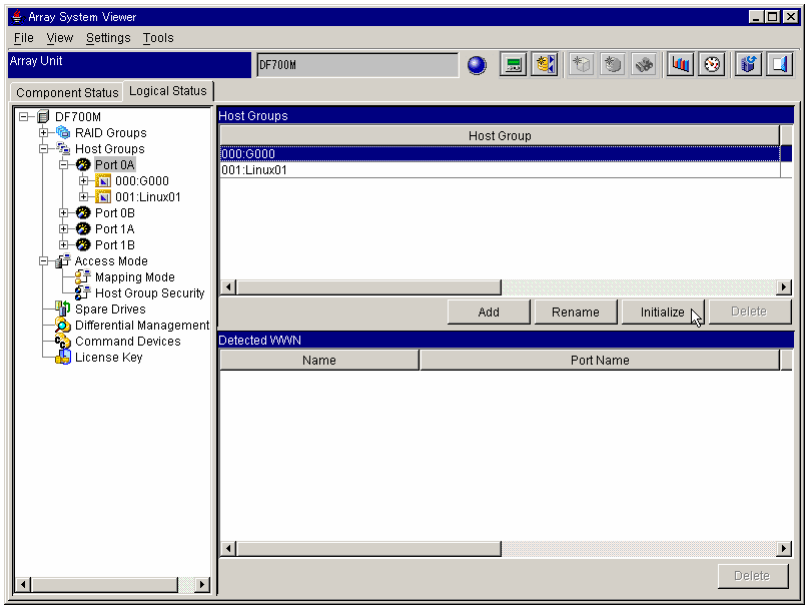
Host Group 0 can be reset to the default state.

When Host Group 0 is reset to the default state, WWNs that belong to Host Group 0 are deleted and the settings of the Logical Units that belong to Host Group 0 are also deleted. The host group Option of Host Group 0 is reset to the default state and the host group Name is reset to G000.

To initialize Host Group 0:

1. Select Host Group **0** to be initialized, and click **Initialize**.

   Observe any warnings that appear, and click **OK** to continue.



4.8 Changing a WWN

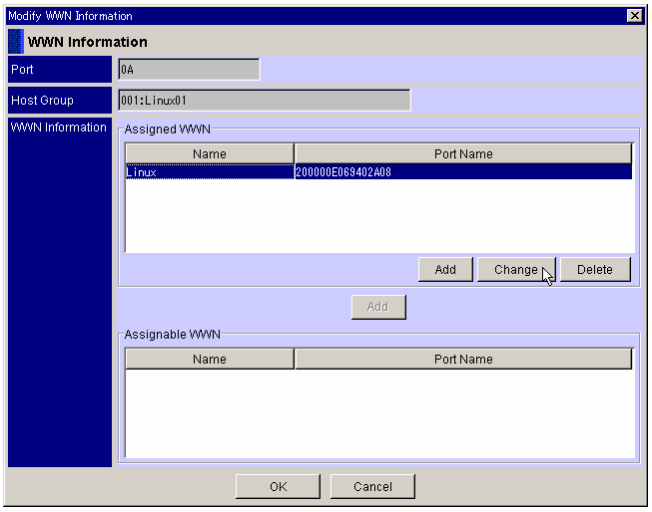
To change a WWN:

1. Select a **WWN** icon in a host group, and click **Modify WWN Information**.

   The **WWN Information Property** window is displayed.

2. Select a **Name** to be changed and click **Change**.

   The **WWN** dialog box is displayed.



3. Enter the name information and click **OK**.

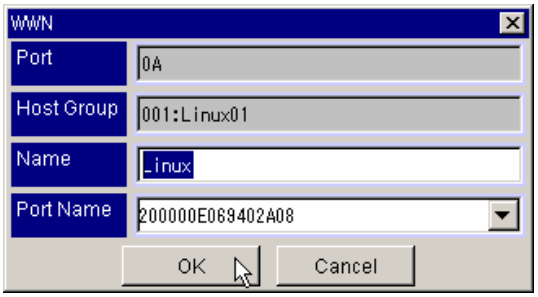
   – **Name**

   Enter the name of the host group with 16 or less alphanumeric characters (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

   Spaces at the top or end are ignored. The same name cannot be used in the same port.

   – **Port Name**

   Enter the port name using sixteen hexadecimal numerals.



   The information that has been entered is displayed on **WWN Information Property**.

4. Click **OK** on **WWN Information Property**.

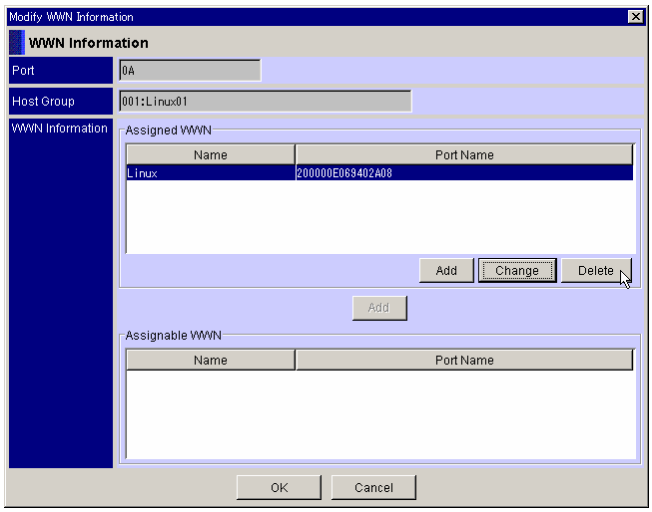
4.9 Deleting a WWN

To delete a WWN:

1. Select a **WWN** icon in a host group and click **Modify WWN Information**.

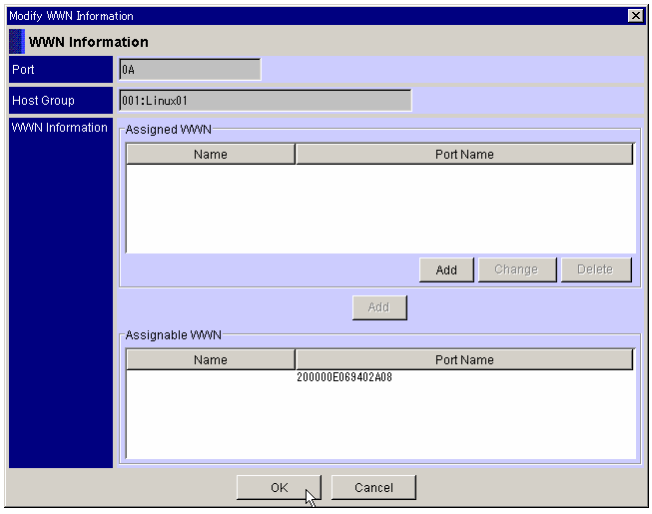
   WWN Information Property is displayed.

2. Select the **Name** to be deleted in **Assigned WWN** list and click **Delete**.



If the WWN to be deleted is an entered WWN and has not been connected to the host after the entry, the WWN to be deleted is deleted from the **Assigned WWN** list.

When the WWN to be deleted is a Logined WWN, or it has been connected to the host of the WWN after the entry, the WWN to be deleted is moved from the **Assigned WWN** list to the **Assignable WWN** list.

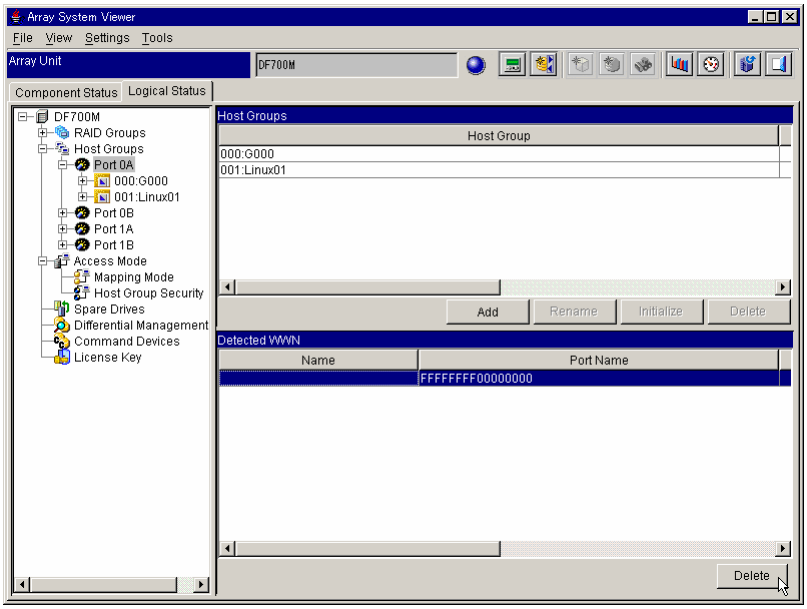


3. In the **WWN Information Property** window, click **OK**.
4. The confirmation message is displayed. Click **OK**.

4.10 Deleting a Logged-In WWN

To delete a logged-in (Logined) WWN:

1. In **Port**, select a **Logined WWN** to be deleted, and click **Delete Logined WWN**.



When a WWN that has been already assigned to a host group is deleted from the **Logined WWN** list, the WWN is deleted from the list but the assignment to the host group remains.

2. The confirmation message is displayed. Click **OK**.

Chapter 5 iSCSI Networks and LUN Manager: Overview

In this chapter:

- Overview of LUN Manager for iSCSI (section 5.1)
- The iSCSI Protocol (section 5.2)
- Network Configuration for iSCSI (section 5.3)
- Overview of Setting Up Disk Subsystems on an iSCSI Network (see section 5.4)
- Requirements and Specifications (section 5.5)

5.1 Overview of LUN Manager for iSCSI

LUN Manager, which is operated through Storage Navigator Modular software, manages access paths among hosts and logical units (LUs) for each port in your disk subsystem.

LUN Manager has the following features:

- Connecting multiple hosts to a disk subsystem port

  With LUN Manager, you can connect more than one host to a port on your disk subsystem. On a disk subsystem with two ports, port A could connect to a Windows host and Solaris host, and port B could connect to another Windows host, an AIX host, and an HP-UX host.

  When setting up host connections in LUN Manager, for each host you specify the settings for Host Connection Mode, LU, and iSCSI Name. Each host can access a logical unit simulating a dedicated port to the host even if that host shares the port with other hosts.

- Mapping logical units (LUs) to hosts

  With LUN Manager, you can map or assign your disk subsystem LUs to the hosts on your network. You have complete flexibility to share or restrict LU access among the hosts.

- Network security

  With LUN Manager, you can enable or disable CHAP (Challenge Handshake Authentication Protocol), a security protocol that requires users to enter a password for access.

Figure 5.1 shows how multiple hosts on an iSCSI network can share ports on a disk subsystem. Note that the logical units are grouped into targets. Each host is associated with one target that can contain one or multiple logical units. Hosts can share targets so that the hosts have access to the same logical units.

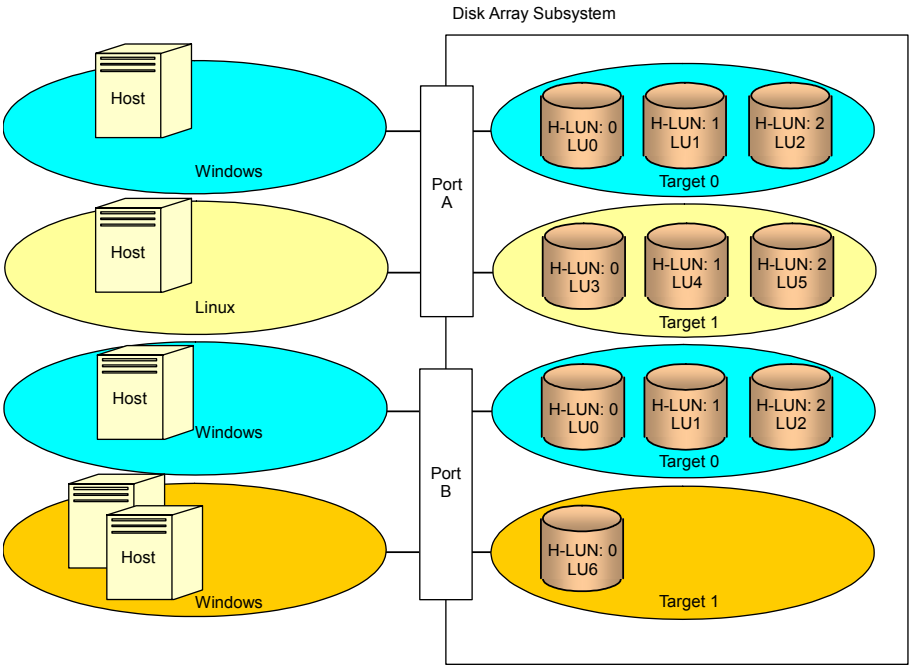


Figure 5.1 Targets (groups of logical units) are assigned to hosts

When setting up your disk subsystem with LUN Manager, you set up host access to LUs through targets:

1. Select a port and create one or more targets for the port.
2. Map LUs to each target. You can map the same LUs to more than one target. For example, Target 0: LU0, LU1, LU2, LU3; Target 1: LU0, LU1, LU4, LU5.
3. Assign one or more hosts to each target. (To assign a host to a target, select the initiator of the host bus adaptor and add it to the target.) Once you assign a host to a target, the host can access the LUs on that target. When you assign hosts to the same target, the hosts have access to the same LUs. When you assign hosts to different targets, the hosts may or may not share access to LUs, depending on whether the same LUs have been mapped to different targets.

5.2 The iSCSI Protocol

iSCSI (Internet SCSI) is a protocol for sending and receiving a SCSI command via an IP network. iSCSI transfers data in block units.

An IP-SAN that uses an existing Ethernet can be constructed by using iSCSI.

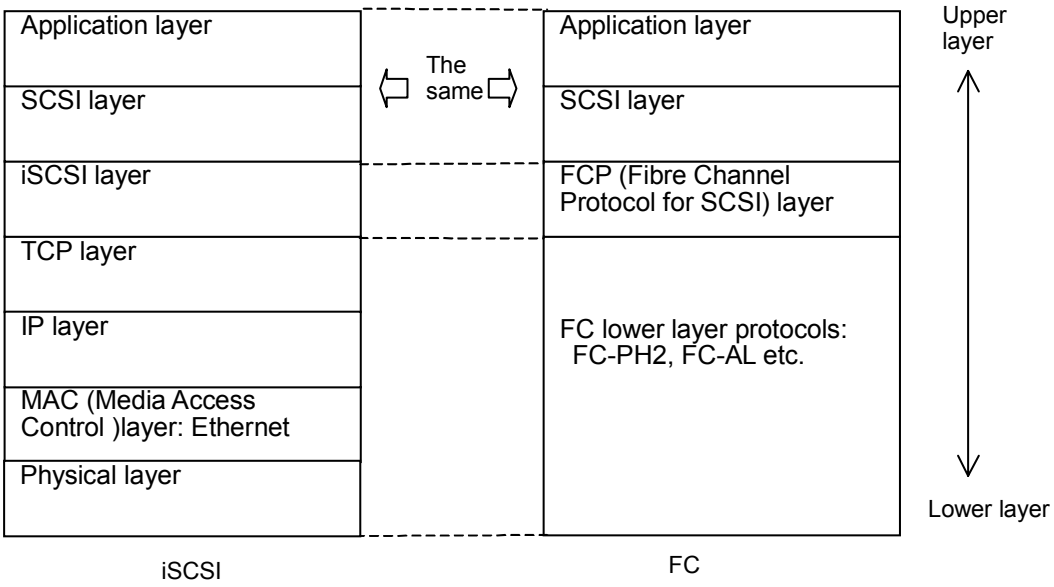


Figure 5.2 iSCSI Protocol Stack

5.3 Network Configuration for iSCSI

iSCSI makes it possible to construct an IP-SAN by connecting many hosts and disk arrays at a low cost. However, iSCSI greatly increases the I/O workload of the network and the disk array. When using iSCSI, it is very important that you configure the network so that the workload among the network, port, controller, and disk drive is properly distributed.

Even though the LAN switches and NICs are the same, there are some important differences when you use iSCSI, particularly regarding the LAN connection. You need to pay particular attention to the following:

- iSCSI consumes almost all of the available Ethernet bandwidth, unlike a conventional LAN connection. This can significantly degrade the performance of both the iSCSI traffic and the LAN. Therefore, it is very important that you separate the iSCSI IP-SAN and the office LAN.
- Host I/O load will affect the iSCSI response time. In general, the greater the I/O traffic, the lower the iSCSI performance.
- If you need high performance and high reliability, fibre-channel is recommended.
- You need to have a failover path between host and AMS/WMS iSCSI, so that you can update the micro-program without stopping the system.

5.4 Overview of Setting Up Disk Subsystems on an iSCSI Network

To understand how to set up the disk subsystem on your iSCSI network, read Chapter 6, iSCSI Network Configuration. Also, refer to the user guide for your disk subsystem.

To Set Up and Manage iSCSI Network Storage with LUN Manager:

1. Use Storage Navigator Modular to set up LUs (logical units) and RAID groups on the disk subsystem. Refer to the user guide for your version of Storage Navigator Modular:
   - *Storage Navigator Modular for Web User's Guide* (MK-95DF719)
   - *Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711)
   - *Storage Navigator Modular Command Line Interface (CLI) User's Guide* (MK-95DF712)

   Important: To prevent unauthorized access to the disk subsystem during setup, perform steps 1 and 2 with the disk subsystem ***not*** connected to the network.
2. Use LUN Manager to set up the following on the disk subsystem:
   - For each subsystem port that will connect to the network, add one or more targets and set up target options. See sections 7.1, Adding a Target and 7.2, Setting a Target Option.
   - Map the LUs to targets. See section 7.3, Mapping Logical Units to Targets.
   - Register CHAP users that are authorized to access the logical units. See section 7.10, CHAP User.
   - Keep a record of the iSCSI names and related settings to simplify making any changes later. See section 6.5,.
3. Physically connect the disk subsystem to the network.
4. Connect hosts to their targets on the disk subsystem by using the Initiator function in LUN Manager to select the host's initiator driver or the initiator iSCSI name of the HBA. See section 7.4, Adding an Initiator.
5. As a security measure, use LUN Manager in assignment mode to determine input/output paths between hosts and LUs. The input/output path is a route through which access from the host is permitted.
   - When connecting multiple servers to a subsystem port, verify and set the queue depth. If additional commands from the additional servers exceed the port's limit, increase the queue depth setting. See section 5.5, Requirements and Specifications and section 6.7, Queue Depth Setting
6. Test host connections to the LUs on the disk subsystem. See section 6.8, Testing the Host Connection with Ping.
7. Perform maintenance as needed: host and HBA addition, LU addition, HBA replacement, and switch replacement. See section 6.5, Adding and Replacing Equipment.

5.5 Requirements and Specifications

Table 5.1 Requirements and Specifications for iSCSI

Item	Specifications
Target	• Up to 128 (255: the micro program version 0750/A or later) Targets can be set for each Port. • Target 0 (zero) is required.
Setting/Deleting a Target	• Targets 1 through 127 (1 through 254: the micro program version 0750/A or later) can be set or deleted. • Target 0 (zero) cannot be deleted. To delete initiator iSCSI Name, options, and LU Mapping of Target 0 (zero), you must first initialize Target 0.
Target alias	• A name is assigned to a target alias upon creation. This target alias can be changed.
iSCSI Name	• Used for identifying initiators and targets. iSCSI Name needs to have a World Wide Unique value. • iqn and eui are supported. • iSCSI Name of a target is automatically set as a World Wide Unique when initializing the target. The value can be changed by purchasing the LUN Manager, however the customer needs to assure the World Wide Uniqueness of the new iSCSI Name. ***Note***
Initiator iSCSI Name	• Up to 128 (255: the micro program version 0750/A or later) initiators driver or initiator iSCSI name of HBAs, may be set for one Target per port. • The same Initiator iSCSI Name can also be set to the other Target on the same port. • The Initiator iSCSI Name to be set to the Target can also be selected from the initiator drivers connected to the port and the detected Initiators of the HBA.
Target iSCSI Name	• The Target iSCSI Name can be set for each Target. • The same Target iSCSI Name cannot be set to another Target on the same port.
Initiator Name	• An Initiator Name can be assigned to an initiator iSCSI Name allocated to the Target. An Initiator Name can be deleted. • An Initiator Name assigned to an initiator iSCSI Name is valid until the initiator iSCSI Name is deleted.
Discovery	• SendTargets and iSNS are supported.
Authorization of login	• None and CHAP are supported.
User Authorization Information	• User authentication may be set for up to 256 (512: the micro program version 0750/A or later) ports and be assigned to a target. • None and CHAP are supported. • The user authentication information can be set to the target that has been set by the LUN Manager. • The same user authentication information can also be set to other targets on the same port.
Host Connection Mode	• The Host Connection Mode of the target may be changed.
LU Mapping	• LU Mapping can be set to the target. • Up to 256 LU Mappings can be set for a target. Up to 256X128 (256X255: the micro program version 0750/A or later) LU Mappings can be set for a Port.

Item	Specifications
Enable/Disable Settings for each Port	• When LUN Manager is disabled, previously set LUN Manager information is saved and is available when LUN Manager is enabled again.
Online setting	• When adding, modifying, or deleting LUN Manager settings, it is not necessary to reboot the disk array subsystem.
Making Settings	Storage Navigator Modular (Version 3.00 or later) is required.
Microcode	Version 0730/A or later is required.
Use of LUN Manager together with other optional functions	TrueCopy remote replication cannot be used.

Note: If the new iSCSI Name is not World Wide Unique and overlapped to the other one as a result, the communication will not be guaranteed.

Table 5.2 Combinations of OS and HBA for iSCSI

OS	Software Initiator/HBA	Remarks
Windows® XP	Microsoft® iSCSI Software initiator + NIC	
Windows® Server™ 2003	Microsoft® iSCSI Software initiator + NIC Qlogic® HBA	
Windows® 2000	Microsoft® iSCSI Software initiator + NIC Qlogic® HBA	
Linux®	SourceForge iSCSI Software initiator + NIC Qlogic® HBA	

Chapter 6 iSCSI Network Configuration

In this chapter:

- Configuration Examples (section 6.1)
- Configuration Issues (section 6.2)
- Network Connections: Ports, When to Use Switches, Settings (section 6.3)
- Assigning Targets and LUs to Hosts (section 6.4)
- Adding and Replacing Equipment (section 6.5)
- Preventing Illegal Access (section 6.6)
- Queue Depth Setting (section 6.7)
- Testing the Host Connection with Ping (section 6.8)

6.1 Configuration Examples

The subsystem is connected to a host with an Ethernet cable (category 6). The end of the cable on the host side is connected to an iSCSI HBA or Network Interface Card (NIC). The end of the cable on the subsystem side is connected to a port of the disk array subsystem.

Direct Attached and the Network Switch (Network Attached) are supported connection methods, and an IP-SAN connection using an L2 Switch/L3 switch is also supported.

6.1.1 Direct Attached Connection

Figure 6.1 illustrates a Direct Attached Connection.

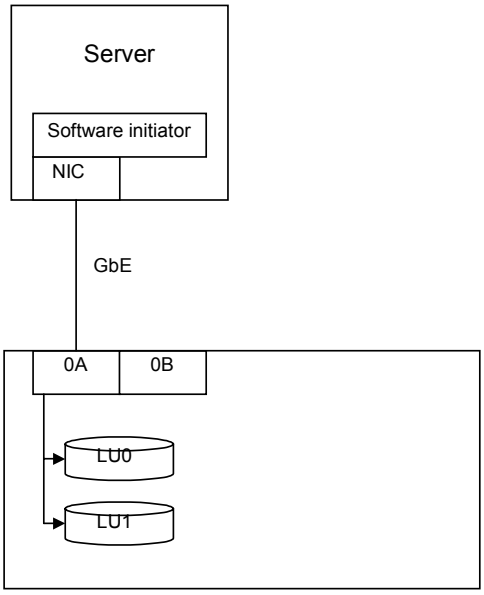


Figure 6.1 Direct Attached-1 for iSCSI

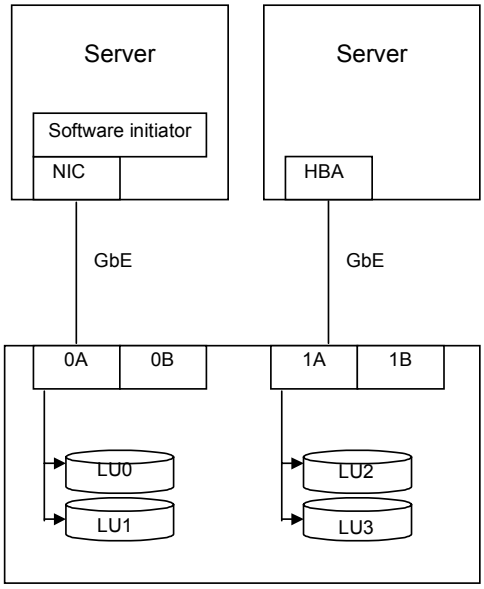


Figure 6.2 Direct Attached-2 for iSCSI

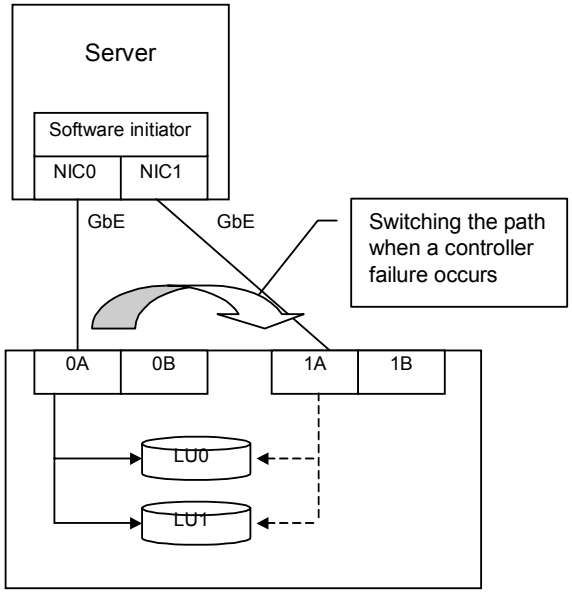


Figure 6.3 Direct Attached-3 for iSCSI

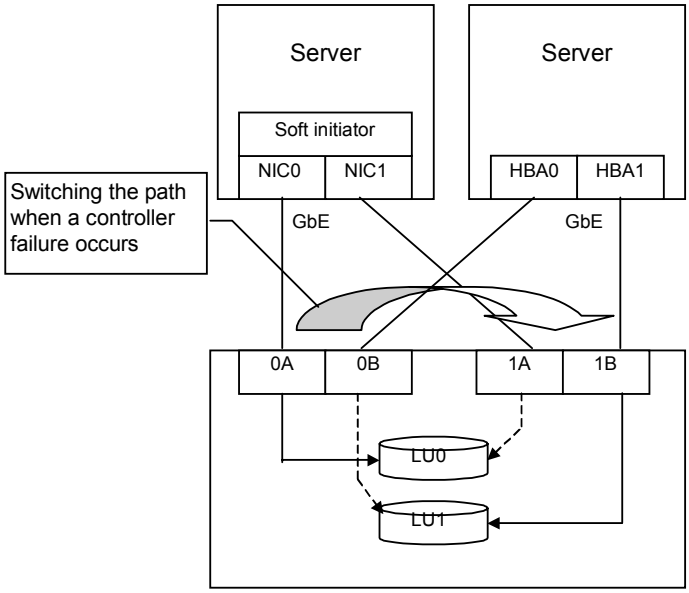


Figure 6.4 Direct Attached-4 for iSCSI

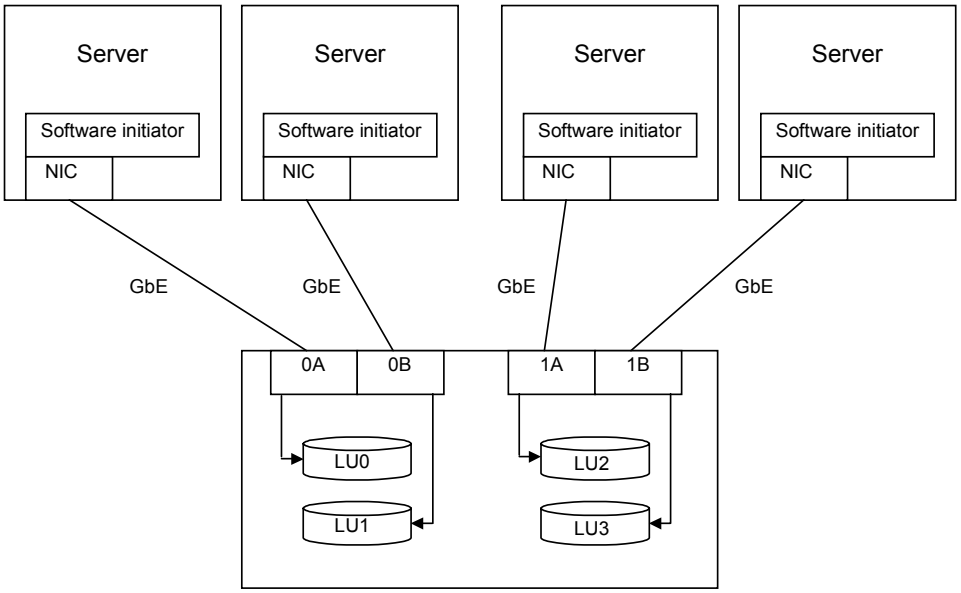


Figure 6.5 Direct Attached-5 for iSCSI

6.1.2 Network Attached Connection

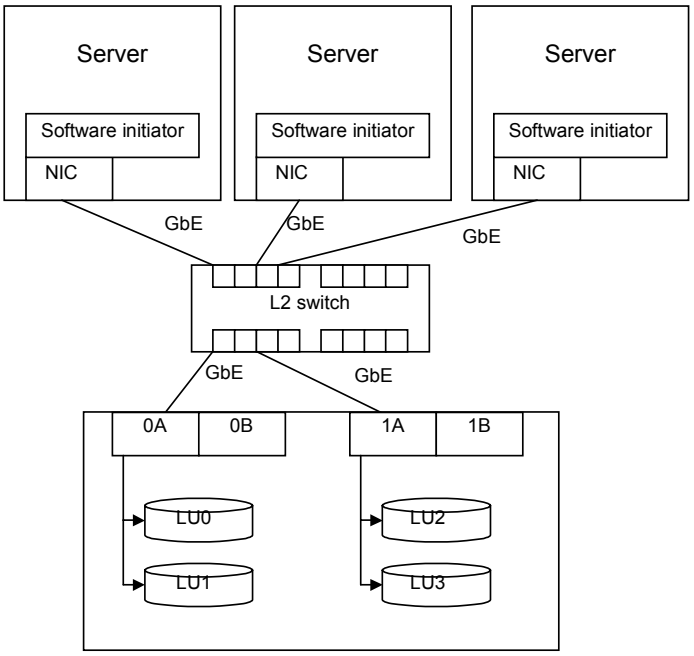


Figure 6.6 Switch Connection-1 for iSCSI

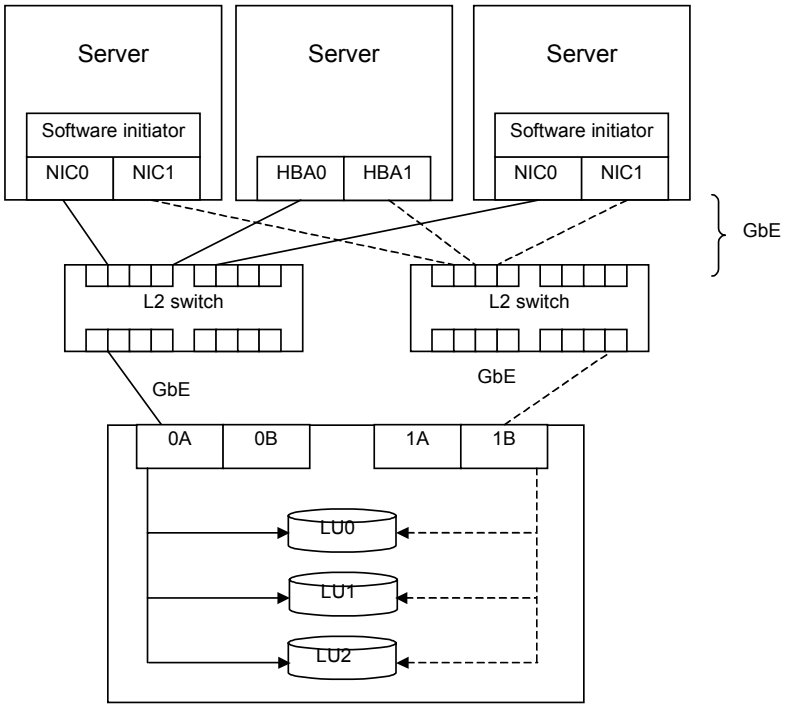


Figure 6.7 Switch Connection-2 for iSCSI

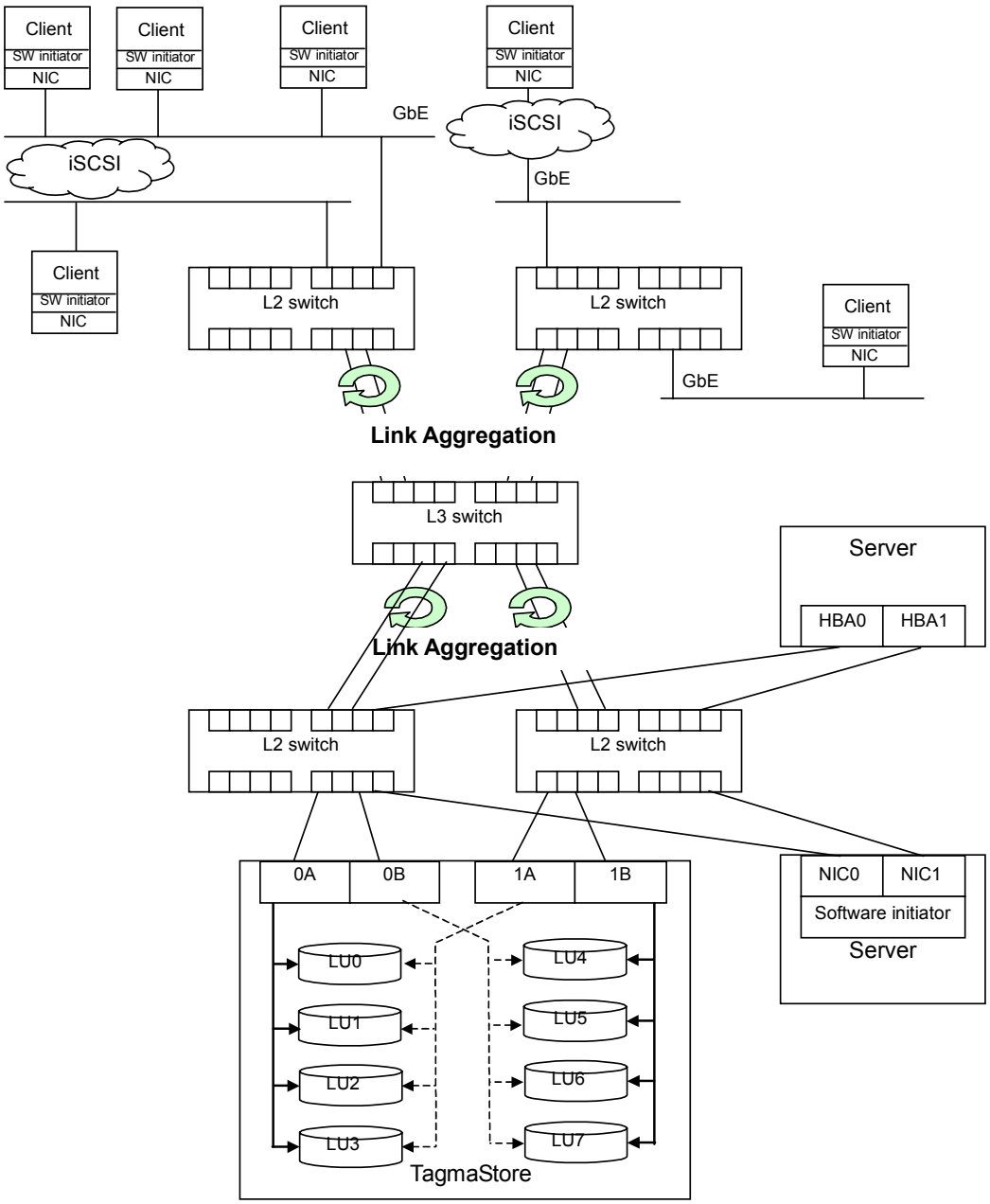


Figure 6.8 Switch Connection-3 for iSCSI

6.2 Configuration Issues

Before configuring a disk subsystem to your iSCSI network, consider the following configuration issues.

6.2.1 Network Boot Disk is Not Supported

Do not use an AMS/WMS disk subsystem as a Netboot device. It does not support operation as a network boot disk.

6.2.2 Subsystem Reboot Not Required with LUN Manager Changes

With LUN Manager, you can add, modify, or delete a target during system operation. For example, if an additional disk is installed or an additional host is connected, an additional target may still be created. If removing an existing host, the target that is connected to the host is deleted first and then the host is removed.

After adding, modifying, or deleting the settings using LUN Manager, it is not necessary to reboot the disk array subsystem.

6.2.3 Ensuring that Host Demand on Subsystem Does Not Exceed Bandwidth

Make sure that host demand on the disk subsystem does not exceed available bandwidth. Consider the following:

- Common office applications (word processing and spreadsheets) average about 5-MB bandwidth per host.
- Periodic-access applications such as anti-virus software can cause increase bandwidth demand. Run only one application at a time and schedule applications to run during non-peak times.
- Multiple hosts connected to a single subsystem port can increase bandwidth demand through the port. When using two ports on a disk subsystem, connect hosts to balance demand across both ports.

6.2.4 Increasing Fault Tolerance with Redundant Paths

Consider using redundant paths to help ensure disk subsystem availability when hardware components fail. For more information, refer to your disk subsystem user guide.

6.2.5 Multiple Host Connections to iSCSI Ports Can Affect Performance

It is possible to connect up to 128 (255: the micro program version 0750/A or later) hosts to an iSCSI port. Too many hosts, however, can increase network traffic beyond the processing capacity of the port. A Gigabit Ethernet limits the maximum bandwidth of an iSCSI port to about 100 MB and exceeding this limit causes command delays and timeouts. If necessary, decrease the number of hosts and I/Os, or increase the number of disk arrays. When using LUN Manager, you should design a system configuration to evenly distribute traffic concentrated at the port, controller, and disk drive.

6.2.6 Using iSNS Versus Using IP Addresses to Identify Targets

Using iSNS (Internet Storage Name Service) facilitates the discovery and management of targets on the network without needing to know IP addresses. To implement iSNS requires a server attached to the IP-SAN.

6.2.7 iSCSI Digests and Performance

For disk subsystems that support both an iSCSI Header digest and an iSCSI Data digest, you can enable the digests to verify the integrity of network data. However, the verification has a modest cost in processing power at the hosts and disk arrays, in order to generate and check the data digest code. Typically data transfer decreases to about 90%. (This rate will be affected by network configuration, hosts' performance, hosts' application, etc.)

Note: Enable digests when using an L3 switch (including router) to connect the host to the disk subsystem iSCSI port.

To enable header and data digests, refer to your iSCSI initiator documentation, which may describe it as CRC (Cyclical Redundancy Checking), as CRC32, or as a checksum parameter.

6.2.8 Host Competition for Disk Access within a RAID Group Lowers Performance

When two or more hosts are connected to a disk array subsystem and the LUs assigned to each host belong to the same RAID group, concurrent access to the same disk drive will occur. Because of this conflict for access to the disk drive, performance may decrease. Ideally, LUNs in one RAID group should only be accessed by one host. To avoid a conflict, you should never have more than one host access multiple LUNs in one RAID group.

The number of RAID groups that can be created is determined by the number of mounted disk drives and the RAID level of the RAID groups to be created. If unable to create as many RAID groups as hosts to be connected, organize the RAID groups according to operational states of the hosts (see Figure 6.9 and Figure 6.10).

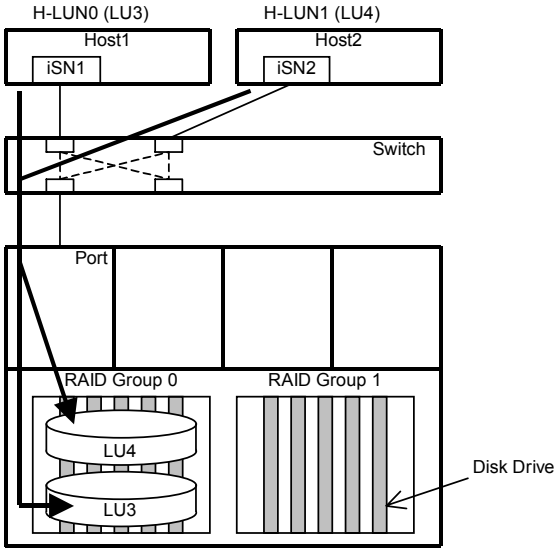


Figure 6.9 Hosts Connected to the Same RAID Group Decreases Performance

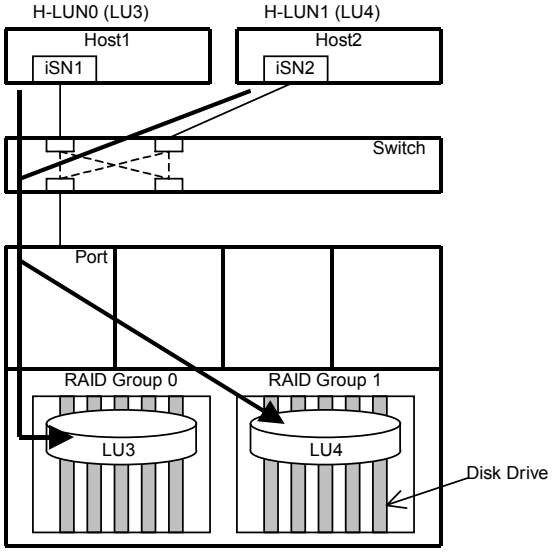


Figure 6.10 Hosts Connected to Different RAID Groups

6.2.9 Security for iSCSI Networks

To provide network security, consider implementing one or more of the following:

- Closed IP-SAN

  In the point of view of security, it is effective to design IP-SAN completely isolated from the other external networks.

- CHAP authentication

  The user is authenticated using CHAP. You must register the CHAP user who is authorized for the connection and the Secret in the disk array subsystem.
  The user can be authenticated for each target by using LUN Manager.

  The user name and the secret for the user authentication on the host side are first set to the port, and then assigned to the target. The same user name and secret may be assigned to multiple targets within the same port.

  You can import CHAP authentication information in a CSV format file. For details, refer to the *Storage Navigator Modular Graphical User Interface (GUI) User's Guide* (MK-95DF711). For security, you can only import, and not export CHAP authentication files with LUN Manager. Always keep CSV files secure in order to prevent others from using the information to gain unauthorized access.

  When registering for CHAP authentication you must use the iSCSI name, acquiring the iSCSI Name for each platform and each HBA. Set the port-based VLAN of the Network Switch if necessary. Refer to your disk subsystem user's guide for details.

- Verify host/LU paths with LUN Manager

  Determine input/output paths between hosts and LUs according to the assignment mode using LUN Manager. The input/output path is a route through which access from the host is permitted.

6.3 Network Connections: Ports, When to Use Switches, Settings

- Design the connections of the hosts and the disk arrays for constructing the iSCSI environment. When connecting the disk array subsystem to more hosts than its ports, design the Network Switch connection and the VLAN.
- Choose a network interface for each host, either an iSCSI HBA (host bus adapter) or a NIC (network interface card) with a software initiator driver. The NIC and software initiator combination costs less, but the HBA, with its own processor, minimizes demand on the server from protocol processing.
- If the number of hosts to connect is greater than the number of iSCSI ports, network switches are needed to connect them.
- AMS/WMS iSCSI cannot connect directly to a switch that does not support 1000BASE-T (full duplex). However, a switch that supports both 1000BASE-T (full duplex) and 1000BASE-SX or 100BASE-TX, will make AMS/WMS iSCSI allow communication with 1000BASE-SX or 100BASE-TX.
- All connections direct to iSCSI in the IP-SAN should be 1000BASE-T (full duplex).
- 100BASE-T decreases IP-SAN performance. Instead, use 1000BASE-T (full duplex) for all connections.
- AMS/WMS iSCSI doesn't support direct, or indirect connections to a network peripheral that only supports 10BASE.
- The network switch is available, as long as is transparent to disk arrays (port base VLAN etc.).
- AMS/WMS iSCSI does not support tagged VLAN or link aggregation. The packets to transfer such protocols should be filtered out in switches.
- When IP-SAN is designed, it is similar to construct the traditional network. Overlapping of addresses or loop made in a subnet will cause serious degrade of communication performance and even cause disconnections.
- Network switches with management functions such as SNMP can facilitate network troubleshooting.
- It is required to separate an IP-SAN (i.e., the network on that iSCSI communication is done) from the other network (management LAN, office LAN, other IP-SAN, etc.) when you need the performance of iSCSI communication or security of iSCSI communication. Port VLAN function of a switch will be able to separate the networks logically.
- When multiple NICs are installed in a host, they should have addresses that belong to different network segments.

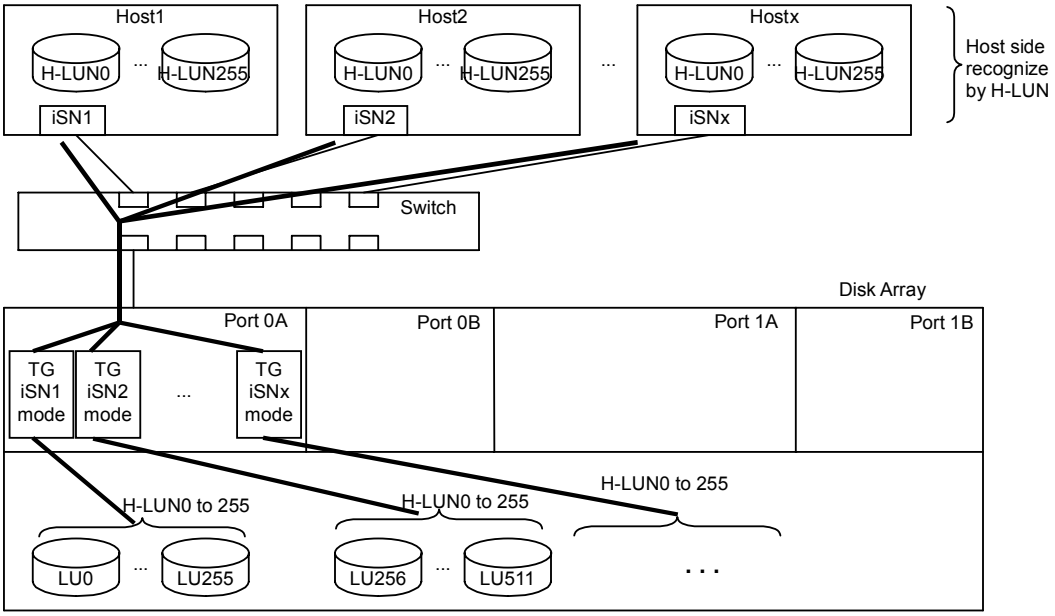
For iSCSI port network settings:

- Make sure to set the IP address (IPv4) to each iSCSI port, to not overlap the other ports (including other network equipment ports). Then set the appropriate subnetmask and default gateway address to each port.
- Targets are set to the subordinate of iSCSI ports. Target 0 is made in default for each iSCSI ports.
- Each iSCSI target is assigned its iSCSI name automatically.
- When connecting hosts and one port of the disk array subsystem using the network switch, a control to distinguish accessible host is required for each LU.

6.4 Assigning Targets and LUs to Hosts

The host recognizes LUN(s) in the range between H-LUN0 and H-LUN255. When you assign LU(s) in the range more than 256 LUs to the host, you must set the target LU Mapping to be between H-LUN0 and H-LUN255.

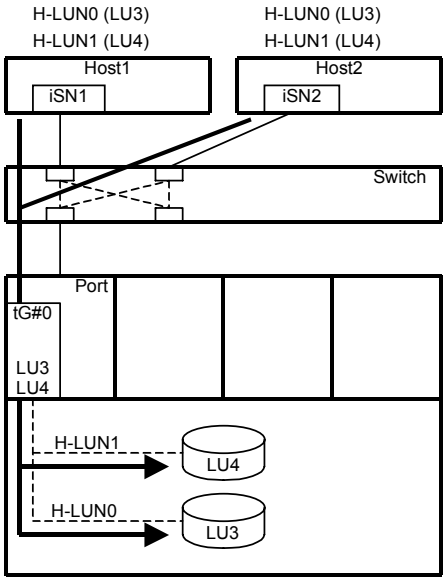
Up to 256 LU Mappings can be set for a target. Up to 256×128 (256X255: the micro program version 0750/A or later) LU Mappings can be set for a Port.



(iSN: iSCSI Name, TG: Target)

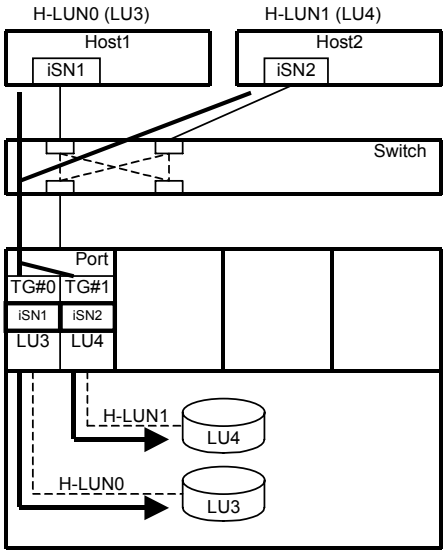
Figure 6.11 Mapping LU(s) in the Range between LU256 and LU511 to the Host

When assigning LU3 to Host 1 and LU4 to Host 2, both hosts can access the same LU if the LU mapping is set alone as shown in Figure 6.12. When LUN Manager or CHAP is used in this case, the host (iSCSI Name) access to each LU can be distinguished even in the same port as shown in Figure 6.13.



(TG: Target, iSN: iSCSI Name)

Figure 6.12 LUN mapping only example: Different hosts can still access both LUs



(TG: Target, iSN: iSCSI Name)

Figure 6.13 Example of LUNs assigned to targets: Host access to LUs is separated

6.5 Adding and Replacing Equipment

After installing iSCSI, perform the following tasks:

- Add a host and HBA

  When assigning LUs within the disk array subsystem to a host and an HBA, add a target to the disk array subsystem. When adding a setting of CHAP, it is not necessary to restart the disk array subsystem. Execute a host boot or a disk recognition command after setting CHAP.

- Add an LU

  When adding a LU to the disk array subsystem and assigning it to a host that has been connected, add a mapping of the LU to the target to which the host belongs. When adding the setting for CHAP, it is not necessary to restart the disk array subsystem. Execute a host boot or the disk recognition command after making a setting of CHAP.

- Replace HBA

  When replacing an HBA of a host, the setting for CHAP must be modified. Change the iSCSI User Name of the HBA. If you do not make this change, the host will not be able to access the LU after the replacement of the HBA.

  It is necessary to manage the settings that have been made for the disk array subsystem by keeping a documented record. When an HBA is replaced, change the iSCSI Name accordingly. In this way, you can identify the iSCSI Name that was set before the replacement by referring to the record.

  Each setting for CHAP must be documented when the configuration is created so that the previous setting can be reviewed before making a change to the setting.

- Replace the switch

  When the Network Switch is replaced, you must set the connections as they were before the replacement.

- If you replace an HBA in a host attached to a disk array subsystem using Target, you must change the iSCSI Name setting in CHAP.

After adding or replacing equipment, always test the host connection and let the host recognize the LU.

6.6 Preventing Illegal Access

When connecting hosts and one port of a disk array subsystem using the switch, a control to each LU is required to distinguish its accessible host.

When assigning LU3 to Host 1 and LU4 to Host 2, both hosts can access the same LU if the LU mapping is set as shown in Figure 6.14. When LUN Manager or CHAP is used in this case, the host (iSCSI Name) access to each LU can be distinguished even within in the same port (see Figure 6.15).

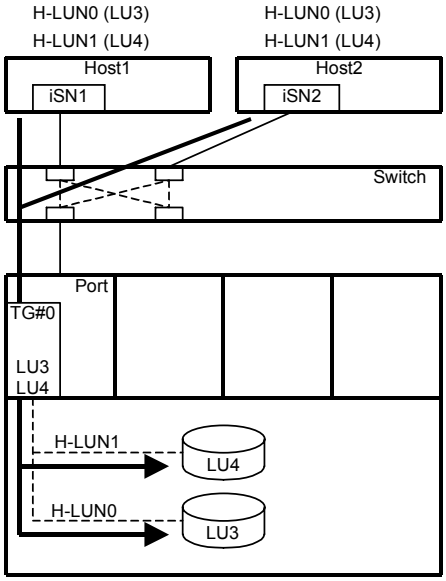


Figure 6.14 LU Mapping Does not Restrict Host Access

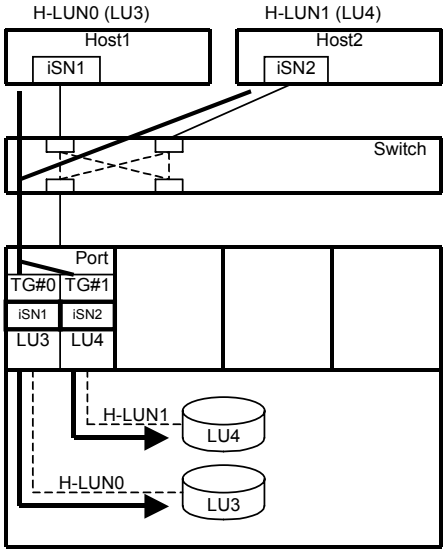


Figure 6.15 Using LUN Manager or CHAP to Restrict Host Access

6.7 Queue Depth Setting

When connecting multiple hosts to a single port, ensure that the queue depth of the port is not exceeded, and specify the queue depth so that the sum for all hosts does not exceed the allowed limit per port.

When a host queues successive commands to the disk array subsystem before execution of a previous command can complete, the number of times successive commands are issued is called Queue Depth. When two or more hosts are connected to a port of a disk array subsystem, the number of Queue commands for the port is increased because the host issues commands to each disk array subsystem separately.

Multiple hosts can be connected to a single port. The queue depth for each port is limited and performance drops if that limit is exceeded. You should therefore specify the queue depth so that the sum for all hosts does not exceed the value of the limit per port. The disk array subsystem reports the Queue Full status with commands received after the limit is exceeded. Since the host that has received notice of the Queue Full status stops issuing the multiplex command, a decrease in host performance may occur. To avoid such a situation, queue depth should be carefully determined when designing the system.

Notes:

- If a queue depth setting is increased, traffic on the disk array subsystem also increases. Traffic on the host and switch may also increase. This should also be taken into consideration when changing a queue depth setting.
- The formula for defining Queue Depth on the host side varies depending on the type of operating system or HBA. When determining the overall queue depth settings for hosts, consideration should be given to the port limit.

6.7.1 The Default Queue Depth Configuration of Each System

The default Queue Depth setting for each host operating system is shown in Table 6.1. Each system has an individual Queue Depth value unit and setting unit.

Table 6.1 The Queue Depth Configuration for iSCSI

Platform	HBA	Queue Depth		Unit of Setting
		Unit of Value	Default	
Windows®	Microsoft® initiator			
	Qlogic®	Port	16	HBA
Linux®	Software initiator			
	Qlogic®	Port	16	HBA

6.7.2 Queue Depth Limits of System Combination

When the following host operating system combination is connected to a single port of the disk array subsystem, you must set the queue depth value described in Table 6.2.

Table 6.2 Queue Depth Limits of System Combination for iSCSI

System Combination	Setting Queue Depth
Windows NT®/Windows® 2000/2003 MSCS	Max.16 commands per port (for Qlogic® HBA)

6.7.3 Increasing Queue Depth Setting and Port Sharing

Figure 6.16 shows how to determine queue depth when a port is shared.

In this example, Host 1, Host 2, Host 3, and Host 4 are connected to a port that is given a limit of 512 commands. In this case, the queue depth for the port must be specified so that a sum of numbers of queue depth for each Hosts A, B, C, and D does not exceed *X*.

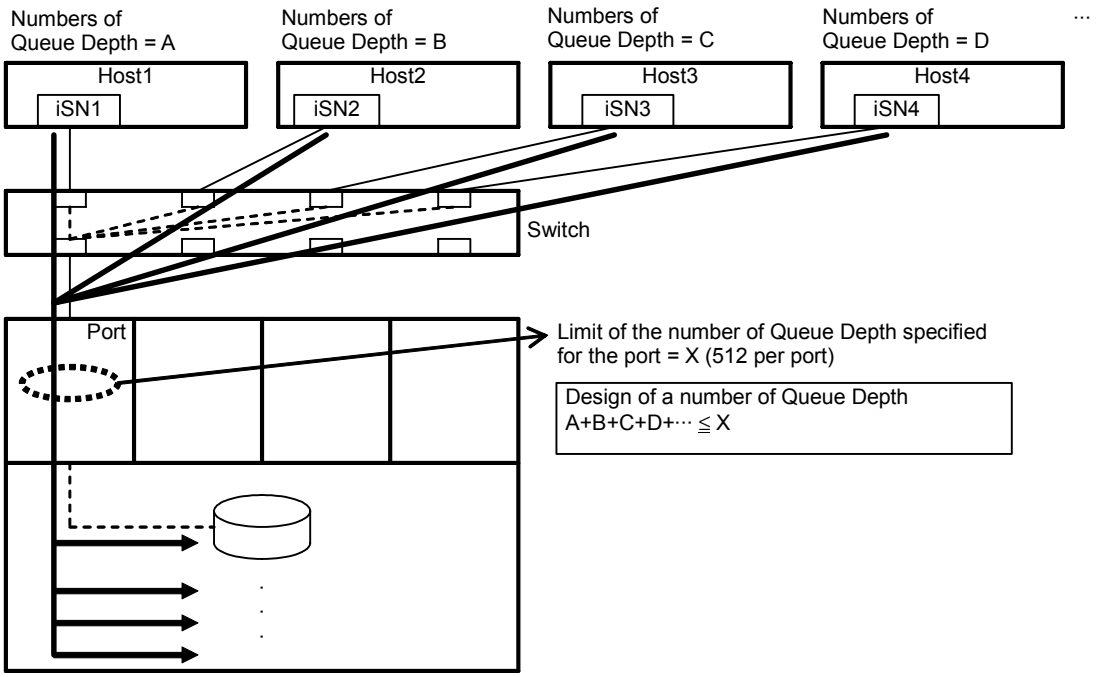


Figure 6.16 Ensuring that the Queue Depth Does Not Exceed the Port Limit

6.7.4 Increasing Queue Depth Through Path Switching

Figure 6.17 shows how to determine the queue depth when an alternative path is configured. The system shown has a configuration with an alternative path and the Host 1 and Host 2 sides are assigned to the Primary and Secondary paths, respectively.

Commands are generally issued to a LU via the Primary path on the Host 1 side. In this configuration, commands to be issued via the Primary path are moved to the Secondary path because path switching is done, and the queue depth for a port connected to a host on the Secondary path is increased. You must specify the appropriate queue depth for each host so that the number does not exceed its limit even after the path switching is done.

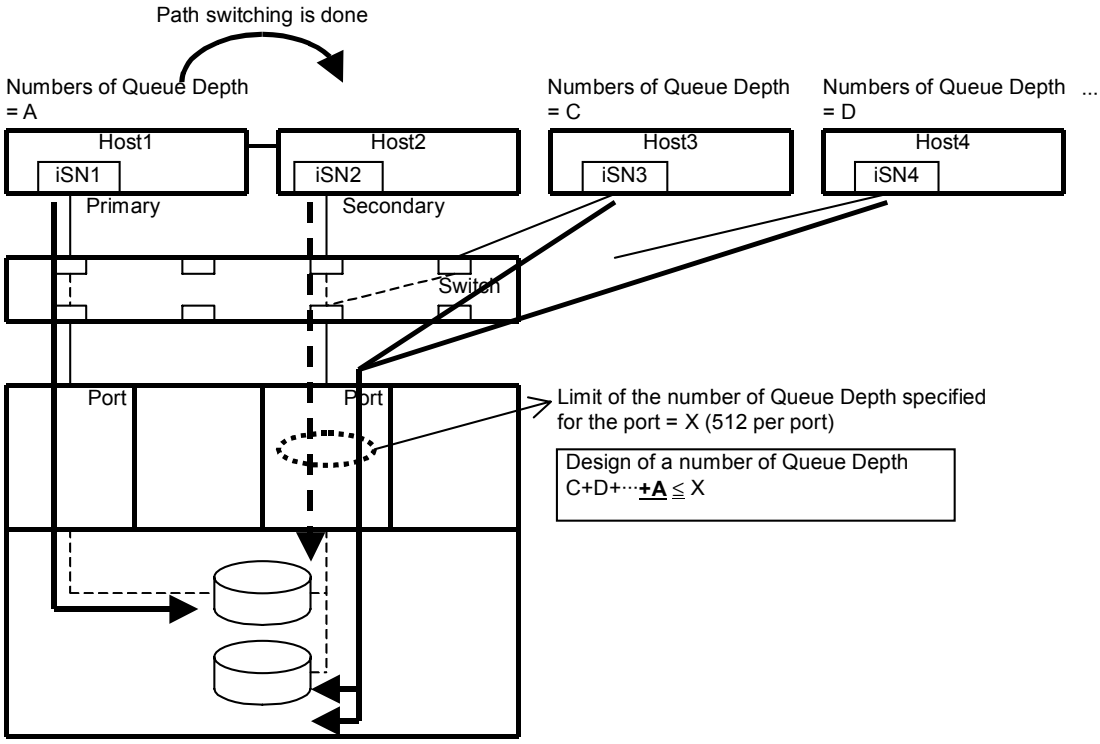


Figure 6.17 Increment of Queue Depth Generated Due to Path Switching

6.7.5 Allocation of Queue Depth According to Priority of Host Job

Figure 6.18 shows how to determine the Queue Depth when the priority order is given to jobs of connected hosts. To raise the priority of a specific host job, increase the queue depth for the host. When a queue depth for a certain host is increased, it is necessary to have the number for the port concerned not exceed its limit. This is done by reducing the numbers for the other hosts connected to the port.

Note: If the disk array subsystem does not have prioritized order control, you must not exceed the limit for the host queue depth number.

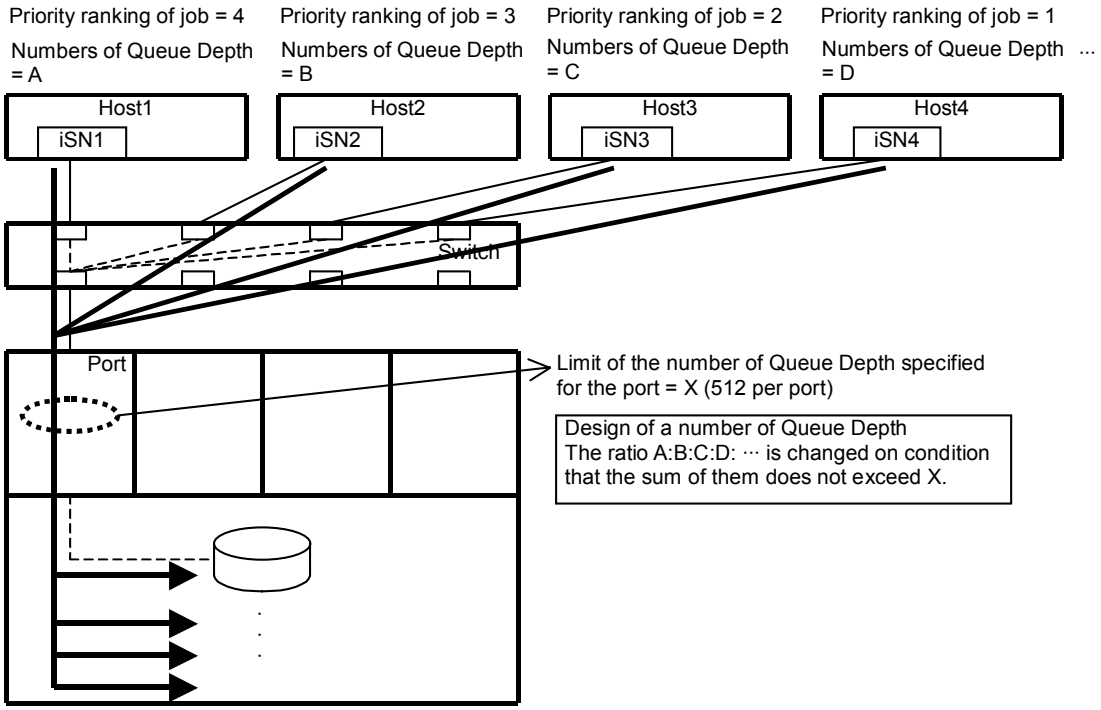


Figure 6.18 When Priority Order is Given to Host Jobs

6.8 Testing the Host Connection with Ping

The disk subsystem iSCSI port responds to ping up to 404 bytes payload, but not more than 404 bytes payload.

Sending PING to an unreachable address might cause the delay of the host I/O processing on the controller. Pinging from both ports on a controller at the same time may cause an I/O timeout. It is strongly recommended that ping tests should be executed when no I/O exists on the controller.

Chapter 7 iSCSI and LUN Manager Software Procedures

This chapter explains how to execute the LUN Manager feature using the GUI version of Navigator. For CLI installation, see Appendix A.

In this chapter:

- Adding a Target (section 7.1)
- Setting a Target Option (section 7.2)
- Mapping Logical Units to Targets (section 7.3)
- Adding an Initiator (section 7.4)
- Changing a Target Information (section 7.5)
- Deleting a Target (section 7.6)
- Initializing Target 0 (section 7.7)
- Changing an Initiator Information (section 7.8)
- Deleting an Initiator Information (section 7.9)
- CHAP User (section 7.10)

7.1 Adding a Target

To create a target for each Port, you must:

- Set the target Security to **enable** for each port
- Create a target

Using LUN Manager, a system engineer connects a port of the disk array subsystem to a host using the Switching-Hub etc., and then sets a data input/output path between the host and the LU. This setting specifies which host can access which LU.

To set a data input/output path, the hosts that are authorized to access the LU must be classified as a Target. That Target is then set to the port.

For example, when a Windows® Host (initiator iSCSI Name A) and a Linux Host (initiator iSCSI Name B) are connected to Port A, you must create Targets of LUs to be accessed from the Windows® Host (initiator iSCSI Name A) and by the Linux Host (initiator iSCSI Name B) as shown in Figure 5.1.

Set a **Target** option (Host Connection Mode) to the newly created Target to confirm the setting.

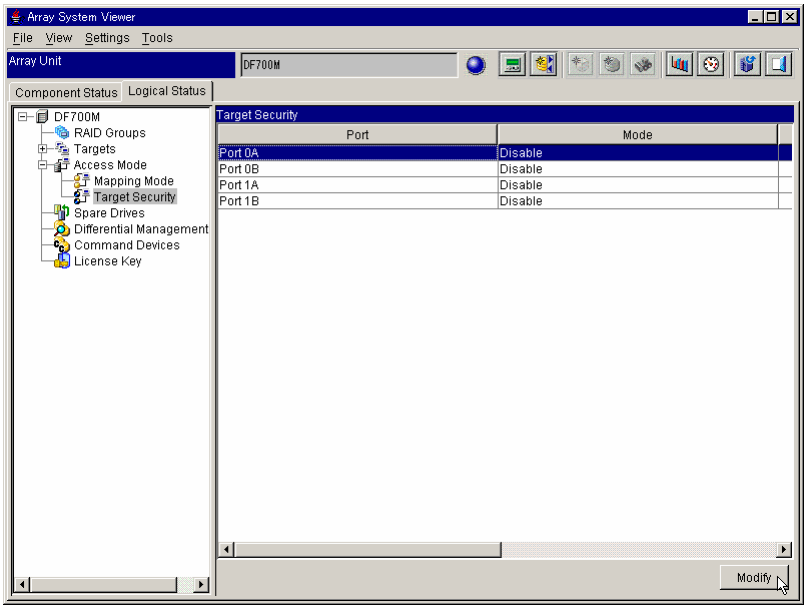
7.1.1 Setting the Target Security

The Target Security default setting is **disable** for each port.

To Enable or Disable Target Security for each port:

1. Start Storage Navigator and change the operation mode to **Management Mode**.
2. Register the subsystem in which you will enable or disable target Security. Connect to the subsystem.

   The **Array System Viewer** window appears and displays the connected subsystem.
3. Click the **Logical Status** tab.
4. Click the **Target Security** icon in **Access Mode**.
5. Select the port for which you want to set the access mode to enable/disable.
6. Click **Modify**.

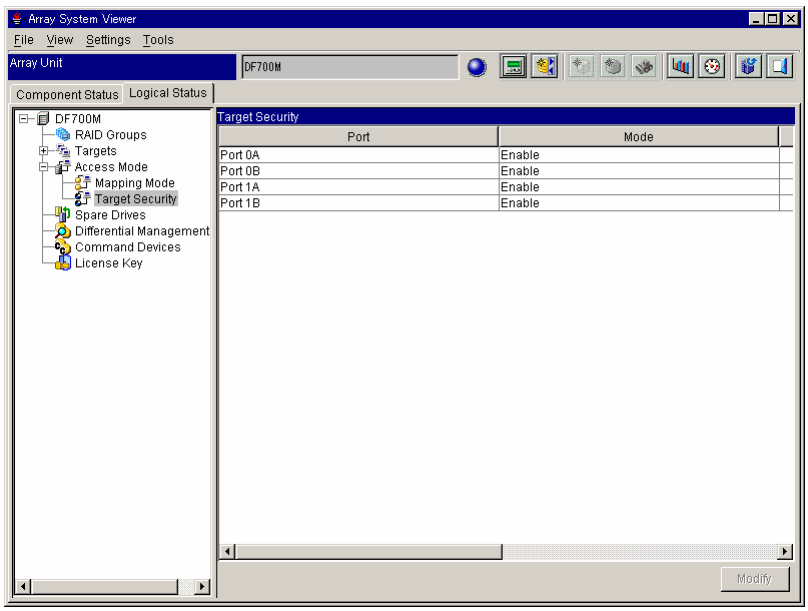


7. Select the **Enable** or **Disable** option and click **OK**.

8. Observe any messages that appear and click **OK** to continue.

   If the Target Security has been set to enable, **Detected Initiator** is displayed.

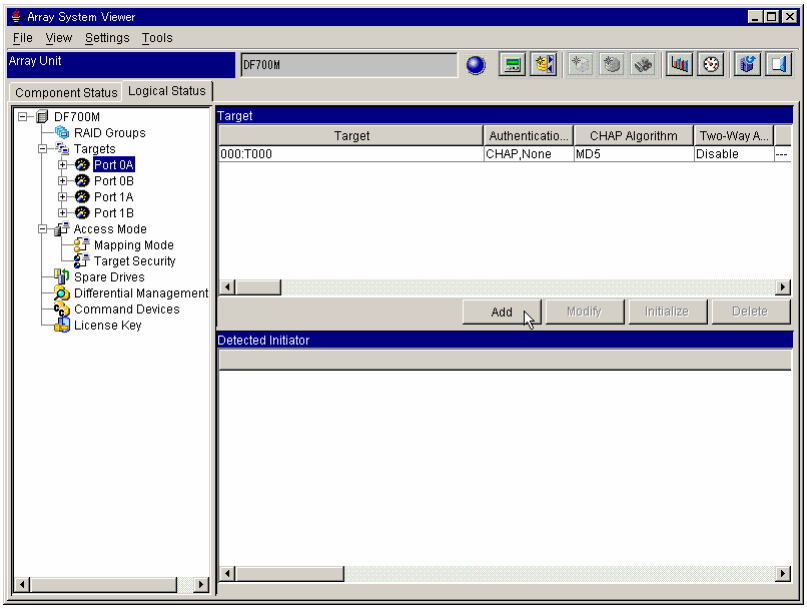
   The iSCSI Name of the HBA that is connected to the selected Port is displayed in the **Detected Initiator**.



7.1.2 Adding a Target

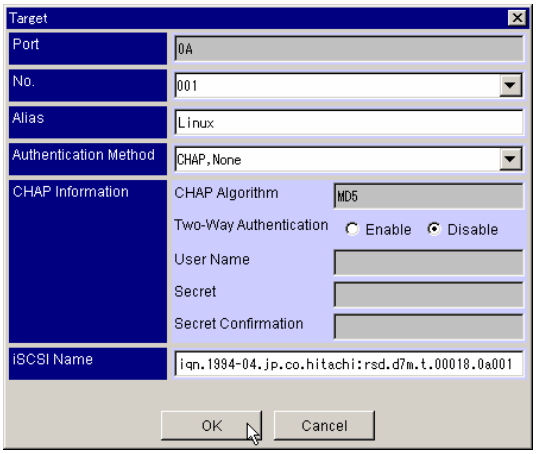
To create targets for each port:

1. In the **Logical Status** tab under **Targets**, select a port.



2. Click **Add** in the main window.

   The **Target** dialog box appears.



3. Enter the following and click **OK:**
   - **No.**

     Enter a numeral from 1 through 127.
   - **Alias**

     Enter the alias of the target with 32 or less alphanumeric characters (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

     Spaces at the top or end are ignored. The same name cannot be used in the same port.
   - **Authentication Method**

     Select the **CHAP**, **None**, or **CHAP,None**.
   - **CHAP Information**

     CHAP Algorithm: MD5 is always displayed.

     Two-Way Authentication: Select the **Enable** or **Disable** radio button.

     When selecting the **Enable** radio button, specify the following items:
     - **User Name**

       Enter the name of the User with 256 or less alphanumeric character. The following symbols can be used:

       . - + @ _ = : / [ ] - (space).
     - **Secret**

       Enter a Secret using 12 to 32 alphanumeric characters. The following symbols can be used.

       (. - + @ _ = : / [ ] - (space))

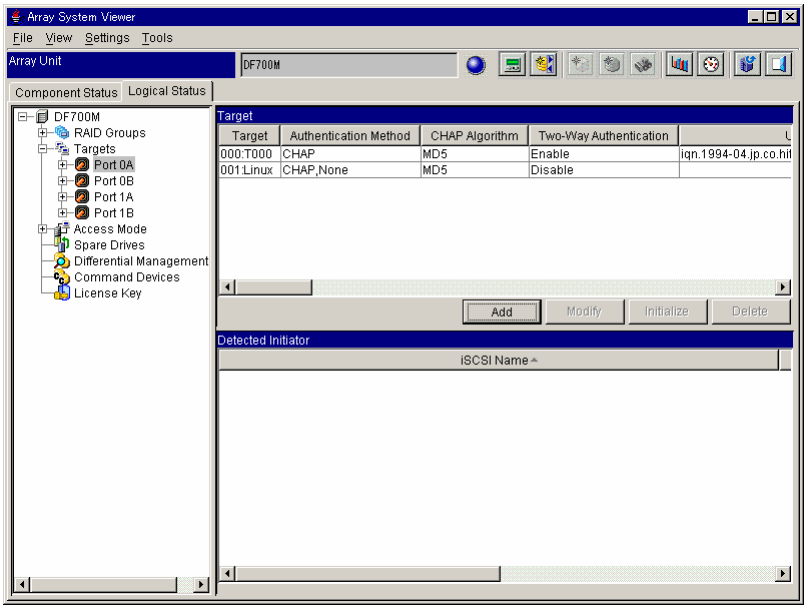
       When Microsoft® iSCSI software initiator is used on the host to authenticate, the Secret should be from 12 through 16 characters.
     - **Secret Confirmation**

       Enter the characters that enter into the **Secret**.
   - **iSCSI Name**

     Enter the name of the iSCSI Name with 223 or less alphanumeric characters. A period (.), hyphen (-), and colon (:) can be used.

4. The confirmation message is displayed. Click **OK**.

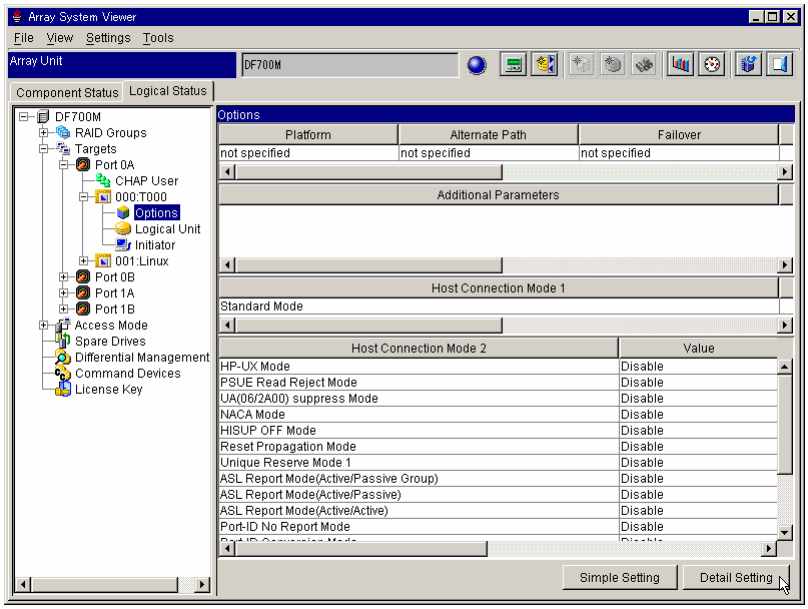
   The **Array System Viewer** window shows the target information.



7.2 Setting a Target Option

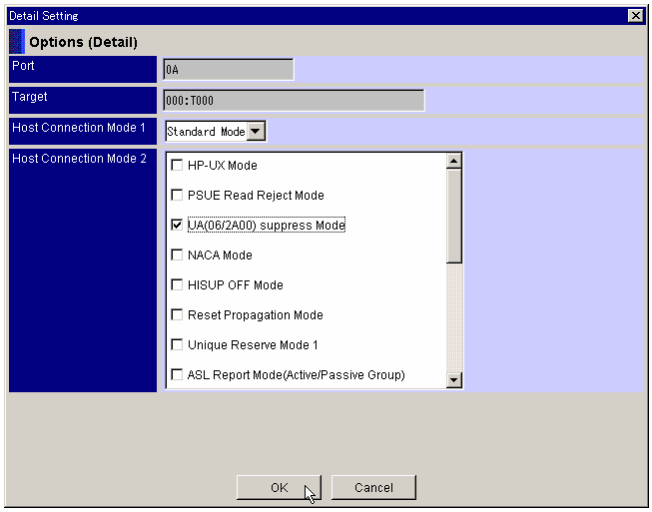
To set a target Option for each target:

1. Select an **Options** icon in the target and click **Detail Setting**.



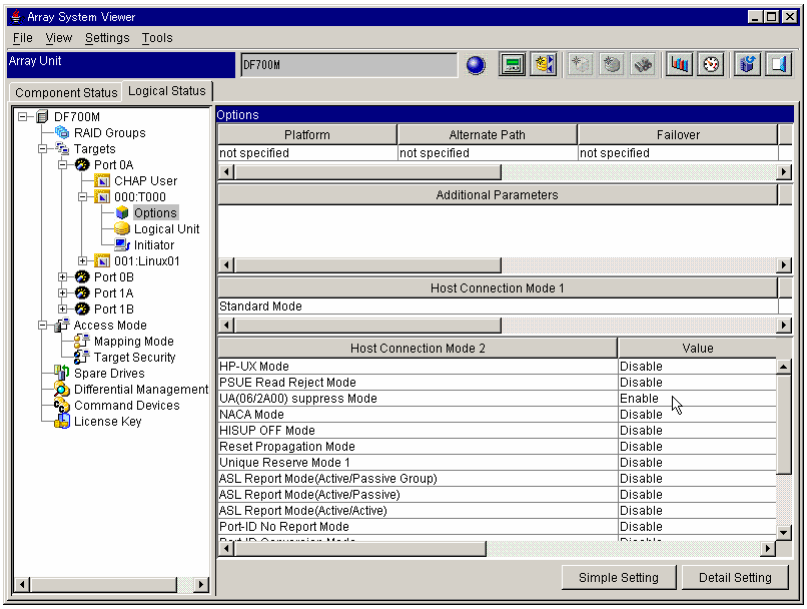
The **Option Property** screen is displayed.

2. Specify **Host Connection Mode 1** and **Host Connection Mode 2**, and click **OK**.



3. Observe any messages that appear and click **OK** to continue.

   The **Array System Viewer** window shows the updated information.



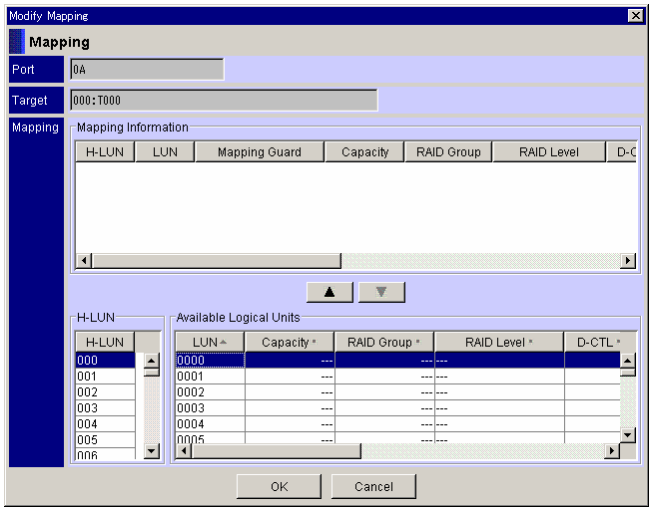
7.3 Mapping Logical Units to Targets

After setting a host to a Target, the LU is connected to the Target by mapping a LU to the Target.

A host (OS or driver) cannot identify a LU without LUN0. It is necessary to set H-LUN = 0 to the target in this case.

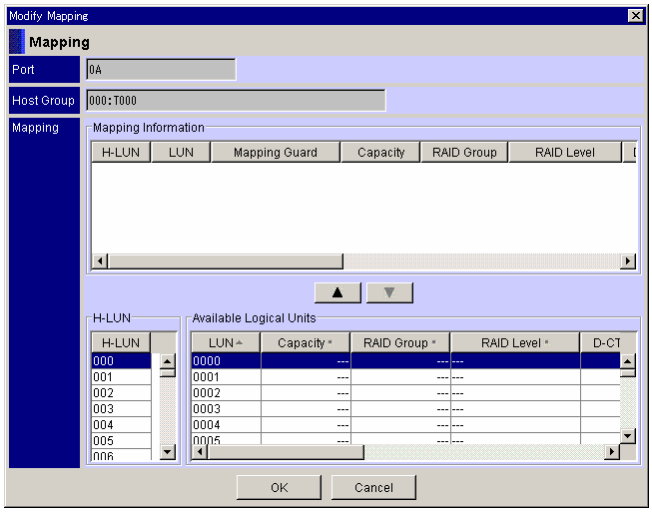
To map Logical Units to each target:

1. Select a **Logical Unit** icon in the target and click **Modify Mapping**.



The **Mapping Property** is displayed.

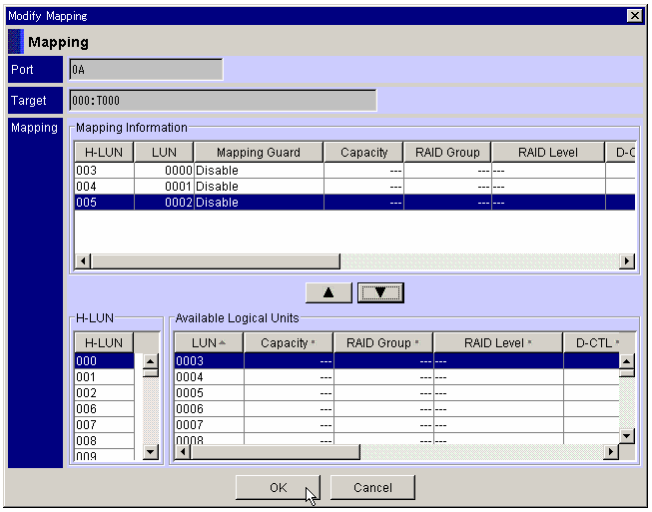
You must set **Enable** to **Mapping Mode** to set LU Mapping.



2. Select an **H-LUN** to be added. Select **LUN**, and click the ▲ button. The added contents are displayed in the **Mapping Information** list.

   To delete the H-LUN, click the line to be deleted in the **Mapping Information** list and click the ▼ button.

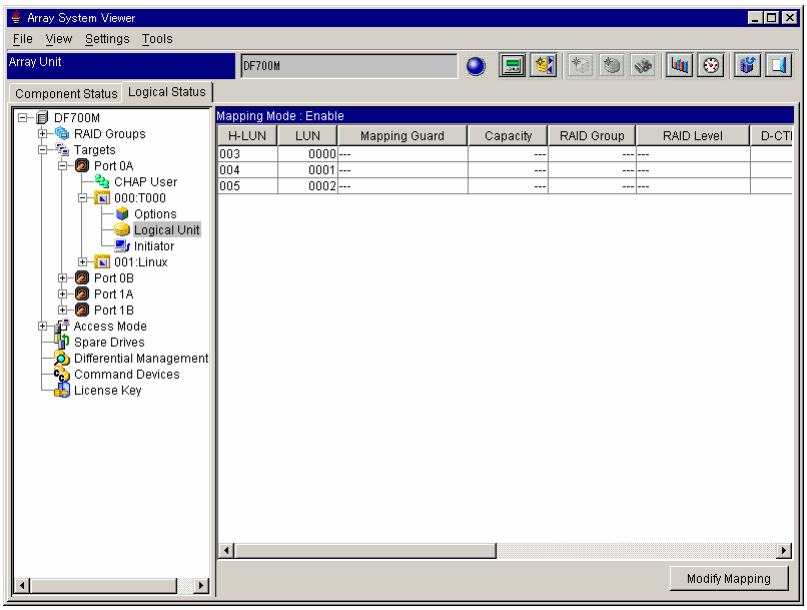
   The deleted contents disappear from the display of the **Mapping Information** list.



3. Click **OK**.

4. The confirmation message is displayed. Click **OK**.

   The information that has been set is displayed.



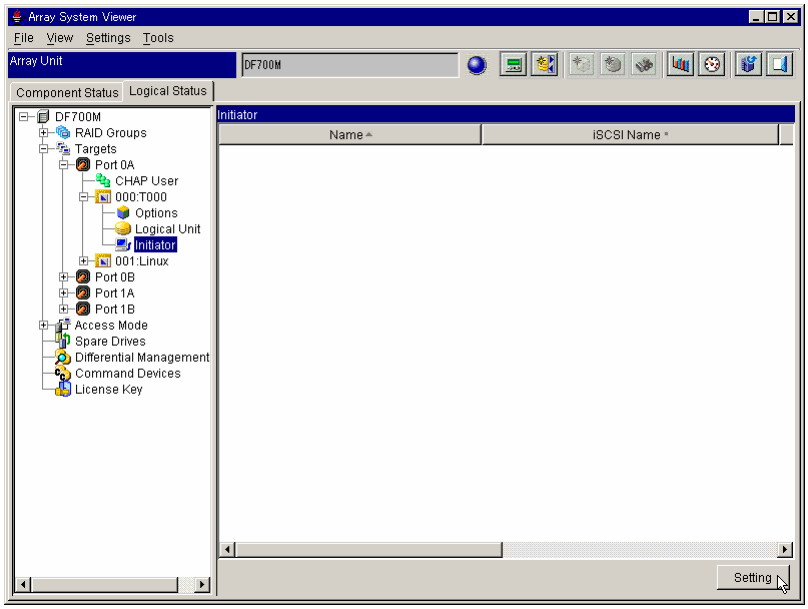
7.4 Adding an Initiator

Initiators of an HBA are set to each target. When a port is connected to a host, the initiators of HBAs that are listed in **Detected Initiator** can be selected and added to the target.

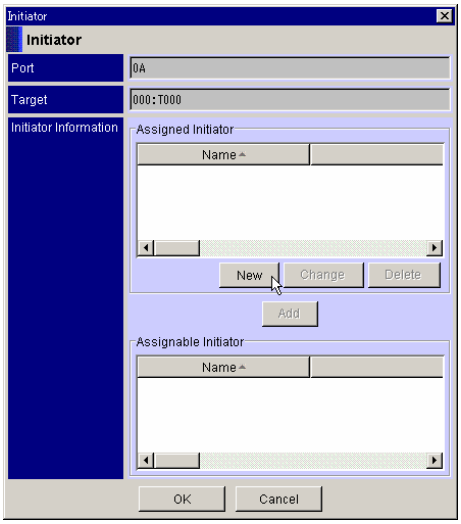
7.4.1 Adding an Initiator

To add an Initiator:

1. Select an **Initiator** icon in the target, and then click **Setting**.

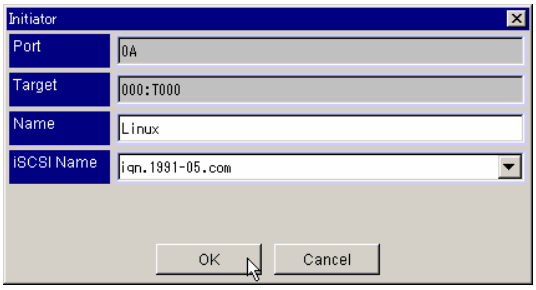


The **Initiator Property** window is displayed.



2. In the **Initiator Property** window, click **New**.

   The **Initiator** dialog box is displayed.



3. Enter the following and click **OK**.

   – **Name**

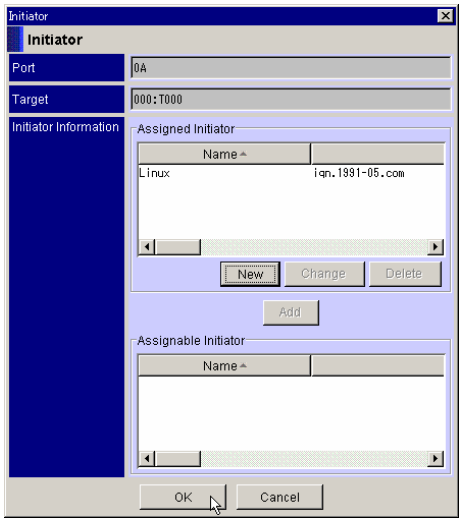
     Enter the name of the target with 32 or less alphanumeric characters (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

     Spaces at the top or end are ignored. The same name cannot be used in the same port.

   – **iSCSI Name**

     Enter the name of the iSCSI Name with 233 or less alphanumeric character. A period (.), hyphen (-), and colon (:) can be used.

   The **Initiator Property** window shows the updated information.



Note: Up to 128 Initiators can be assigned for a port. The total of the number of Initiators that have been already assigned (**Assigned Initiator**) and the number of Initiators that can be assigned (**Assignable Initiator**) further is, 128 for a Port. If the number of Initiators assigned to a port exceeds 128 and further input is impossible, delete an Initiator that is not assigned to a target.

4. In the **Initiator Property** window, click **OK**.
5. The confirmation message is displayed. Click **OK**.

7.4.2 Selecting and Adding an Assignable Initiator

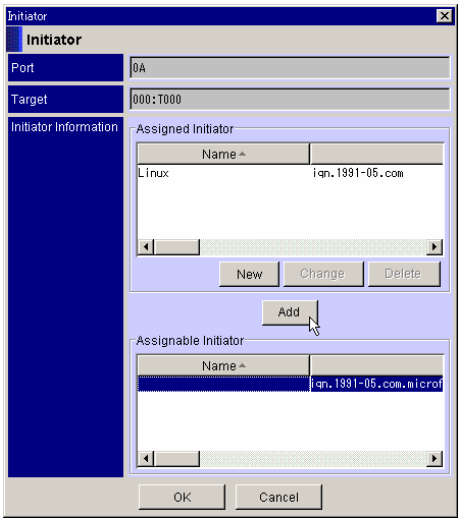
To select and add an assignable Initiator:

1. Select an **Initiator** icon in the target and click **Setting**.

   The **Initiator Property** window is displayed.

   Initiators of HBAs being connected to the Port are displayed in **Assignable Initiator**.

2. Select Initiator in the **Assignable Initiator** list and click ▲.



   The selected Initiator is displayed in the **Assigned Initiator** list.

3. In the **Initiator Property** screen, click **OK**.

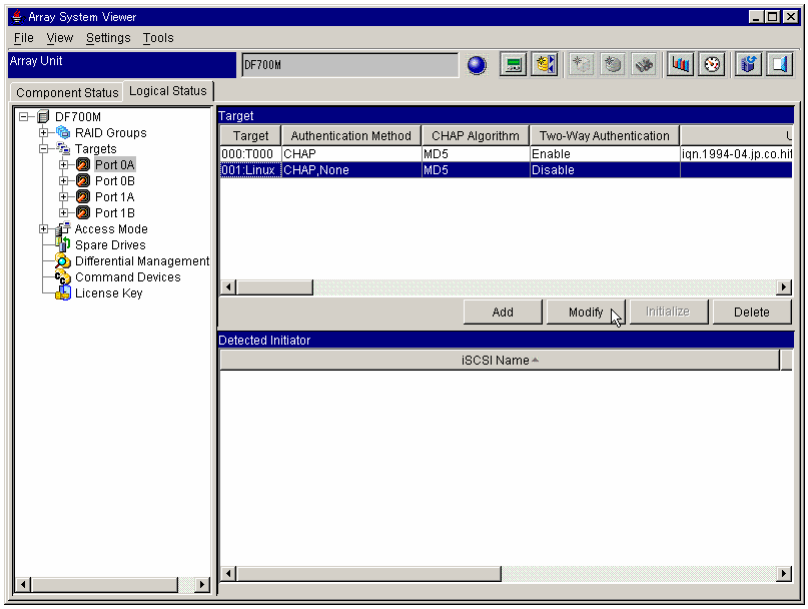
4. The confirmation message is displayed. Click **OK**.

Note: In some cases, the Initiator is not listed in the **Assignable Initiator** list, even though the Port is connected to a host. When the Initiator to be assigned to a target is not listed in the **Assignable Initiator** list, input and add it.

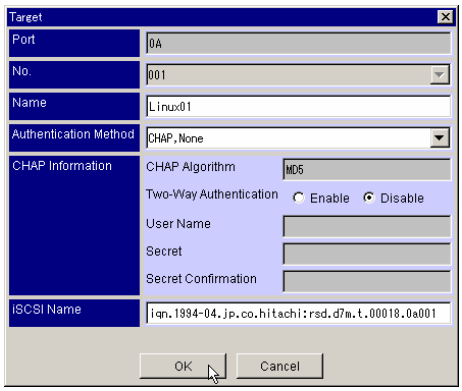
7.5 Changing a Target Information

To change the target information:

1. Select the **Target** requiring the target information, and click **Modify**.



2. Enter new information for the target.



- **Name**

  Enter the alias with 32 or less alphanumeric characters (excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

  Spaces at the top or end are ignored. The same name cannot be used in the same port.

- **Authentication Method**

  Select the **CHAP**, **None**, or **CHAP,None**.

- **CHAP Information**

  CHAP Algorithm: MD5 is always displayed.

  Two-Way Authentication: Select the **Enable** or **Disable** radio button.

  When **Enable** is selected, specify following items.

  User Name: Enter the name of the User with 256 or less alphanumeric character. The following symbols can be used:

  . - + @ _ = : / [ ] - (space)

  Secret: Enter a Secret using 12 to 32 alphanumeric characters. The following symbols can be used:

  . - + @ _ = : / [ ] - (space).

  When Microsoft® iSCSI software initiator is used on the host to authenticate, the Secret should be from 12 through 16 characters.

  Secret Confirmation: Enter the characters that for the **Secret**.

- **iSCSI Name**: Enter the name of the iSCSI Name with 223 or less alphanumeric character. A period (.), hyphen (-), and colon (:) can be used.

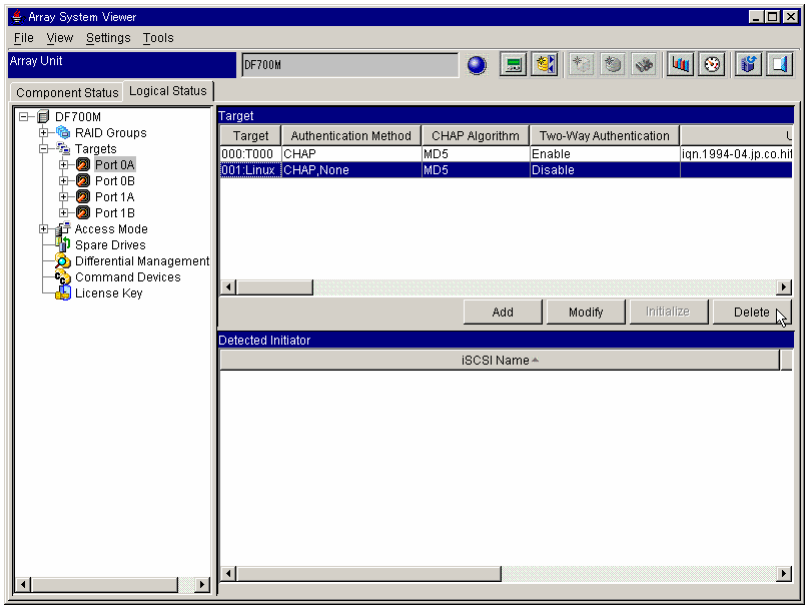
3. Click **OK** to confirm the change.

7.6 Deleting a Target

Note: Target 0 cannot be deleted. When deleting all the Initiators and all the Logical Units in Target 0, initialize Target 0 (see section 7.7).

To delete a target:

1. Select the **Target** to be deleted and click **Delete**.



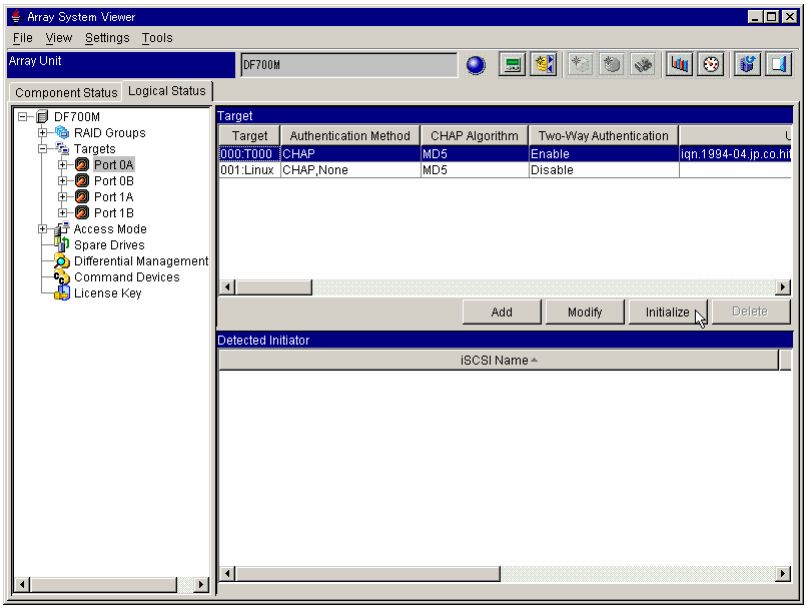
2. Observe any warnings that appear and click **OK** to continue.

7.7 Initializing Target 0

Target 0 can be reset to the default state. Target 0 is reset to the default state, Initiators that belong to Target 0 are deleted and the settings of the Logical Units that belong to Target 0 are also deleted. The **Target** option of Target 0 is reset to the default state and the target name is reset to T000.

To initialize Target 0:

1. Select **Target 0** to be initialized and click **Initialize**.



2. Observe any warnings that appear and click **OK** to continue.

7.8 Changing an Initiator Information

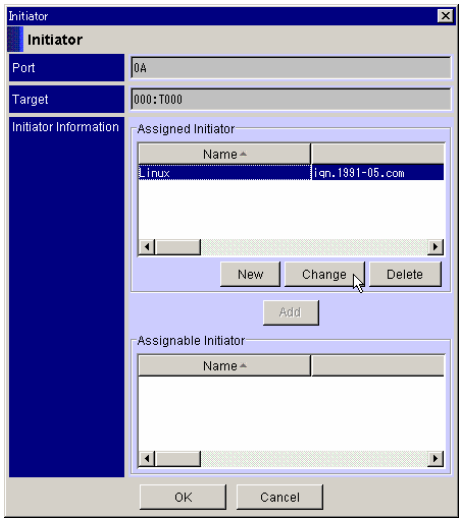
To change Initiator information:

1. Select an **Initiator** icon in the target, and click **Setting**.

   The **Initiator Property** window is displayed.

2. Select a **Name** to be changed and click **Change**.

   The **Initiator** dialog box is displayed.



   The **Initiator** dialog box is displayed.

3. Enter the **Name** or the **iSCSI Name** and click **OK**.

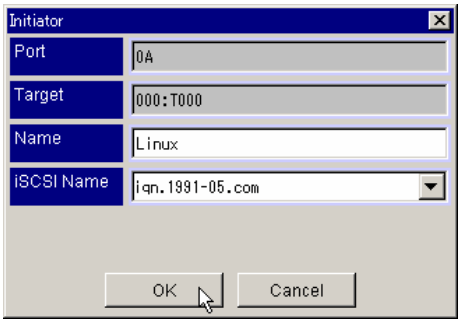
   – **Name**

     Enter the name of the target with 32 or less alphanumeric character. (Excluding \, /, : , , , ;, *, ?, “, <, >, | and ‘).

     Spaces at the top or end are ignored. An identical name cannot be used in an identical Port.

   – **iSCSI Name**

     Enter the name of the iSCSI Name with 223 or less alphanumeric character. A period (.), hyphen (-), and colon (:) can be used.



The information that has been entered is displayed on **Initiator Property**.

4. Click **OK** on **Initiator Property**.

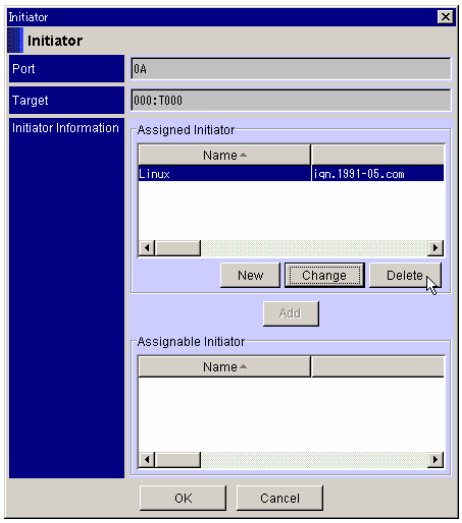
7.9 Deleting an Initiator Information

To delete Initiator information:

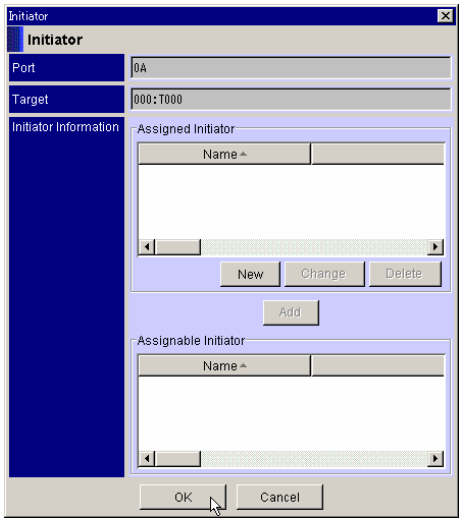
1. Select an **Initiator** icon in the target, and click **Setting**.

   The **Initiator Property** window is displayed.

2. Select the **Name** to be deleted in **Assigned Initiator** list and click **Delete**.



When the Initiator to be deleted is a Detected Initiator, or has been connected to the Host of the Initiator after the entry, the Initiator to be deleted is moved from the **Assigned Initiator** list to the **Assignable Initiator** list



3. In the **Initiator Property** window, click **OK**.
4. The confirmation message is displayed. Click **OK**.

7.10 CHAP User

The user authentication information can be set to the Target to authorize access for the Target and to increase security.

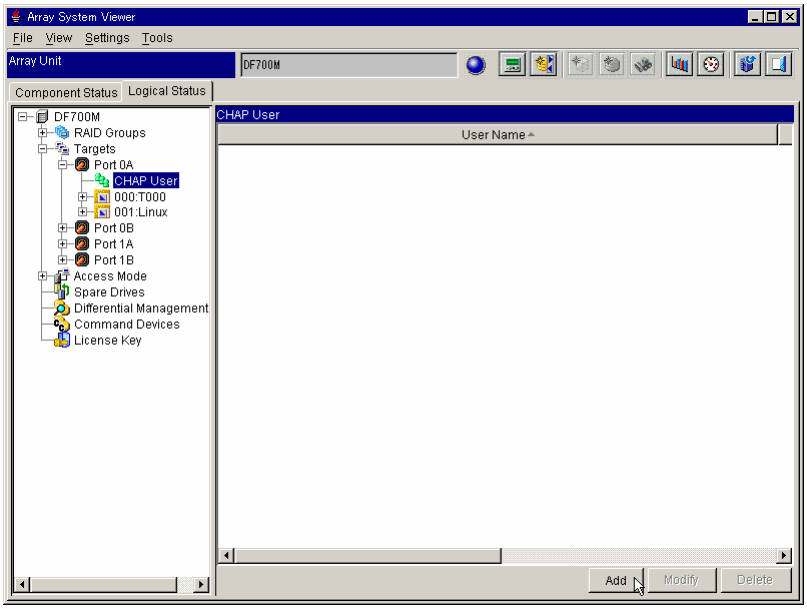
The User Name and the Secret for the user authentication on the host side are first set to the port, and then assigned to the Target. The same User Name and Secret may be assigned to multiple targets within the same port.

The User Name and the Secret for the user authentication are set to each Target.

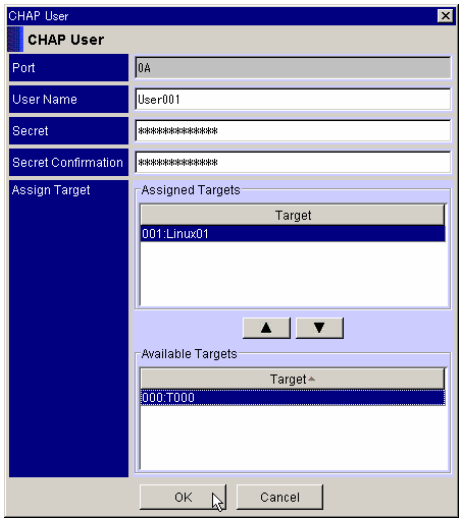
7.10.1 Adding a CHAP User

To add a CHAP User:

1. Select a **CHAP User** icon in a port and click **Add**.



The **CHAP User** dialog box is displayed.



2. In the **CHAP User** dialog box, enter the **User Name**, **Secret**, and **Secret Confirmation**.
3. From the **Available Targets** list, select the target to be assigned and select the ▲ button.
   - **User Name**

     Enter the name of the User with 256 or less alphanumeric character. The following symbols can be used. (. - + @ _ = : / [ ] - (space))
   - **Secret**

     Enter the Secret using 12 to 32 alphanumeric characters. The following symbols can be used: (. - + @ _ = : / [ ] - (space))

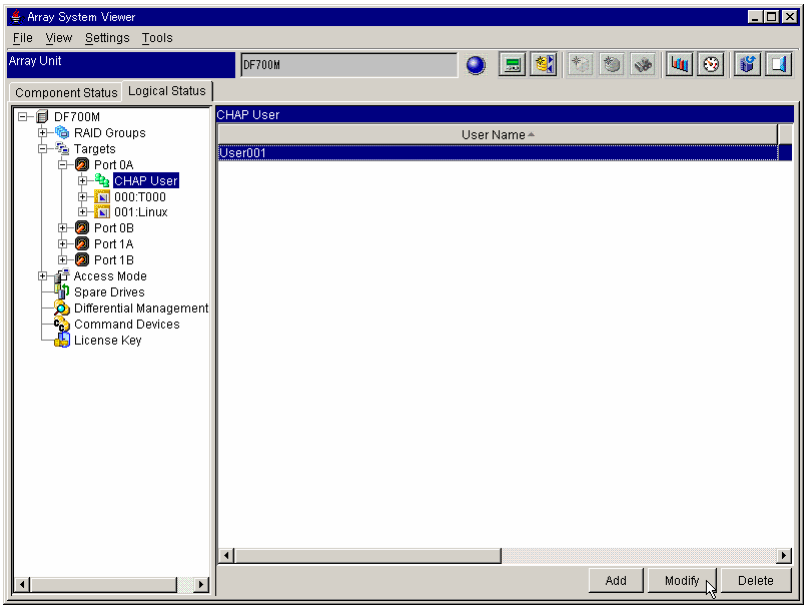
     When Microsoft® iSCSI software initiator is used on the host to authenticate, the Secret should be from 12 through 16 characters.
   - **Secret Confirmation**

     Enter the characters of the **Secret**.
4. In the **CHAP User** dialog box, click **OK**.
5. The confirmation message is displayed. Click **OK**.

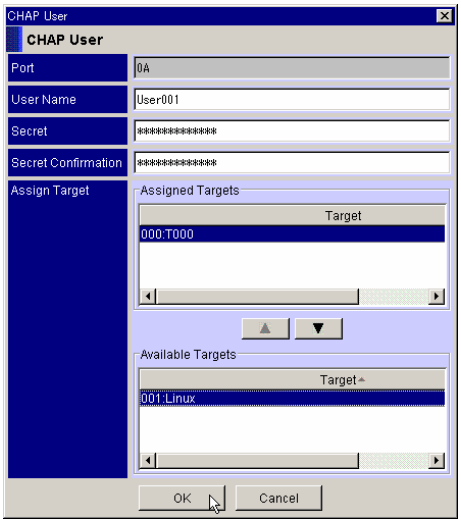
7.10.2 Changing the CHAP User

To change the CHAP User:

1. Select a **CHAP User** to be changed from the **CHAP User** list, and click **Modify**.



The **CHAP User** dialog box is displayed.

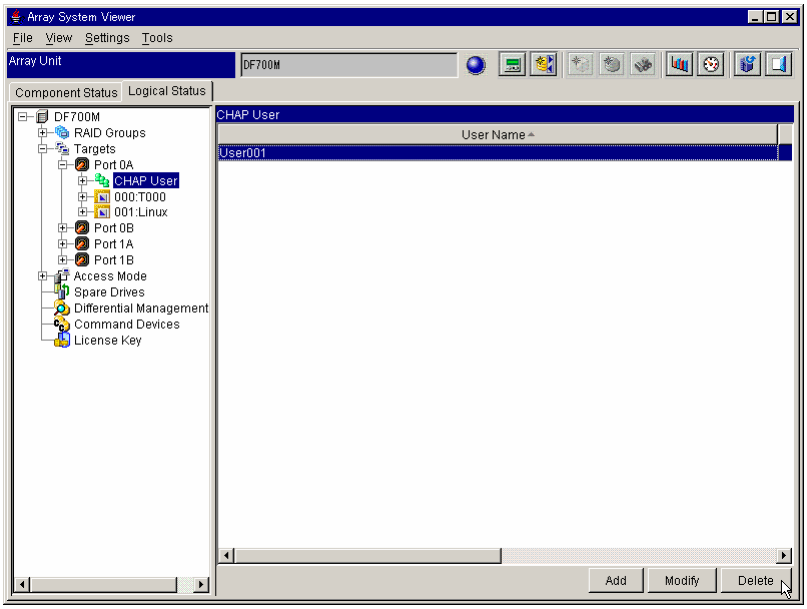


2. Enter the **User Name**, **Secret**, and **Secret Confirmation**.
3. Change the assigned target and click **OK**.
4. The confirmation message is displayed. Click **OK**.

7.10.3 Deleting the CHAP User

To delete the CHAP User:

1. Select the **CHAP User** to be deleting from the **CHAP User** list, and click **Delete**.



2. Observe any warnings that appear and click **OK** to continue.

Chapter 8 Troubleshooting

8.1 Troubleshooting

The Hitachi TagmaStore™ Adaptable Modular Storage subsystem is a high-performance, high-capacity storage array with added features designed to reduce the possibility of data loss due to the failure of any single component. For troubleshooting information on the AMS/WMS subsystem, please refer to the *TagmaStore™ Adaptable Modular Storage 200 User's Guide, (MK-95DF713)* and the *TagmaStore™ Adaptable Modular Storage 500 User's Guide, (MK-95DF714)*.

8.2 Calling the Hitachi Data Systems Technical Support Center

If you need to call the Hitachi Data Systems Technical Support Center, be sure to provide as much information about the problem as possible. Include the circumstances surrounding the error or failure and the exact content of any error codes and/or messages displayed. The worldwide Hitachi Data Systems Technical Support Centers are:

- Hitachi Data Systems North America/Latin America
  San Diego, California, USA
  1-800-446-0744
- Hitachi Data Systems Europe
  Contact Hitachi Data Systems Local Support
- Hitachi Data Systems Asia Pacific
  North Ryde, Australia
  61-2-9325-3300

Appendix A Command Line Interface Procedures

Note: When following the command-line examples in this appendix, be sure to replace the parameters shown with the correct parameters for your systems.

This appendix includes the following:

- Installing LUN Manager (section A.1)
- Uninstalling LUN Manager (section A.2)
- Enabling or Disabling LUN Manager (section A.3)
- Adding a host group (section A.4)
- Setting a host group option (section A.5)
- Setting Logical Units (LU Mapping) (section A.6)
- Adding a WWN (section A.7)
- Changing a host group Name (section A.8)
- Deleting a host group (section A.9)
- Initializing Host Group 0 (section A.10)
- Changing a WWN (section A.11)
- Deleting a WWN (section A.12)
- Deleting a Logined WWN (section A.13)
- Adding a Target (section A.14)
- Setting a Target Option (section A.15)
- Setting Logical Units (section A.16)
- Adding an Initiator (section A.17)
- Changing Target Information (section A.18)
- Deleting a Target (section A.19)
- Initializing Target 0 (section A.20)
- Changing Initiator Information (section A.21)
- Deleting an Initiator (section A.22)
- Adding CHAP User (section A.23)
- Changing CHAP User Information (section A.24)
- Deleting CHAP User (section A.25)

A.1 Installing LUN Manager

The **LUN Manager** option is usually unselectable (locked). To make this option available, you must install LUN Manager and make its functions selectable (unlocked). To install this function, use the required key code or key file provided with the optional feature.

LUN Manager is installed and uninstalled through Storage Navigator.

Note: Before installing and uninstalling, make sure that the array unit is in normal operating condition. If a failure such as a controller blockade has occurred, installation and uninstallation operations cannot be performed.

To install the LUN Manager feature using the CLI version of Navigator:

1. From the command prompt, register the subsystem (array unit) in which you will install the LUN Manager feature. Connect to the subsystem.
2. Install the optional features by executing the `auopt` command as follows:

Example 1:

Navigator: Version 5.00 or later and Cache Partition Manager is enabled.

```
% auopt –unit subsystem-name –lock off –keycode manual-attached-keycode
Password: manager-password
Are you sure you want to install the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is installed successfully.
%
```

Navigator: Less than version 5.00 and Cache Partition Manager is enabled.

```
% auopt –unit subsystem-name –lock off –keycode manual-attached-keycode
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
When Cache Partition Manager is enabled, if the option using data pool will be e
nabled the default cache partition information will be restored.
Do you want to continue processing? (y/n [n]): y
The option is unlocked.
%
```

Navigator: Less than version 3.00 and Cache Partition Manager is enabled.

```
% auopt -unit subsystem-name -lock off -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to unlock the option? (y/n [n]): y
The option is unlocked.
%
```

Example 2:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name                  Type      Term     Status
LUN-MANAGER                  Permanent ---      Enable
%
```

A.2 Uninstalling LUN Manager

To uninstall LUN Manager, use the key code provided. After uninstalling LUN Manager, the software is locked and not available until it is installed by a key code or key file.

Note: When disabling or uninstalling LUN Manager, you must first disable the host group Security for all ports.

LUN Manager is installed and uninstalled through Navigator.

To uninstall LUN Manager using the CLI version of Navigator:

1. From the command prompt, register the subsystem (array unit) in which you will uninstall the LUN Manager feature and connect to the subsystem.
2. Uninstall the optional features by executing the `auopt` command as follows:

   Example 1:

   Navigator: Version 5.00 or later

```
% auopt –unit subsystem-name –lock on –keycode manual-attached-keycode
Password: manager-password
Are you sure you want to de-install the option? (y/n [n]): y
The option is de-installed successfully.
%
```

   Navigator: Less than 5.00 version

```
% auopt -unit subsystem-name -lock on -keycode manual-attached-keycode
Password: manager-password
Are you sure you want to lock the option? (y/n [n]): y
The option is locked.
%
```

   Example 2:

```
% auopt -unit subsystem-name -refer
Password: manager-password
DMEC002015: No information displayed.
%
```

A.3 Enabling or Disabling LUN Manager

LUN Manager can be set to enable or disable after installation. This allows LUN Manager to be activated or deactivated without using a key code or key file.

Note: When disabling or uninstalling this LUN Manager feature, you must disable the host group Security for all ports.

To enable/disable LUN Manager using the CLI version of Navigator:

1. From the command prompt, register the subsystem in which you will change the status of the LUN Manager feature and connect to the subsystem.
2. Execute the `auopt` command to change the status (enable or disable) of the LUN Manager feature.

   The following is an example of how to change the status from enable to disable. To change the status from disable to enable, enter **enable** after the **-st** option.

   Example 1:

```
% auopt -unit subsystem-name -option LUN-MANAGER -st disable
Password: manager-password
Are you sure you want to disable the option? (y/n [n]): y
The option has been set successfully.
%
```

   Example 2:

```
% auopt -unit subsystem-name -refer
Password: manager-password
Option Name                    Type      Term     Status
LUN-MANAGER                    Permanent ---      Disable
%
```

A.4 Adding a Host Group

To create a host group for each port, you must:

- Set the host group Security to enable for each port
- Create a host group

A.4.1 Setting the Host Group Security

The host group default setting is **disable** for each port.

To set the host group Security to be valid or invalid:

1. From the command prompt, register the subsystem in which you want to set the host group security information and connect to the subsystem.
2. Execute the `auhgwwn` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A

   Use **off** with **-hgs** option, when disabled LUN Manager is changed.

   Example (AMS500):

```
% auhgwwn -unit df700 -set -hgs 0 A on
Password: manager-password
Are you sure you want to enable the host group security on port0A? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the port from the host.
Before setting, stop access to the port from the host.
Do you want to continue processing? (y/n [n]): y
The security information has been set successfully.
%
```

4. Specify as shown, when the checking information has been set:

   Example:

```
% auhgwwn –unit df700 -refer
Password: manager-password
Port  0A  host group Security  ON
Port  0B  host group Security  OFF
Port  1A  host group Security  OFF
Port  1B  host group Security  OFF
%
```

A.4.2 Adding a Host Group

To create host groups for each Port:

1. From the command prompt, register the subsystem (array unit) in which you want to set the host group information and connect to the subsystem.
2. Execute the `auhgdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1
   - Host group name: win001

   Example:

```
% auhgdef -unit df700 -add 0 A -gno 1 -gname win001
Password: manager-password
Host group information has been set successfully.
%
```

4. Specify as shown, when setting the following information:

   Example (AMS500):

```
% auhgdef -unit df700 -refer
Password: manager-password
Port 0A
  Group  HostGroupName
      0  G000
      1  win001
Port 0B
  Group  HostGroupName
      0  G000
Port 1A
  Group  HostGroupName
      0  G000
Port 1B
  Group  HostGroupName
      0  G000
%
```

A.5 Setting a Host Group Option

To set a host group option for each host group:

1. From the command prompt, register the subsystem (array unit) in which you want to set the host group option information and connect to the subsystem.
2. Execute the `auhgopt` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1
   - Host Connection Mode 1: Standard
   - Host Connection Mode 2: UA(06/2A00) suppress Mode

   Example:

```
% auhgopt -unit df700 -set 0 A -gno 1 -HostConnection standard -UASuppress enable
Password: manager-password
Are you sure you want to set the host group option? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the host group from the
host.
Before setting, stop access to the host group from the host.
Do you want to continue processing? (y/n [n]): y
The host group option has been set successfully.
%
```

A.6 Setting Logical Units (LU Mapping)

To set Logical Units to be recognized by each host to each host group:

1. From the command prompt, register the subsystem (array unit) in which you want to set the logical unit mapping information and connect to the subsystem.
2. Execute the `auhgmap` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1
   - Logical Unit to be recognized by the host: 0
   - Subsystem internal Logical Unit: 0

     It is necessary to set **Enable** to **Mapping Mode** for setting LU Mapping.

   Example:

```
% auhgmap -unit df700 -add 0 A 1 0 0
Password: manager-password
The mapping information has been set successfully.
%
```

4. Specify as shown, when setting the following information:

   Example:

```
% auhgmap -unit df700 -refer
Password: manager-password
Mapping mode = ON
Port  Group         H-LUN  LUN
  0A  001:win001        0    0
%
```

A.7 Adding a WWN

The WWNs of HBAs are set to each host group (see section A.7.1).

When a Port is connected to a host, WWNs of HBAs that are listed in **Logined WWN** can be selected and added to the host group (see A.7.2).

For the process of obtaining WWN information, refer to Appendix B.

A.7.1 Adding a WWN

To add a WWN:

1. From the command prompt, register the subsystem (array unit) in which you want to set the WWN information and connect to the subsystem.
2. Execute the `auhgwwn` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1
   - Host information (port name): 200000e069402a08
   - WWN nickname: win001

   Example:

```
%auhgwwn -unit df700 -set -permhg 0 A 200000e069402a08 -wname win001
         -gno 1
Password: manager-password
The security information has been set successfully.
%
```

4. Specify the following information:

   Example (AMS500):

```
% auhgwwn -unit df700 -refer
Password: manager-password
Port  0A  host group Security  ON
  Logined WWN
    Name      Port name
  Assigned WWN
    Name      Port name          host group
    win001    200000E069402A08   001:win001
  Assignable WWN
Port  0B  host group Security  OFF
Port  1A  host group Security  OFF
Port  1B  host group Security  OFF
%
```

A.7.2 Selecting and Adding an Assignable WWN

To display the Assignable WWN list and to assign the WWN on the Assignable WWN list:

1. From the command prompt, register the subsystem (array unit) in which you want to set the WWN information and connect to the subsystem.
2. Execute the `auhgwwn` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 0

Example:

```
% auhgwwn -unit df700 -refer -permhg 0 A -gno 0
Password: manager-password
Port  0A  host group Security  ON
  Assigned WWN
    Name      Port name          host group
  Assignable WWN
    Name      Port name
              10000000C9290680
% auhgwwn -unit df700 -assign -permhg 0 A 10000000C9290680 -gno 0
Password: manager-password
The security information has been set successfully.
% auhgwwn -unit df700 -refer -permhg 0 A -gno 0
Password: manager-password
Port  0A  host group Security  ON
  Assigned WWN
    Name      Port name          host group
              10000000C9290680   000:G000
  Assignable WWN
    Name      Port name
%
```

A.8 Changing a Host Group Name

To change a host group name:

1. From the command prompt, register the subsystem (array unit) in which you want to change the host group name and connect to the subsystem.
2. Execute the `auhgdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1
   - Current host group name: win001
   - New host group name: win002

   Example:

```
% auhgdef -unit df700 -chg 0 A -gno 1 -newgname win002
Password: manager-password
Are you sure you want to change the name of host group? (y/n [n]): y
Host group information has been set successfully.
%
```

A.9 Deleting a Host Group

To delete a host group:

1. From the command prompt, register the subsystem (array unit) in which you want to delete the host group and connect to the subsystem.
2. Execute the `auhgdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1

Example:

```
% auhgdef -unit df700 -rm 0 A -gno 1
Password: manager-password
Are you sure you want to delete specified host group(s)? (y/n [n]): y
After setting, access from hosts associated with the host group will be denied.
Do you want to continue processing? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the host group from the
host. Do you want to continue processing? (y/n [n]): y
Host group information has been set successfully.
%
```

A.10 Initializing Host Group 0

To initialize the host group:

1. From the command prompt, register the subsystem (array unit) in which you want to initialize the specified host group 0 and connect to the subsystem.
2. Execute the `auhgdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A

Example:

```
% auhgdef -unit df700 -init 0 A
Password: manager-password
Are you sure you want to initialize host group 0? (y/n [n]): y
After setting, access from hosts associated with the host group 0 will be denied.
Do you want to continue processing? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the host group from the
host. Do you want to continue processing? (y/n [n]): y
Host group information has been set successfully.
%
```

A.11 Changing a WWN

To change a WWN:

1. From the command prompt, register the subsystem (array unit) in which you want to change the WWN information and connect to the subsystem.
2. Execute the `auhgwwn` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 1
   - Host information (port name): 200000e069402a08
   - WWN nick name: winNT01

   Example:

```
%auhgwwn -unit df700 -chg -rename 0 A 200000e069402a08 -gno 1
         -newwname winNT01
Password: manager-password
The security information has been set successfully.
%
```

4. Specify the following information:

   Example:

```
% auhgwwn -unit df700 -refer
Password: manager-password
Port  0A  host group Security  ON
  Logined WWN
    Name      Port name
  Assigned WWN
    Name      Port name          host group
    winNT01   200000E069402A08   001:win001
  Assignable WWN
Port  0B  host group Security  OFF
Port  1A  host group Security  OFF
Port  1B  host group Security  OFF
%
```

A.12 Deleting a WWN

To delete the WWN on the assigned WWN list:

1. From the command prompt, register the subsystem (array unit) in which you want to delete the WWN information and connect to the subsystem.
2. Execute the `auhgwwn` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host group number: 0
   - Host information (port name): 200000e069402a08

   Example:

```
% auhgwwn -unit df700 -rm -permhg 0 A 200000e069402a08 -gno 0
Password: manager-password
The security information has been set successfully.
%
```

4. Specify the following information:

   Example:

```
% auhgwwn -unit df700 -refer -permhg 0 A -gno 0
Password: manager-password
Port  0A  host group Security  ON
  Assigned WWN
    Name      Port name          host group
  Assignable WWN
    Name      Port name
              200000E069402A08
%
```

A.13 Deleting a Logined WWN

To display and delete the logined WWN on the logined WWN list:

1. From the command prompt, register the subsystem (array unit) in which you want to delete the WWN information and connect to the subsystem.
2. Execute the `auhgwwn` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Host information (port name): 200000e069402a08

Example:

```
% auhgwwn -unit df700 -refer -login 0 A
Password: manager-password
Port  0A  host group Security  ON
  Logined WWN
    Name       Port name
    Linux      200000E069402A08
               10000000C9290680

% auhgwwn -unit df700 -rm -perm 0 A 200000e069402a08
Password: manager-password
Are you sure you want to delete selected WWN? (y/n [n]): y
The security information has been set successfully.
%
```

A.14 Adding a Target

To create a target for each Port, you must:

- Set the Target Security to enable for each port
- Create a target

A.14.1 Setting the Target Security

The Target Security default setting is **disable** for each port.

To set the Target Security to be valid or invalid:

1. From the command prompt, register the subsystem in which you want to set the target security information and connect to the subsystem.
2. Execute the `autargetini` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A

   Use **off** with **-tgs** option, when disabled LUN Manager is changed.

   Example (AMS500):

```
% autargetini  -unit df700 -set -tgs 0 A on
Password: manager-password
Are you sure you want to enable the target security on port0A? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the port from the host.
Before setting, stop access to the port from the host.
Do you want to continue processing? (y/n [n]): y
The initiator information has been set successfully.
%
```

4. Specify when the information has been set:

   Example:

```
% autargetini  -unit df700 -refer
Port  0A  Target Security  ON
  Target                Name            iSCSI Name
Port  0B  Target Security  OFF
Port  1A  Target Security  OFF
Port  1B  Target Security  OFF
%
```

A.14.2 Adding a Target

To create targets for each Port:

1. From the command prompt, register the subsystem in which you want to set the target information and connect to the subsystem.
2. Execute the `autargetdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1
   - Target 1 alias: win001
   - Target 1 iSCSI name: iqn.ams500-1
   - Authentication Method: None

   Example:

```
% autargetdef -unit df700 -add 0 A -tno 1 -tname win001 -ialias iqn.ams500-1
             -authmethod None
Password: manager-password
Are you sure want to add the target information? (y/n [n]): y
Please input Secret.
Secret: authentication-password
Re-enter Secret: authentication-password
The target information has been added successfully.
%
```

4. Specify the following information:

   Example:

```
% autargetdef -unit df700 -refer
Port  0A
                      Authentication                  Mutual
  Target              Method         CHAP Algorithm   Authentication User Name

                                                          iSCSI Name
  000:T000            CHAP           MD5              Enable         iqn.1994-
04.jp.co.hitachi:rsd.d7m.t.00018.0a000

                                                          iqn.1994-
04.jp.co.hitachi:rsd.d7m.t.00018.0a000
  001:win001          None           ---              ---            ---

                                                          iqn.ams500-1
Port 0B
                      Authentication                  Mutual
  Target              Method         CHAP Algorithm   Authentication User Name
    :
    :
%
```

A.15 Setting a Target Option

To set a target option for each target:

1. From the command prompt, register the subsystem in which you want to set the target option information and connect to the subsystem.
2. Execute the `autargetopt` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1
   - Host Connection Mode 1: Standard
   - Host Connection Mode 2: UA(06/2A00) suppress Mode

   Example:

```
% autargetopt -unit df700 -set 0 A -tno 1 -HostConnection standard -UASuppress enable
Password: manager-password
Are you sure you want to set the target option? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the target from the host.
Before setting, stop access to the host group from the host.
Do you want to continue processing? (y/n [n]): y
The target option has been set successfully.
%
```

A.16 Setting Logical Units

To set Logical Units to be recognized by each host to each target:

Note: This process is called LU Mapping.

1. From the command prompt, register the subsystem in which you want to set the logical unit mapping information and connect to the subsystem.
2. Execute the `autargetmap` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1
   - Logical Unit to be recognized by the host: 0
   - Subsystem internal Logical Unit: 0

     It is necessary to set **Enable** to **Mapping Mode** for setting LU Mapping.

   Example:

```
% autargetmap -unit df700 -add 0 A 1 0 0
Password: manager-password
Are you sure you want to add the mapping information? (y/n [n]): y
The mapping information has been set successfully.
%
```

4. Specify the following information:

   Example:

```
% autargetmap -unit df700 -refer
Mapping mode = ON
Port  Target               H-LUN    LUN
  0A  001:win001           0          0
%
```

A.17 Adding an Initiator

The iSCSI Name of each HBA is set to each target and is used to identify hosts.

When a port is connected to a host, an iSCSI name of an HBA listed in **Detected Initiator** can be selected and added to the target.

1. From the command prompt, register the subsystem in which you want to set the initiator information and connect to the subsystem.
2. Execute the `autargetini` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1
   - Initiator name: Linux
   - iSCSI Name: iqn.1991-05.com

   Example:

```
%autargetini -unit df700 -add 0 A -tno 1 -iname Linux -ininame iqn.1991-05.com
Password: manager-password
Are you sure you want to add the initiator information? (y/n [n]): y
The initiator information has been set successfully.
%
```

A.18 Changing Target Information

To change target information:

1. From the command prompt, register the subsystem in which you want to change the target information and connect to the subsystem.
2. Execute the `autargetdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1
   - Current target alias: win001
   - New target name: win002

Example:

```
% autargetdef -unit df700 -chg 0 A -tno 1 -newtalias win002
Password: manager-password
Are you sure you want to change the target information (y/n [n]): y
After setting except Alias, access from hosts associated with the target will be
denied.
Do you want to continue processing? (y/n [n]): y
When setting starts, the subsystem stops accepting access from its related hosts
 to the target abnormally.
Before setting, be sure to stop access from the hosts to the target.
Do you want to continue processing? (y/n [n]): y
Please input Secret.
Secret: secret-password
Re-enter Secret: secret-password
The target information has been changed successfully.
%
```

A.19 Deleting a Target

To delete a target:

1. From the command prompt, register the subsystem in which you want to delete the target and connect to the subsystem.
2. Execute the `autargetdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1

Example:

```
% autargetdef -unit df700 -rm 0 A -tno 1
Password: manager-password
Are you sure you want to delete specified target? (y/n [n]): y
After setting, access from hosts associated with the target will be denied.
Do you want to continue processing? (y/n [n]): y
When setting starts, the subsystem stops accepting access to the target from the host.
Do you want to continue processing? (y/n [n]): y
The targets has been deleted successfully.
%
```

A.20 Initializing Target 0

To initialize Target 0:

1. From the command prompt, register the subsystem in which you want to initialize the specified Target 0 and connect to the subsystem.
2. Execute the `autargetdef` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A

Example:

```
% autargetdef -unit df700 -init 0 A
Password: manager-password
Are you sure you want to initialize target 0? (y/n [n]): y
After setting, access from hosts associated with the target will be denied.
Do you want to continue processing? (y/n [n]): y
The target 0 has been initialized successfully.
%
```

A.21 Changing Initiator Information

To change Initiator Information:

1. From the command prompt, register the subsystem in which you want to change the initiator information and connect to the subsystem.
2. Execute the `autargetini` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Current iSCSI Name: iqn.ams500-1
   - New iSCSI Name: iqn.1994-04.com

   Example:

```
%autargetini -unit df700 -chg 0 A -iname iqn.ams500-1 -newiname iqn.1991-04.com
Password: manager-password
Are you sure you want to change the initiator information? (y/n [n]): y
The initiator information has been changed successfully.
%
```

A.22 Deleting an Initiator

To delete an Initiator:

1. From the command prompt, register the subsystem in which you want to delete the initiator and connect to the subsystem.
2. Execute the `autargetini` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 1
   - Initiator name: iqn.1994-04.com

Example:

```
%autargetini -unit df700 -rm 0 A -tno 1 -iname iqn.1994-04.com
Password: manager-password
Are you sure you want to delete the initiator information? (y/n [n]): y
The initiator information has been deleted successfully.
%
```

A.23 Adding a CHAP User

To add a CHAP User:

1. From the command prompt, register the subsystem in which you want to add the CHAP User and connect to the subsystem.
2. Execute the `auchapuser` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - Target number: 0
   - CHAP User name: mng001

Example:

```
%auchapuser -unit df700 -add 0 A -user mng001 -tno 0
Password: manager-password
Are you sure you want to add the CHAP user information? (y/n [n]): y
Please input Secret.
Secret: authentication-password
Re-enter Secret: authentication-password
The CHAP user information has been added successfully.
%
```

A.24 Changing CHAP User Information

To change CHAP User information:

1. From the command prompt, register the subsystem in which you want to change the CHAP User information and connect to the subsystem.
2. Execute the `auchapuser` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - CHAP User name: mng001
   - Current assigned target number: 0
   - New assigned target number: 1

Example:

```
%auchapuser -unit df700 -assign 0 A -user mng001 -tno 1
Password: manager-password
Are you sure you want to assign the target? (y/n [n]): y
The target has been assigned successfully.
%
```

A.25 Deleting CHAP User

To delete a CHAP User:

1. From the command prompt, register the subsystem in which you want to delete the CHAP User and connect to the subsystem.
2. Execute the `auchapuser` command to specify the subsystem.
3. Use the following settings:
   - Subsystem name: df700
   - Controller: 0
   - Port: A
   - CHAP User name: mng001

Example:

```
%auchapuser -unit df700 -rm 0 A -user mng001
Password: manager-password
Are you sure you want to delete the CHAP user information? (y/n [n]): y
The CHAP user information has been deleted successfully.
%
```

Appendix B Using the WWN Change Operation when the HBA is Replaced

If you replace an HBA of the host (server) using LUN Manager, you must change the associated WWN setting of LUN Manager.

In this appendix:

- WWN Change Procedure when an HBA is Replaced (section B.1)
- Obtaining the WWN of a Host (section B.2)

B.1 WWN Change Procedure when an HBA is Replaced

To change a WWN when an HBA is replaced:

1. Check the WWN before and after HBA replacement.

   (For checking the WWN after HBA replacement, see section B.2.)

2. Change the WWN before HBA replacement to the WWN after HBA replacement by the following LUN Manager setting procedure.

   (For further information about changing the settings, see section 4.8.)

3. Restart the host with the replaced HBA. Verify that the LU was recognized; this verification must occur before HBA replacement can be recognized after the replacement. If the LU is not recognized, LUN Manager was not correctly set. Repeat Step 2 to set the WWN again.

B.2 Obtaining the WWN of a Host

The port name and N_port ID of a host (required as host identification information) can be obtained using the host console.

This section explains how to obtain the WWN of a host on the following systems:

- Solaris™
- HP-UX
- AIX®
- IRIX®
- Windows NT®/Windows® 2000/2003
- BladeSymphony Server

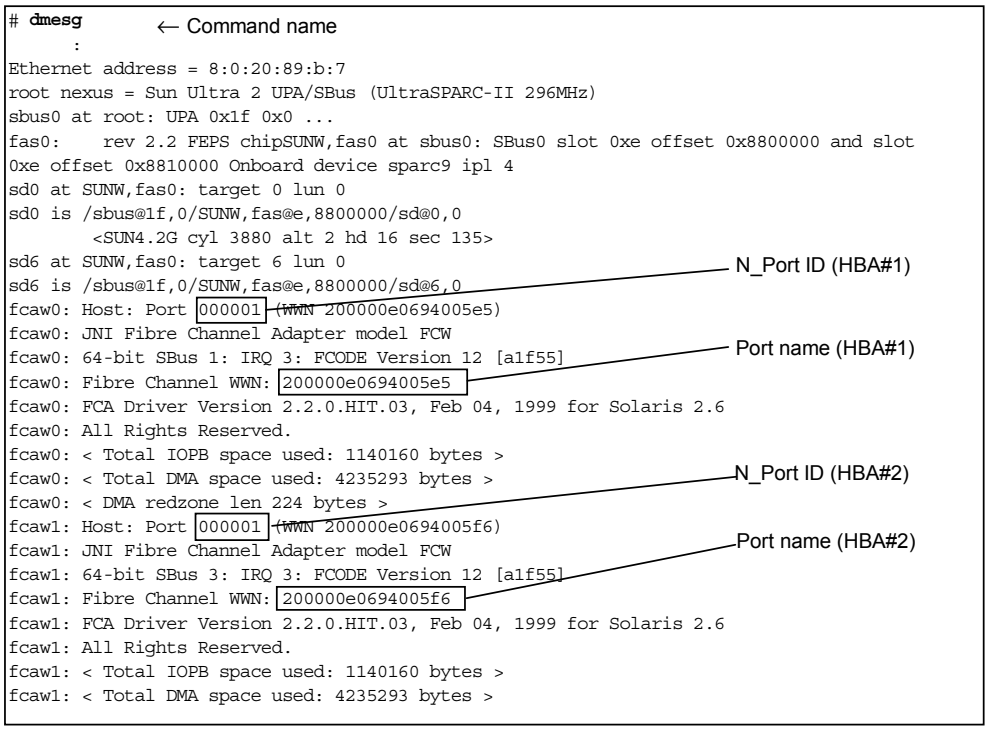
B.2.1 Solaris™

There are two methods for obtaining the WWN of a host:

Method 1:

To obtain the WWN of a host when the JNI HBA is FC64-1063 or FCI-1063 (driver version HIT.06.01 earlier):

1. Execute the following command to obtain the WWN of the HBA.



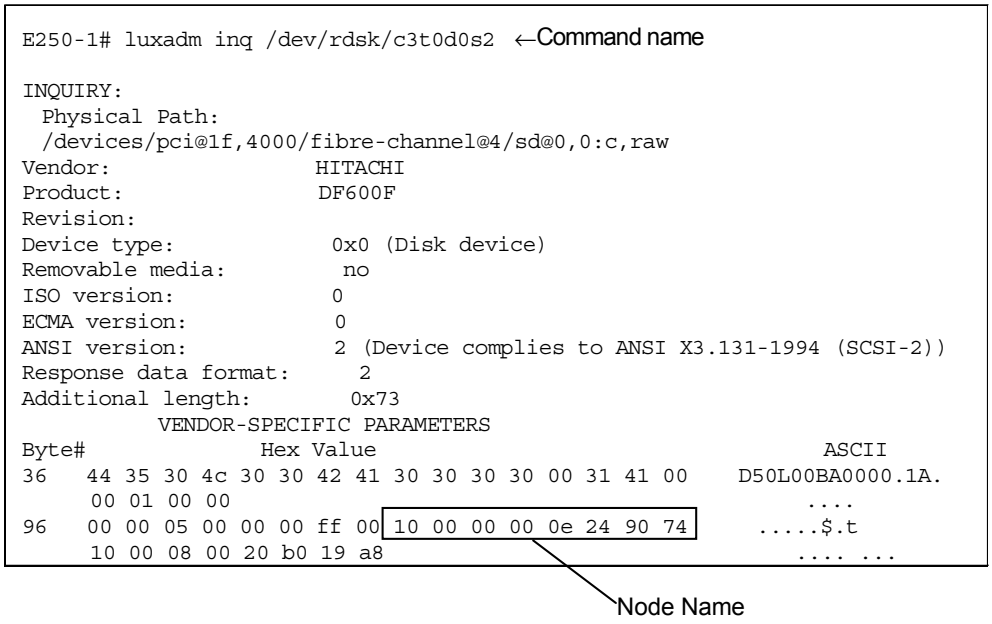
2. Read and record the port name and the N_Port ID.

Method 2:

When the JNI HBA is FC64-1063 or FCI-1063 (driver version HIT.07 later), or FCE-1063, FCE-6410, FCE-6460, FCE-1473, FCC-6460, the system parameters of the subsystem must be changed.

1. Execute the following command to obtain the file name of the HBA.

   Example:



2. Refer to the node name shown in the previous output example. The port name can be obtained from the node name. When the node name is 100000000e249074, the port name is obtained through replacement of the top byte, that is, 10 with 20. In this case, the port name is 200000000e249074.

   Example:

   Node name: 100000000e249074

   ↓

   Port name: 200000000e249074

To determine an HBA Location:

Identify the WWN using the WWN label attached to the JNI HBA.

B.2.2 HP-UX

To obtain the WWN of a host when the HP HBA is A3404A, A3740A, A5158A, A6684A, A6685A, or A6795A:

1. Execute the following command to obtain the file name of the HBA.

   Example:

```
# ioscan -nfC fc
Class   I H/W Path Driver S/W State  H/W Type   Description
=============================================================
fc    0 0/4/0/0  fcT1 UNCLAIMED  UNKNOWN    PCI SerialBus (107e0004)
fc    1 0/5/0/0  fcT1 UNCLAIMED  UNKNOWN    PCI SerialBus (107e0004)
fc    2 0/8/0/0  td CLAIMED   INTERFACE  HP Tachyon TL/TS Fibre Channel Mass S
torage Adapter
                 /dev/td2          <-- Device file Name
fc    3 0/12/0/0 td CLAIMED   INTERFACE  HP Tachyon TL/TS Fibre Channel Mass S
torage Adapter
                 /dev/td3          <-- Device file Name
fc    4 1/10/0/0  fcT1 UNCLAIMED  UNKNOWN    PCI SerialBus (107e0004)
fc    5 1/12/0/0  fcT1 UNCLAIMED  UNKNOWN    PCI SerialBus (107e0004)
```

2. Refer to the device file name shown in the output example above. In this example, the device file names are: /dev/td2 and /dev/td3.

3. Using the device file names shown above, execute the command shown in the following example to obtain the WWN of the HBA.

   Example:

```
# fcmsutil /dev/td3
              Vendor ID is = 0x00103c
              Device ID is = 0x001028
        TL Chip Revision No is = 2.3
     PCI Sub-system Vendor ID is = 0x00103c
         PCI Sub-system ID is = 0x000006
           Previous Topology = PTTOPT_FABRIC
          Local N_Port_id is = 0x011600
     N_Port Node World Wide Name = 0x50060b000008829f   <-- Node Name
     N_Port Port World Wide Name = 0x50060b000008829e   <-- Port Name
             Driver state = AWAITING_LINK_UP
           Hardware Path is = 0/12/0/0
       Number of Assisted IOs = 504123690
   Number of Active Login Sessions = 0
```

4. Refer to the port name shown in the example above.

To determine an HBA Location:

When HP-UX is running in HP9000, you may not be able to match the HBA with the WWN because there is no way to identify the HBA address based on the slot location. In this case, correlate the HBA with a WWN using the following procedure:

1. Connect the host and the subsystem, and then start the system.
2. Execute the following command to obtain the device file name of the HBA.

   Example:

```
# ioscan -nfC fc
Class   I H/W Path Driver S/W State  H/W Type   Description
=============================================================
fc    0 0/4/0/0  fcT1 UNCLAIMED  UNKNOWN   PCI SerialBus (107e0004)
fc    1 0/5/0/0  fcT1 UNCLAIMED  UNKNOWN   PCI SerialBus (107e0004)
fc    2 0/8/0/0  td  CLAIMED   INTERFACE  HP Tachyon TL/TS Fibre Channel Mass S
torage Adapter                  Address of /dev/td2
          /dev/td2                                    Device file Name
fc    3 0/12/0/0  td  CLAIMED   INTERFACE  HP Tachyon TL/TS Fibre Channel Mass S
torage Adapter                  Address of /dev/td3
          /dev/td3                                    Device file Name
fc    4 0/10/0/0  fcT1 UNCLAIMED  UNKNOWN   PCI SerialBus (107e0004)
fc    5 0/12/0/0  fcT1 UNCLAIMED  UNKNOWN   PCI SerialBus (107e0004)
```

3. Disconnect the Fibre channel cable of the HBA of the WWN that you want to identify.
4. Determine which disk is currently connected and its correspondence with the device file of the HBA.

   Example:

```
# ioscan -nfC disk
Class    I  H/W Path     Driver  S/W State  H/W Type    Description
=============================================================================
disk     0  0/0/1/0.2.0   sdisk   CLAIMED    DEVICE     HP     DVD-ROM 6x/32x
                   /dev/dsk/c0t2d0  /dev/rdsk/c0t2d0
disk     1  0/0/2/0.6.0   sdisk   CLAIMED    DEVICE     SEAGATE ST39102LC
                   /dev/dsk/c1t6d0  /dev/rdsk/c1t6d0
disk     2  0/0/2/1.6.0   sdisk   CLAIMED    DEVICE     SEAGATE ST39103LC
                   /dev/dsk/c2t6d0  /dev/rdsk/c2t6d0
disk   169  0/8/0/0.1.19.232.0.0.0  sdisk   CLAIMED    DEVICE     HITACHI DF600F
                   /dev/dsk/c19t0d0  /dev/rdsk/c19t0d0
disk   170  0/8/0/0.1.19.232.0.0.1  sdisk   CLAIMED    DEVICE     HITACHI DF600F
                   /dev/dsk/c19t0d1  /dev/rdsk/c19t0d1
        :                  HBA address                    not connected
disk   141  0/12/0/0.1.19.228.0.0.0 sdisk   NO_HW      DEVICE     HITACHI DF600F
                   /dev/dsk/c21t0d0  /dev/rdsk/c21t0d0
disk   297  0/12/0/0.1.19.228.0.0.1 sdisk   NO_HW      DEVICE     HITACHI DF600F
                   /dev/dsk/c21t0d1  /dev/rdsk/c21t0d1
        :
```

   As indicated in the above example, the disks identified as NO-HW are not connected. According to this information and the address of the device file of the HBA, the device file name of the HBA, whose cable has been disconnected, is: /dev/td3.

   Execute the `fcmsutil` command to obtain the WWN of the /dev/td3.

5. Plug in the disconnected Fibre channel cable.

B.2.3 AIX®

To obtain the WWN of a host when the IBM® is FC6227 or FC6228:

1. Execute the following command to obtain the device file name of the HBA:

   Example:

```
# lsparent -C -k iocb
    fcs0 Available 27-08 FC Adapter
    fcs1 Available 3A-08 FC Adapter
    fcs2 Available 31-08 FC Adapter
```

   device file Name

2. Refer to the Device file name shown in the example above. In this example, the device file names are: fcs0, fcs1, fcs2, and fcs3.

3. Using the device file names given in the previous example, execute the following example to obtain the WWN of the HBA.

   Example:

```
# lscfg -vl fcs0
DEVICE            LOCATION          DESCRIPTION

fcs0              27-08             FC Adapter

      Part Number.................09P1162
      EC Level....................D
      Serial Number...............KT04904230
      Manufacturer................0010
      FRU Number..................09P1173
      Network Address.............10000000C925437E
      ROS Level and ID............02903290
      Device Specific.(Z0)........4002206D
      Device Specific.(Z1)........10020193
      Device Specific.(Z2)........3001506D
      Device Specific.(Z3)........02000909
      Device Specific.(Z4)........FF101450
      Device Specific.(Z5)........02903290
      Device Specific.(Z6)........06113290
      Device Specific.(Z7)........07113290
      Device Specific.(Z8)........20000000C925437E
      Device Specific.(Z9)........SS3.22A0
      Device Specific.(ZA)........S1F3.22A0
      Device Specific.(ZB)........S2F3.22A0
      Device Specific.(YL)........P1-I8/Q1
```

   Port Name

   The value shown in the Network Address section in the output example above is the port name.

To determine an HBA Location:

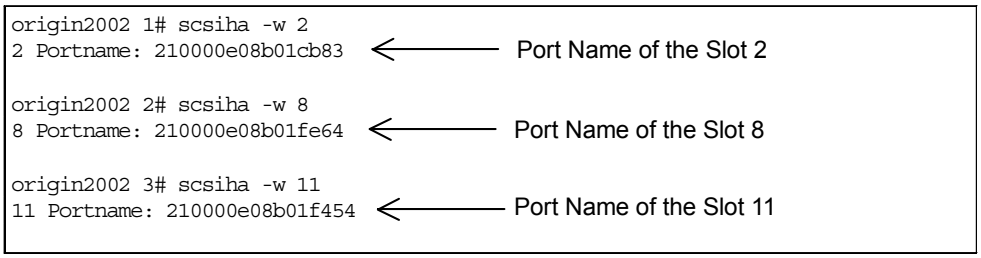
Identify the WWN using the WWN label attached to the **IBM®** HBA.

B.2.4 IRIX®

To obtain the WWN of a host when the SGI™ is XT-FV-1PORT:

1. Execute the following command to obtain the WWN of the HBA:

   Example:



2. Refer to the port name shown in the output example above.

To determine an HBA Location:

The location and arrangement of slots vary, depending upon the model of SGI™ server. Match the HBA and WWN by referring to the slot location of each model.

B.2.5 Windows NT®/ Windows® 2000/2003

There are two methods for obtaining the WWN of a host:

- Emulex® Port Driver/SCSI Miniport Driver
- Qlogic® QLA2460/QLA2462/QLE2460/QLE2462/QLA2200F/QLA2300F

B.2.5.1 Emulex® Port Driver

When the Emulex® driver is installed on the host, the Emulex® Configuration Tool (elxcfg.exe) is installed on Windows NT®/Windows® 2000/2003. Run the Emulex® Configuration Tool to obtain the WWN of the host. Follow these steps:

1. Start the **elxcfg.exe**.
2. Double-click **HBA** to obtain the **WWN** on the Available Adapter list. (Adapters corresponding to the number of installed HBAs are displayed.)
3. The **Port WWN** (Port Name) and **Node WWN** (Node Name) are displayed in the **Adapter Information** screen.
4. When two or more HBAs are installed, repeat Steps 2 and 3.

B.2.5.2 Emulex® SCSI Miniport Driver

When the Emulex® driver is installed on the host, the LightPulse™ Utility/NT (lputilnt.exe) is installed on Windows NT®/Windows® 2000/2003. Run the LightPulse™ Utility/NT to obtain the WWN of the host. Follow these steps:

1. Start the **lputilnt.exe**.
2. Select **Adapter X** on the display. (Adapters corresponding to the number of installed HBAs are displayed.)
3. Select **Adapter Revision Levels** from the **Category** menu.

   IEEE Address XX-XX-XX-XX-XX-XX (6 bytes) appears on the bottom of the screen.
4. Enter **10-00** before the IEEE Address XX-XX-XX-XX-XX-XX. This is a port name.

   Example:

   `10-00-XX-XX-XX-XX-XX-XX`

   The node name is equal to the port name.

   The N_Port ID is omitted.
5. When two or more HBAs are installed, repeat Steps 2 through 7.

Note: The LightPulse™ Utility/NT is supported by the Emulex® driver of version 4.2 or later. If the version is earlier than 4.2, check the IEEE Address by the label on the board.

B.2.5.3 Qlogic® QLA2460/QLA2462/QLE2460/QLE2462

To obtain the WWN of a host on Windows NT®:

1. When the host starts up or when the QLA2460/QLA2462/QLE2460/QLE2462 board is initialized for rebooting, the message **Press<CTL-Q> for Fast!UTIL** appears.

   Press CTRL-Q and the Qlogic® Fast!UTIL utility starts.

2. Select an adapter corresponding to the HBA.

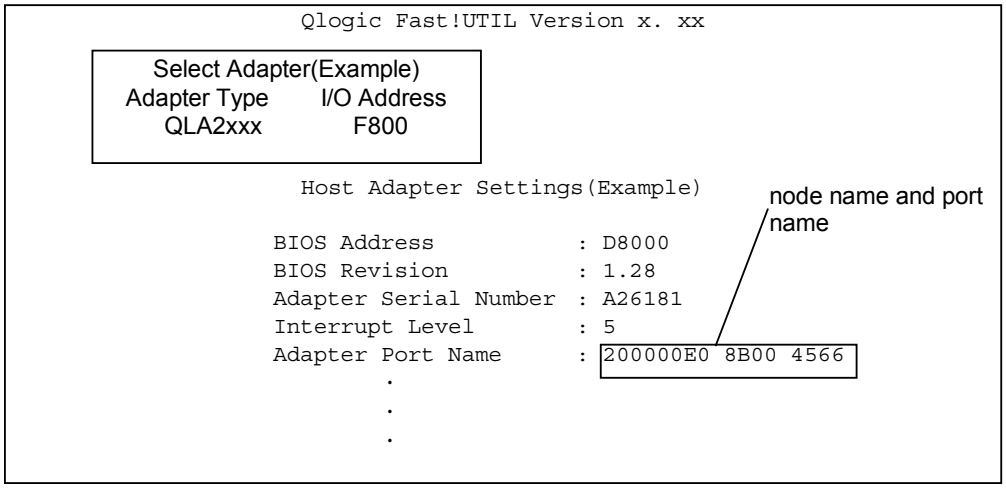
3. Select **Configuration Settings** from the Fast!UTIL option and press **Enter**.

4. Select **Adapter Settings** from Configuration Setting and press **Enter**.

   Read the value in the Adapter Port Name field on the Adapter Settings window. This contains the node name and the port name of the host (set for security).

5. If multiple HBAs are installed, repeat Steps 2 through 5 for each one.

Example:



B.2.5.4 Qlogic® QLA2200F/QLA2300F

To obtain the WWN of a host on Windows NT®:

1. When the host starts up or when the QLA2200F/QLA2300F board is initialized for rebooting, the message **Press<ALT-Q> for Fast!UTIL** appears.

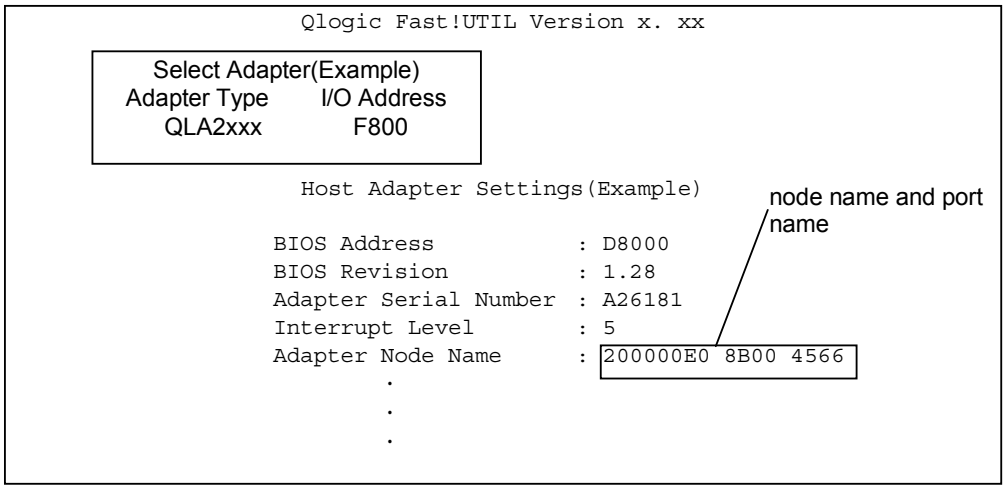
   Press ALT-Q and the Qlogic® Fast!UTIL utility starts.

2. Select an adapter corresponding to the HBA.
3. Select **Configuration Settings** from the **Fast!UTIL** option and press **Enter**.
4. Select **Host Adapter Settings** from Configuration Setting and press **Enter**.

   Read the value in the Adapter Node Name field on the host Adapter Settings window. This contains the node name and the port name of the host (set for security).

5. If multiple HBAs are installed, repeat Steps 2 through 5 for each one.

Example:



B.2.6 BladeSymphony Server

The WWN of a host is written on the HBA board.

Appendix C Verifying and Setting the Queue Depth

In this appendix:

- Overview of Queue Depth Configuration (section C.1)
- Solaris™ Queue Depth (section C.2)
- HP-UX Queue Depth (section C.3)
- AIX® Queue Depth (section C.4)
- IRIX® Queue Depth (section C.5)
- Windows NT®/Windows® 2000/2003 Queue Depth (section C.6)

C.1 Overview of Queue Depth Configuration

Multiple servers can be connected through one port. Since this increases commands that can be handled by one port, a decrease in system performance may occur if a set limit is exceeded. Do not exceed this limit per port.

Table C.1 The Queue Depth Configuration

Platform	HBA	Queue Depth		Unit of Setting
		Unit of Value	Default	
Solaris™		LU	256	OS
HP-UX		LU	8	LU
AIX®		LU	1	LU
IRIX®		LU	1	LU
Windows®	Emulex® (Port)	LU	8	HBA
	Emulex® (MiniPort)	LU	32	HBA
	Qlogic®	Port	16	HBA

C.2 Solaris™ Queue Depth

Verifying Queue Depth

Execute the following command to verify queue depth set for a Solaris™ system.

Example:

```
# adb -k /dev/ksyms /dev/mem
physmem 7171
sd_max_throttle/D
sd_max_throttle:
sd_max_throttle:                64
```

Setting Queue Depth

1. Make a backup of the **/etc/system** file.
2. Edit the **/etc/system** file as shown in the example below.
3. Save your changes and exit the text editor.
4. Shutdown and reboot to apply the queue depth setting.

Example:

```
set sd:sd_max_throttle=64               <-- add this line to /etc/system file

set ssd:ssd_max_throttle=64             <-- add this line to /etc/system file
                                            (for SUN generic Host Bus Adapter)
```

C.3 HP-UX Queue Depth

The queue depth is set for the disk device managed by Logical Volume Manager (LVM).

Verifying Queue Depth

Execute the following command to verify the queue depth set for the HP system.

Example:

```
# scsictl -a /dev/rdsk/c22t1d0          <-- Verify the Queue Depth for device
file(c22t1d0)
immediate_report = 0; queue_depth = 8
#
```

Setting the Queue Depth

Execute the following command to set and verify the queue depth set for the HP system.

Example:

```
# scsictl -a -m queue_depth=32 /dev/rdsk/c22t1d0   <-- Set Queue Depth value(32) to the
device file
immediate_report = 0; queue_depth = 8              (c22t1d0)
# scsictl -a /dev/rdsk/c22t1d0
immediate_report = 0; queue_depth = 32
#
```

The `scsictl` command allows you to view and change the queue depth parameter for each device one at a time. The queue depth resets to the default value the next time the system is restarted. You will need to create and register a start-up script to set queue depth for the disk array subsystem each time you restart.

C.4 AIX® Queue Depth

Before installing the Hitachi Dynamic Link Manager™, you should set the queue depth to LUs.

Verifying Queue Depth

Execute the following command to verify the Queue Depth set for the AIX® system.

Example:

```
# lsattr -El hdisk1                                    <-- show the Device Parameter
for hdisk1
scsi_id       0xe8               SCSI ID                          False
lun_id        0x1000000000000    Logical Unit Number ID           False
location                         Location Label                   True
ww_name       0x50060e8000427730 FC World Wide Name               False
pvid          none               Physical volume identifier       False
queue_depth   32                Queue DEPTH                     True     <-- Queue Depth of
hdisk1
q_type        simple             Queuing TYPE                     True
q_err         yes                Use QERR bit                     True
clr_q         no                 Device CLEARS its Queue on error True
rw_timeout    30                 READ/WRITE time out value        True
start_timeout 60                 START unit time out value        True
reassign_to   120                REASSIGN time out value          True
#
```

Setting the Queue Depth

Execute the following command to set the Queue Depth set for the AIX® system.

Example:

```
# chdev -l hdisk1 -a queue_depth=32
hdisk1 changed
#
```

C.5 IRIX® Queue Depth

Command tag queuing (CTQ) must be enabled to optimize the performance of the disk array subsystem. Since CTQ is disabled by default in IRIX® systems, you need to enable it and set the Queue Depth for each LU using the **fx** utility.

Setting the Queue Depth

Execute the following command to set the Queue Depth for the IRIX® system.

Example:

```
origin2002 9# fx -x "dksc(2,1,0)"      <-- Start the fx utility and enter LU
                                           (controller_number:2 drive_number:1
lun_number:0)
fx version 6.5, Jan  8, 2002
...opening dksc(2,1,0)
...drive selftest...OK
Scsi drive type == HITACHI DF600F

----- please choose one (? for help, .. to quit this menu)-----
[exi]t             [d]ebug/           [l]abel/           [a]uto
[b]adblock/        [exe]rcise/        [r]epartition/

fx> /label/set/param <-- Set the device parameter

fx/label/set/parameters: Error correction = (enabled)
fx/label/set/parameters: Data transfer on error = (enabled)
fx/label/set/parameters: Report recovered errors = (enabled)
fx/label/set/parameters: Delay for error recovery = (enabled)
fx/label/set/parameters: Err retry count = (0)
fx/label/set/parameters: Transfer of bad data blocks = (disabled)
fx/label/set/parameters: Auto bad block reallocation (write) = (enabled)
fx/label/set/parameters: Auto bad block reallocation (read) = (enabled)
fx/label/set/parameters: Read ahead caching = (enabled)
fx/label/set/parameters: Write buffering = (disabled)
fx/label/set/parameters: Drive disable prefetch = (0)
fx/label/set/parameters: Drive minimum prefetch = (0)
fx/label/set/parameters: Drive maximum prefetch = (0)
fx/label/set/parameters: Drive prefetch ceiling = (0)
fx/label/set/parameters: Enable CTQ = (disabled) enable     <-- Enter "enable"
fx/label/set/parameters: CTQ depth = (2) 64 <-- Enter desired Queue Depth
fx/label/set/parameters: Read buffer ratio = (0/256)
fx/label/set/parameters: Write buffer ratio = (0/256)
 * * * * * W A R N I N G * * * * *
about to modify drive parameters on disk dksc(2,1,0) ok? yes        <-- Enter "yes"

----- please choose one (? for help, .. to quit this menu)-----
[exi]t             [d]ebug/           [l]abel/           [a]uto
[b]adblock/        [exe]rcise/        [r]epartition/

fx> exi      <-- Exit the fx utility

label info has changed for disk dksc(2,1,0).  write out changes? (yes)

origin2002 10#
```

C.6 Windows NT®/Windows® 2000/2003 Queue Depth

Emulex® Port Driver

When the Emulex® driver is installed on the host, the Emulex® Configuration Tool (**elxcfg.exe**) is installed on Windows NT®/Windows® 2000/Windows® 2003. Run the Emulex® Configuration Tool to verify and set the Queue Depth to each HBA.

The port driver can set the Queue Depth for each LU.

1. Execute **elxcfg.exe**.
2. Select the HBA to set the Queue Depth on the Available Adapter list. (Adapters corresponding to the number of installed HBAs are displayed.)
3. Set the desired Queue Depth to the Maximum Queue Depth (see Figure C.1).

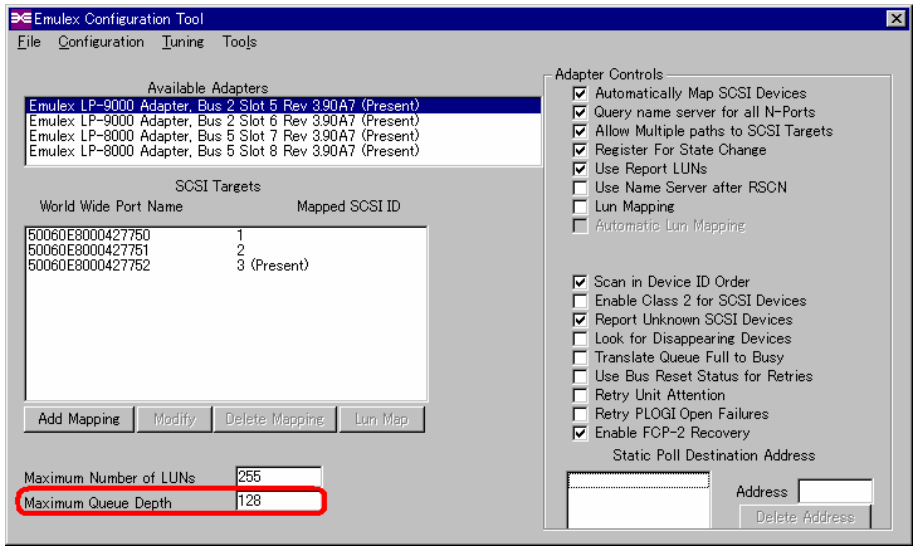


Figure C.1 Emulex® Configuration Tool

Emulex® SCSI Miniport Driver

When the Emulex® driver is installed on the host, the Emulex® Configuration Tool (elxcfg.exe) is installed on Windows NT®/Windows® 2000/Windows® 2003. Run the Emulex® Configuration Tool to verify and set the queue depth for each HBA.

The SCSI Miniport Driver can set the Queue Depth for each LU.

1. Start **lputilnt.exe**.
2. Select the HBA to set the Queue Depth on the display. (Adapters corresponding to the number of installed HBAs are displayed.)
3. Select the **Driver Parameters** in the Category drop-down list (refer the Figure C.2).
4. Double-click the Queue Depth parameter (refer the Figure C.3).
5. Set the desired Queue Depth as a hexadecimal value in the **Modify Driver Parameter** screen (refer the Figure C.4).

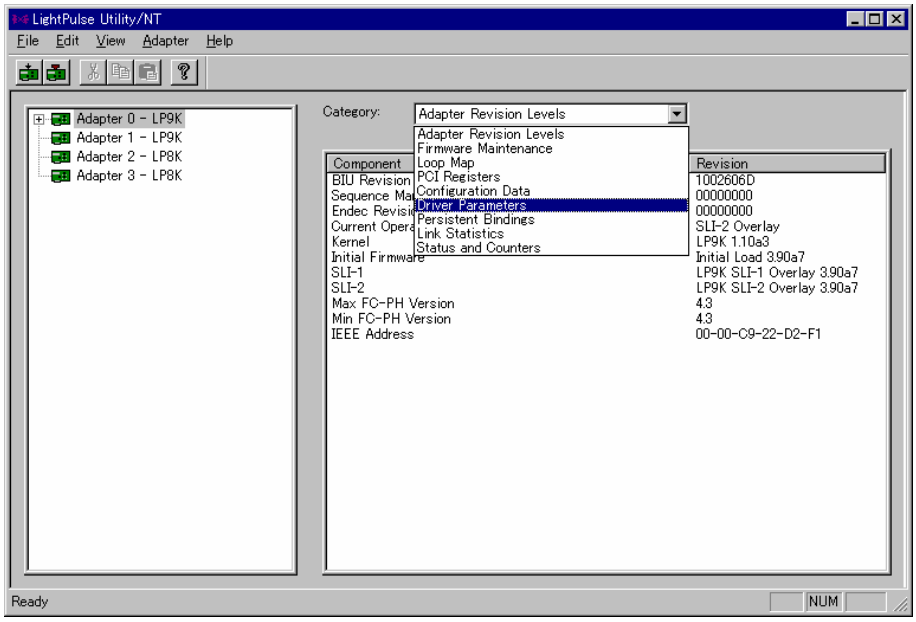


Figure C.2 Selecting the Drive Parameters

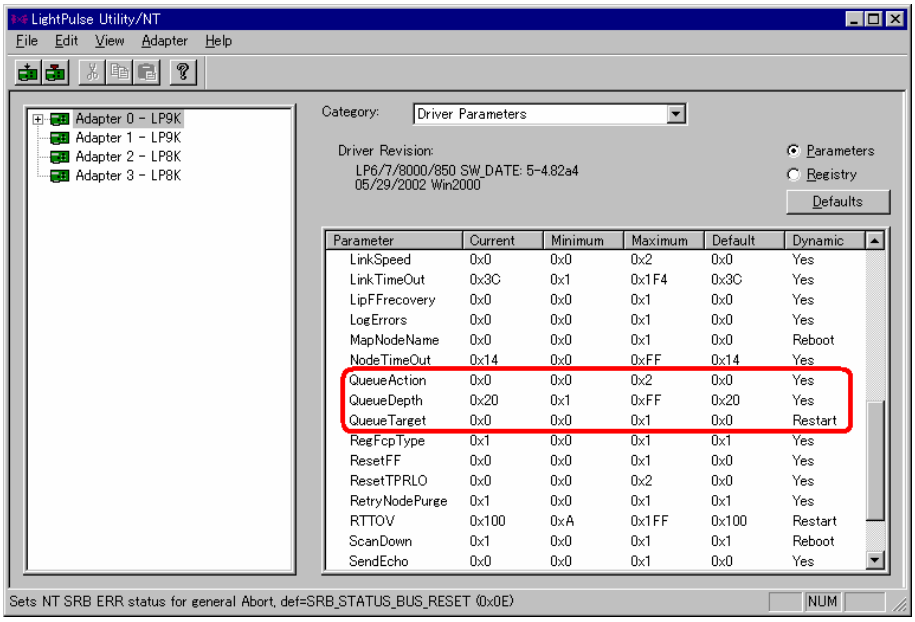


Figure C.3 Selecting the Queue Depth

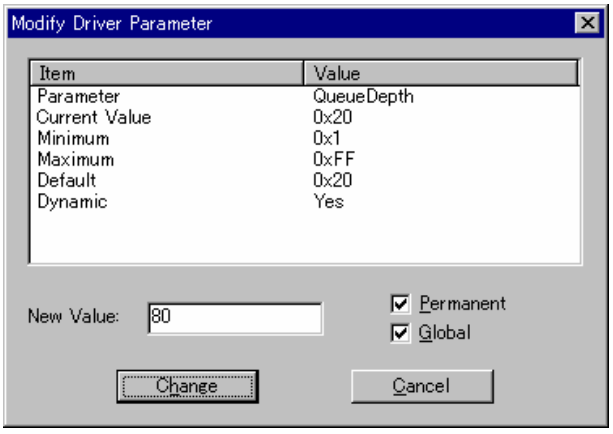


Figure C.4 Setting the Queue Depth Value

Qlogic® HBA

The Qlogic® HBA can set the Queue Depth for each LU.

1. When the host starts up, press the Q key while holding down the Ctrl or Alt key.
2. Select an adapter corresponding to the HBA. (Adapters corresponding to the number of installed HBAs are displayed.)
3. Select **Configuration Setting** and press the **Enter** key.
4. Select **Advanced Adapter Setting** and press the **Enter** key.
5. Set the desired queue depth to **Execution Throttle**.

Acronyms and Abbreviations

CLI	command line interface
CRC	Cyclic Redundancy Check
CTQ	command tag queuing
FC	Fibre Channel
GUI	graphical user interface
HBA	host bus adapter
H-LUN	host-logical unit number
IETF	Internet Engineering Task Force
iSCSI	Internet SCSI
iSNS	internet Storage Name Service
LU	logical unit
LUN	logical unit number
LUN Security	now known as SANtinel
LVM	Logical Volume Manager
NIC	network interface card
RFC	Request for Comments
SAN	Storage Area Network
SCSI	Small Computer Systems Interface
WWN	world wide name

Index