

Command View ESL/Secure Manager Mapping Algorithms



Overview.....	2
Abbreviations, Acronyms, and Definitions.....	2
Background Information	2
Interface Manager Modes: Automatic and Manual	2
Basic vs. Advanced Secure Manager	3
Interface Manager Discovery.....	3
Secure Manager Mapping Rules	4
1. Devices are ordered based on type and logical position (drive number)	4
2. Each map will start with LUN 0.....	5
3. New maps remove gaps in the LUN map, but modified maps leave them	5
4. If there is more than one FC port on a FC interface controller, load balancing algorithms are used.....	5
5. Maintain FC Port/LUN Map after cabling change on same Interface Controller.....	7
6. Advanced Secure Manager map creation is done like Basic Secure Manager but then removes devices and gaps if necessary	7
7. Maintain current FC Port/LUN assignments when adding devices in Advanced Secure Manager	8
8. If modifying an existing map to remove device access with Advanced Secure Manager any gap made is retained	9
9. If devices are removed and added with Advanced Secure Manager, attempts are made to not disturb the other device mappings	9
10. Active Fabric is the last LUN on a map of each FC port	11
A Note on Basic Secure Manager and Manual Mapping	13
Example 1 – ESL 9000, 2 1-Port IC’s, 8 Drives.....	14
Example 2 – ESL 9000, 2 1-Port IC’s, 8 Drives, Odd Cabling.....	15
Example 3 – ESL 9000, 2 e2400-160’s, 8 Drives	16
Example 4 – ESL 9000, 2 e2400-160’s, 8 Drives, Cables Swapped.....	17
Example 5 – ESL 9000, 1 e2400-160, 8 Drives.....	18
Example 6 - ESL-E Series, 8 Drives	19
For more information.....	20

Overview

Command View ESL's Secure Manager feature enables users to grant fibre channel host bus adapters access to devices in a tape library. Secure Manager automatically generates the fibre channel port LUN to target device mappings that will be presented to a specific host bus adapter (or host). This document details how Secure Manager performs this mapping and illustrates how Secure Manager behaves with typical library configurations.

At a basic level, the process includes the following steps:

1. Determine which devices are connected to a FC interface controller.
2. Logically order the devices using device type and the logical tape drive location (or number).
3. The devices are then load balanced across the FC interface controller's fiber channel ports.
4. For each fibre channel port, a sequential LUN value is given to each device assigned to that port.

The process is repeated for all FC interface controllers.

Abbreviations, Acronyms, and Definitions

AF	Active Fabric: The controller LUN for a particular FC port. It is used to create a target for the FC interface controller for use with some implementations of Direct Backup/X-copy and to enable Library and Tape Tools communication with the FC interface controller.
CVESL	Command View for ESL management station software
FC	Fibre Channel; a high-speed serial protocol capable of large cable distances and scalability. It is frequently used to create SANs.
Interface Controller	HP FC interface controller; includes e1200, e1200-160, e2400 and e2400-160 embedded Network Storage Routers that work with the Interface Manager
Interface Manager	HP Interface Manager; a management card that is embedded in an ESL library and manages one or more FC interface controllers
L&TT	Library and Tape Tools; free diagnostic software for HP tape drive products. It is used for flashing firmware, pulling diagnostic information, running tests and verifying installations.

Background Information

Interface Manager Modes: Automatic and Manual

The Interface Manager card operates in two different modes: automatic and manual. In automatic mode, the Interface Manager automatically configures and enforces a consistent configuration across all FC interface controllers including port settings and mapping. By enforcing this configuration, automatic mode greatly speeds up the mapping and port configuration process as well as eliminating the chance that a FC interface controller will be improperly set up.

There are some specific configurations that automatic mode will not address. For these cases, the Interface Manager provides a manual mode. However, as the name implies, manual mode fully relies on the user to correctly set up and maintain the fibre port and map settings, therefore manual mode requires more handling from the administrator and increases the chances that errors will be made in the FC interface controller configurations.

For simplicity and reliability, automatic mode is the recommended mode setting for nearly all installations. However, certain configurations require the library administrator to put the Interface Manager in manual mode.

The conditions where Manual mode is needed:

- FC interface controllers are connected to mixed topologies (e.g. connected to switches and directly to host HBAs)
- The FC interface controllers are connected to a mix of 2Gbit/s and 1Gbit/s switches
- A specific operating system or software application is being used that has unique fibre LUN mapping requirements
- The configuration requires that 3 or 4 tape drives be assigned to a single fibre channel port instead of 1 or 2

NOTE: When you change from Manual to Automatic mode you will lose any customizations created in Manual mode.

Basic vs. Advanced Secure Manager

Command View ESL provides a default implementation of Secure Manager known as *Basic Secure Manager*. Basic Secure Manager allows the library administrator to grant or deny a fibre channel host bus adapter access to all devices in a tape library. Also, in Basic Secure Manager, all hosts use the same device mapping. Therefore if you enter Manual mode and change the map for one host, the changes are seen by all hosts that are assigned access to the library.

If the customer purchases and installs a Secure Manager license, *Advanced Secure Manager* will be enabled. Advanced Secure Manager allows the library administrator to grant or deny hosts access to any combination of devices in the library. Unlike Basic Secure Manager, each host can have a unique map. For example, the master server in a backup solution might be the only server that can control the library robotics. In this scenario, all backup servers may be granted access to the tape drives in the library, but will be denied access to the robotics controller. The master server would be granted access to the robotics controller and possibly one or more tape drives.

Interface Manager Discovery

When the Interface Manager is initialized, all FC interface controllers register with the Interface Manager. The Interface Manager then interrogates each FC interface controller to determine which devices are available. If a tape drive is discovered, the tape drive is interrogated to determine drive attributes and device serial number.

NOTE: If the tape library robotics controller is not discovered by the Interface Manager, the discovery process cannot complete successfully. In this case, Secure Manager will be disabled until robotics connectivity is established. This is done because the Interface Manager must rely on the library controller to identify the drives belonging to the library and their logical positions.

Once the robotics controller is discovered, the Interface Manager issues a “read element status” command to determine the drive configuration of the library. The Interface Manager uses the read element status data to determine the number of drives in the library, the logical position of each drive in the library, and the serial number for each drive. The Interface Manager can then correlate the serial numbers returned by the robotics controller with the serial number reported by each tape drive to determine the physical location of each tape drive in the library.

For example:

The tape drive connected to *SCSI Bus 0* on *IC 1* reports a serial number of "XYZ." Also assume the robotics controller reports that the library has 8 tape drives and logical tape drive 4 has a serial number of "XYZ." The Interface Manager can then use the serial number "XYZ" to identify the tape drive at *SCSI Bus 0, IC 1* as logical tape drive 4. If the physical location for each reported tape drive is correlated to the logical drive number, then the Interface Manager discovery process completes successfully and Secure Manager will be available.

Secure Manager is also available for target devices that were previously discovered but are currently offline. For example, if tape drive 2 was initially discovered and subsequently taken offline for repair, Secure Manager will operate with the previous device attributes until the drive is brought back online.

Secure Manager Mapping Rules

The fibre channel port LUN to TARGET device mapping created by Secure Manager is referred to as a *Device Map* in Command View ESL. Secure Manager uses the following rules when creating and modifying a Device Map. Each rule is covered in more depth in the following sections.

1. Devices are ordered based on type and logical position (drive number).
2. Each map will start with LUN 0.
3. New maps remove gaps in the LUN map, but modified maps leave them.
4. If there is more than one FC port on a FC interface controller, then load balancing algorithms are used.
 - a. The first two tape devices are assigned to the first FC port at the next available LUN. The next two tape devices are assigned to the second FC port at the next available LUN.
 - b. If there are remaining tape devices, then the next two tape devices are assigned to the first FC port, and the next two to the second FC port. This is repeated until all tape devices are assigned.
5. Maintain FC Port/LUN Map after cabling change on same Interface Controller.
6. Advanced Secure Manager map creation performs Basic Secure Manager but then removes devices and gaps if necessary.
7. Maintains current FC Port/LUN assignments when adding devices in Advanced Secure Manager.
8. If devices are removed with Advanced Secure Manager any gap made is retained.
9. If devices are removed and added with Advanced Secure Manager, attempts are made to not disturb the other device mappings.
10. Active Fabric is the last LUN on a map of each FC port.

1. Devices are ordered based on type and logical position (drive number)

- Secure Manager uses the drives' logical position (drive number) as the basis for all mapping operations.
- Robotics are always first in the order of devices therefore they are always assigned LUN 0.
- Drives have the next priority. They are ordered based on their logical position (the lower the logical position or drive number, the lower the assigned LUN).
- Active Fabric, if present, will be the last device in a map.

Table 1. Normal device ordering

LUN	FC Port 0
0	Robotics
1	Drive 1
2	Drive 2
3	AF

2. Each map will start with LUN 0

LUN maps always start with LUN 0. Therefore the first device in any map will be assigned to 0.

3. New maps remove gaps in the LUN map, but modified maps leave them

New maps are filled without any gaps in the LUN numbering sequence. If a particular host is denied access to a drive, a new LUN map for that host will **NOT** have an empty placeholder for that drive. Instead the next logical drive will receive the LUN number that would have been used by the inaccessible drive.

Modified maps do leave gaps in the LUN map. If a host previously could see all library devices and then later access was withdrawn for a device, and doing this created a gap in the LUN map, that gap would remain in order to maintain the addresses of the remaining devices in the map.

NOTE: Once the FC interface controller has been rebooted after adding a host and configuring its access, the LUN map is created. Any changes to device access thereafter will follow the rules for modifying an existing map rather than the rules for creating new maps.

Table 2. New and Modified maps on a 1FC port FC interface controller for a host that can't access drive 2

NEW		MODIFIED	
LUN	FC Port 0	LUN	FC Port 0
0	Drive 1	0	Drive 1
1	Drive 3	1	-
2	-	2	Drive 3

4. If there is more than one FC port on a FC interface controller, load balancing algorithms are used

Tape devices attached to a particular FC interface controller are sorted in ascending order by logical position in the library. The first two tape devices are assigned to the first FC port at the next available LUNs. The next two tape devices are assigned to the second FC port at the next available LUNs. If there are more than two tape devices per FC port then the following tape devices are assigned in a similar fashion starting over at the first FC port.

Secure Manager takes the following steps when load balancing target devices across FC ports on a dual port FC interface controller (such as an e2400-160):

1. If the robotics controller is attached to the FC interface controller, it is mapped to FC port 0 at LUN 0.

Table 3. Load Balancing with Robotics and 4 Tape Drives on a 2 FC Port FC interface controller

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive 4
2	Drive 2	-

2. The tape devices attached to the FC interface controller are sorted in ascending order by logical position in the library.
3. The first two tape devices are assigned to the first FC port at the next available LUNs.

Table 4. Load balancing with 2 drives on a 2 FC Port FC interface controller

LUN	FC Port 0	FC Port 1
0	Drive 1	-
1	Drive 2	-

NOTE: The drives are both assigned to FC Port 0 so that if drives 3 and 4 are added later, the maps will be contiguous.

4. Then next two tape devices are assigned to the second FC port at the next available LUNs.

Table 5. Load Balancing with 3 Tape Drives on a 2 FC port FC interface controller

LUN	FC Port 0	FC Port 1
0	Drive 1	Drive 3
1	Drive 2	-

Table 6. Load Balancing with 4 Tape Drives on a 2 FC Port FC interface controller

LUN	FC Port 0	FC Port 1
0	Drive 1	Drive 3
1	Drive 2	Drive 4

5. If there are remaining tape devices, then the next two tape devices are assigned to the first FC port, the next two to the second FC port. This is repeated until all tape devices are assigned.

Table 7. Load Balancing with Robotics and 8 Tape Drives on a 2 FC port FC interface controller

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive 4
2	Drive 2	Drive 7
3	Drive 5	Drive 8
4	Drive 6	-

The above algorithms are applied to all FC interface controllers in the library.

5. Maintain FC Port/LUN Map after cabling change on same Interface Controller.

If a device's cable is moved from one port to another on the same FC interface controller, Secure Manager will attempt to maintain the current FC Port/LUN mapping for the device.

Because devices are mapped by logical position the Interface Manager can correct for devices that have been cabled to different ports on the FC interface controller at power up and FC interface controller reboot. This remapping is not available if the tape device has been moved to a different FC interface controller. The purpose of this feature is to maintain a consistent view of the devices for the hosts connected to the library.

6. Advanced Secure Manager map creation is done like Basic Secure Manager but then removes devices and gaps if necessary

Advanced Secure Manager mapping starts the same way as Basic Secure Manager LUN mapping. Then for each host that can't see the entire library, devices are removed from the map and any gaps they make will be removed.

NOTE: Once the FC interface controller has been rebooted after adding a host and configuring its access, the LUN map is created. Any changes to device access thereafter will follow the rules for modifying an existing map rather than the rules for creating new maps.

Table 8. Advanced Secure Manager Mapping Step 1: Maps are created using the same rules as Basic Secure Manager

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive 4
2	Drive 2	-

Table 9. Advanced Secure Manager Mapping Step 2: Devices the host can access are removed

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive-4
2	Drive 2	-

Table 10: Advanced Secure Manager Mapping Step 3: Remove gaps in the map

LUN	FC Port 0	FC Port 1
0	Drive 1	Drive 3
1	Drive 2	-
2	-	-

7. Maintain current FC Port/LUN assignments when adding devices in Advanced Secure Manager

If an existing map is modified to add a device, previous FC Port/LUN assignments will be retained in an attempt to present a consistent device mapping to the host. The device map is not re-ordered when devices are added.

NOTE: Devices are added to the FC Port that they would have been assigned to using Basic Secure Manager Rules.

Single Fibre Channel Port Example:

Assume Advanced Secure Manager is enabled and that a host has initially been given access to the robotics and drives 2-4:

Table 11. Map for host with access to robotics and drives 2-4.

LUN	FC Port 0
0	Robotics
No Access to Drive 1	
1	Drive 2
2	Drive 3
3	Drive 4

If the library administrator later grants the host access to Drive 1, the current FC Port/LUN mappings will be retained and the new Device Map will look like:

Table 12. Map for host given access to drive 1 after robotics and drives 2-4 were mapped.

LUN	FC Port 0
0	Robotics
1	Drive 2
2	Drive 3
3	Drive 4
4	Drive 1

8. If modifying an existing map to remove device access with Advanced Secure Manager any gap made is retained

If Advanced Secure Manager is used to remove access to a device for a host with a preexisting map, any gap this change makes will be maintained.

Table 13. 1 FC port Advance Secure Manager Device Access Removal: Removing device

LUN	FC Port 0
0	Robotics
1	Drive 1
2	Drive 2

Table 14. 1 FC port Advance Secure Manager Device Access Removal: End result

LUN	FC Port 0
0	-
1	Drive 1
2	Drive 2

NOTE: There are three methods of removing the gap(s) created by this process. (1) All hosts using this map need to be removed and re-added and a new map needs to be created. (2) Changing the Mode from Automatic to Manual and back to Automatic will clear out all customizations (not recommended unless the number of customizations is low). (3) Add access to a device connected to that FC interface controller and that would normally be mapped to that FC port and it will fill the first gap in the LUN order.

9. If devices are removed and added with Advanced Secure Manager, attempts are made to not disturb the other device mappings

If host access is changing to adding and remove devices, efforts are made to not disturb the devices. If possible, the newly added device will fill the gap made by the removed device. This is done to retain the LUN assignments of the other devices. A device will only be added back to the FC port that

it would have been assigned to in Basic Secure manager (i.e. Robotics and drives 1 and 2 will always be on FC port 0).

Table 15. Advance Secure Manager Device Access Change Step 1 (1FC Port): Remove devices

LUN	FC Port 0
0	Robotics
1	Drive 1
2	Drive 2

Table 16. Advance Secure Manager Device Access Change Step 2 (1FC Port): Add devices to fill gaps if possible

LUN	FC Port 0
0	Drive 3
1	Drive 1
2	Drive 2

Example:

A host has access to the robotics and drives 2, and 4.

Table 17. Map from 2 FC port IC with access to the robotics, and drives 2 and 4

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 4
1	Drive 2	-

Advanced Secure manager is used to remove access to the robotics and add access to drive 3

Table 18. Robotics access is removed

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 4
1	Drive 2	-

Table 19. Access to Drive 3 is added

LUN	FC Port 0	FC Port 1
0	-	Drive 4
1	Drive 2	Drive 3

10. Active Fabric is the last LUN on a map of each FC port

One Active Fabric (AF) controller LUN is included as the last LUN in each FC port map that has a drive with a Direct Backup (X-Copy) license. Active Fabric is used by L&TT to communicate with the FC interface controllers and by some software for X-Copy/Direct Backup (a licensed functionality) implementation.

IMPORTANT: Active Fabric is NOT displayed in Secure Manager.

Active Fabric doesn't conform to the rules that other devices are governed by. It will always be the last LUN in the map for each FC port. If another device is added to the end of the list it will take the LUN currently occupied by AF and AF will take the LUN after the device. If the last device is removed, then AF will move to fill in the gap.

Table 20. Map of 4 drive library on a 2 FC port IC with Direct backup enabled on Drive 3 or 4 and AF visible

LUN	FC Port 0	FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive 4
2	Drive 2	AF

Example: AF mapping when access to a device is added

Table 21. LUN map where access to drive 2 is not granted and Direct Backup is enabled for drive 1

LUN	FC Port 0
0	Robotics
1	Drive 1
2	AF

Table 22. AF LUN map placement after adding drive 2

LUN	FC Port 0
0	Robotics
1	Drive 1
2	Drive 2
3	AF

Example: AF mapping when access to a device is removed

Table 23. LUN map where access to drive 2 is being removed and direct backup is enabled for drive 1

LUN	FC Port 0
0	Robotics
1	Drive 1
2	Drive 2
3	AF

Table 24. AF map placement after drive 2 is removed

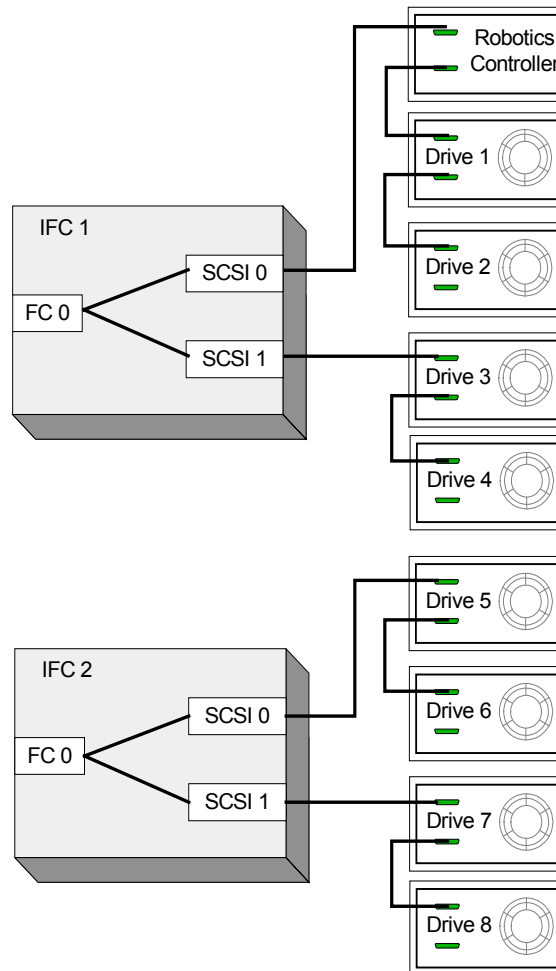
LUN	FC Port 0
0	Robotics
1	Drive 1
2	AF

A Note on Basic Secure Manager and Manual Mapping

If Basic Secure Manager is used, all devices are included in the map. Every host that is granted access to the library has the same view of the devices. For example, if a device map is modified (manual mode) for a particular host all hosts will see the modifications.

Example 1 – ESL 9000, 2 1-Port IC's, 8 Drives

Figure 1. ESL 9000 with 2 1-FC Port FC interface controllers and 8 Tape Drives (2 per SCSI bus)

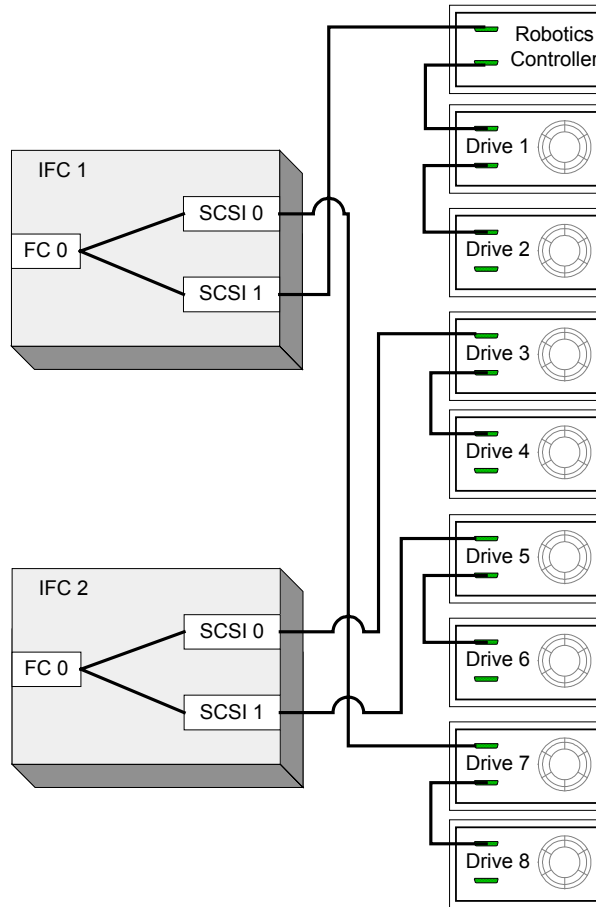


Secure Manager will generate the following default mapping if a host is granted access to all devices:

LUN	FC interface controller 1: FC Port 0	FC interface controller 2: FC Port 0
0	Robotics	Drive 5
1	Drive 1	Drive 6
2	Drive 2	Drive 7
3	Drive 3	Drive 8
4	Drive 4	-

Example 2 – ESL 9000, 2 1-Port IC's, 8 Drives, Odd Cabling

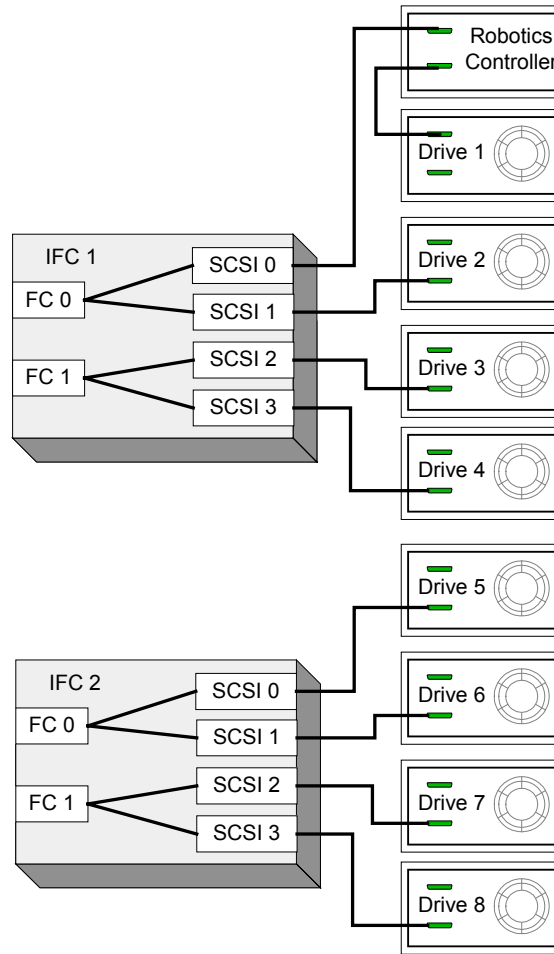
Figure 2. ESL 9000 with 2 1-FC Port FC interface controllers and 8 Drives and non-standard cabling



LUN	FC interface controller 1: FC Port 0	FC interface controller 2: FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive 4
2	Drive 2	Drive 5
3	Drive 7	Drive 6
4	Drive 8	-

Example 3 – ESL 9000, 2 e2400-160's, 8 Drives

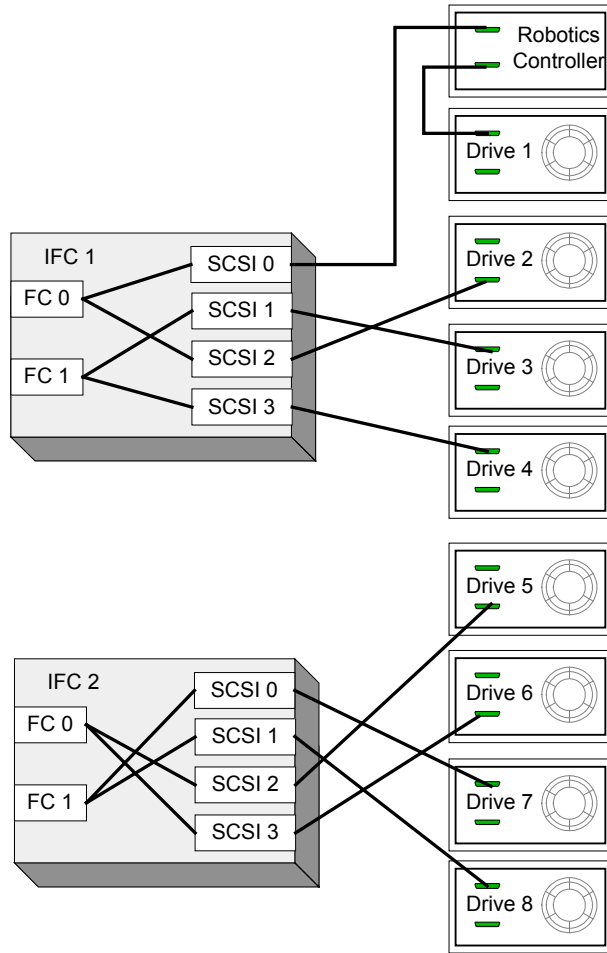
Figure 3. ESL 9000 with 2 e2400-160 FC interface controllers and 8 drives



LUN	FC interface controller 1		FC interface controller 2	
	FC Port 0	FC Port 1	FC Port 0	FC Port 1
0	Robotics	Drive 3	Drive 5	Drive 7
1	Drive 1	Drive 4	Drive 6	Drive 8
2	Drive 2	-	-	

Example 4 – ESL 9000, 2 e2400-160's, 8 Drives, Cables Swapped

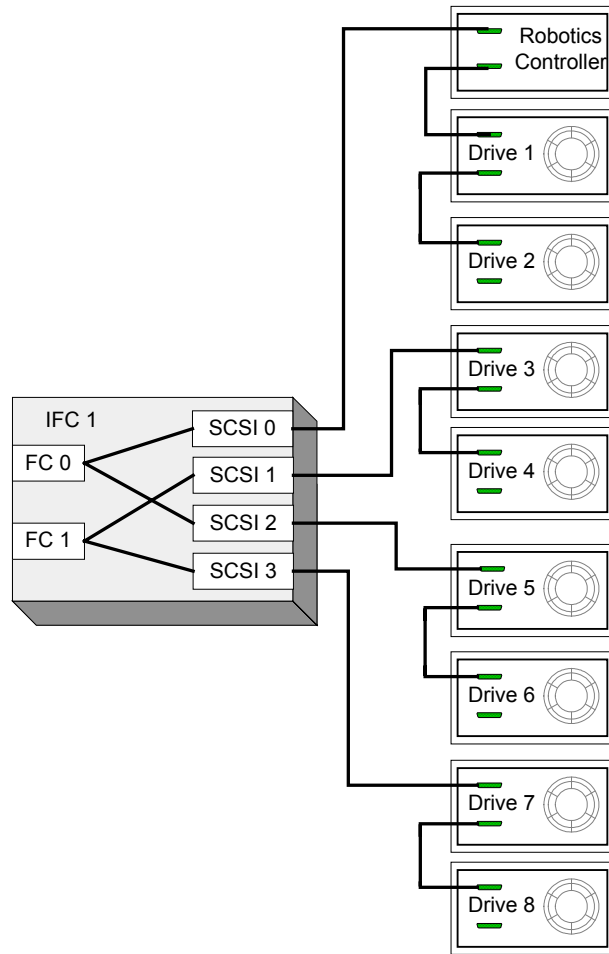
Figure 4. ESL 9000 with 2 e2400-160 FC interface controllers and 8 Drives (Cable Swap Drive 2 and Drive 3; cable Swap Drive 5 and Drive 7; and Cable Swap Drive 6 and Drive 8)



LUN	FC interface controller 1		FC interface controller 2	
	FC Port 0	FC Port 1	FC Port 0	FC Port 1
0	Robotics	Drive 3	Drive 5	Drive 7
1	Drive 1	Drive 4	Drive 6	Drive 8
2	Drive 2	-	-	

Example 5 – ESL 9000, 1 e2400-160, 8 Drives

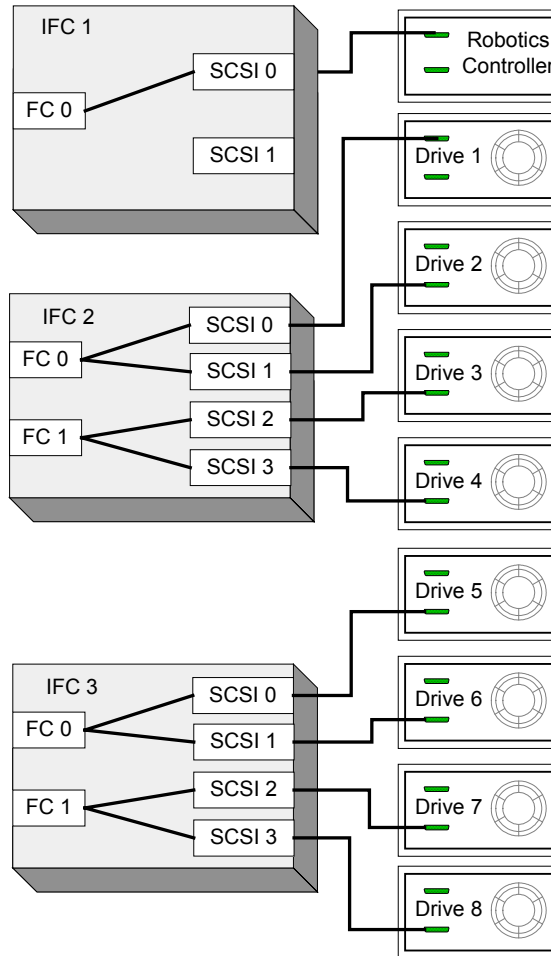
Figure 5. ESL 9000 with 1 e2400-160 FC interface controller and 8 Drives (Cabled with 2 drives per bus)



FC interface controller 1		
LUN	FC Port 0	FC Port 1
0	Robotics	Drive 3
1	Drive 1	Drive 4
2	Drive 2	Drive 7
3	Drive 5	Drive 8
4	Drive 6	-

Example 6 - ESL-E Series, 8 Drives

Figure 6. ESL-E Series Library with an e1200-160 and 2 e2400-160 FC interface controllers and 8 drives



	FC interface controller 1		FC interface controller 2		FC interface controller 3	
LUN	FC Port 0	FC Port 1	FC Port 0	FC Port 1	FC Port 0	FC Port 1
0	Robotics	-	Drive 1	Drive 3	Drive 5	Drive 7
1	-	-	Drive 2	Drive 4	Drive 6	Drive 8

For more information

www.hp.com/support/cvesl

HP Automation Business Segment, 2004

© 2003 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Itanium is a trademark or registered trademark of Intel Corporation in the U.S. and other countries and is used under license.

XXXX-XXXXEN, 07/2003

