

IBM Storage Area Network Data Gateway Module



Setup, Operator, and Service Guide

IBM Storage Area Network Data Gateway Module



Setup, Operator, and Service Guide

Note:

Before using this information and the product it supports, read the general information in "Safety" on page xv, and "Notices" on page 213. To ensure that you have the latest publications, visit the web site at: <http://www.ibm.com/storage/ito>

Second Edition (August 2001)

This edition applies to the *IBM Storage Area Network Data Gateway Module Setup, Operator, and Service Guide* and to all subsequent releases and modifications until otherwise indicated in new editions. This edition replaces GA32-0436-00.

You may use the form at the back of this publication to send us comments about this publication or, if the form has been removed, address your comments to:

IBM Corporation
Department GZW
9032 S Rita Road
Tucson, AZ 85775-4706

You can also send your comments electronically to:

www.storage.ibm.com/feedback/feedback.htm

For additional information on IBM storage products, visit the Web site at:

www.ibm.com/storage

Publications are not stocked at the address given above. If you want additional IBM publications, ask your IBM representative or write to the IBM branch office serving your locality.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 2001. All rights reserved.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	xi
Tables	xiii
Safety	xv
Danger Notice	xv
Caution Notice	xv
Attention Notice	xvi
Laser Safety and Compliance	xvii
Class I Laser Product	xvii
About this Book	xix
Who Should Use this Book	xix
Related Publications	xix
Web Sites	xix
Chapter 1. Introduction	1
Overview of the SAN Data Gateway Module	2
Configuration Support	2
Address Mapping	2
Interface Protocol Awareness	2
IBM StorWatch Specialist	3
Access Security Capabilities	3
Data Mover	3
SAN Data Gateway Module Description and Features	4
Description of Subsystems	4
Environment Subsystem	5
Power Subsystem	5
Temperature Subsystem	6
Fibre Channel Interfaces	7
Ultra2 SCSI I/O Interfaces	8
Ethernet	8
Service Port	8
Firmware	9
LED Indicators	9
Operating Specifications	10
Physical Dimensions	10
Operating Environment	10
Power Consumption	10
Service Capabilities	11
POST	11
Health Check	11
Event Log	11
Diagnostic Suite	11
Service Tools	12
Service Port Terminal Requirements	12
Service Tool Kit	12
Generic Tools	12
Field Replaceable Units	13
Introduction to the IBM StorWatch Specialist	14
Client-Server Model	14
Features	15
SCSI Device Address Mapping	17

Address Persistency	19
Alternate SCSI IDs	20
Default Alternate SCSI ID	20
Changing the Alternate SCSI ID	20
Setting Up Access Control.	21
Fibre Channel Port Modes and Connection Options	21
Port Modes	21
Public and Private Loops	21
Connection Types	22
Preserving the Gateway Configurations	22
 Chapter 2. Installation	 23
Pre-Installation Checklist	24
Installation Checklist	25
StorWatch Specialist Installation Checklist	27
Host Adapter Setup	28
Startup Sequence Guidelines	28
Installing the IBM StorWatch Specialist Software	29
Server	29
Client	29
Installation Requirements	29
Installing the Software in Microsoft Windows NT	30
Startup and Configuration	30
 Chapter 3. Using the IBM StorWatch SAN Data Gateway Specialist	 33
Starting the StorWatch Specialist	34
File Menu	36
Save Current View	36
Save Current View as	36
Opening a Previous View	37
Exit	37
View Menu	38
Tree View.	38
SAN Data Gateway Module Front Panel View	43
Refresh Gateway View	43
Admin Menu	44
Connecting to Server	44
Logging On	45
Changing Password	45
Adding a New User	46
Removing a User	46
Tools Menu	47
Discover Net.	48
Connecting a Gateway	49
Disconnecting a Gateway	49
Health Check	50
Events Menu	51
Saving Gateway Configuration	55
Loading Gateway Configuration.	56
Controls Menu	57
Feature Enable.	57
Access Options.	58
SNMP Community Strings.	60
SCSI Channel	61
Fibre Channel	63
Device Mapping	64

Pre-Assigning Device Numbers	67
Updating Firmware	70
Restarting the Gateway.	70
Identifying the Gateway.	71
Chapter 4. Remote Event Notification.	73
Event Logging and Viewing	74
Events and Traps	75
Heartbeats	76
Health Check	76
Setting Up the Health Check	77
Health Check Level Control	78
Health Check Interval	79
Performance Impact of Health Checks	79
Chapter 5. Maintenance Analysis Procedures	81
Start MAP.	82
Checking Event Code or Error Symptom	82
Inspecting LED Status Indicators	82
Checking for Problems on Attached SCSI Devices	83
Checking Fibre Channel Host Versions	83
Checking Gateway Product Versions	83
Checking the Event Log	84
Quick Component Check	84
Performing a Health Check	84
Checking the Host Event Log	84
Service Reference Table	85
Action reference table	88
Database Full MAP	89
Device Access MAP	89
Checking Fibre Channel Port Status	89
Checking SCSI Channel Devices	90
Checking Channel Zoning Settings	90
Checking Fibre Channel Initiator Port Mode	90
SCSI MAP	90
Getting SAN Data Gateway Module SCSI Information	90
Checking Attached SCSI Devices from the Service Port	91
Comparing Listed Versus Physical Devices	91
Comparing Listed Versus Supported Devices	91
Checking SCSI Bus Termination	91
Checking for Multiple SCSI IDs	92
Incorrect Device Type	93
Examining SCSI Cables	93
Examining SCSI Connectors	94
SCSI Health Check	94
SCSI Loopback Test	94
Testing SCSI Cables	95
Isolating SCSI Devices	95
Restoring SCSI Setup	96
Fibre Channel MAP	96
Verify Fibre Channel Connections	96
Examining Cables.	97
Checking Optical Cable Type.	97
Fibre Channel Loopback Test	97
Testing Fibre Channel Optical Cable	98
Replacing Fibre Channel Cable	99

Replacing Fibre Channel Device	99
Gateway MAP	99
Observing Operational LED Patterns	100
Temperature MAP	100
Notification of Problems in Temperature Subsystem	100
Resolving Temperature Alarm	100
Power MAP	101
Ethernet MAP	101
Service Port MAP	105
Checking the RS-232 Cable	105
Checking the Connection with Boot Messages	105
Chapter 6. Removal and Replacement Procedures	107
Handling Electrostatic Discharge Sensitive Parts	108
Remove and Replace GBIC.	108
Remove GBIC.	108
Replace GBIC.	108
Remove and Replace Gateway	109
Remove Gateway	109
Replace Gateway	109
Verify New Gateway	110
Gateway Network Setup	115
Appendix A. Connecting to the Service Port	117
Service Port Connections	118
Connecting the Service Terminal	119
Hardware Required	119
Initial Setup of HyperTerminal	119
Verifying the Connection	119
Updating Firmware and Configurations.	120
Updating Gateway Firmware	120
Saving a Configuration File	120
Loading a Configuration File	121
Zmodem Status Code Table	121
Appendix B. Service Port Command Reference	123
Commands	127
arptabShow	127
cd	127
clearReservation [devId]	127
cleHelp	128
cleShow [lun]	128
cleShowAll	128
csEtimeShow	128
dataScrubberDisable	128
dataScrubberEnable	128
diagBoot	128
diagHelp	129
disableCC [option number]	129
elTest	130
enableCC	130
envMonShow	130
envMonRangeShow	132
ethAddrSet	132
ethDisable	133
ethEnable	133

fcConnTypeGet [port]	133
fcConnTypeSet [port],[connection]	134
fcFibreSpeedGet	134
fcFibreSpeedSet	134
fcGbicShow	135
fcPortModeGet [port]	135
fcPortModeSet [port],[mode]	136
fcRestart [port]	137
fcShow [level]	137
fcShowDevs	139
fcShowNames	139
fcTxDisable	140
fcTxEnable	140
gateAddrGet	140
gateAddrSet	141
hardwareConfig	141
help	142
hlthChkHelp	143
hlthChkIntervalGet	143
hlthChkIntervalSet	143
hlthChkLevelGet	143
hlthChkLevelSet	144
hlthChkNow	144
host	144
host add,[hostname],[ipaddress]	144
host delete,[hostname]	144
host list	145
hostAdd	145
hostNameSet	145
hostTypeShow	145
icmpstatShow	146
ifShow	146
inetstatShow	147
initializeBox	147
ipstatShow	147
licenseShow	147
loggerDump [number]	148
loggerDumpCurrent [level]	148
ls or ll	149
macShow	149
mapCompressDatabase	149
mapHelp	150
mapRebuildDatabase	150
mapShowDatabase	150
mapShowDevs	151
mapWinnowDatabase	152
mbufShow	152
netHelp	153
normalBoot	154
reboot	154
reset	154
ridtag [value]	154
rm	155
route	155
rz	156
scsiAltIdGet [channel]	157

scsiAltIdSet [channel],[id]	157
scsiChannelTest [x,y]	157
scsiHostChanGet [channel]	158
scsiHostChanSet [channel],[mode]	158
scsiHostIdGet [channel]	158
scsiHostIdSet [channel],[id]	159
scsiRescan [channel]	159
scsiResetDisableGet [channel]	159
scsiResetDisableSet [channel],[mode]	160
scsiShow	160
scsiTermGet [channel]	161
scsiTermSet [channel],[termination]	162
setFcFrameSize [channel],[size]	162
setFcHardId [channel],[id]	163
setFcNormal	163
setFcScsiChanMask [channel],[scsiChannel],[allow]	163
setFcSplit	163
setHost [port] OS	163
setSnaCCLun [newLUN]	164
shellLock	165
showBox	165
snaVersion	166
sncFeatureEnable [licensekeystring]	166
snmpCommunitiesShow	166
snmpHelp	167
snmpReadCommunityAdd [string],[view]	167
snmpReadCommunityRemove [string]	167
snmpTrapCommunitySet [string],[view]	168
snmpWriteCommunityAdd [string],[view]	168
snmpWriteCommunityRemove [string]	168
supportDump	168
sysConfigShow	169
sysVpdShow, sysVpdShowAll	169
sz [filename]	171
targets	171
tcpstatShow	171
trapDestAdd, trapDestRemove, trapDestShow	172
udpstatShow	173
uptime	173
userAdd, userDelete, userList	173
userHelp	174
version	174
xscsiAltIdGet [channel]	174
xscsiAltIdSet [channel],[id]	175
xscsiHostChanGet [channel]	175
xscsiHostChanSet [channel],[mode]	175
xscsiHostIdGet [channel]	176
xscsiHostIdSet [channel],[id]	176
xscsiResetDisableGet [channel]	176
xscsiResetDisableSet [channel],[mode]	176
xscsiTermGet [channel]	177
xscsiTermSet [channel],[termination]	177
Appendix C. Application Notes	179
Fibre Channel Loop Addressing—Hard Versus Soft IDs	180
Address Numbering	180

Loop ID Assignment	180
Benefits and Drawbacks	180
Planning for Persistence	180
Assigning a Hard ID to a Gateway Fibre Channel Port	180
Understanding and Modifying Devices	181
Gateway Discovery and Mapping.	181
Changing the Command and Control LUN	183
Compressing the Address Map Database.	184
Customizing the Address Map Database	184
Setting Up a Redundant Dual SCSI Configuration	188
Introduction.	188
Setting SCSI IDs of Gateways and Target Devices	188
Disabling SCSI Channel Reset During Startup	190
Creating Identical Persistent Address Maps	190
Adding Devices to an Existing Redundant Configuration	191
Microsoft Cluster Server Notes	191
Relevant Knowledge Base Articles	191
Requirements and Settings	192
Appendix D. Diagnostic Command Reference	195
Boot Modes	196
Entering Diagnostic Mode	196
Restoring Normal Mode	196
Special Procedures	197
Health Check	197
Event Log Dump.	199
Retrieving the Code 43 Dump File	199
Boot Mode Commands	200
diagBoot.	200
normalBoot.	200
Diagnostic Commands	201
elTest	201
fcSlotTest [x]	202
scsiChannelTest [x,y]	202
xscsiChannelTest [x,y].	203
Appendix E. Startup Message Reference	205
Boot Rom Messages	205
LIC Initialization Messages	205
Final Startup Messages	206
Appendix F. POST Error Codes.	207
POST Boot Behavior	207
ROM Init.	207
Initial POST	207
Notices	213
Trademarks.	214
Electronic Emission Statements	214
Federal Communications Commission (FCC) Class B Statement	214
Industry Canada Class B Emission Compliance Statement	215
Avis de conformité à la réglementation d'Industrie Canada	215
European Union (EU) Electromagnetic Compatibility Directive	215
Germany Electromagnetic Compatibility Directive	215
Japan VCCI Class A ITE Electronic Emission Statement	216
Taiwan Class A Electronic Emission Statement.	216

Korean Government Ministry of Communication Statement	216
IBM Agreement for Licensed Internal Code	216
Actions You Must Not Take	217
IBM License Agreement for Machine Code	217
Statement of Limited Warranty.	218
Production Status	218
IBM Warranty for Machines	218
Warranty Service.	219
Extent of Warranty	220
Limitation of Liability	220
Glossary	221
Index	223

Figures

1.	SAN Data Gateway Module in a tape library	2
2.	Serverless Backup.	3
3.	LEDs	9
4.	GBIC with dust protector	13
5.	The Gateway	13
6.	StorWatch Specialist application model.	14
7.	Rear-view of a tape library	17
8.	Gateway seated in a tape library	25
9.	Logging on to the Server	31
10.	Creating a New Administrator Account	31
11.	Connecting to the Server	34
12.	Logging on to the Server	34
13.	Initial Tree View	35
14.	File Menu	36
15.	Saving the Current View	36
16.	Saved Views	37
17.	View Menu	38
18.	Expanded Tree View	38
19.	Tree View Icons for Channel Modes and Channel Types	39
20.	Tree View Icons for Devices.	39
21.	Information about a Selected Channel	40
22.	Information about a Selected Device	41
23.	Information about a Selected Host	42
24.	Front Panel View.	43
25.	Admin Menu	44
26.	Connecting to the Server	44
27.	Logging On to the Server.	45
28.	Changing a Password	45
29.	Adding a New User	46
30.	Removing a User.	47
31.	Tools Menu	47
32.	Discover Net	48
33.	Connecting to a Gateway.	49
34.	Disconnecting a Specific Gateway	49
35.	Health Check Pull-Down Menu.	50
36.	Setting Health Check Interval	50
37.	Event Log Pull-Down Menu	51
38.	Selecting the Event Viewing Level	52
39.	Typical Event Log	52
40.	Saving an Event Log	53
41.	Clearing the Event Log	53
42.	Setting Event Thresholds	54
43.	Trap Symbol	54
44.	Received Event Traps Window.	55
45.	Saving the Gateway Configuration	55
46.	Loading a Gateway Configuration.	56
47.	Loading a Gateway Configuration from the Server	56
48.	Controls Menu.	57
49.	Enabling Optional Features	57
50.	Enabling the Data Mover Feature.	58
51.	Selecting an Access Control Option	58
52.	Channel Zoning Settings	59
53.	Modifying the SNMP Community Strings	60

54.	Setting SCSI Channel Parameters	61
55.	Setting Advanced SCSI Channel Options	62
56.	First Warning Before a SCSI Reset	62
57.	Second Warning Before a SCSI Reset	63
58.	Fibre Channel Parameters Default Settings	64
59.	Right-click menu: Device mapping	65
60.	Devices available for mapping	65
61.	Device mapping window	66
62.	Devices that have been remapped	67
63.	Add new SCSI device	68
64.	Add new Fibre Channel device.	68
65.	New SCSI channel device	69
66.	Unmapped devices warning	69
67.	Updating Firmware Files	70
68.	Warning Displayed Before Restarting a Gateway	70
69.	Identifying the Gateway	71
70.	Viewing Events in the Gateway View Event Log	74
71.	Trap Symbol	75
72.	Event Trap Messages Displayed by the Client	75
73.	Successful Health Check	77
74.	Setting the Health Check Interval	79
75.	SCSI Cabling and Termination	92
76.	Gateway Panel	96
77.	Fibre Channel LEDs	98
78.	Ethernet LEDs	102
79.	Gateway in tape library	109
80.	Gateway Cable Connections	110
81.	Gateway Ethernet Port	111
82.	Gateway Panel	114
83.	Service Port Pin-Out	118
84.	showBox Command Display of Gateway.	165
85.	ROM Init	207
86.	Initial POST	207
87.	Simple Access	208
88.	Bitwalk Test	208
89.	Memory Size	208
90.	Pattern Test	209
91.	Address Test	209
92.	Identify and Execute	209
93.	Start of Bootrom	210
94.	NMI 1	210
95.	NMI 2	210

Tables

1. Definition of Terms used in Environmental Monitoring	5
2. Power Ranges	6
3. Sample Statements Accompanying Voltage Trap Messages	6
4. Event Conditions	7
5. Sample Statements Accompanying Fan Trap Messages	7
6. Example of Gateway mapping of SCSI addresses for a typical tape library configuration	18
7. Pre-Installation Checklist	24
8. Installation Checklist	25
9. Post-Installation Checklist	27
10. Health Check Levels	51
11. Event Viewing Levels	74
12. Gateway LED Display Meaning	82
13. Service reference table	85
14. Action reference table	88
15. Post Repair Checklist.	113
16. DB-9 RS-232 Connector Pin Assignments	118
17. Null-Modem Cable Connections	118
18. Zmodem Status Codes	121
19. Management and Configuration Commands Grouped by Function	123
20. Environmental Channels	130
21. Type of port connection	133
22. Port numbering	134
23. Meaning of Speed Settings	134
24. Port numbering	135
25. Port number and meaning	136
26. Firmware states by function	138
27. Event viewing levels	148
28. showBox Abbreviations for Ultra2 SCSI Channels	166
29. Annotated Device Map	185
30. Interface Type Descriptions	186
31. Recommended SCSI ID Assignments.	189
32. Knowledge Base Articles	192
33. Supported Configuration Requirements	192
34. QLogic Host Adapter Settings.	192
35. QLogic Advanced Adapter Settings.	192
36. Single-Port Fibre Channel Optical Interfaces	202

Safety

When using this product, observe the danger, caution, and attention notices that are contained in this guide. The notices are accompanied by symbols that represent the severity of the safety condition.

Most danger or caution notices contain a reference number (RSFTDxxx or RSFTCxxx). Use the reference number to check the translation in *Translated Safety Notices for External Storage Devices*, SA26-7197.

The sections that follow define each type of safety notice and give examples.

Danger Notice

A danger notice calls attention to a situation that is potentially lethal or extremely hazardous to people. A lightning bolt symbol always accompanies a danger notice to represent a dangerous electrical condition. A sample danger notice follows:




DANGER

An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the system or the products that attach to the system. It is the customer's responsibility to ensure that the outlet is correctly wired and grounded to prevent an electrical shock. (RSFTD201)

Caution Notice

A caution notice calls attention to a situation that is potentially hazardous to people because of some existing condition. One of several symbols can accompany a caution notice:

If the symbol is ...	It means ...
	A hazardous electrical condition with less severity than electrical danger.
	A generally hazardous condition not represented by other safety symbols.
	A hazardous condition due to mechanical movement in or around the product.

If the symbol is ...	It means ...
	A hazardous condition due to the weight of the unit. Weight symbols are accompanied by an approximation of the product's weight.

Sample caution notices follow:



CAUTION:
The controller card contains a lithium battery. To avoid possible explosion, do not burn, exchange, or charge the battery. Discard the controller card as instructed by local regulations for lithium batteries. (RSFTC228)



CAUTION:
Do not attempt to use the handle on the module to lift the entire device (module and enclosure) as a unit. First remove the module; then use two hands to lift the enclosure. (RSFTC356)



CAUTION:
This assembly contains mechanical moving parts. Use care when servicing this assembly.



CAUTION:
The weight of this part or unit is more than 55 kilograms (121.2 pounds). It takes specially trained persons with a lifting device to safely lift this part or unit. (RSFTC206)

Attention Notice

An attention notice indicates the possibility of damage to a program, device, or server, or to data. An exclamation point symbol may accompany an attention notice but is not required. A sample attention notice follows:



Attention: If you use a power screwdriver to perform this procedure, it could destroy the tape.

Laser Safety and Compliance

Before using the Storage Area Network (SAN) Data Gateway Module, review the following laser safety information.

Class I Laser Product

The SAN Data Gateway Module contains components that comply with performance standards that are set by the U.S. Food and Drug Administration for a Class I laser product. Class I laser products do not emit hazardous laser radiation. The module's protective housing and scanning safeguards ensure that laser radiation is inaccessible during operation or is within Class I limits. External safety agencies have reviewed the SAN Data Gateway Module and have obtained approvals to the latest standards as they apply.

About this Book

This book provides information about the IBM SAN Data Gateway Module. It also provides instructions for installing, using, and servicing the product.

Who Should Use this Book

This book is for system administrators who will install and use the SAN Data Gateway Module.

Related Publications

Refer to the following publications for additional information about Storage Area Networks (SANs).

- *IBM SAN Survival Guide*, SG24-6143
- *Designing an IBM Storage Area Network*, SG24-5758
- *Planning and Implementing an IBM SAN*, SG24-6116
- *Introduction to Storage Area Networks, SAN*, SG24-5470

Additional information is available from IBM. For a list of publications available in your country or region:

- In the U.S. and Puerto Rico, call 1-800-426-7282.
- In the United Kingdom, call 01705-565000 or 0161-9056001.
- In Canada, call 1-800-465-1234.
- In other countries or regions, contact the IBM support organization that services your area, your IBM marketing representative, or your IBM reseller.

Web Sites

The IBM web site also contains information about the SAN Data Gateway Module. Visit the web site at:

www.ibm.com/storage/lto

For additional information on SANs, visit the IBM web site at:

www.redbooks.ibm.com

Chapter 1. Introduction

This chapter describes the IBM Storage Area Network (SAN) Data Gateway Module. The SAN Data Gateway Module will be referred to in the rest of this chapter by the name Gateway. This chapter provides the following information:

- An overview of the Gateway
- A description of the product and its features
- LED indicators
- A list of the operating specifications
- A list of service capabilities
- A list of service tools
- A list of field replaceable units
- An introduction to the IBM StorWatch Specialist
- Small computer system interface (SCSI) device address mapping
- Address persistency
- Alternate SCSI ID's
- How to set up access control
- Fibre Channel port modes and connection options
- How to preserve the SAN Data Gateway Module configurations

Overview of the SAN Data Gateway Module

The Gateway is the interface between the tape library and a storage area network (SAN) or Fibre Channel (FC) host. The Gateway provides Fibre Channel connectivity to the SCSI tape drives (**1** in Figure 1) and medium changer (**2** in Figure 1) in the tape library.

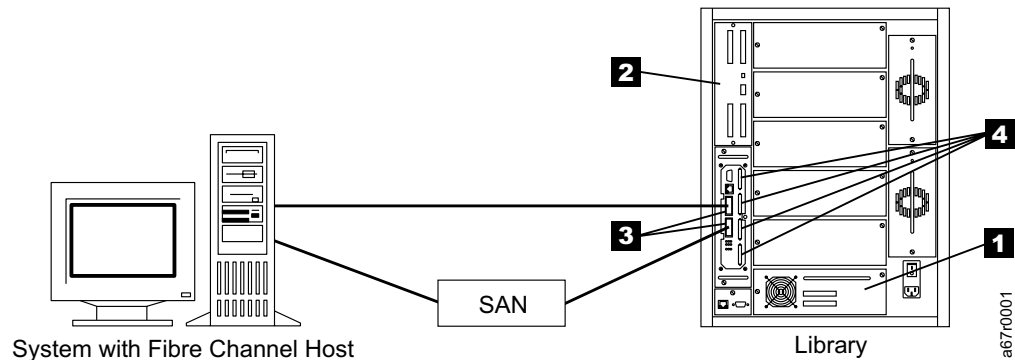


Figure 1. SAN Data Gateway Module in a tape library

For additional information on SANs, visit the IBM web site at:

www.redbooks.ibm.com

Configuration Support

The Gateway has two Fibre Channel interfaces or ports and four SCSI interfaces or ports (see **3** and **4** in Figure 1). The Fibre Channel ports are equipped with 2 Gigabit, SC-style shortwave multimode Gigabit Interface Converter (GBIC) modules. The Fibre Channel ports are capable of communicating reliably at distances of up to 300m over 50µm multimode-optical fiber cables. The four SCSI ports are Ultra2, low voltage differential (LVD), with VHDCI-style connectors.

Note: Only shortwave (SW) GBICs and LVD drives are supported.

Address Mapping

The Gateway maps addresses across and between different interfaces and preserves the persistency of the address maps across system, device, and the Gateway power ups. The Gateway supports the attachment of up to 255 unique devices across multiple interfaces.

Interface Protocol Awareness

The Gateway has full knowledge of the SCSI-3 and SCSI-2 protocols for disk, tape, and tape medium changer devices. Along with this interface protocol awareness is the Gateway's awareness of the host and devices that are attached to its interfaces.

IBM StorWatch Specialist

The StorWatch Specialist offers full capability for remote management, configuration, and event notification. Each Gateway has internal event logging, event analysis, and periodic health checks for predictive failure analysis. All of these management, configuration, and notification capabilities are accessible via standard Simple Network Management Protocol (SNMP) for use with major network management applications. The StorWatch Specialist offers Java application software for the Gateway remote management and configuration.

Access Security Capabilities

The Gateway provides access security between the SCSI and Fibre Channel ports. Using the StorWatch Specialist, access of any Fibre Channel port to any SCSI port can be enabled or disabled. The default access is any Fibre Channel port to any SCSI port.

Channel zoning is a means of managing the access security between Fibre Channel ports and SCSI channels on a channel-by-channel basis.

Channel zoning can be used to secure access between a server and its storage. For example, one FC host can have access to certain SCSI drives on one FC port while another FC host can have access to other SCSI drives through the second FC port.

The default settings allow all FC ports to access all SCSI channels.

Channel zoning capability is always available to users of the Gateway.

Data Mover

Data Mover capability lets the Gateway move data directly between storage devices that are attached to it (see Figure 2). This direct movement of data can be from disk to tape, or tape to disk. The Data Mover function begins when the host sends a command to the Gateway to move data. The host command will specify what data should be moved and where it should be moved to. After receiving this command, the Gateway acts as the initiator and handles the actual movement of the data. Data Mover frees up valuable system resources on the server and substantially increases the speed of backup and restore operations.

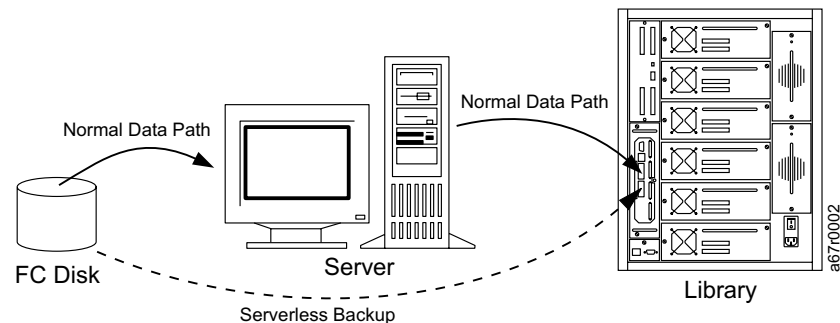


Figure 2. Serverless Backup

Data Mover is the engine for server-free backup and restore applications that support the extended copy specification (American National Standards Institute (ANSI) T10/99-143r1).

Data Mover capability is always available to users of the Gateway.

SAN Data Gateway Module Description and Features

This section describes the capabilities of the product and outlines key features of its interfaces. The Gateway consists of two internal circuit cards and includes the following features:

- An IBM 405GP 200 MHz processor, with integrated instruction and data caches, and internal serial input/output (I/O) and Ethernet interfaces
- An Intel 80303 100 MHz processor, with integrated instruction and data caches
- 32 MB ECC-protected SDRAM program memory
- 64 MB ECC-protected SDRAM data buffer memory
- FLASH memory for operational firmware, power on self-test code, diagnostic functions, and system utilities
- Non-volatile SRAM for persistent configuration tables and event logs
- VxWorks™ real-time operating system (RTOS)
- 2 64–66 MHz PCI buses
- Ethernet port. See “Ethernet” on page 8.
- RS-232 port. See “Service Port” on page 8.
- Chassis, all metal chassis
- Power entry. See “Power Subsystem” on page 5.
- Cooling. See “Temperature Subsystem” on page 6.

Description of Subsystems

The Gateway consists of the following subsystems.

- Environment
 - Power
 - Temperature
- Fibre Channel
- SCSI
- Ethernet
- Service port
- Firmware

Environment Subsystem

The power subsystem and temperature subsystem comprise the Gateway's environment subsystem. They are designed to allow operational monitoring of environmental information. This is reported to the user as pertaining to one of three ranges of values or "states": nominal, warning, and alarm. The ERR light comes on for all warnings and alarms; both power and temperature. To locate the corresponding trap event code use Table 3 on page 6 and Table 5 on page 7.

Table 1. Definition of Terms used in Environmental Monitoring

State	Meaning
Nominal	A value that falls within the nominal range indicates a satisfactory operational state. No user action is necessary.
Warning	A value that falls within the warning range indicates that operations are less than satisfactory. Users should consult the appropriate Maintenance Analysis Procedure (MAP) in "Chapter 5. Maintenance Analysis Procedures" on page 81.
Alarm	A value that falls within the alarm range indicates that operations are seriously compromised. Users should consult the appropriate Maintenance Analysis Procedure (MAP) in "Chapter 5. Maintenance Analysis Procedures" on page 81.

A report of the environmental sensor's current state and measured value can accompany a trap event code, a health check code, or the output of a service port command. Values associated with a particular state are provided in Table 4 on page 7.

Power Subsystem

The power subsystem includes:

- DC power connector to your tape library
- Internal power regulators
- Voltage monitors

Power is supplied to the Gateway from the tape library in two values, a 12V dc and a 5V dc. The Gateway transforms these into a 3.3V dc and a 2.5V dc. As long as the incoming power stays within the nominal range (see Table 2), the Gateway should generate power at 3.3V and 2.5V. If any of the voltages vary into the warning or alarm ranges indicated in Table 2 on page 6, trap event codes are generated. See Event Codes 58, 59, and 60 in Table 3 on page 6. In addition to the trap event code and its message, a text description of the specific situation will be displayed. The text is displayed in a StorWatch Specialist pop-up window, in the event log contents, and as a console message. See Table 3 on page 6 for samples of the statements that accompany voltage trap event code messages 58, 59, and 60.

Table 2. Power Ranges

Power	State		Range (in Volts)
12V	Nominal		10.8 - 13.2
	Warning	Voltage too low	10.56 - ≤10.8
		Voltage too high	>13.2 - 13.44
	Alarm	Voltage critically low	≤10.56
		Voltage critically high	>13.44
5V	Nominal		4.9 - 5.1
	Warning	Voltage too low	4.8 - ≤4.9
		Voltage too high	>5.1 - 5.2
	Alarm	Voltage critically low	≤4.8
		Voltage critically high	>5.2
3.3V	Nominal		3.23 - 3.37
	Warning	Voltage too low	3.17-≤3.23
		Voltage too high	>3.37 - 3.43
	Alarm	Voltage critically low	≤3.17
		Voltage critically high	>3.43
2.5V	Nominal		2.45 - 2.55
	Warning	Voltage too low	2.4 - >2.45
		Voltage too high	>2.55 - 2.6
	Alarm	Voltage critically low	≤2.4
		Voltage critically high	>2.6

Table 3. Sample Statements Accompanying Voltage Trap Messages

Trap Event Code	Statement
Code 58	Input power: +12 volts state changed: warning to nominal, 12.47V
Code 59	Local power: +3.3 volts state changed: ALARM to warning, 3.19V
Code 60	Input power: +12 volts state changed: nominal to ALARM, 13.45V
Code 60	Local power: +3.3 volts state changed: nominal to ALARM, 3.44V

Temperature Subsystem

The temperature subsystem includes:

- High-velocity fan

Trap event codes 66, 67, and 68 reference fan state. If the installed fan is a tachometer output fan, nominal fan speed is recorded in NVRAM after fan installation. If measured fan speed varies into the warning or alarm state, trap event codes are generated. See Table 4 for event conditions. If the installed fan is a rotor stall fan, then trap event code 67 is never generated. In addition to the trap event code and its message, a text description about the specific problem is displayed in a StorWatch Specialist pop-up window, in the event log contents, and as a console message. See Table 5 on page 7 for samples of the statements that accompany fan trap event code messages 66, 67, and 68.

Table 4. Event Conditions

State	Value
Nominal	For Tachometer output fans, the speed recorded at installation, or up to 11% less. For rotor stall fans, the fan is not stalled.
Warning	For Tachometer output fans, 12%-18% less than speed recorded at installation.
Alarm	For Tachometer output fans, more than 18% less than speed recorded at installation. For rotor stall fans, the fan is stalled.

Table 5. Sample Statements Accompanying Fan Trap Messages

Trap Event Code	Statement
Code 66	Fan State Changed: Warning to Nominal, 1
Code 67	Never generated for rotor stall fans.
Code 68	Fan State Changed: Nominal to ALARM, 0

Fibre Channel Interfaces

The SAN Data Gateway Module has two Fibre Channel ports. They are each equipped with a 2-Gigabit bi-directional SC-style shortwave multimode Gigabit Interface Converter (GBIC). The Fibre Channel ports support both 2 Gbit and 1 Gbit data links and can be connected to the storage area network or directly to Fibre Channel hosts.

Cables should be 50µm duplex multimode with an SC connector on the GBIC end and a connector appropriate to the host bus adapter (HBA) in use on the host end. Maximum cable length is 300 meters.

For more functional information, see “Appendix C. Application Notes” on page 179.

Fibre Channel ports support the following public and private loop modes:

- Target
- Initiator
- Target and initiator

Fibre Channel ports also support the following topologies:

- Loop
- Point-to-point
- Loop preferred

The Fibre Channel processor is in compliance with the following standards and specifications:

- Fibre Channel Arbitrated Loop (FC-AL-2) working draft, rev 6.4, August 28, 1998
- Fibre Channel Fabric Loop Attachment (FC-FLA) working draft, rev 2.7, August 12, 1997
- Fibre Channel Private Loop SCSI Direct Attach (FC-PLDA) working draft, rev 2.1, September 22, 1997
- Fibre Channel Tape (FC-TAPE) profile, T11/98-124vD, rev 1.13, February 3, 1999
- Fibre Channel protocol SCSI (FCP-SCSI)
- Fibre Channel internet protocol (IP)
- Fibre Channel virtual interface (FC-VI)

Ultra2 SCSI I/O Interfaces

The key features and capabilities of the Gateway's Ultra2 SCSI I/O interfaces are listed below.

- Four Ultra2 SCSI channels--low voltage differential/single-ended/ (LVD/SE)--with internal termination are available.
- SCSI channels have automatic speed and width negotiation capability for wide or narrow bus widths and standard, fast, ultra, or ultra 2 speeds. These parameters are viewed from the StorWatch Specialist.
- The default SCSI ID of each channel is 7 and can be changed from the StorWatch Specialist.
- Each SCSI channel supports up to 15 SCSI target IDs and up to 32 logical unit numbers (LUNs) per ID (subject to an overall total of 255 devices). The Gateway uses one LUN for command and control so that the remaining 255 LUNs are available for SCSI devices. For each Fibre Channel port, the Gateway occupies one Fibre Channel ID and all SCSI target devices are available as LUNs on the same Fibre Channel ID.
- The unit provides SCSI-3 68-pin VHDCI connectors for maximum mechanical reliability.
- External components include all cables, terminators, tape drives, and medium changers connected to the Gateway.

The SCSI interfaces are compliant with the following SCSI specifications:

- ANSI T10/1071D Rev. 6, SCSI-3 Fast-20
- ANSI T10/375D Rev. 10t, SCSI-2
- ANSI T10/1142D Rev. 20b, SCSI-3 Parallel Interface -2

Ethernet

The Ethernet subsystem has a PCI-attached network interface chip, and hardware to attach to a 10/100 Base-T port with an RJ-45 connector for out-of-band management. This is used for remote management of the Gateway. When the Gateway boots in diagnostic mode, the Ethernet Subsystem is locked out from any shell-based command and control. It can be connected to a network hub by using an unshielded twisted-pair Ethernet cable. The Ethernet port complies with the Institute of Electrical and Electronics Engineers (IEEE) 802.3 specification.

External components include any cabling, hubs, and switches that connect the Gateway to the network.

Service Port

Note: The service port connects to the host serial port with a 9-pin null-modem cable.

The service port is an RS-232 connection with a 9-pin D-shell connector (data terminal equipment (DTE)). It operates at 19 200 baud, 8-bits, no parity, and one stop-bit, XON/XOFF flow control. I/O is compatible with VT-100 terminals (or terminal emulators). It is used as a command and control interface to the Gateway.

The real-time licensed internal code (LIC) provides a shell interface for operators to type commands at the console. It is through this mechanism that the operator first sets up the Gateway.

External components include an RS-232 9-pin null-modem cable and an RS-232 or PC terminal attached to the Gateway.

The service port is used for local service and diagnostics when you use a terminal session to the shell interface.

The service port is configured at:

- 19 200 Baud
- 8 data bits
- No parity
- One stop-bit
- XON/XOFF

Firmware

The Gateway is a programmable device and contains an operating system and operational firmware.

If you are instructed to update your Gateway firmware, see “Updating Firmware and Configurations” on page 120. To update your StorWatch Specialist firmware, see “Updating Firmware” on page 70.

LED Indicators

The User panel of the Gateway provides LEDs that indicate the status and activity of the Gateway and its interfaces. See Figure 3.

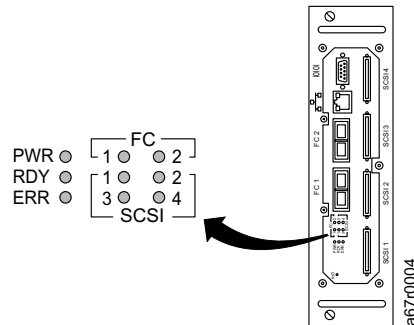


Figure 3. LEDs

When your tape library is first turned on, some of the LEDs will be on and others will flash while the tape library and the Gateway are booting.

The following list describes how to interpret the LED signals. See also, “Appendix F. POST Error Codes” on page 207.

Fibre Channel 1-2

For each Fibre Channel, the LED will be OFF when the Channel is not connected. It will be ON when the Channel is connected to a live Fibre Channel device. It will flash OFF and ON at a one-second rate when there is activity on the Channel.

SCSI 1-4

For each SCSI channel, the LED will be OFF when no devices have been detected on the port. It will be ON when a target has been found on the channel. It will flash OFF and ON at a one-second rate when there is activity on the channel. The LED will return to the OFF state if the channel is reset.

Power The PWR (Power) LED will be ON when the Gateway has power. It will flash if the on-board power sensors determine that any of the required supply voltages are out of range.

Ready The RDY (Ready) LED indicates status of Ready. Normally the RDY LED flashes once per second indicating good health. The RDY LED begins flashing after the Gateway has finished booting. If the RDY LED remains ON or OFF for more than a few seconds, it means that there is a problem.

The RDY LED will flash rapidly, four times per second, when the Gateway is running in diagnostic state.

ERR The ERR (Error) LED indicates that an error condition exists. This may indicate such errors as over-temperature conditions, fan stalled, or other internally detected error conditions. To locate the corresponding trap event code use Table 3 on page 6 and Table 5 on page 7.

Operating Specifications

This section contains the physical, electrical, and environmental specifications for the Gateway.

Physical Dimensions

The following information shows the physical dimensions of the Gateway:

- Height: 8.1 in (20.57 cm)
- Depth: 11 in (27.94 cm)
- Width: 2.2 in (5.59 cm)
- Weight: 4 lbs (+/-1 lb)

Operating Environment

Operating Temperature: 10–38°C (50–100°F)

Storage Temperature: –40–60°C (40–140°F)

Humidity: 20–80%

Power Consumption

The Gateway is powered by your tape library. Maximum power consumption is 64 watts, in active mode.

Note: For the 3583 Ultrium Scalable Tape Library only, the tape library must be powered with the new power architecture to support the additional power consumption. The NPA label is located on the power supply.

Service Capabilities

The Gateway service capabilities include the following:

- Power-on self-test (POST)
- Health check
- Event log
- Diagnostic suite

POST

POST initializes SDRAM and performs low-level hardware tests on the 405GP-related peripherals. POST then transfers control to the VxWorks BOOTROM program to handle the loading of the operational firmware.

Health Check

Health check queries all subsystems for their operational status. Health Check has four levels. A Level 1 health check is the most basic check and a Level 4 health check is the most complete.

Event Log

The Gateway maintains an event log within its on-board flash file system. These logs may be interrogated from either the StorWatch Specialist application or the Gateway's service port. Event codes and messages generated by the Gateway's subsystems are recorded in the event log file. The event codes and messages are reported via the SNMP to the StorWatch Specialist client monitoring application if the event threshold for an event is reached.

Diagnostic Suite

The diagnostic suite is a subset of the manufacturing test program. When enabled, the diagnostic suite is capable of performing external loop-back testing of all major hardware interfaces (SCSI, Fibre Channel, and Ethernet).

Service Tools

This section lists the following:

- Service port terminal requirements
- Service tool kit
- Generic tools (not provided)

Service Port Terminal Requirements

- An RS-232 terminal or PC/Laptop with terminal emulation software
- VT-100 compatible control characters
- 19 200 Baud
- 8 data bits
- No parity
- One stop-bit
- XON/XOFF flow control

Service Tool Kit

The service tool kit includes the following:

- Poly bag with label, PN 19P3346
- One null-modem cable
- .5 meter VHDCI-to-VHDCI SCSI wrap plug
- One Fibre Channel wrap plug
- One Ethernet wrap plug
- One SC to SC coupler

Generic Tools

The following list of tools may be required during service and are not shipped with the Gateway.

- Phillips head screwdriver: number 2 head
- Allen wrench: 1/8 inch
- Anti-static protection: wrist strap with grounding lead
- Dusting spray: compressed gas used to dust off optical connectors on the GBIC and fiber cable ends

Field Replaceable Units

Field replaceable units (FRUs) are the smallest part of a machine that are easily diagnosed and replaced. In today's environment, this may be the entire machine.

This section lists the field replaceable units (FRUs).

- Gigabit Interface Converter (GBIC). See Figure 4.
- The Gateway. See Figure 5.

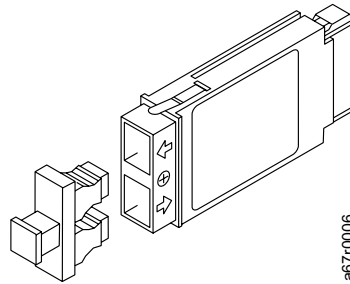


Figure 4. GBIC with dust protector

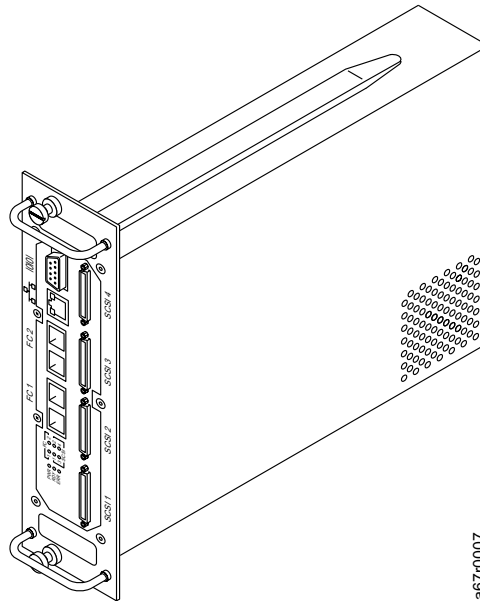


Figure 5. The Gateway

Introduction to the IBM StorWatch Specialist

Use the StorWatch Specialist to configure and monitor multiple Gateways remotely. The StorWatch Specialist uses a combination of industry-standard SNMP requests. The StorWatch Specialist also uses a method or technology known as SCSI over TCP, which encapsulates SCSI commands or data (or both) in TCP packets.

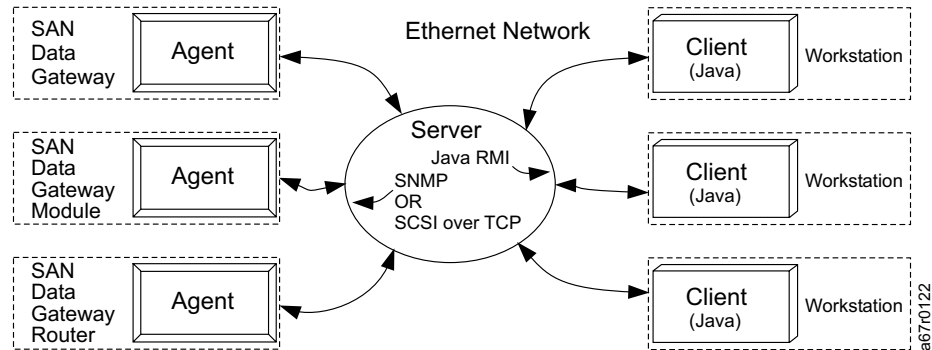


Figure 6. StorWatch Specialist application model

Client-Server Model

The StorWatch Specialist is part of a three-part client/server model.

Agent

Note: There is one StorWatch Specialist for all SAN Data Gateways.

Each Gateway is a stand-alone, SNMP-manageable host. The IBM StorWatch Specialist uses SNMP as the primary method of communication with the agents. This allows you to set and retrieve information that controls the operation of the agent. It also provides alerts (traps) when an event has occurred that requires intervention. The SCSI/TCP component allows you to update firmware on the Gateway, target devices, and manipulate device operating parameters. The agent component is embedded in the operating software of the Gateway.

Server

The server component is a Java application that runs on a host computer system (see "Installation Requirements" on page 29). The server is responsible for maintaining communication with the managed agents. The server acts as an intermediary between the agent running on the Gateway and multiple clients. It provides security features by maintaining account names and passwords on behalf of the client application. By keeping track of different client configurations, a user can recall a saved configuration from any client.

The server coordinates the requests from multiple clients to manage multiple Gateways. Communication between the server and the agent is carried out either by SNMP or SCSI/TCP, as required. Specifically, the Java Management Application Programming Interface (JMAPI) is used, where possible, to provide an industry standard and transportable interface. All communication between the clients and the server is implemented using the Java remote method invocation (RMI), a form of remote procedure call (RPC).

The server is written to be both transportable and efficient. Multiple clients can share data the server already knows about rather than having to request the data again. In addition, the server receives all traps from the agent and forwards them to clients that are registered to receive them.

Client

The client is also a Java application. One or more clients connect to a server to manage the Gateway. The client operates from any compatible computer, as long as a Transmission Control Protocol/Internet Protocol (TCP/IP) connection is established to the server component. This allows for dial-in configurations by using Point-to-Point Protocol (PPP), intranet, and Internet access (where allowed by local network policy and firewall configurations).

The client is the application that provides the user interface and allows viewing and manipulating all Gateway and device parameters. Each client can be configured by the individual user to show only the Gateway of interest. This means that one client can monitor one Gateway and other managers can be responsible for different Gateways, without interfering with each other.

The client uses Java RMI calls to communicate with the server and SCSI/TCP to communicate directly to the Gateway.

Features

SNMP

SNMP implements industry-standard SNMP v1 protocol, including support for the full MIB-II (RFC 1213), the host MIB (RFC 1514), and the Gateway MIB.

SNMP community strings serve to group network devices into logical collections for management purposes. The community strings on the server must match those on the Gateway that you are managing.

- The read community queries the Gateway
- The write community controls the Gateway
- The trap community receives event messages from the Gateway

The Gateway can maintain 32 read and write community strings and one trap community string.

SNMP Community Support

A set of commands is provided for manipulating the SNMP community strings. These strings act as passwords for authenticating requests that are made from managing applications such as the StorWatch Specialist.

There are three different communities defined:

- A read community allows the **Gets** command only
- A write community allows the **Sets** command, that is, it allows changes to be made
- A trap community defines the community string that a trap recipient will allow

In order for a managing application to view or control an SNMP agent (such as the Gateway), it must provide the correct community string for each request. The StorWatch Specialist allows up to 32 community strings for each of the read and write communities. There is only a single trap community string. See the SNMP commands in "Appendix A. Connecting to the Service Port" on page 117 for further information.

Security

You must log on to a server to access permissions administration. Two levels of privilege control what type of access is allowed:

- Administrator privileges allow full read and write access, including the changing of parameters
- User privileges allow the viewing of data and parameters only (read access)

Service port access is managed with user accounts that are created using Telnet or the serial interface on the StorWatch Specialist.

SAN Access Control

Channel zoning allows selective SCSI channels to be available to selective SAN connections.

Saved Views

Each user can store preferred views on the server. Loading a previous view automatically connects the user to one or more Gateways in a single step rather than specifying connections to Gateways individually. Because they are stored on the server, the same views are available to the user from any client.

Network Discovery

Network discovery allows you to locate any Gateway based on network addresses and network masks. This allows management of a Gateway without knowing the specific Internet Protocol (IP) address beforehand. Alternatively, the IP address (or name, if it can be resolved) of a Gateway can be entered directly by the user for instant access.

StorWatch Specialist Configuration

You can set up a Gateway with a number of non-default parameters, such as routing tables, channel settings, and event management variables.

Software Updates

You can update the Gateway firmware from the client. You can also send device microcode to individual target devices to update their firmware.

Event Logging

You can retrieve and view the Gateway event logs in a table. Filtering based upon the significance of events simplifies fault isolation.

Health Checks

Instantaneous and periodic health checks allow you to monitor each Gateway and the devices attached to it. You can select the level and interval of the health check to obtain greater confidence, or to minimize the impact on system performance.

Views

Two different viewing modes are available:

- **Tree view** shows all available Gateways and expands to show greater levels of detail.
- **Front panel view** shows the status of the indicators for a selected Gateway.

Heartbeat

Each component of the StorWatch Specialist monitors the components with which it communicates to ensure continuity of service. If the Gateway is not available, the server component notifies monitoring clients.

SCSI Device Address Mapping

The function of the Gateway is to connect a SCSI Library to the SAN or to a Fibre Channel Host. It is the library's "gateway" to the SAN. The four SCSI ports of the Gateway are connected to the tape library medium changer and the tape drives. The two Fibre Channel ports of the Gateway connect to the SAN or to a Fibre Channel host. These two Fibre Channel ports provide two independent paths to the SCSI devices in the tape library. A tape library attached to a SAN is available to all hosts on the SAN. The Gateway and all attached devices appear on the SAN or Fibre Channel host as a single Fibre Channel Loop ID (LID) with each device addressable at a unique LUN of that LID.

It is important to understand how devices attached to the SCSI channels appear to the Gateway and to the host systems. These devices would appear differently if they were attached directly to a host system without any intervening Gateway. A brief explanation follows. More detail is available in "Understanding and Modifying Devices" on page 181.

When the Gateway powers up, it scans the SCSI bus for attached devices. It "learns" the devices attached to it in terms of three parameters:

- The Gateway SCSI channel to which the device is attached
- The Device Target ID (SCSI address of the device)
- The Device Logical Unit Number (LUN)

These three parameters uniquely define the SCSI devices that are attached to the Gateway. Once the Gateway knows what SCSI devices are attached to it, it will proceed to give each device a Gateway LUN Assignment. Figure 7 shows a typical tape library configuration and Table 6 on page 18 shows the resulting Gateway LUN Assignments for each SCSI device.

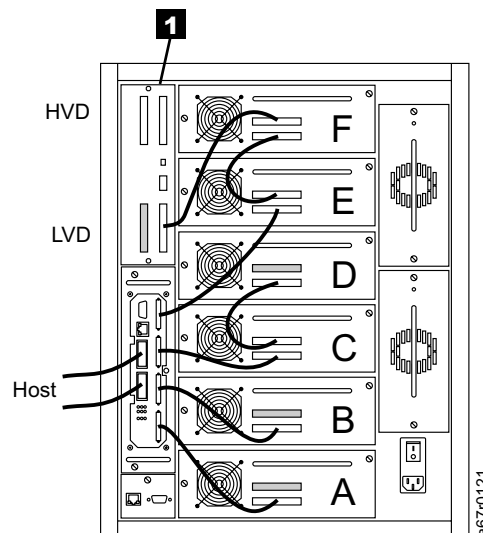


Figure 7. Rear-view of a tape library

Table 6. Example of Gateway mapping of SCSI addresses for a typical tape library configuration

Device Attached to Gateway	Gateway SCSI Channel	Device Target ID	Device LUN	Gateway LUN Assignment
Tape Library Medium Changer (1 in Figure 7 on page 17)	4	6	0	1
Tape Drive A (bottom)	1	8	0	2
Tape Drive B	2	9	0	4
Tape Drive C	3	10	0	6
Tape Drive D	3	11	0	8
Tape Drive E	4	12	0	10
Tape Drive F (top)	4	13	0	12

The Gateway starts the mapping process with its SCSI channel one. It finds the attached device that has the lowest Device Target ID and LUN. It assigns a new LUN value to that device (the Gateway LUN assignment). The Device LUN is not changed, but the Gateway assigns a separate Gateway LUN that will be used by the Gateway to identify that device to other devices outside the Gateway. Any host connected to a device through the Gateway will recognize the device by this Gateway LUN assignment and not by the device target ID and device LUN. The Gateway LUN assignment of 0 is reserved for the Gateway itself. LUN 0 is referred to as the Gateway Command and Control LUN. When assigning LUN's the Gateway will start with the lowest available LUN and assign that to the next device. All tape drives are assigned only even LUN's. The medium changer is always assigned an odd number. Since there is only one medium changer in the library, it will generally be assigned a LUN of 1. Assignment of LUN's for devices on channel one will continue in order of Device Target ID and Device LUN until all devices have received a Gateway LUN assignment. When channel one has been mapped, the Gateway will continue mapping channel two, three, and four in the same manner as channel one.

Address Persistency

The address map can contain up to 255 entries and is stored in non-volatile memory within the Gateway. The StorWatch Specialist has functions to manage the persistent device map. These functions are available in the **Controls** menu under **Device Mapping**. Commands to manipulate device map are also available over the service port. See “Appendix A. Connecting to the Service Port” on page 117 and “Appendix B. Service Port Command Reference” on page 123 for more information about the service port commands.

Once a Gateway LUN assignment is made to a specific channel, device target ID, and device LUN, that assignment will persist even if connected devices are powered down, replaced, or if the Gateway itself is powered down. LUN assignments will persist until a `mapRebuildDatabase` command is issued through the service port to reset all the LUN assignments. Some examples will help illustrate the address persistency:

1. If a drive in the tape library is replaced, the device target ID for the new drive will be set by the library. The target ID will be the same as the previous drive unless the user takes proactive steps to change the target ID through the tape library front panel. Upon powering-up the tape library, the new drive will occupy the same Gateway LUN assignment as the previous drive because the Gateway SCSI channel, the device target ID and the device LUN are the same as the previous drive. The replacement of drives does not force any new mapping of addresses if the new drive target ID is not changed and it is connected to the same Gateway SCSI channel as the old drive.
2. In the example configuration above, if the device target ID of Drive A was changed from 8 to 3 and the tape library was power cycled, Drive A would receive a new Gateway LUN assignment of 14. The Gateway LUN assignment of 2 would be preserved for a device on Gateway SCSI channel 1, with a target ID of 8, and a LUN of 0. Since no device currently matches that criteria, LUN 2 would not be active. If the device target ID of Drive A were changed back to 8 and the tape library power cycled, then Drive A would again have the Gateway LUN assignment of 2. LUN 2 would again be active and now LUN 14 would be inactive.

Persistency of addresses is important because host systems can become confused when a device appears at a different address than expected. If a device address changes, a restart of the host system may be required to relearn the new address of the device. If many host systems have access to the changed device, many systems may be affected. Persistency of addresses assures that a host will find a device where it expects it to be.

Alternate SCSI IDs

A host sends **Inquiry** or **Test Unit Ready** commands to a tape drive or changer device during system startup when it scans the SCSI buses. If another host is sharing the device and the device is busy with input and output (I/O) activity, it could take several minutes for the device to respond.

In a standard queuing model, the I/O command would block the command sent by the second host starting up. This command, sent by the second host could time-out, preventing the host from finding the device. The Gateway can issue a command to the drive, while another command is already in process. Additional commands are sent from a second or alternate ID on the SCSI channel. This technique allows the **Inquiry** or **Test Unit Ready** commands to be processed immediately.

When a Gateway receives a command from another initiator for the same device, the Gateway issues a command to the device by sending it from the alternate ID. The majority of the commands received by the Gateway are returned to the initiator with reservation conflict status. The Gateway uses the alternate ID to issue the following commands to the target device.

INQUIRY, TEST UNIT READY, PREVENT/ALLOW MEDIUM REMOVAL, RELEASE, REQUEST SENSE
--

Default Alternate SCSI ID

When the Gateway scans a SCSI channel, it determines which IDs are currently being used by target devices and sets the alternate ID to the highest ID not in use. The default primary SCSI ID is 7. If no target is present at ID 6, the Gateway chooses ID 6 for the alternate ID. Both the primary ID and alternate ID may be explicitly set, if necessary.

Changing the Alternate SCSI ID

The alternate ID can be set to any SCSI ID between 0 and 15. A system administrator could choose to explicitly set the ID to prevent the Gateway from selecting a particular ID not currently in use. This allows a device with a particular ID to be added in the future. The performance criteria based on SCSI bus priority may be a good reason for explicitly setting both the primary and the alternate SCSI IDs, rather than just accepting the defaults. See Figure 55 on page 62.

Setting Up Access Control

The Gateway allows you to connect more than one host to it. In the default configuration, all hosts can access all target devices. Host operating systems do not always handle multiple systems using the same target devices simultaneously. When more than one host tries to use the same disk drives or LUN, the file systems on those devices become corrupted. If multiple hosts access the same tape device, backup and restore operations might be interrupted.

If you choose the channel zoning feature, you can set the desired access between SAN connections and individual SCSI channels.

For further information about channel zoning see “Access Options” on page 58.

Note: Cluster configurations and some newer backup programs do manage concurrent access to devices.

If access control is not used for tape devices, the tape application must support reserve/release or provide some method (hardware, software, or manual) to control access to data on tape.

Fibre Channel Port Modes and Connection Options

The Fibre Channel ports support private and public Fibre Channel fabric loop attachments. Both loop and point-to-point connection options are available. The default port mode setting is public target, and the default connection setting is loop. From the IBM StorWatch Specialist, you can view the settings and change port parameters.

Port Modes

Target

In this mode, the port operates as a target allowing a Fibre Channel initiator (host or Fibre Channel switch) to attach to it. The port operates as either a private loop or a public loop, depending on whether a host or fabric is attached to it.

Initiator

In this mode, the port operates as an initiator allowing Fibre Channel targets (disks, tape devices, or Fibre Channel switch) to be attached to it.

Target and Initiator

In this mode, the Gateway can see target devices on the Fibre Channel, and initiators on the Fibre Channel have access to targets attached to the Gateway. The port operates simultaneously as a target and initiator.

Public and Private Loops

Public

With this option, the Gateway scans the loop for fabric devices. If it finds a fabric device, it logs in and queries the name server for target devices that are available on the fabric. If it finds targets attached to the fabric, it adds all of them to the device map. You can select this option if you are connecting a Fibre Channel switch to the port and you want the Gateway to see all available target devices attached to the switch. Otherwise, if target devices are connected directly to the port, it automatically switches to private mode.

Private

With this option, the Gateway scans the local loop for devices, but does not check for fabric devices. You can select this option if you are connecting target devices directly to the port.

Connection Types

Loop

With this connection option, the port operates with attached loop-capable devices. If a point-to-point device is attached, the Gateway will not be able to communicate with it.

Point-to-Point

With this connection option, the port supports point-to-point fabric connection (FC port login). It also operates in “old port mode” for compatibility with N-port devices that do not support loop. If loop-capable devices are attached, the Gateway cannot communicate with them.

Loop Preferred

With this connection option, the port operates in loop mode unless it detects a connection to a N-port device. If the port detects a connection to a N-port device, it automatically switches to the point-to-point connection option.

Preserving the Gateway Configurations

It is important to preserve the mapping of device addresses. The Gateway automatically saves the device map in nonvolatile storage to ensure that the persistence between starts and power cycles.

To provide a backup of the device maps and other configured parameters, use the StorWatch Specialist to save each Gateway configuration when you:

- Install the Gateway
- Add new devices
- Remove devices permanently
- Change target IDs or LUNs

Use the IBM StorWatch Specialist to save or load the configuration. See “Saving Gateway Configuration” on page 55 and “Loading Gateway Configuration” on page 56. You must save the configuration so that it can be reloaded in case you need to replace the Gateway base field replaceable unit (FRU).

Note that the Ethernet addresses and names are not included in the “saved” configuration file.

Note: Save a backup copy of your Gateway configurations frequently.

Chapter 2. Installation

This chapter covers installation of the IBM SAN Data Gateway Module, attached SCSI devices, and the host adapter. The SAN Data Gateway Module will be referred to in the rest of this chapter by the name Gateway. Before installing the Gateway, you must perform the steps in the pre-installation checklist.

Note: Ensure Gateway SCSI interfaces match the SCSI interfaces of the attached SCSI devices (LVD).

Instructions on how to install the product are divided into three sections:

- Pre-installation checklist

Before you install the Gateway, check the steps in Table 7 on page 24.

- Installation checklist

Has instructions on how to install the Gateway and the “Installation Checklist” on page 25, lists the steps you must perform to complete the installation.

- StorWatch Specialist installation checklist

After you install the Gateway, perform the steps in the “StorWatch Specialist Installation Checklist” on page 27.

Pre-Installation Checklist

It is important that you review the steps in Table 7 before you begin to install the Gateway. This ensures a successful installation of the product.

Note: Some steps may vary depending on which host platform you are attaching to the Gateway.

Table 7. Pre-Installation Checklist

Step	Action or decision	Comments and reference
1	Install any required host platform OS service pack or patches. For example, Microsoft® Windows NT® 4.0 with Service Pack 5, and any required software patches.	For a current list of supported platforms, required host platform code and updates, and information about how to obtain them, see the web site at: www.ibm.com/storage/ito
2	Install any required Fibre Channel host bus adapter firmware, HBA BIOS, and device driver.	For the latest list of supported HBA firmware, BIOS, and device drivers, see the web site at: www.ibm.com/storage/ito See also "Host Adapter Setup" on page 28.
3	If you connect more than one host to the Gateway, you may need to choose an access control option. If so, install the Host Registration Service on the Fibre Channel hosts that will be connected to the Gateway.	For the latest information, see the web site at: www.ibm.com/storage/ito
4	Ensure that all host fiber cables: <ul style="list-style-type: none">• Have been ordered with the product or have been pre-installed and checked• Are marked with:<ul style="list-style-type: none">– Host server identifier– Gateway identifier	Refer to the HBA specification provided with your HBA and to "SAN Data Gateway Module Description and Features" on page 4.
5	<ul style="list-style-type: none">• Mark both ends of each SCSI cable with:<ul style="list-style-type: none">– Target ID and channel number– Gateway ID and channel number	This step is usually performed during target installation.
6	Decide the Gateway network parameters. Assign the Ethernet port configuration information: <ul style="list-style-type: none">• Static IP address _____• Subnet mask (optional) _____• User defined Gateway name (optional) _____ <p>If the Gateway is not on the same TCP/IP subnet as the server¹, assign the default network gateway address or route table entries or both.</p> <p>Attention: Save this configuration information for future reference.</p>	Obtain your Gateway network parameters from your network administrator. Attention: Use of incorrect network parameters can cause problems on the Ethernet network. The default name is "gateway". If you choose a different name it becomes the prompt displayed on the service terminal. Choosing a different name may be useful if you have more than one Gateway.
7	Run the Ethernet cable from the NT server ¹ to the network hub.	None
8	Run the Ethernet cable from the network hub to the location where the Gateway will be installed.	None

¹ Server in this context means the computer used for the IBM StorWatch Specialist.

Installation Checklist

- The installation checklist has instructions on how to install the Gateway.
- Table 8 and Figure 8 provide the steps to install the Gateway.
- If the Gateway is already installed go to step 3 on page 25.

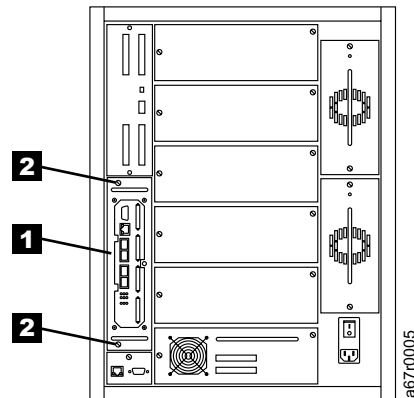


Figure 8. Gateway seated in a tape library

Table 8. Installation Checklist

Step	Action or decision	Comments and reference
1	Acquire information for Ethernet installation.	See step 7 in the "Pre-Installation Checklist" on page 24.
2	Insert the Gateway (1 in Figure 8) in the empty bay of your tape library. Align the power connection and seat unit firmly. Tighten the two thumbscrews (2 in Figure 8).	If the Gateway is already installed, continue with step 3.
3	Connect the service terminal to the service port and start up a terminal emulation session.	See "Appendix A. Connecting to the Service Port" on page 117.
4	Power on the tape library and observe the startup messages on the service terminal.	Look for the message that reads: Done executing startup script. Also, see "Appendix E. Startup Message Reference" on page 205. Within one minute, the ready LED should start flashing once per second. If you do not see the message Done executing startup script or if the ready LED is not flashing, go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
5	Invoke the initializeBox command from the service terminal. After you issue the command, the Gateway will restart automatically.	See "Appendix B. Service Port Command Reference" on page 123. Attention: This command erases all configuration information. Use the initializeBox command only when you install the Gateway for the first time.
6	Look for the message Done executing startup script on the service terminal.	None
7	Power off the tape library.	None

Table 8. Installation Checklist (continued)

Step	Action or decision	Comments and reference
8	<p>Connect the SCSI cables from the target devices to the Gateway.</p> <p>Note: This is an example configuration. See Figure 7 on page 17.</p> <ul style="list-style-type: none"> • Connect tape drive A on the tape library to SCSI 1 on the Gateway. • Connect tape drive B on the tape library to SCSI 2 on the Gateway. • Connect tape drive C on the tape library to SCSI 3 on the Gateway. • Connect tape drive D to tape drive C. • Connect tape drive E on the tape library to SCSI 4 on the Gateway. • Connect tape drive F to tape drive E. • Connect the tape library medium changer to tape drive F on the tape library. 	See "Checking for Problems on Attached SCSI Devices" on page 83.
9	Power on the tape library.	Within one minute, the ready LED should start flashing once per second and the message Done executing startup script should be displayed on the service terminal. For problems see "Checking for Problems on Attached SCSI Devices" on page 83.
10	Verify the host is set to the correct operating system.	See "hostTypeShow" on page 145.
11	Issue the targets command from the service terminal.	See "Appendix B. Service Port Command Reference" on page 123.
12	<ol style="list-style-type: none"> 1. Configure the Ethernet port (host name, address [see "ethAddrSet" on page 132], routes, enable ethernet, terminate, and restart). See Table 19 on page 123. 2. Connect the Ethernet cable from the network hub to the Gateway. 3. Observe the Ethernet link light-emitting diode (LED). 	<ol style="list-style-type: none"> 1. Configure the Ethernet port using information from the "Pre-Installation Checklist" on page 24. 2. If the Ethernet link LED is not on, go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
13	<ol style="list-style-type: none"> 1. Turn off the Fibre Channel hosts. 2. Connect the fiber cables from the Fibre Channel host bus adapters to the Gateway. 3. Turn on the Fibre Channel hosts. 	If the SAN connection status LED for the attached hosts is not on, check the fiber cables.
14	<ol style="list-style-type: none"> 1. Issue the fcShow command from the service terminal to show the status of each Fibre Channel interface that is installed and connected. 2. Issue the fcShowDevs command from the service terminal to show SCSI target devices that are connected as detected by the Fibre Channel interface. 	<p>See "Appendix B. Service Port Command Reference" on page 123.</p> <ol style="list-style-type: none"> 1. Look for the message Firmware State = Ready for each Fibre Channel interface. If the message Firmware State NOT = Ready, go to "Checking Fibre Channel Port Status" on page 89. 2. Check to see that all the SCSI target devices are detected by each Fibre Channel interface. If not, go to "Checking SCSI Channel Devices" on page 90.
15	Verify that all target devices are available to the host systems.	Use the appropriate host system utilities for disk and tape. If all devices are not available, restart the host systems and check again. If the problem persists, go to "Start MAP" on page 82.

Table 8. Installation Checklist (continued)

Step	Action or decision	Comments and reference
16	Perform the steps in the post-installation checklist (Table 9).	<p>In SAN configuration, two specific areas require attention.</p> <ol style="list-style-type: none"> 1. Access control 2. Saving the configuration <p>For more information about access control and saving the configuration, see "Setting Up Access Control" on page 21 and "Preserving the Gateway Configurations" on page 22.</p>

StorWatch Specialist Installation Checklist

Perform the steps listed in Table 9 after you complete the installation.

Table 9. Post-Installation Checklist

Step	Customer actions	Comments and references
1	Install the StorWatch Specialist software.	<p>See "Installing the IBM StorWatch Specialist Software" on page 29.</p> <p>The designated system will be used as the central point for monitoring and controlling Gateway management and configuration. It is not connected to the Gateway Fibre Channel interface.</p> <p>See the web site at: www.ibm.com/storage/ito for an updated list of supported systems.</p> <p>Also, see the web site at: www.ibm.com/storage/ito for an updated version of the StorWatch Specialist software.</p>
2	Ensure that the designated system has access to the same Ethernet subnet as the StorWatch Specialist server.	Consult with your network administrator.
3	Start the StorWatch Specialist server.	See "Startup and Configuration" on page 30.
4	<p>Start the StorWatch Specialist client:</p> <ol style="list-style-type: none"> 1. Connect to the server (if it does not find the server running on the same system). 2. Log on. 3. Add a new administrator account and password. 4. Log off and log on using the new administrator account. 	<p>See "Starting the StorWatch Specialist" on page 34.</p> <p>Connect using the name or IP address of the designated server system.</p> <p>See "Startup and Configuration" on page 30.</p>
5	From the client, connect to the desired Gateway.	See "Connecting a Gateway" on page 49.
6	Save your user and administrator setups.	See "Save Current View" on page 36.
7	<p>If later firmware is available, perform the following for each Gateway:</p> <ol style="list-style-type: none"> 1. Update the firmware 2. Restart 	<p>See the web site at: www.ibm.com/storage/ito to download the latest available firmware.</p> <p>See "Controls Menu" on page 57.</p>
8	If you chose an access control option in "Pre-Installation Checklist" on page 24, use the IBM StorWatch Specialist software.	See "Access Options" on page 58.

Table 9. Post-Installation Checklist (continued)

Step	Customer actions	Comments and references
9	At this time you <i>must</i> save your Gateway configuration.	See "Saving Gateway Configuration" on page 55.
10	Become familiar with using the StorWatch Specialist.	See "Chapter 3. Using the IBM StorWatch SAN Data Gateway Specialist" on page 33.
11	You must use the StorWatch Specialist to monitor and maintain your Storage Area Network. If a trap or event is reported by the StorWatch Specialist, check the reported event codes. See "Action reference table" on page 88 to perform the recommended action.	See "Chapter 4. Remote Event Notification" on page 73.
Note: It is highly recommended that you save your Gateway configuration periodically. You <i>must</i> save your configuration if you make changes to access control or operating parameter settings.		

Host Adapter Setup

Hosts are connected to the Gateway through specific Fibre Channel host bus adapters (HBAs). The installation procedure varies slightly, depending on which adapter you will be using. The procedure involves these steps:

1. Install the adapter in the host system.
2. Turn on the power to the host system and update the adapter firmware, if necessary.
3. Start the operating system and install the device driver for the HBAs.
Perform steps 4 and 5 after the Gateway is installed and connected to the host system.
4. Restart and verify that the device driver has started and that expected target devices are seen by the operating system.
5. Install optional utility software, if desired.

For guidelines to configure the Gateway for maximum performance, refer to the host section of your tape library's documentation.

Startup Sequence Guidelines

You must start the tape library with the Gateway installed and the attached hosts in a specific order. When you add or remove SCSI devices or update firmware, you must restart. The following procedures describe the situations and order of procedure when you restart the tape library installed with the Gateway.

Attention: Before you restart the Gateway, you must stop all input and output (I/O) activity between the host and SCSI devices.

1. Gateway

The Gateway scans the SCSI buses when it starts. If you add or remove SCSI devices after the Gateway has started, the Gateway will not detect the changes. You can invoke a SCSI rescan or restart operation from either the StorWatch Specialist client or the service terminal.

2. Fibre Channel hosts

Before you turn on or restart the hosts that are connected with Fibre Channel to the Gateway, you must wait until the Gateway has finished starting. You will know the Gateway has finished starting when the ready light on the front panel blinks at frequency intervals of one second.

- Some operating systems provide you with software methods that allow you to add or remove SCSI devices dynamically after the host has started. To ensure reliable operation, restart the host.
- If you update the Gateway firmware, you must restart the Gateway to use the new firmware. To ensure compatibility between the firmware features or functions and the host, restart the host.
- If you update SCSI device firmware, the Gateway Explorer application does not display the new firmware version until the Gateway has issued a SCSI inquiry. The SCSI inquiry occurs when the Gateway rescans the SCSI buses. The SCSI inquiry also occurs when the StorWatch Specialist client application or the service terminal rescans the SCSI buses.

Installing the IBM StorWatch Specialist Software

The StorWatch Specialist software allows you to manage multiple Gateways from any location on your network. The system consists of two Java applications. You can install the server on a single system on your network and manage connections between multiple clients and multiple Gateways.

This section describes the installation and initial configuration of the server and client components. The installation for the StorWatch Specialist consists of three components, as described in “Client-Server Model” on page 14. The agent component is provided as part of the operating software already installed on the Gateway hardware.

The installation program installs the appropriate software components on your server and client system. It also installs the Java runtime environment (JRE).

Server

The system used for the server does not need to be used as a client and can be placed in a locked closet. It does need network access to the Gateways it will be managing, so appropriate routes need to be set up on the server system and on the Gateways.

Client

The client system can be located anywhere as long as it can connect to the server system using TCP/IP.

Installation Requirements

For an updated list of supported platforms and installation instructions, see the web site at:

www.ibm.com/storage/lto

An example of the installation requirements for Windows NT follows.

Installing the Software in Microsoft Windows NT

The following information shows the minimum server and client system requirements for installing the StorWatch Specialist software on the Microsoft Windows NT operating system.

Server system requirements

- Windows NT 4.0 server or workstation, Service Pack 5 or later
- Minimum memory: 64 MB
- Free hard disk space: 40 MB
- Ethernet with TCP/IP protocol installed

Client system requirements

- Windows NT 4.0 server or workstation, Service Pack 5 or later
- Minimum memory: 96 MB
- Free hard disk space: 30 MB

Perform the following steps to install the software on Windows NT:

1. Log on to the target machine with administrator privileges.
2. Download the latest Gateway firmware from the web site at: www.ibm.com/storage/lto
3. The default installation option is set to install the StorWatch Specialist client. You must install both the server and the StorWatch Specialist client software. One workstation on the network must contain the server software. The client software can also be on the same workstation. More than one client only can be installed on the same network.

Startup and Configuration

The first time you install the server component, there is one predefined user account that has administrative privileges. That account is called *Admin* and the default password is *password*. Note that user names and passwords are case-sensitive.

1. Start the server application.
2. Start the client application.
3. Connect the server (this is automatically done if the server and client are started and run on the same system).
4. Log on to the server. See Figure 9 on page 31.
5. Add a new user account with administrative privileges. See Figure 10 on page 31.

Note: For information about starting the StorWatch Specialist server and client for Solaris, AIX, and other platforms, refer to the following web site at:

www.ibm.com/storage/lto

To start the server using Windows NT:

1. Click **Start**.
2. Click **Programs** —> **StorWatch Specialist** —> **Server**.

To start the client using Windows NT or Windows 2000:

1. Click **Start**.
2. Click **Programs** —> **StorWatch Specialist** —> **Client**.

To log on, type Admin in the **Enter User Name** field and type password in the **Enter Password** field, then click **OK** (see Figure 9).

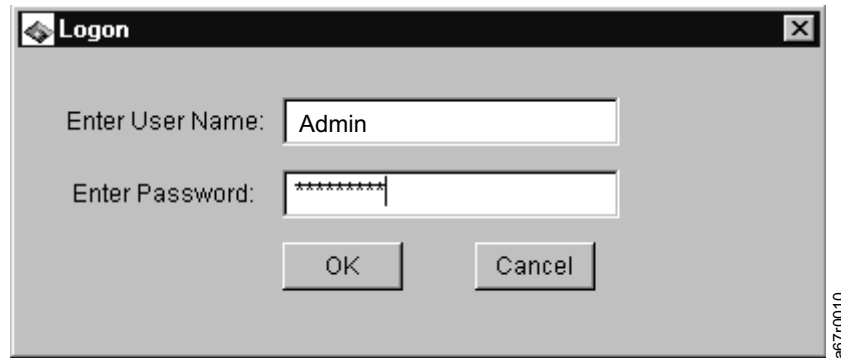


Figure 9. Logging on to the Server

To add a new administrator account, click **Admin —> Add User**. Type in the information in all the fields of the Add New User pop-up window (see Figure 10). After you add a new administrator account, the **StorWatch Specialist** account is deactivated.

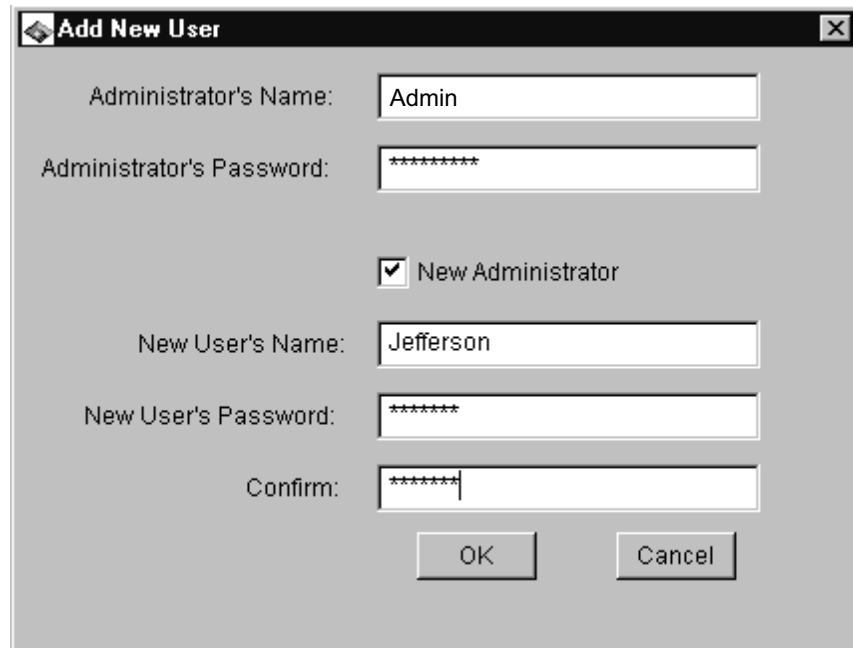


Figure 10. Creating a New Administrator Account

Note: Save your administrator account information in a secure location.

Use the new administrator account to set up other user accounts (with or without administrator privileges) that you might need.

Chapter 3. Using the IBM StorWatch SAN Data Gateway Specialist

Menus in the StorWatch Specialist allow you to view the SAN Data Gateway Module, the devices connected to them, and to perform various actions. The SAN Data Gateway Module will be referred to in the rest of this chapter by the name Gateway. From the main window, six major menu groups are available:

- File
- View
- Admin
- Tools
- Controls
- Help

Some menu options will appear grayed, signifying that they are currently disabled. Options can be disabled for one of two reasons:

- Insufficient user privileges
- The option does not apply to the currently selected item

There are two privilege modes:

- User
User privilege allows you to only read data. User privilege does not allow you to make changes to the Gateway setting, configurations, or to the list of users.
- Administrator
Administrator privilege allows you to have full read and write access to all options.

Unless otherwise noted below, administrator privilege is required to modify any parameter.

See “Startup and Configuration” on page 30 for information on starting the server component.

Starting the StorWatch Specialist

Before a client can manage any Gateway, it must connect to the server. If the server and client are running on the same system, you must start the server first, then start the client. When the application starts, it displays the Connect to Server pop-up window. See Figure 11.

Enter either an Internet Protocol (IP) address or a name which is resolved by the

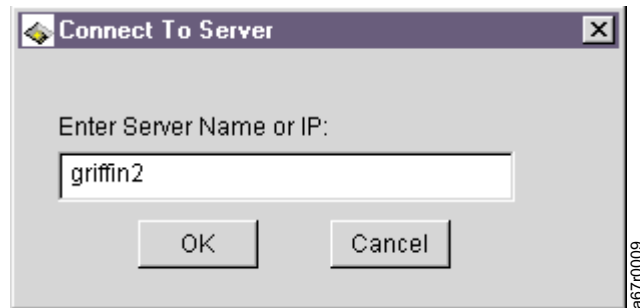


Figure 11. Connecting to the Server

client system. Log on after connecting to the server. See Figure 12.

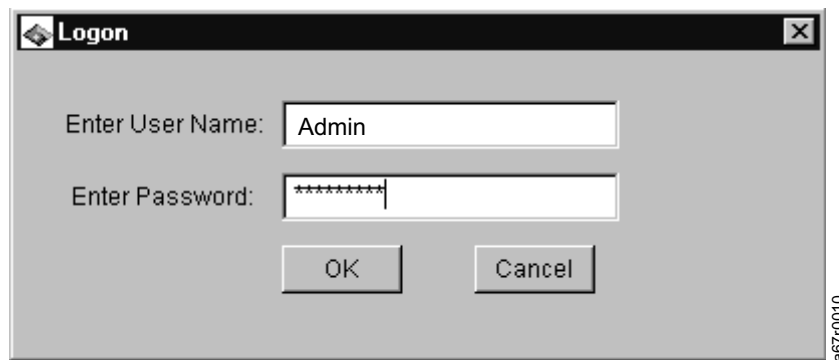


Figure 12. Logging on to the Server

Unless you have added your own administrator-level account, use the default account as specified in “Startup and Configuration” on page 30.

At this point:

- Retrieve a saved setup. See “File Menu” on page 36.
- Perform a “Discovery” of all Gateways on a subnet. See “Tools Menu” on page 47.
- Connect directly to a Gateway. See “Tools Menu” on page 47.

Figure 13 shows the initial tree view for a client connected to a Gateway.

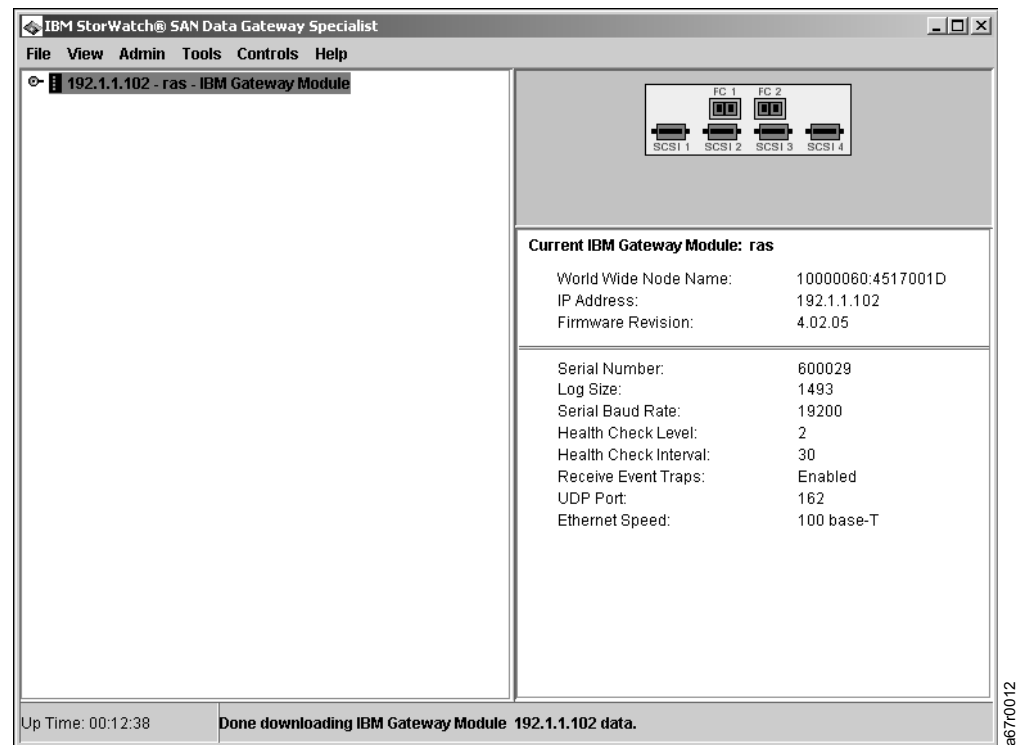


Figure 13. Initial Tree View

The tree view in Figure 13 is an unexpanded tree view for a single Gateway. For an expanded view, see Figure 18 on page 38.

The Gateway's main screen is made up of two panels:

1. Tree view panel on the left.
2. Data panel on the right.

On the top, right side of the screen, is a representation of the Gateway's channel configuration as it appears on the back of the Gateway.

The Gateway IP address is displayed to the right of the Gateway icon followed by the Gateway name and device type.

Product data for the selected Gateway is displayed textually below the channel configuration graphic.

At the lower left of the window, the up time for the selected Gateway is displayed. Up time indicates how many hours, minutes, and seconds have elapsed since the Gateway was last started.

The area at the very bottom margin of the window is used to display status messages. See "View Menu" on page 38.

File Menu

The File menu items allow you to load, manipulate, and save view files. See Figure 14.

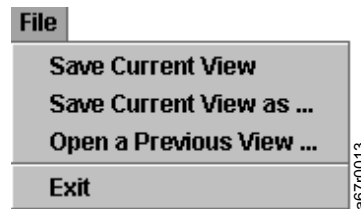


Figure 14. File Menu

A view file is a list of Gateways viewed at any one given time. Each user can save preferred views on the server. Loading a previous view automatically connects the user to one or more Gateways in a single step. Because the view files are stored on the server, the same views are available to use from any client.

You can have many views. At the beginning of a session, you can choose to load a view by clicking on **Open a Previous View**. All the views that you saved previously (for your logon account only) are displayed so that you can recall an earlier viewing environment.

Save Current View

The current collection of Gateways being viewed defines the view. For this option to be available (not grayed-out), the current view name must be known either from a previous loading or from a **Save Current View as** operation. For example, if you initially load a view containing Gateways A, B, and C, and during the course of the session, disconnect from B. Performing a **Save Current View** saves only A and C and the original view is overwritten by the new view. If you did not perform a **Save Current View**, the original view of Gateways A, B, and C is still valid for the next time that view is loaded.

Save Current View as

When you click on **Save Current View as...**, you are prompted to enter a name or short phrase that identifies the view (see Figure 15). Enter this name or phrase and click **OK**. You can choose to reload the same view in the future.



Figure 15. Saving the Current View

Opening a Previous View

Figure 16 is an example list of views that are previously saved by a user. From this list you can select a view by clicking on the name, and then selecting an action option.

If you click **Load**, you are returned to the main window. In a few seconds the StorWatch Specialist establishes connections to all of the Gateways in the view and displays them on the window.

If you click **Delete**, the selected view is removed from the list. You can delete any views that you choose.

If you click **Close**, the window closes, and you are returned to the main window.

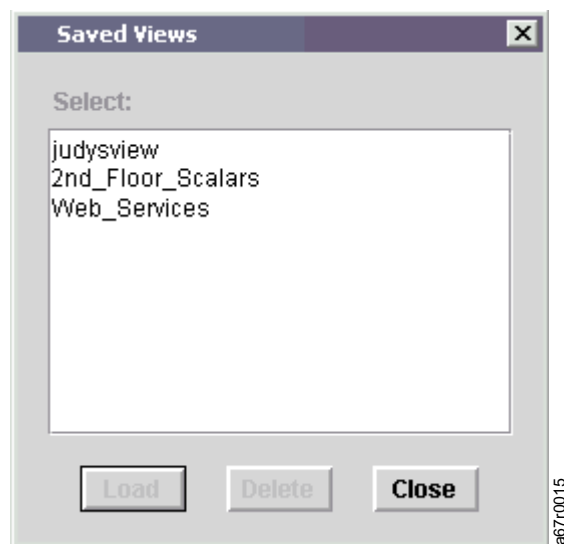


Figure 16. Saved Views

Exit

Exit stops the StorWatch Specialist client and closes the window.

Note: If you exit after making changes to a view without selecting a save option, the changes you made are lost.

View Menu

The View menu offers two display options. You can view the entire collection of Gateway in a hierarchical tree, or you can view the front panel of a single Gateway. See Figure 17.

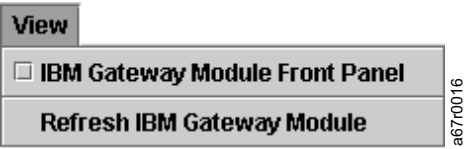


Figure 17. View Menu

Tree View

The tree view is the default view and is selected when the Gateway front panel option is unchecked. In the tree view, you see icons representing one or more Gateways in a hierarchical tree structure.

When you click the node symbol, to the left of the Gateway icon, the tree view expands to show connected elements that are represented by other icons (see Figure 18). Gateway nodes expand to show channels and channels expand to show attached devices. Product data for the selected tree node is displayed on the right side of the window. When you click the node symbol of an expanded element, its tree collapses.

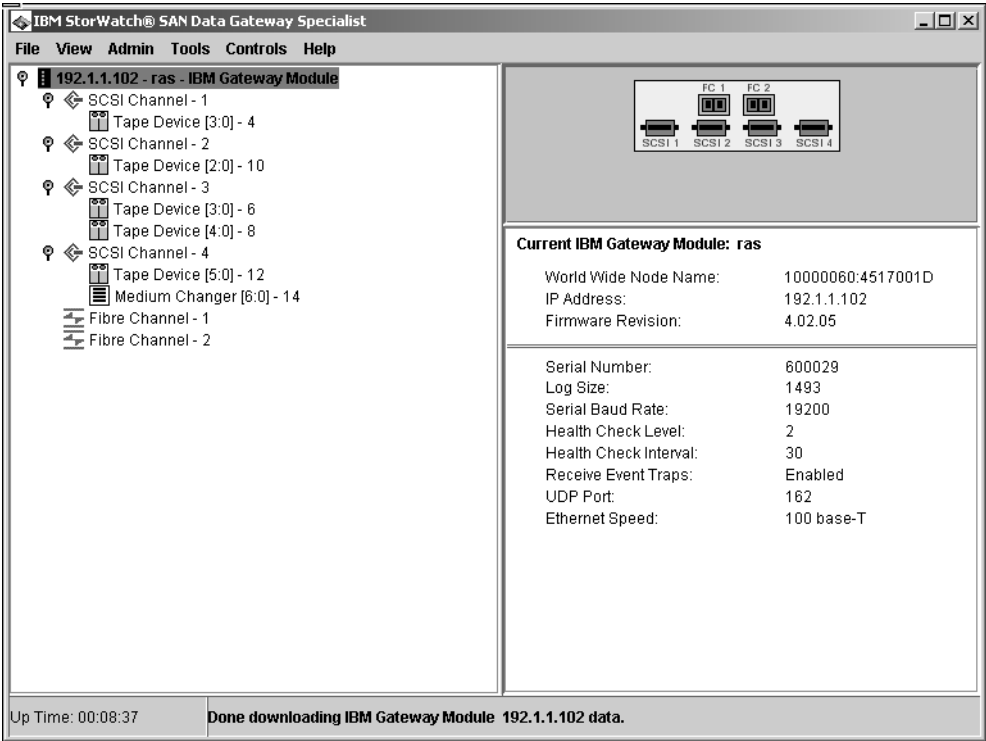


























Figure 18. Expanded Tree View

The icons used in the tree view carry specific meaning, both in their design and in their color. See Figure 19 and Figure 20.

Tree View Icon	Mode	Channel Type	Front Panel Icon
Blue 	Target	Ultra2/3 SCSI Low Voltage Differential	
Green 	Initiator	Ultra2/3 SCSI Low Voltage Differential	
Blue 	Target	Ultra2/3 SCSI Low Voltage Differential	
Green 	Initiator	Ultra2/3 SCSI Low Voltage Differential	
Blue 	Target	Short Wave Fiber Optical Long Wave Fiber Optical Copper Fiber	
Green 	Initiator	Short Wave Fiber Optical Long Wave Fiber Optical Copper Fiber	
Purple 	Target/Initiator	Short Wave Fiber Optical Long Wave Fiber Optical Copper Fiber	

a67r0039

Figure 19. Tree View Icons for Channel Modes and Channel Types

Icon	Name
	Disk Device
	Disk Device
	Tape Device
	Tape Device
	Tape Device
	Medium Changer
	Gateway or Router
	IBM Gateway
	Host
	Switch

a67r0019

Figure 20. Tree View Icons for Devices

In Figure 18 on page 38, one of the channel icons in tree view is blue, others are green, and one is purple. Blue indicates that the channel is in target mode. Target is the default mode for Fibre Channels. When channels are set to target mode, you are able to see attached hosts, and switches like the Brocade switch, which broadcasts a world wide name.

Green indicates that the channel is in Initiator mode. Initiator is the default mode for SCSI Channels. When channels are set to Initiator, you will be able to see attached devices and Gateways.

In addition to target mode and initiator mode, Fibre Channels can function in target and initiator mode. When that is the case, the Fibre Channel icon is purple. Fibre Channel 1 in Figure 18 on page 38 is set to target and initiator mode. You will be able to see hosts and devices, as well as cascaded Gateways when a channel is set to target and initiator mode. If there is no node symbol preceding a Channel, as for example Fibre Channel 2 in Figure 18 on page 38, there are no attached elements to display. StorWatch Specialist will not display an icon for a switch that does not broadcast a WWN. If there is no node symbol preceding a SCSI Channel set to target mode, a SCSI host could still be attached. The StorWatch Specialist does not display SCSI hosts.

In Figure 18 on page 38, the Gateway is selected. Product information about the Gateway appears in the data panel, which is in the lower right half of the StorWatch Specialist main screen. The data panel presents a variety of information, including the unit's WWN, IP address, firmware revision, serial number, and Ethernet speed.

When a channel is selected, the lower part of the data panel display includes the WWN, port mode, connection type, and maximum speed. See Figure 21. The firmware revision level of the HBA attached to the selected channel is presented as distinct from the firmware revision level of the Gateway.

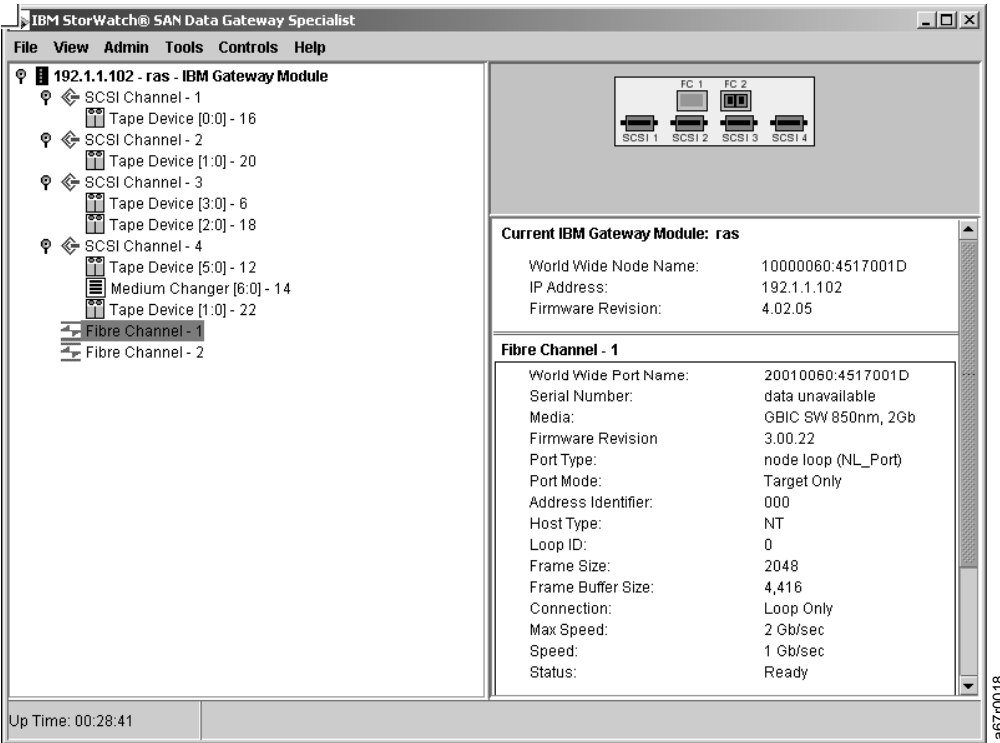


Figure 21. Information about a Selected Channel

When a device is selected, information about its width and speed are included in the lower portion of the data panel. See Figure 22.

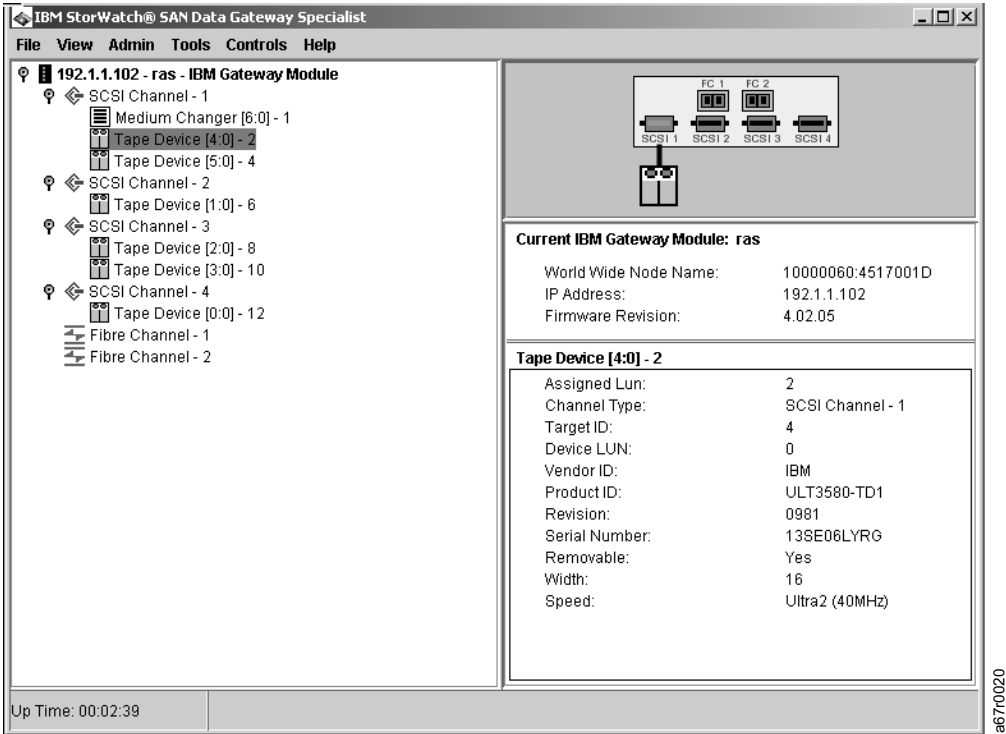


Figure 22. Information about a Selected Device

When a host is selected, information about its WWN, network name, operating system, and HBA attachment, is all included in the lower portion of the data panel. See Figure 23.

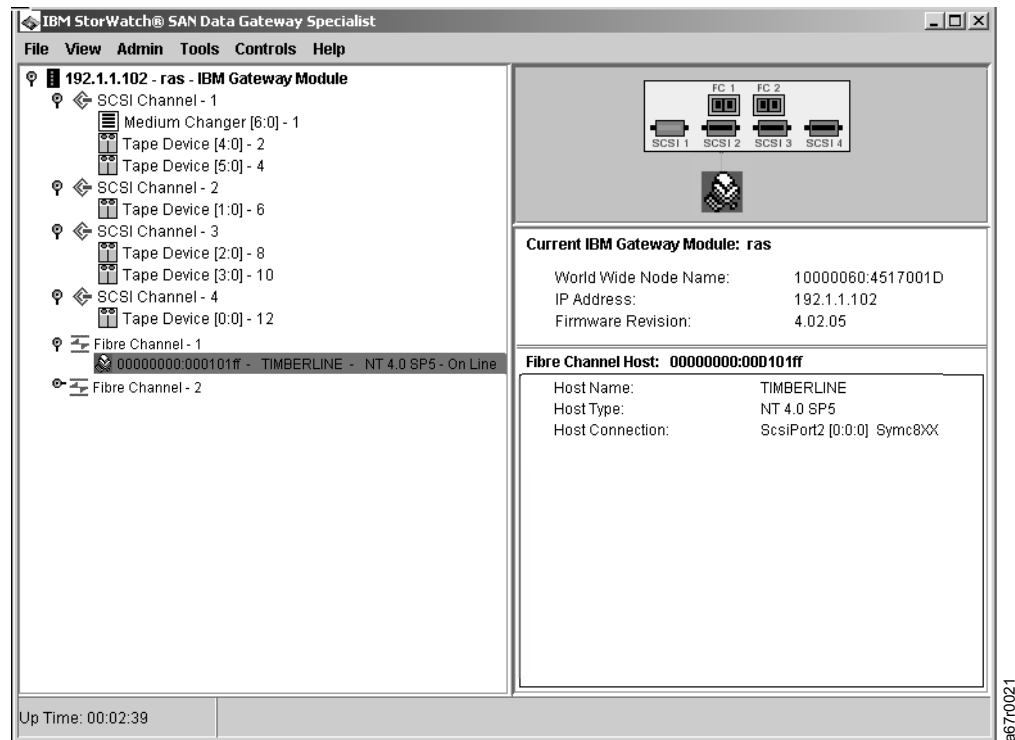


Figure 23. Information about a Selected Host

Each component in tree view (host, channel, device, or the Gateway itself) states the data panel IP address, name, WWN, and firmware revision level of the current Gateway.

Some information that is presented in the tree view panel is also presented in the Data panel. For example, both tree view and the data panel display the channel number, target ID, device LUN and assigned LUN of a device. Tree view graphically specifies the device type. The data panel displays textual information about the vendor ID, product ID, serial number, as well as other information about the size and capacity of the device.

At the top of the data panel there is a graphic showing the front of the Gateway. In Figure 22 on page 41, for example, the slot where the selected device attaches is shown in green. The slot is connected by a black line to an icon appropriate to the device being represented. For hosts, the slot is connected by an orange line to an icon representing the host. See Figure 23. Note that when the channel itself is selected neither the host nor the device icon appears in the Gateway front view graphic.

SAN Data Gateway Module Front Panel View

Checking the Gateway front panel option displays a front panel view. The front panel of the Gateway is visible from the back of the tape library. See Figure 24 for an example of a front panel view. The front panel lights reflect the status of the light-emitting diodes (LED)s on the front panel of the Gateway. The lights are refreshed automatically, about five times per second. Data pertinent to the Gateway is displayed below the front panel view.

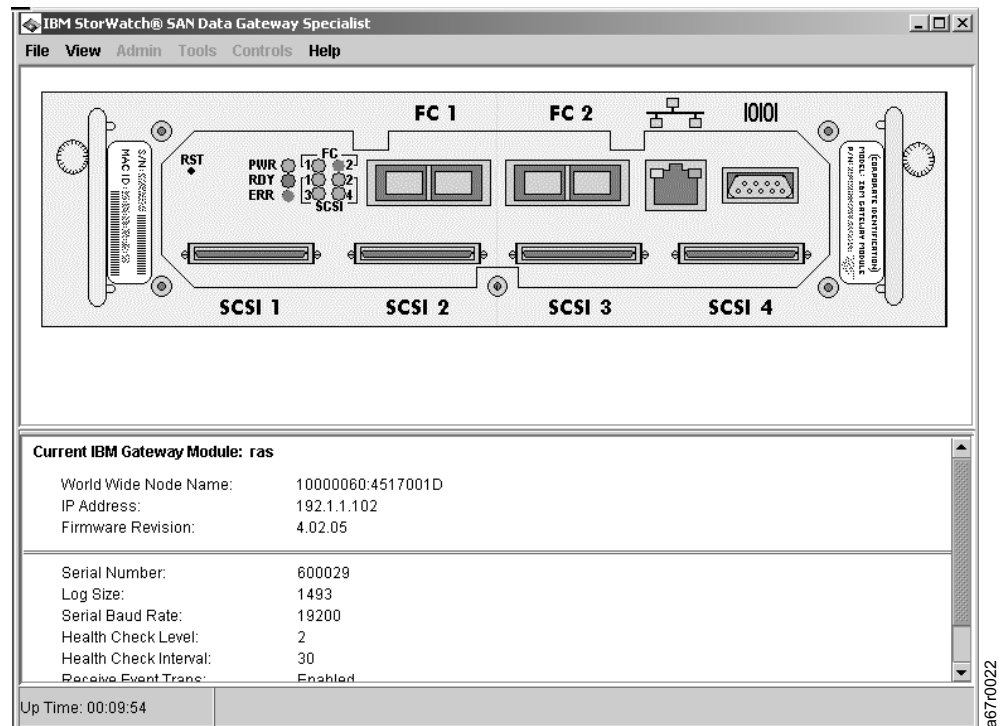


Figure 24. Front Panel View

Refresh Gateway View

When you click **Refresh Gateway**, the StorWatch Specialist client requests the server to contact the selected Gateway and update all data. This refreshes the data for the Gateway, and all attached devices to the most current information.

Admin Menu

The Admin menu allows you to connect to the server, log on, change passwords, add users, or remove users. See Figure 25.



Figure 25. Admin Menu

Connecting to Server

When you click **Connect to Server**, you are prompted to enter the name or IP address of the server machine. See Figure 26. You will receive a message that your connection was successful or unsuccessful in the status message line at the bottom of the display window. After you make a successful connection, log on to the server.

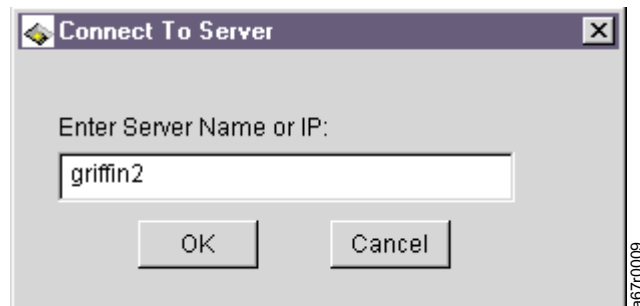


Figure 26. Connecting to the Server

Logging On

To log on, enter a user name and password. See Figure 27. If your logon is successful, a message that shows the user privilege level is displayed on the message line. If your logon is unsuccessful, the status line shows the reason for the logon failure.

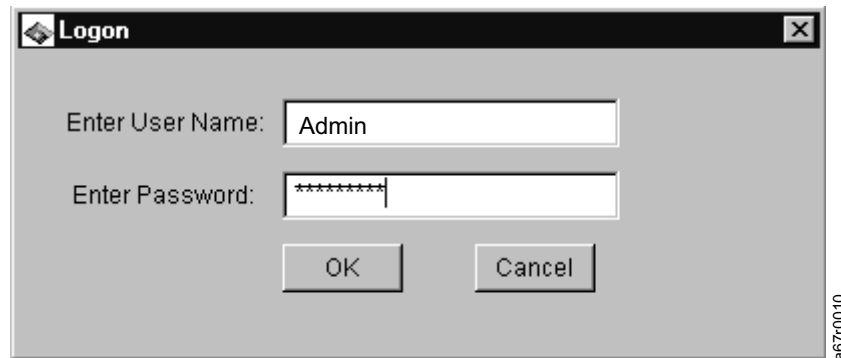


Figure 27. Logging On to the Server

Changing Password

After you log on successfully, click **Change Password** to change the password. See Figure 28. Type the current password, the new password, and the new password again to confirm the spelling of the new password. Click **OK** to verify whether or not the new password is valid. You will see a message on the main display window that shows the status of your transaction.

If you do not want to change your password, click **Cancel** and you will return to the main display window (your old password remains in effect).

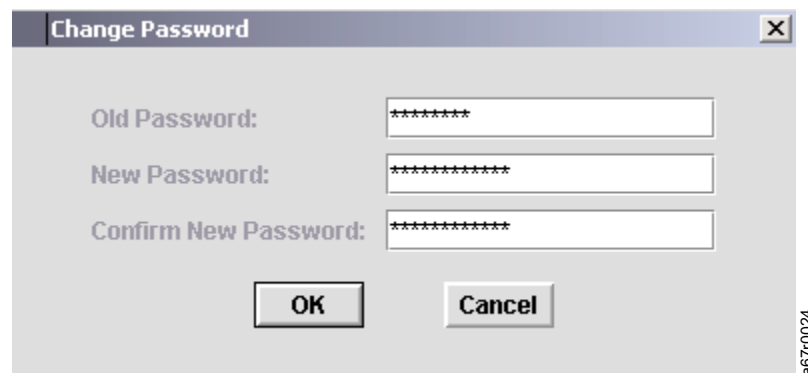
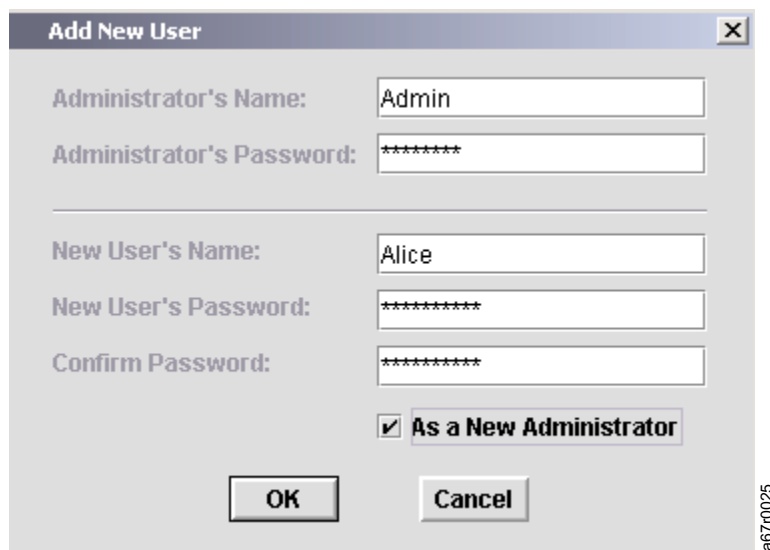


Figure 28. Changing a Password

Adding a New User

After you log on successfully, click **Add User** to add a new user. See Figure 29. This option requires administrator privileges. Type an administrator account name and password, and the new user name and password, typing the password again to confirm. If you want to give the new user administrator privileges, select the **New Administrator** check box. Click **OK** to perform this task and return to the main display window.

A screenshot of a Windows-style dialog box titled "Add New User". The dialog has a close button (X) in the top right corner. It contains several input fields and a checkbox. The first section is for the administrator: "Administrator's Name:" with a text box containing "Admin", and "Administrator's Password:" with a text box containing "*****". The second section is for the new user: "New User's Name:" with a text box containing "Alice", "New User's Password:" with a text box containing "*****", and "Confirm Password:" with a text box containing "*****". Below these fields is a checkbox labeled "As a New Administrator" which is checked. At the bottom are "OK" and "Cancel" buttons. A small vertical text "a67r0025" is visible on the right side of the dialog box.

Add New User

Administrator's Name: Admin

Administrator's Password: *****

New User's Name: Alice

New User's Password: *****

Confirm Password: *****

☒ As a New Administrator

OK Cancel

a67r0025

Figure 29. Adding a New User

Removing a User

After you have logged on with administrator privileges, click **Remove User** to delete a user, see Figure 30 on page 47. Type an administrator name and password. Click on the name of the user that you want to remove. Click **Remove** to remove the user, and click **OK** to close the pop-up window and return to the main display window.

Click **Cancel** to cancel the request and return to the main window.

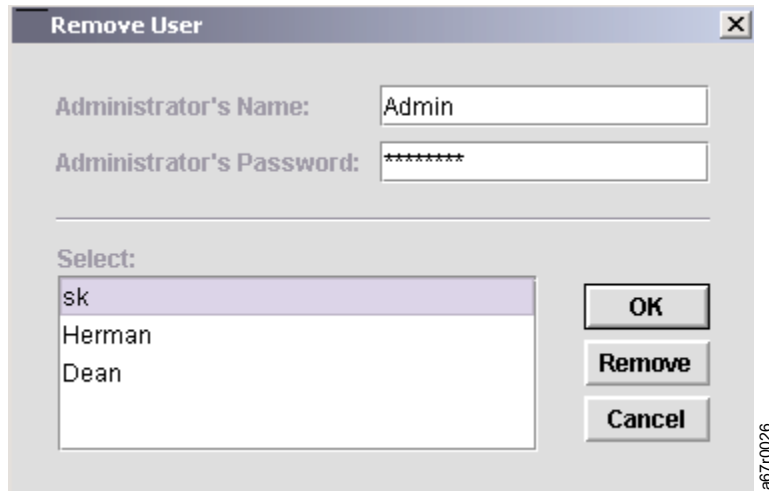


Figure 30. Removing a User

Note: If you lose the administrator password and there is no other account set up with administrator privilege, see the web site at: www.ibm.com/storage/lto.

Tools Menu

The Tools menu allows you to locate and connect to Gateways and to control how the Gateway status is reported. See Figure 31.

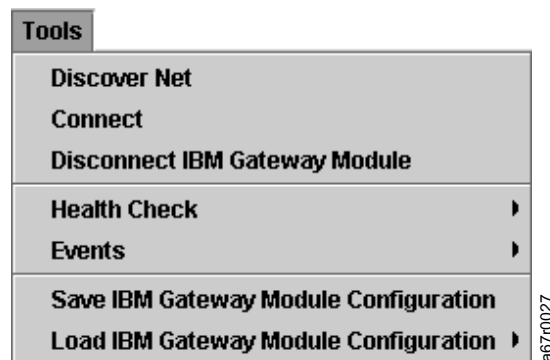


Figure 31. Tools Menu

Discover Net

Click **Discover Net** to discover all Gateways on a subnet (see Figure 32). Type the net address and the mask, which define the subnet where you want to perform the discovery. Type a timeout value in milliseconds to specify the maximum time to wait for a response from a given IP address. If no response occurs within the timeout period, it is assumed that no Gateway resides at that address. The address is incremented to the next value and tested for a response in the same manner. If a Gateway does respond, it becomes part of the reported list of Gateways that will define the new configuration. Before starting the discovery process, you are given an estimate of how long the discovery will take. At that point you will have an opportunity to cancel the process or to continue.

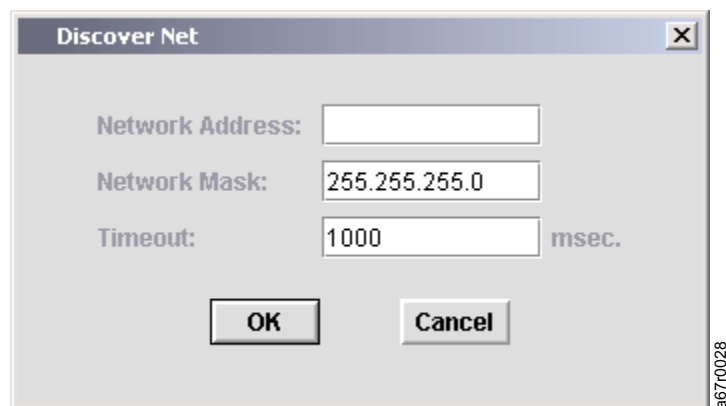


Figure 32. Discover Net

In the network address box, enter “0” in the place of the subnet you wish to explore. For example, the entry “192.168.22.0” searches for IP addresses between “192.168.22.0” and “192.168.30.255”.

In the network mask box enter a subnet mask that matches the class of network you are searching, for example, for a network address entry of “192.168.30.0” leave the default entry “255.255.255.0” as the network mask. For a network address entry of “192.168.0.0” change the network mask to “255.255.0.0”.

You must enter a timeout value in milliseconds to limit how long to wait for a response from each IP address that is checked. You may set the timeout value considerably lower than the default (1000 milliseconds) in order to speed discovery. Before starting the discovery process, you are given an estimate of how long the discovery will take. You have the opportunity to abort the process or continue.

The default timeout value is intentionally set to a high number in order to make certain that all devices on a slow network are discovered.

When the discovery is finished, a tree view displays a node for each Gateway discovered. The collection of Gateways displayed at the end of a discovery defines the current view. If a view was already loaded, the new Gateways discovered become part of that view *only if you save the current view*. Save the current view by clicking **File → Save Current View**. To create a new view with a different name, click **File → Save Current View as...** (see “File Menu” on page 36).

Connecting a Gateway

Click **Connect SAN Data Gateway Module** to connect to a specific single Gateway. See Figure 33. Type the name or address of the Gateway and click **OK**. To use names, the name must be resolvable to an IP address by the server system. Contact your network administrator for assistance. If found, the Gateway is added to the tree view. If a view was already loaded, the new Gateway becomes part of that view only if you click **File —> Save Current View**. To create a new view with a different name, click **File —> Save Current View as....** See “File Menu” on page 36.

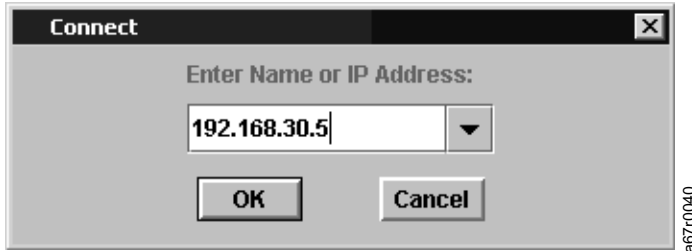


Figure 33. Connecting to a Gateway

Disconnecting a Gateway

Click **Disconnect SAN Data Gateway Module** to disconnect the selected Gateway and remove it from the display. Click **Yes** in the confirmation pop-up window to complete the task. See Figure 34. If you click **File —> Save Current View**, the Gateway is also removed from the view.



Figure 34. Disconnecting a Specific Gateway

Health Check

The Health Check pull-down menu items, see Figure 35, allow you to determine the status of the selected Gateway. You can also test target devices and controllers.

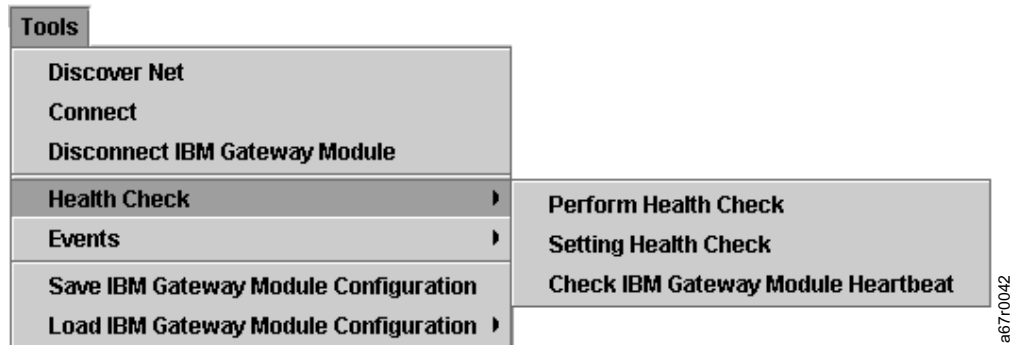


Figure 35. Health Check Pull-Down Menu

Click **Perform Health Check** to request an immediate health check at the current level specified. This check is performed regardless of the health check interval setting.

Click **Setting Health Check** to set the interval, in minutes, between automatic health checks of the selected Gateway. The interval range is 0 to 65 535 minutes (45 days). The default setting is 60 minutes. See Figure 36.

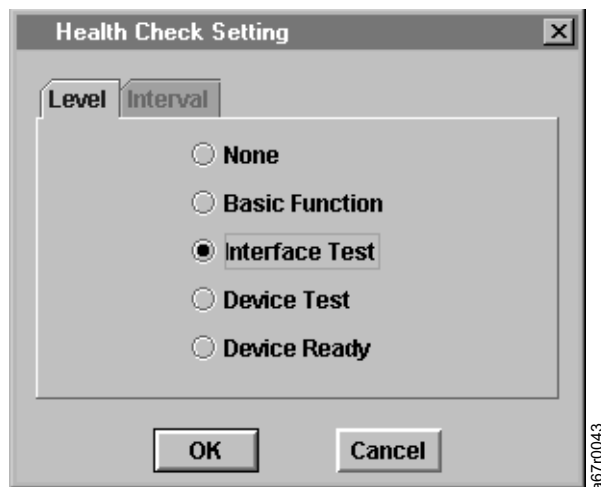


Figure 36. Setting Health Check Interval

Click **Set Health Check Level** to set the level of completeness that each health check performs. For a detailed explanation of the health check function, see “Health Check” on page 76. The health check levels are defined in Table 10.

Table 10. Health Check Levels

Level number	Level name	Function
0	None	No health check is performed.
1	Basic function	Checks the power supply and temperature status.
2	Interface test	Everything from level 1, plus check all interfaces.
3	Device test	Everything from level 2, plus perform device inquiry on each target device.
4	Device ready	Everything from level 3, plus perform test unit ready on each target device (non-removable media only)

Click **Check Gateway Heartbeat** to check communication with the Gateway. A simple request is issued to the Gateway that is currently selected. A message is displayed on the status line that indicates whether or not a response was received. Heartbeat checks are performed at regular intervals as described in “Heartbeats” on page 76. **Check Gateway Heartbeat** is in addition to those checks.

Events Menu

The Events pull-down menu allows you to control how event logs are displayed and how traps are generated. See Figure 37. For an explanation of an event log, see “Chapter 4. Remote Event Notification” on page 73.

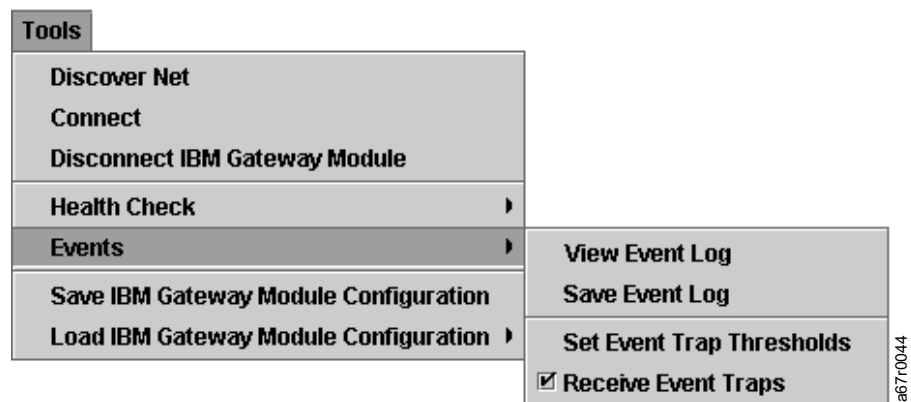


Figure 37. Event Log Pull-Down Menu

Click **View Event Log** to display a list of entries in the event log for the selected Gateway. The event log displays the types of events, depending on the level of events you have chosen to view (see Figure 38 and Figure 39). For an explanation of events, see “Chapter 4. Remote Event Notification” on page 73.

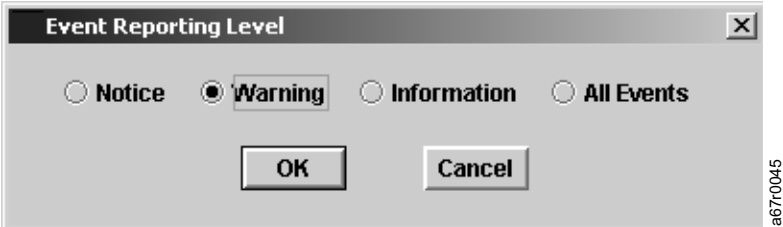


Figure 38. Selecting the Event Viewing Level

The types of events in the event log that match the selected level will be displayed. The most recent events are displayed at the top of the list. To select **Warning** will display warning and notice events. To select **Information** will display information, warning, and notice events. Figure 39 shows the contents of an event log with **Warning** selected.

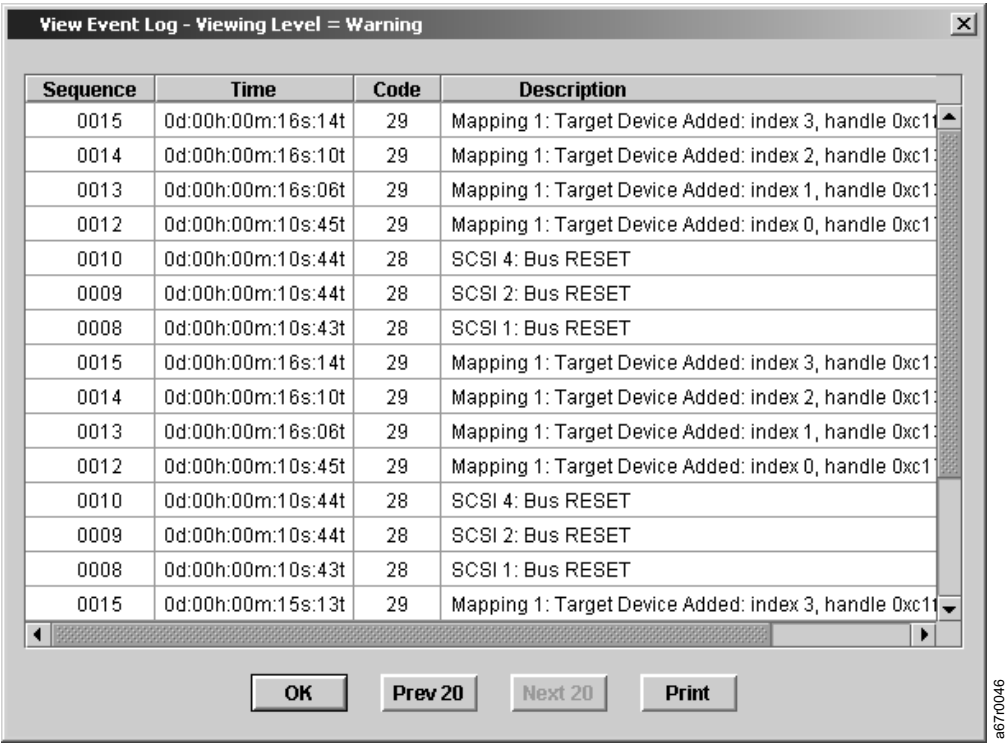


Figure 39. Typical Event Log

If the log is lengthy, you can navigate through it by clicking the **Next 20** and **Prev 20** at the bottom. If you click **Print**, your printer dialog box opens and you must confirm that the log is to be sent to your default printer. The default setting is for all pages to be sent to the printer. Click **OK** to initiate printing. Otherwise, click **Cancel** in the printer dialog box. When you are finished viewing the event log, click **OK**.

Click **Save Event Log** to save a copy of the entire Gateway event log to a text file. A pop-up window is displayed. Type the file name and select the location where you want to save this file. See Figure 40 for an example of the Save Event Log pop-up window.

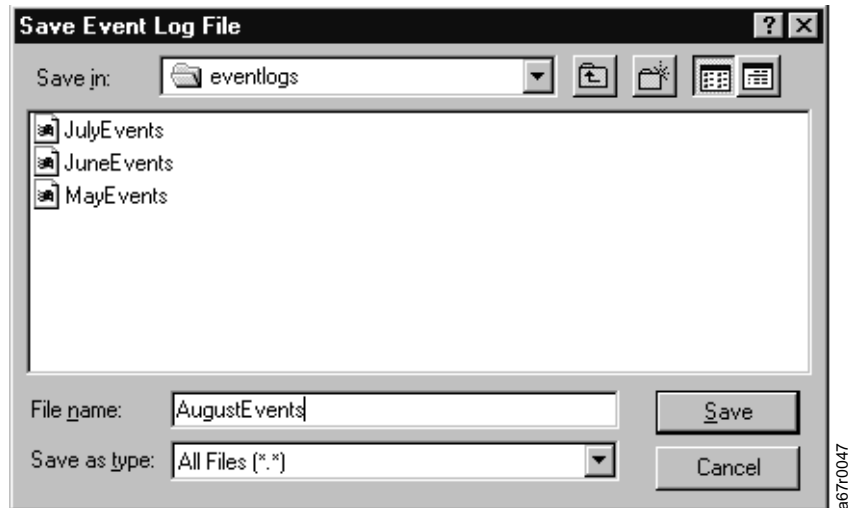


Figure 40. Saving an Event Log

After saving the log, you will have the option to clear the Gateway event log, see Figure 41.

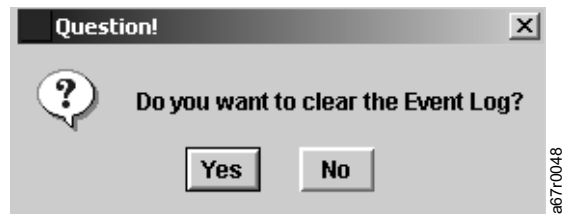


Figure 41. Clearing the Event Log

Click **Set Event Trap Threshold** to display a table listing the events and the current trap threshold level setting. The trap threshold level determines how many times the given event occurs before a trap is issued and you are notified. A user with administrator privilege can modify a threshold level by selecting an event (clicking on it), and then clicking **Change** (see Figure 42). The administrative user will be prompted to enter a new trap threshold level value.

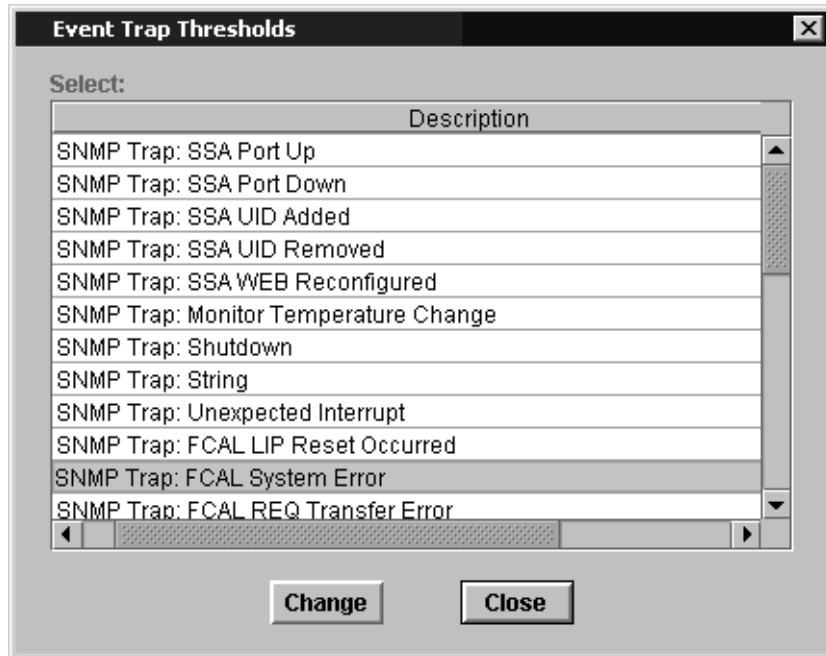


Figure 42. Setting Event Thresholds

A threshold value of zero turns off trap generation for that event. A value of one means that a trap is sent each time the event occurs. Any other value (up to 255) specifies a rate for each ten minute interval. The specified number of events must occur within a ten minute window or no trap will be issued.

Click **Receive event traps** to control whether your StorWatch Specialist client receives trap notifications for the Gateways you are monitoring in your current view. By default, event traps are enabled (indicated by the check mark). Select this option to disable receiving traps (the check mark will be removed).

When a trap is received, the trap symbol shown in Figure 43 is displayed in the status message on the bottom margin area of the main application window. You can look in the Received Event Traps window to see the trap message. The message identifies the Gateway by its IP address. The message includes a date and time stamp, an event code, and a description of the event that caused the trap. For an explanation of event traps, see “Chapter 4. Remote Event Notification” on page 73.



Figure 43. Trap Symbol

Figure 44 shows a typical Received Event Traps window. This example contains some typical health check events and a few SCSI events that might indicate a problem. The Received Event Traps window is always present when the StorWatch Specialist application is running; you can minimize the window, but you cannot close it.



Figure 44. Received Event Traps Window

In Figure 44, the Received Event Traps window contains some typical health check events. The server at 192.168.30.4 was shut down at 5:15 p.m. on August 2 (failed heartbeat occurred), and came back up (revived heartbeat occurred) at 5:48 p.m..

Saving Gateway Configuration

Click **Save SAN Data Gateway Module Configuration** to copy the vital configuration information. Copy the information to a file located on the server, or to a location selected from a file browsing window. See Figure 45. See also "Preserving the Gateway Configurations" on page 22.

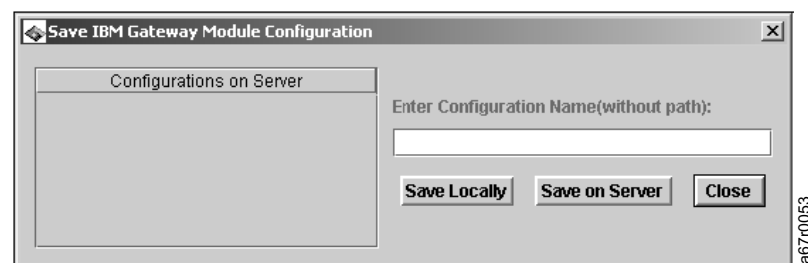


Figure 45. Saving the Gateway Configuration

Enter the name of the configuration that you wish to save or select one from the list of configurations already available on the server. You can save the configuration to a file (click **Save Locally**) or on the server (click **Save On Server**), or both. Click **Close** to clear the pop-up window when you are done.

Note: It is important to save the configuration of each Gateway any time there is a change in the device address maps. This is explained in greater detail on “Preserving the Gateway Configurations” on page 22. After replacing a Gateway, save the configuration both locally and on the server, to ensure that you have access to the file.

Loading Gateway Configuration

The **Load SAN Data Gateway Module Configuration** drop-down list items allow you to restore your former configuration if you replaced the Gateway. You have the option to load a configuration from a file that was saved either locally or on the server.

Click **Load a Local File** to display a list of configuration files in a file browser dialog window. Select the desired configuration file from the list and click **Load**. Before you choose the file, the Gateway sends you a warning. See Figure 46.

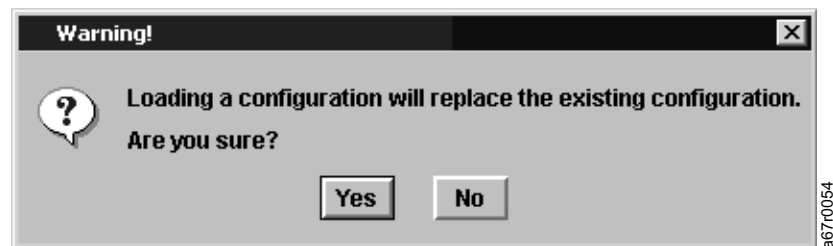


Figure 46. Loading a Gateway Configuration

Note: After you load a saved configuration, see Figure 47, you must restart the Gateway for the configuration changes to take effect.

Figure 47 shows a list of saved configurations.

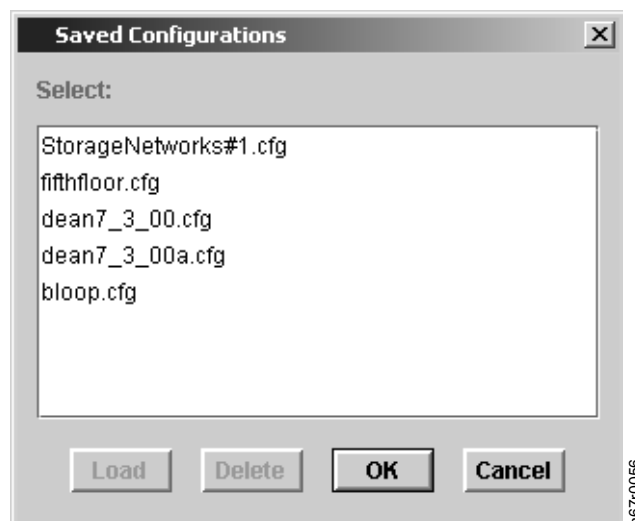


Figure 47. Loading a Gateway Configuration from the Server

Attention: If you replace the Gateway and do not load the saved configuration, you might not be able to use the storage devices attached to the Gateway or data might be lost.

Controls Menu

The Controls menu allows you to control how the selected Gateway and attached devices perform. To access a specific channel or device, select the appropriate item in the menu. See Figure 48.



Figure 48. Controls Menu

Feature Enable

Click **Feature Enable** to enable the data mover features for the selected Gateway. If these features are already enabled, they appear grayed out (disabled) on the menu. See Figure 49.

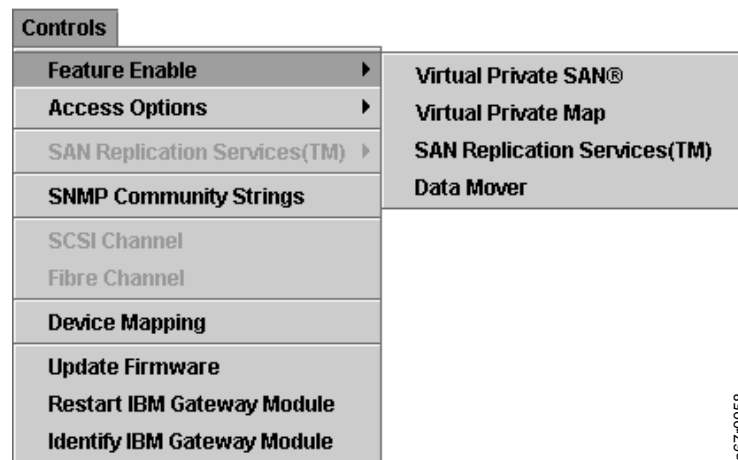


Figure 49. Enabling Optional Features

Data Mover

Click **Data Mover** to use server-free tape backup applications that support SNIA extended SCSI copy. Enabling this feature allows the Gateway to move data directly between storage devices attached to the Gateway.

Note: This feature is factory enabled, you can enable and activate it by entering the word enable.

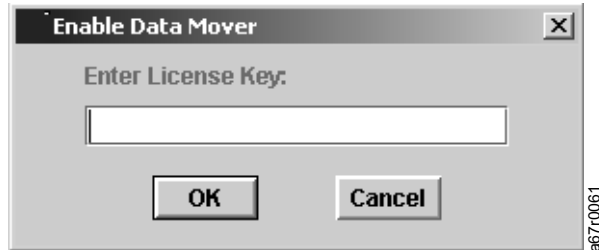


Figure 50. Enabling the Data Mover Feature

Access Options

Click **Access Options** to view or configure access control settings for the selected Gateway.

Three access control options are listed. Virtual Private SAN (VPS) and Virtual Private Map (VPM) are not active. VPS and VPM are used on the SAN Data Gateway and SAN Data Gateway Routers that require a richer set of access control options. Channel Zoning is the active access option for the Gateway.

To prevent more than one host from accessing the same target devices, it is usually necessary to use some type of access control. See "Setting Up Access Control" on page 21.

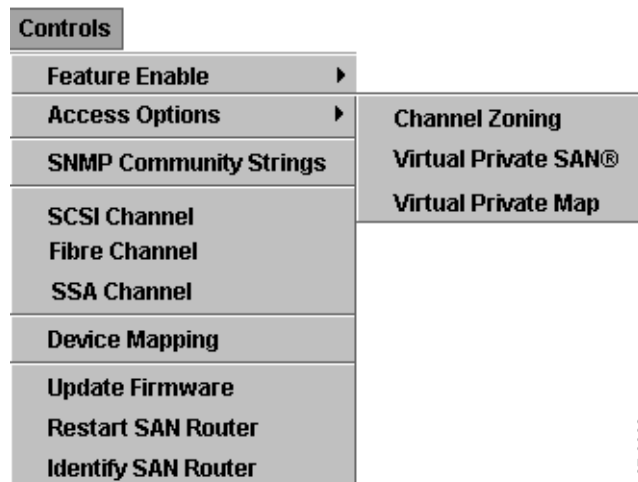


Figure 51. Selecting an Access Control Option

Channel Zoning

Click **Channel Zoning** to configure zones to restrict access between Fibre Channel ports and SCSI channels. The default settings allow all Fibre Channel ports to access all SCSI channels.

When you select this menu option, a pop-up window displays the current channel zoning settings. If you have administrator privileges, you can change the settings. Figure 52 shows the default settings for the Gateway which has two Fibre Channel ports and four SCSI channels.

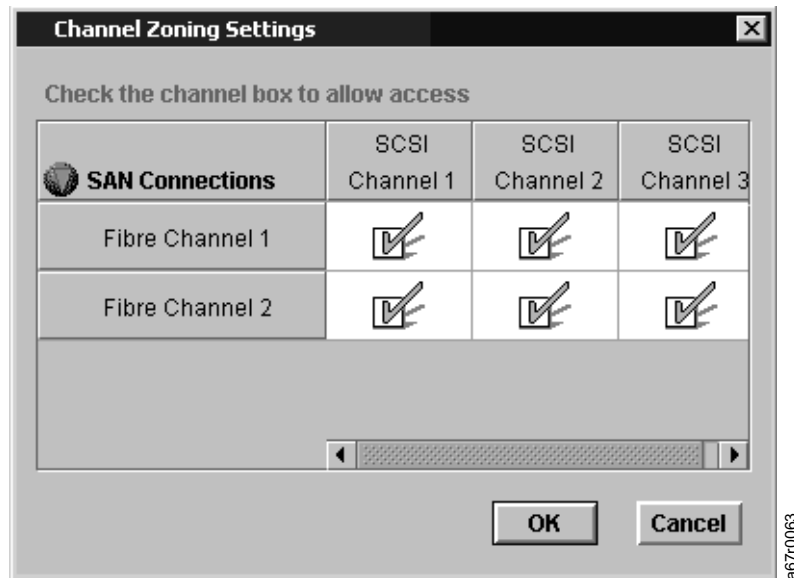


Figure 52. Channel Zoning Settings

Clear the check marks in the boxes to create restricted access zones for the desired SAN connections and SCSI channels. All combinations are possible.

Attention: If you make changes to the channel zoning settings, you must restart the Gateway for the new settings to take effect.

SNMP Community Strings

Click **SNMP Community Strings** to display a pop-up window that allows you to modify the SNMP community strings. See Figure 53. The community strings are stored on the server.

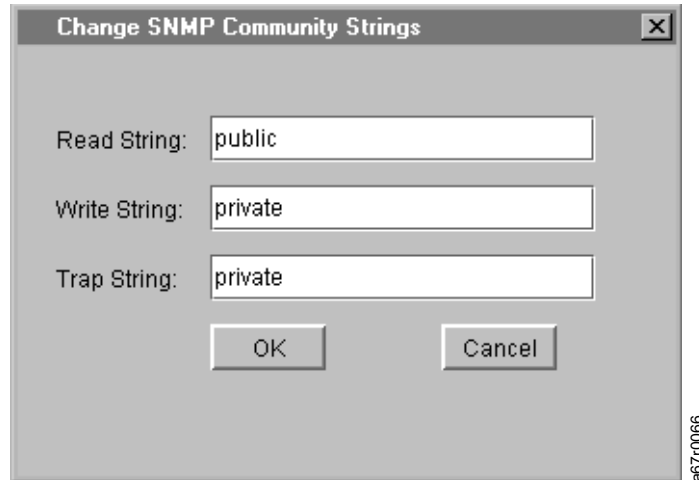


Figure 53. Modifying the SNMP Community Strings

The SNMP community strings serve to group network devices into logical collections for management purposes. The community strings are stored on the server and must match those on the Gateway that you wish to change.

Attention: If changes are made to the SNMP community strings through the service port commands, the StorWatch Specialist should be restarted to reflect these changes.

There are three different communities defined:

- Read** Allows the StorWatch Specialist to get information from Gateways with matching read community string.
- Write** Allows the StorWatch Specialist to manipulate the settings of Gateways with matching write community strings.
- Trap** Allows the StorWatch Specialist to receive trap messages from Gateway with matching trap community strings.

The default settings for the StorWatch Specialist allow the system administrator to control and collect reports from all associated Gateways. See the SNMP suite of service port commands for information about changing community string settings on specific Gateways.

SCSI Channel

Click **SCSI Channel** to view the parameters for the selected SCSI channel. If you have administrator privileges, you can change the settings. See Figure 54.

Attention: If you change any of the SCSI channel parameter settings, you must reset the SCSI channel. Reset the SCSI channel from the Advanced Options window or restart the Gateway to use the new settings.

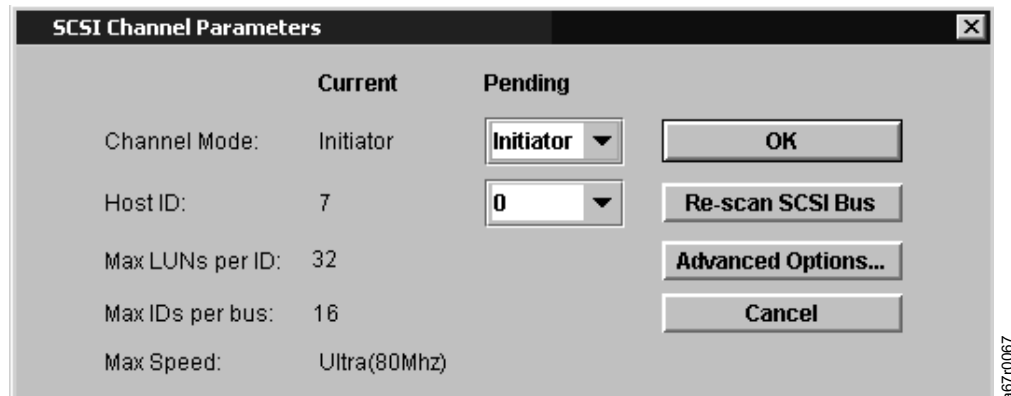


Figure 54. Setting SCSI Channel Parameters

The following text describes the fields shown in Figure 54.

Channel Mode

Identifies the channel as either an initiator or a target.

Host ID

Is typically assigned as 7.

Max LUNs per ID

Is set to a maximum of 32 for each target ID.

Max IDs per bus

Shows that the channel allows up to 16 wide targets.

Max Speed

Shows that the channel will perform at Ultra (80 MHz) speed. Gateway SCSI channels will automatically perform at the speed of the slowest device attached to them. Therefore, to obtain the best performance of Ultra 2/3 SCSI target devices, the SCSI chain should be homogenous.

Click **Rescan SCSI Bus** to rescan the SCSI bus so that the Gateway can detect the devices that have been added or removed. This also refreshes the data for the devices on the SCSI channel and updates the display.

Click **Identify Channel** to flash the SCSI activity light on the front panel of the Gateway. This allows you to observe the actual Gateway and identify which SCSI channel is selected.

Click **Advanced Options** to display a separate window that shows advanced SCSI channel settings that should typically not be changed. Figure 55 shows an example of the advanced SCSI channel controls.

Attention: Changing advanced option settings can disrupt SCSI channel operation and might have unexpected results.

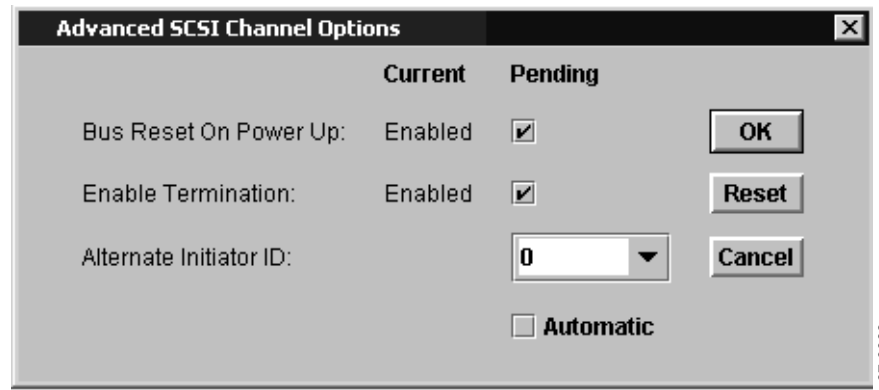


Figure 55. Setting Advanced SCSI Channel Options

The **Bus Reset On Power Up** checkbox is selected by default. Clearing the check mark from this box disables the SCSI bus reset during startups.

The **Enable Termination** checkbox is selected by default. Clearing the check mark from this box disables the internal termination circuits.

The Gateway sets the default **Alternate Initiator ID** automatically. When the Gateway scans the SCSI bus, it determines which IDs are currently being used by target devices. The alternate ID is set to the highest ID not in use. You can change the alternate ID by using the drop-down list or by typing a new number. To restore the automatic default selection, choose “-1” from the drop-down list. See “Alternate SCSI IDs” on page 20 for further information.

Clicking **Reset** reinitializes the SCSI channel and causes the Gateway to abort all pending commands, reset the channel, and perform a rescan.

Figure 56 and Figure 57 on page 63 show the SCSI reset warnings that give you the option to cancel this operation.

Attention: Use **Reset** carefully because it causes pending I/O commands to return failed status back to the host operating system and might have unexpected results. Make sure that all I/O activity has stopped before issuing this command.



Figure 56. First Warning Before a SCSI Reset

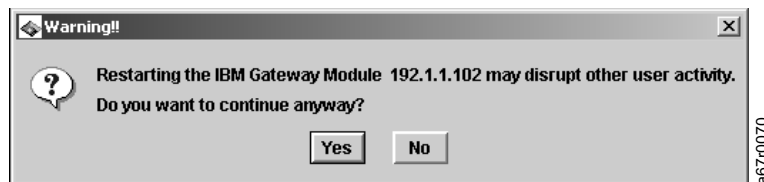


Figure 57. Second Warning Before a SCSI Reset

When you are finished setting advanced SCSI channel parameters, click **OK** to keep your changes and return to the SCSI Channel Parameters window. Click **OK** to save your changes and return to the main window.

Fibre Channel

Click **Fibre Channel** to view parameters for the selected Fibre Channel interface. If you have administrator privileges, you can change the settings. See Figure 58 on page 64.

Figure 58 on page 64 shows the default port mode setting. You have options for changing the port mode and connection. See “Fibre Channel Port Modes and Connection Options” on page 21 for more information.

Note: If you change any of the Fibre Channel parameter settings, you have to restart the Gateway to use the new settings.

Host Type

The Host Type box in the Fibre Channel Parameters screen shown in Figure 58 on page 64 has eight possible values:

- AIX
- HP-UX
- Windows NT (includes Windows 2000)
- Netware
- Gateway
- Generic
- Solaris
- Switch

NT The default setting is NT. The host type is either the name of the host operating system or the type of device attached to the port. This setting controls the way the Gateway translates SCSI commands, such as the format of SCSI sense data, which needs to be presented differently for some hosts.

Loop ID

The default soft loop ID setting should typically not be changed (it might be appropriate however, to use another loop ID setting when using Fibre Channel switches). If you remove the check mark from the box, you can either select a loop ID value from 0 to 125 or type in the value.

Frame Size

Select the frame size from three possible values: 512, 1024, or 2048. The Fibre Channel frame size is specified by each receiving node and need not match any other node. The frame size should typically be set to 2048. (Use a different frame size if required by a particular software application.)

Click **Identify Channel** to make the SAN connection status light for the selected interface flash on the front panel of the Gateway. This allows you to observe the actual Gateway and identify which Fibre Channel interface is selected.

The image shows a 'Fibre Channel Parameters' dialog box with two main sections: 'Current' and 'Pending'. The 'Current' section on the left displays the following settings: Host Type: NT, Loop ID: Soft, Frame Size: 1024, Port Mode: Private Initiator Only, and Connection: Loop. The 'Pending' section on the right allows for configuration of these same parameters. In the 'Pending' section, 'Host Type' is set to 'NT', 'Loop ID' is set to 'Soft' (checked), 'Frame Size' is set to '1024' (selected with a radio button), 'ISP2200 Port Mode' is set to 'Initiator' (selected with a radio button) and 'Private' (selected with a radio button), and 'Connection Options' are set to 'Loop' (selected with a radio button) and 'Loop Preferred' (selected with a radio button). At the bottom of the dialog are four buttons: 'OK', 'Reset', 'Re-scan', and 'Cancel'. A small vertical text 'a67r0071' is visible on the right side of the dialog box.

Figure 58. Fibre Channel Parameters Default Settings

When you are finished viewing or setting Fibre Channel parameters, click **Reset** to make your changes take effect immediately. If you click **OK**, you are reminded that a reset or restart is required for the changes to take effect. Click **OK** to keep your changes and return to the main screen. Click **Cancel** to abort your changes and return to the main screen.

Device Mapping

Using the StorWatch Specialist, you can edit the Gateways persistent address map database and customize the LUN assignment for each target device. Select the Gateway in tree view and then select Device Mapping from the Controls pull-down menu. You may also access the Device Mapping dialog box via the right-click menu. See Figure 59 on page 65.

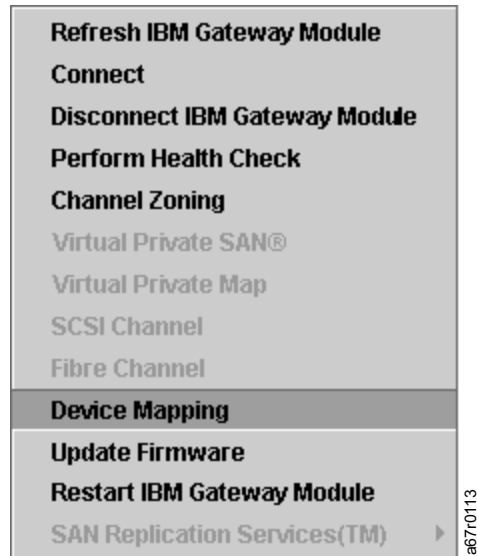


Figure 59. Right-click menu: Device mapping

After you have finished editing the device map, you must reboot the Gateway for any changes to take affect.

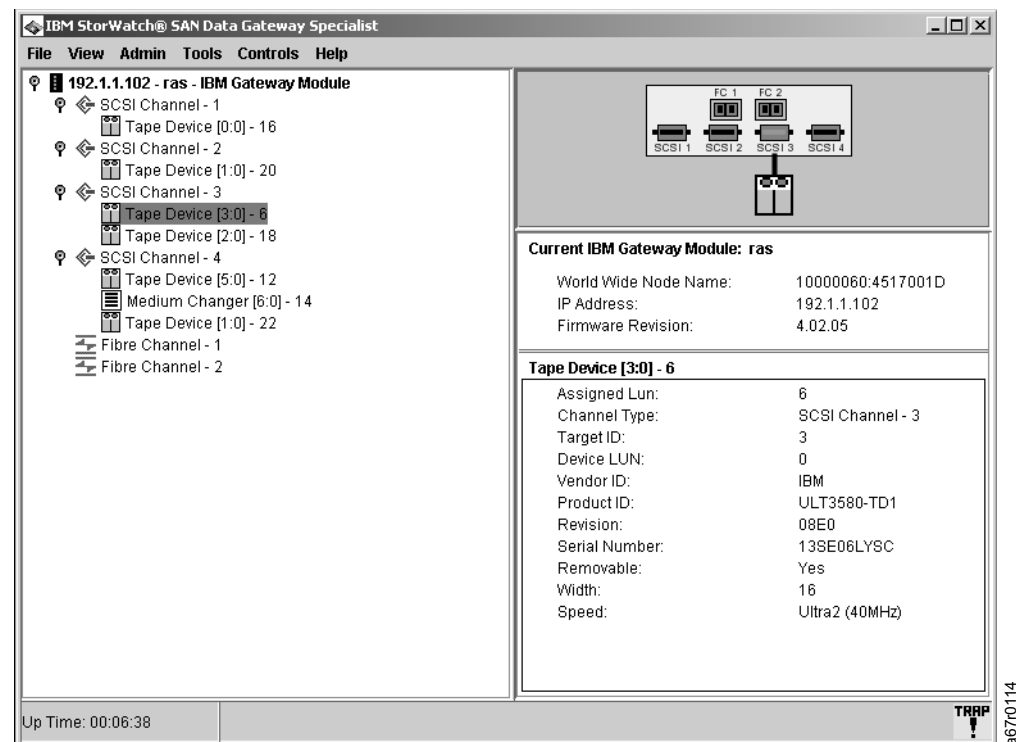


Figure 60. Devices available for mapping

In Figure 60, several SCSI devices are displayed. All are available for mapping. The Target ID of the selected tape device is 3, its Device LUN is 0, and its Assigned LUN is 6. The Data panel uses textual labels to specify this information. Tree view uses the format [Target ID:Device LUN] - Assigned LUN. The Assigned LUN is the LUN number that the Gateway has assigned to this device in its persistent device map.

From the StorWatch Specialist, select the Gateway. From the Controls menu choose Device Mapping. The following display will appear.

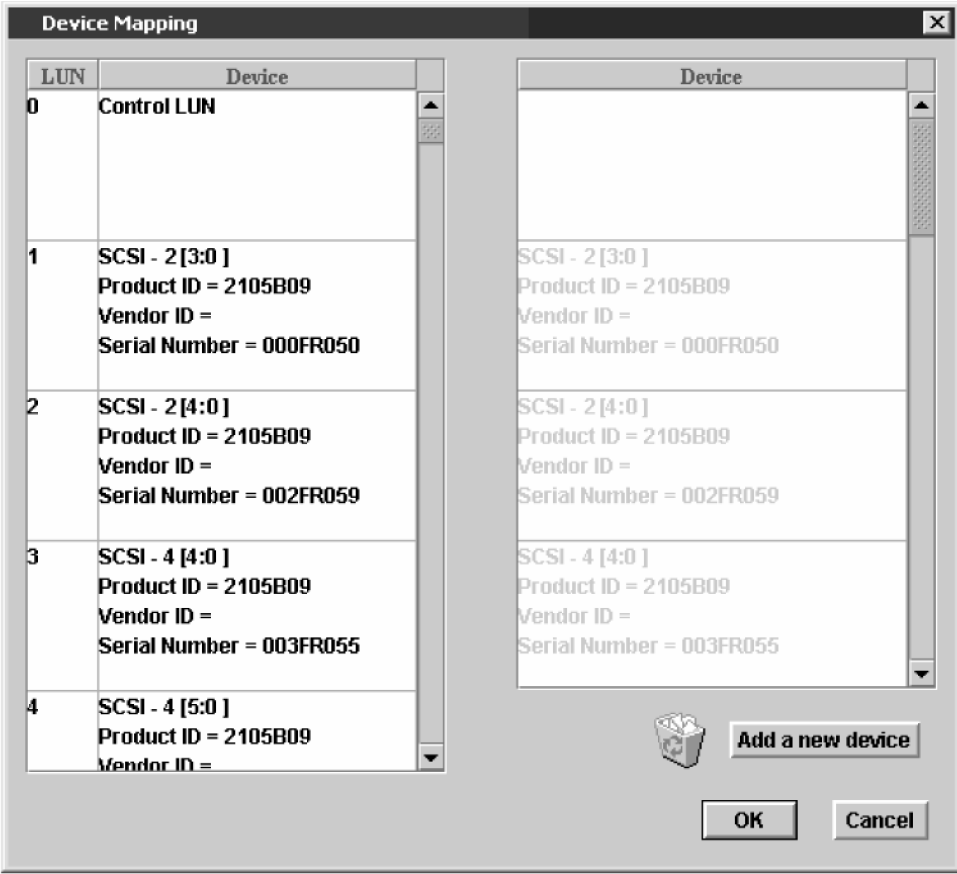


Figure 61. Device mapping window

As shown in Figure 61, devices that have already been entered into the persistent device map appear in black type on the left. The Device Mapping Window uses the format 'Channel [Target ID:Device LUN] after the Channel type, SCSI or Fibre Channel. The assigned LUN for each device shows up only in the left-most column of the window, labeled "LUN". Grayed-out images of these same devices, without the Assigned LUNs, appear in the right-hand column. LUN 0 is typically occupied by the Gateway Command and Control LUN, unless it has been assigned to another LUN.

In order to assign devices to appropriate LUNs, you may drag and drop devices in two different ways. You may move devices back and forth from column to column or you may move them vertically within the left-hand column to different LUNs.

If a device that appears in the Available LUN column is not already assigned, you may delete it by dragging it down to the recycle bin icon.

In Figure 62, LUN 0 is still occupied by the Gateway Command and Control LUN. However, one of the SCSI devices on SCSI 4 has been assigned a lower Assigned LUN than the devices on SCSI 2.

When you are satisfied with the assignments that have been made, press OK. If you decide not to make any changes, press Cancel.

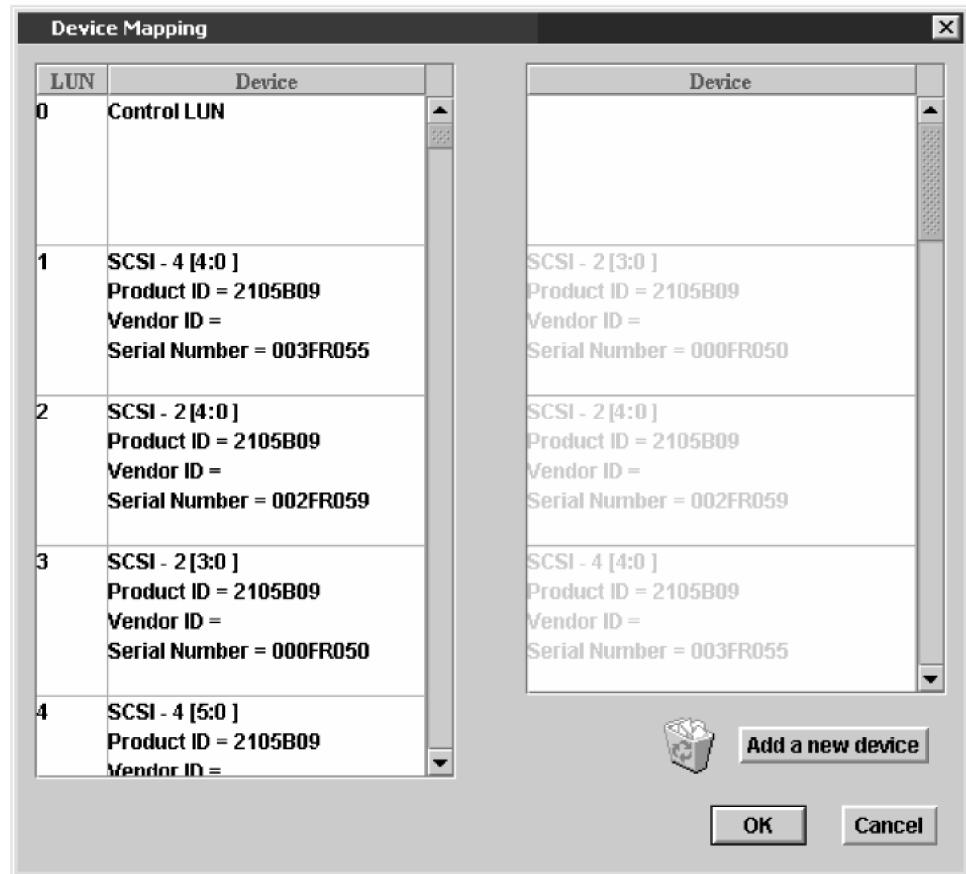


Figure 62. Devices that have been remapped

From the StorWatch Specialist, select the Gateway, and then choose Restart the Gateway from the Controls menu. Reboot the host, or use some other method to ensure that the host is aware of the new device map.

Pre-Assigning Device Numbers

To assign a LUN to a device that is currently not present on the system, but for which a soft LUN assigned during device discovery will not be adequate, press the Add a new device button.

The default device type is SCSI, see Figure 63 on page 68. Fill in the desired Channel Number, Target ID and LUN Number for a SCSI device.

If the device to be added is a Fibre Channel device, use the pull-down to select Fibre, and then fill in the desired LUN and the WWN of the device, if known.



The 'New Device' dialog box is shown with the following fields and values:

Field	Value
Channel Type:	SCSI
Port Number:	1
Target ID:	0
Target LUN:	0

Buttons: OK, Cancel

a67r0117

Figure 63. Add new SCSI device



The 'New Device' dialog box is shown with the following fields and values:

Field	Value
Channel Type:	Fibre
Port Number:	1
Target LUN:	
WWN:	

Buttons: OK, Cancel

a67r0118

Figure 64. Add new Fibre Channel device

The new device or devices will appear in the right-hand column of the Device Mapping Window. In Figure 63, a new entry has been made for a SCSI device that will be connected to SCSI Channel 1. It will have a target ID of 0 and a LUN of 0. It appears in the right-hand column of the Device mapping screen. See Figure 65 on page 69.

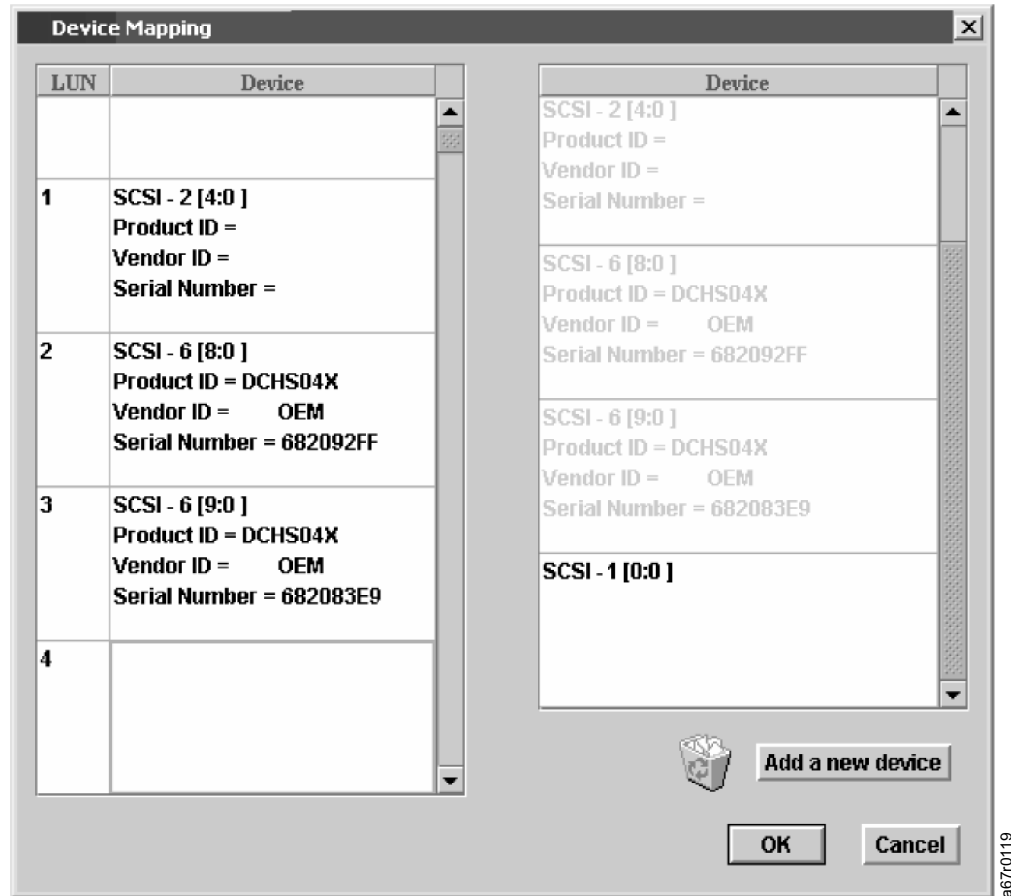


Figure 65. New SCSI channel device

Make sure that each device in the right-hand column is mapped to a LUN in the left-hand column, or the Device Mapping window will not close. See Figure 66. When you have assigned all devices, press OK.

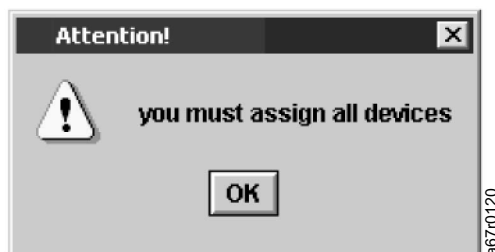


Figure 66. Unmapped devices warning

From the StorWatch Specialist, select the Gateway, then from the Controls menu, choose Restart Gateway. You may also use the right-click menu to reach the Restart Gateway command. See "Restarting the Gateway" on page 70. Reboot the host, or use some other method to ensure that the host is aware of the new device map.

Updating Firmware

Click **Update Firmware** to update Gateway operational firmware.

Attention: You must stop all activity from all of the attached hosts before you update the Gateway firmware. After you update the Gateway firmware, you must restart the Gateway to use the new firmware.

When you click on **Update Firmware**, a file browser window displays so that you can choose a firmware file (must be a binary (.bin) file). See Figure 67. After you select a file, click **Open**. The firmware file is sent to the currently selected device (Gateway or target device). Click **Cancel** to abort the download and return to the main window.

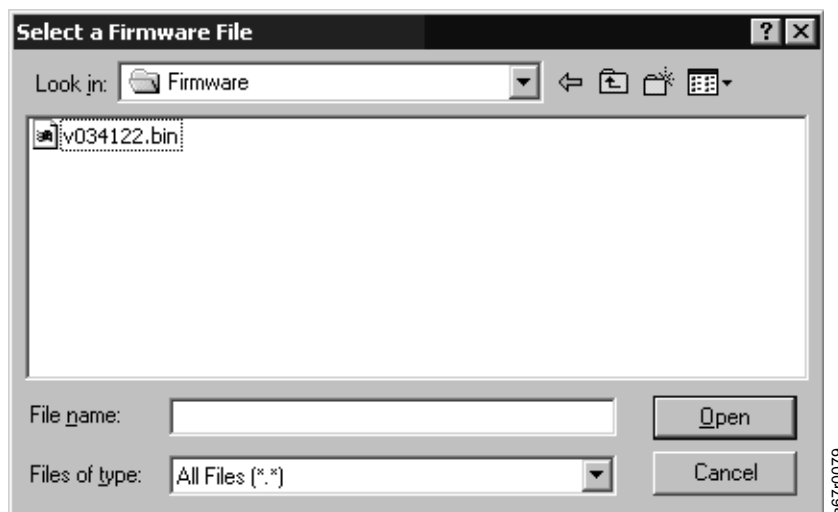


Figure 67. Updating Firmware Files

Restarting the Gateway

Click **Restart SAN Data Gateway Module** to restart the currently selected Gateway.

Attention: Restarting the Gateway immediately stops all I/O activity. Any connected host must stop sending commands to devices attached to the Gateway, or it will cause time outs or other failures to be reported on the host system.

When you select the option to restart, the warning message in Figure 68 displays.

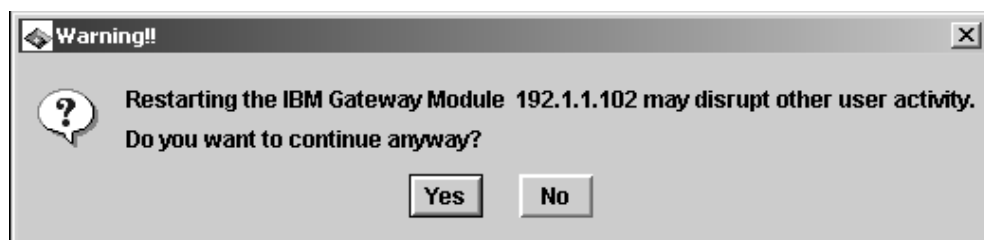


Figure 68. Warning Displayed Before Restarting a Gateway

Identifying the Gateway

Click **Identify SAN Data Gateway Module** to visually identify the selected Gateway. Clicking **Turn Ready LED On** causes the Ready LED to flash rapidly. See Figure 69. Clicking **Cancel** restores the Ready LED to its normal operation and returns you to the main window.

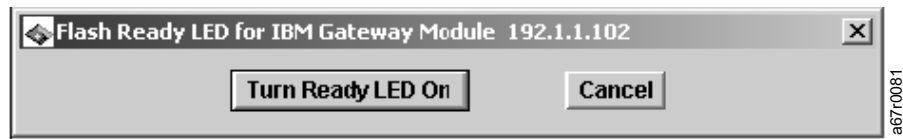


Figure 69. Identifying the Gateway

Chapter 4. Remote Event Notification

This chapter discusses the features of the IBM StorWatch Specialist application that help you maintain and service the SAN Data Gateway Module. The SAN Data Gateway Module will be referred to in the rest of this chapter by the name Gateway. This chapter provides the following information:

- Event logging and viewing
- Events and traps
- Heartbeats
- Health checks
- Problem report

Event Logging and Viewing

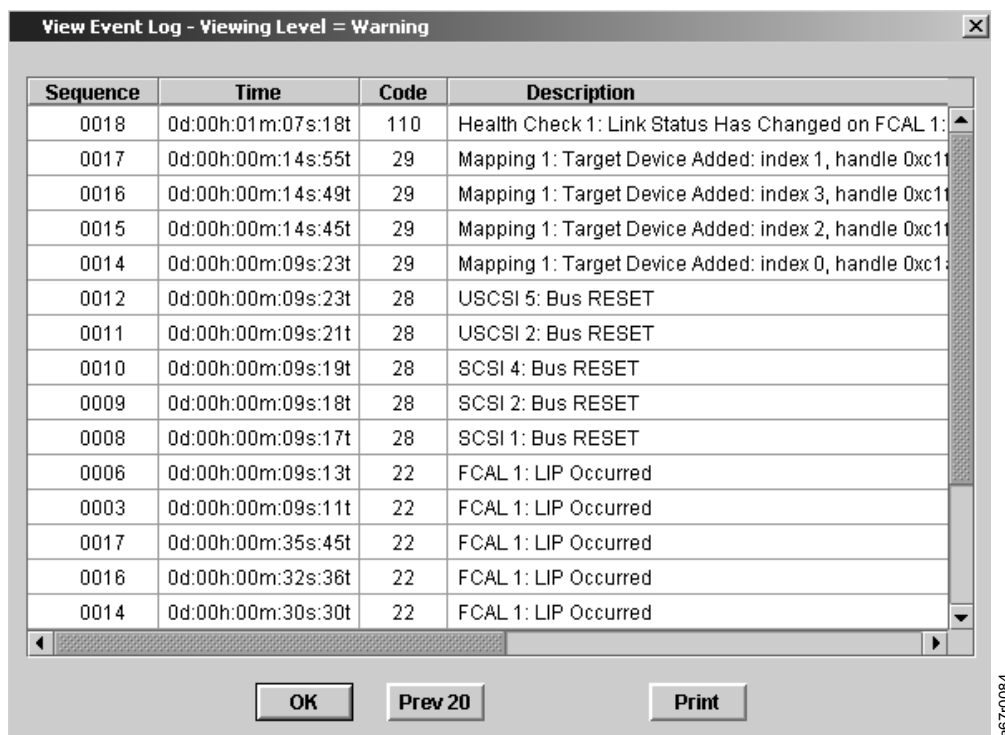
The StorWatch Specialist allows you to retrieve and view event log information that is stored in the nonvolatile memory of the Gateway. The Gateway filters the data based on the setting of the event viewing level. Each event has an assigned viewing level, which indicates a level of severity.

Note: Only a fraction of the possible event codes refer to actual error conditions, and some of those might have indication of error recovery. Other events are recorded for informational purposes.

The event log on the Gateway records all events. The client retrieves only the events it is interested in, based on the client's viewing level (default is set to 2). The event viewing level is cumulative; that is, a viewing level of 3 also displays level 2 and level 1 events. (Level 0 events are only recorded in the Gateway log for console viewing by using the service port.) See Table 11 and Figure 70.

Table 11. Event Viewing Levels

Level	Name	Explanation
0	Private	Events that are never shown by the event viewer but are recorded in the Gateway event log
1	Notice	Conditions that should always be reported, such as temperature alarms and device removals
2	Warning	Events that might result in a later problem
3	Information	Events that are not errors or warnings



Sequence	Time	Code	Description
0018	0d:00h:01m:07s:18t	110	Health Check 1: Link Status Has Changed on FCAL 1:
0017	0d:00h:00m:14s:55t	29	Mapping 1: Target Device Added: index 1, handle 0xc11
0016	0d:00h:00m:14s:49t	29	Mapping 1: Target Device Added: index 3, handle 0xc11
0015	0d:00h:00m:14s:45t	29	Mapping 1: Target Device Added: index 2, handle 0xc11
0014	0d:00h:00m:09s:23t	29	Mapping 1: Target Device Added: index 0, handle 0xc11
0012	0d:00h:00m:09s:23t	28	USCSI 5: Bus RESET
0011	0d:00h:00m:09s:21t	28	USCSI 2: Bus RESET
0010	0d:00h:00m:09s:19t	28	SCSI 4: Bus RESET
0009	0d:00h:00m:09s:18t	28	SCSI 2: Bus RESET
0008	0d:00h:00m:09s:17t	28	SCSI 1: Bus RESET
0006	0d:00h:00m:09s:13t	22	FCAL 1: LIP Occurred
0003	0d:00h:00m:09s:11t	22	FCAL 1: LIP Occurred
0017	0d:00h:00m:35s:45t	22	FCAL 1: LIP Occurred
0016	0d:00h:00m:32s:36t	22	FCAL 1: LIP Occurred
0014	0d:00h:00m:30s:30t	22	FCAL 1: LIP Occurred

OK Prev 20 Print

Figure 70. Viewing Events in the Gateway View Event Log

Events and Traps

Events are recorded in the Gateway event log. For each event, an assigned viewing level corresponds with the event log facility available to the client application. All events are recorded in the Gateway log regardless of the assigned level).

A trap threshold is preset for each event so that when the threshold is reached, a trap message is sent. The count is then reset. If the threshold is 0, no trap messages are sent. A value of 1 or greater, except where noted, means that a trap message is sent each time the threshold is reached. For an explanation of the action numbers, see "Action reference table" on page 88.

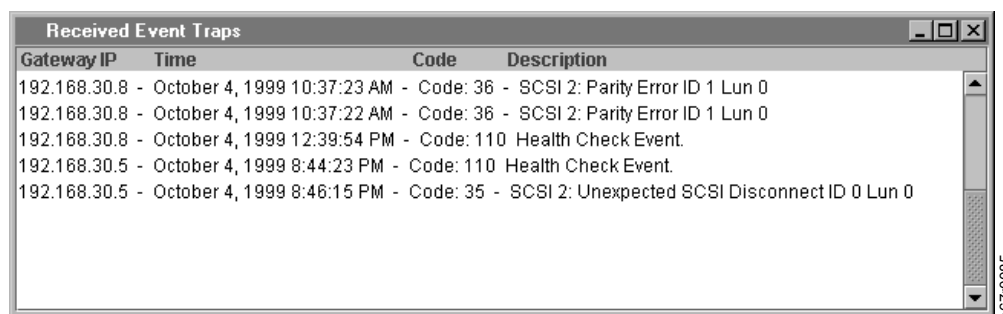
When a trap message is received by the server, it attempts to notify all registered clients. *Registered clients* are clients that are actively monitoring the Gateway that issued the trap.

When a client receives a trap message, the symbol in Figure 71 is displayed in the status message area at the bottom of the StorWatch Specialist application window. This is an indication that a trap message has been received and written to the Received Event Traps window.



Figure 71. Trap Symbol

Figure 72 shows an example of event trap messages in the Received Event Traps window.



Gateway IP	Time	Code	Description
192.168.30.8	- October 4, 1999 10:37:23 AM	- Code: 36	- SCSI 2: Parity Error ID 1 Lun 0
192.168.30.8	- October 4, 1999 10:37:22 AM	- Code: 36	- SCSI 2: Parity Error ID 1 Lun 0
192.168.30.8	- October 4, 1999 12:39:54 PM	- Code: 110	Health Check Event.
192.168.30.5	- October 4, 1999 8:44:23 PM	- Code: 110	Health Check Event.
192.168.30.5	- October 4, 1999 8:46:15 PM	- Code: 35	- SCSI 2: Unexpected SCSI Disconnect ID 0 Lun 0

Figure 72. Event Trap Messages Displayed by the Client

The Internet Protocol (IP) address of the Gateway, a date, timestamp (provided by the server), the event code, and a brief description of the event are displayed. You can click on an event in the window to display more detailed information.

This information helps locate potential problems and should be archived in the SAN Data Gateway Module event log.

Heartbeats

The communication paths between the three components described in “Client-Server Model” on page 14 are checked periodically to make sure that each is listening to the other. These checks are defined as *heartbeats*.

While a Gateway is being monitored, the server application periodically attempts to communicate with it (every two minutes). A fault is reported to any interested client if a Gateway is no longer available.

While a client is connected to a server, the client periodically tests the connection to the server to make sure that it is still available. If the server fails this test, the user is notified, and the connection is closed.

While a client is monitoring one or more Gateways, the server tests the connection to the client at regular intervals. If a client is not available to the server, it is removed from the registry of interested parties.

It is possible for a connection to be temporarily unavailable due to a network condition. The server does not sever a connection based on a missed heartbeat. However, it does attempt to notify a client when a Gateway fails to respond.

Heartbeat failures are assigned event codes, and the server sends notifications to the client when possible. Heartbeat events are not logged in the event log because Simple Network Management Protocol (SNMP) traps are not issued (traps can only come from a Gateway). “Action reference table” on page 88 shows the event codes and threshold settings.

Health Check

The health check function periodically checks the operational state of a Gateway and its attached interfaces and devices.

When the health check is disabled, the Gateway performs no periodic checks beyond monitoring environmental status lines which indicate power supply and temperature conditions. When the health check is enabled, additional status checks are performed.

The health check function posts SNMP traps, when required, to convey status information to management applications. The Gateway broadcasts SNMP traps on the local IP network segment. In addition, specific addresses can be configured and can send directed SNMP traps to host systems that are located on other subnets. The routing information must be set up for directed traps to a different subnet to operate. The server automatically registers itself as a trap recipient when it connects to a Gateway.

Health check failure events are recorded in the event log and a trap message is always sent on each occurrence.

Figure 73 displays a successful health check.

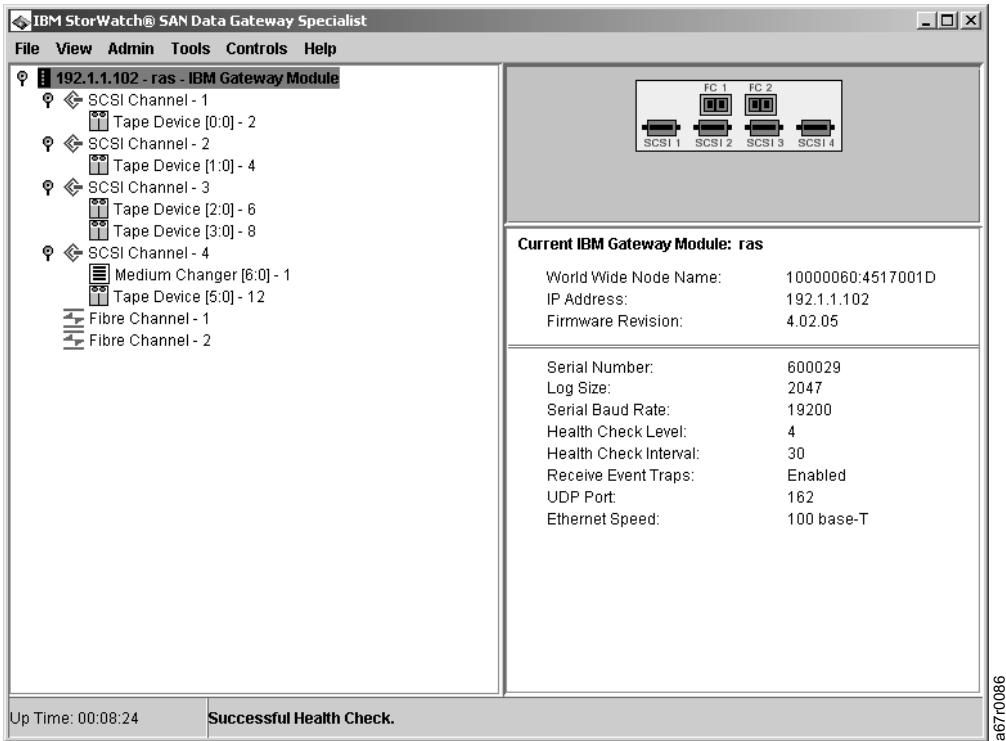


Figure 73. Successful Health Check

Setting Up the Health Check

The health check is enabled when the level is set to a value greater than 0. This can be set from the client application or from the service port.

Health Check Level Control

The health check level can be set to the following levels by using the management application. For more information on the trap messages sent from the health check facility, see “Action reference table” on page 88. The health check level is stored in the Gateway configuration tables and is persistent across restarts. Level **2—Interface Health Check** is the default.

Level 0: No Health Check,

When set to level 0, no health check is performed, but the Gateway monitors the power and temperature and records variations in the event log. Traps for all such events are generated based on the threshold settings, regardless of the health check level.

Level 1: System Health Check,

When set to level 1, the Gateway periodically scans the system resources to locate problems. Health check status will be set if either of the following conditions are true:

- Temperature sensors detect a warning or alarm status
- Power supply sensors detect a change in status since the last report

Level 2: Interface Health Check (default),

Level 2 is a level 1 health check plus an interface health check. An active poll is taken of the interface device, such as a Fibre Channel or small computer system interface (SCSI) controller. A query is sent to the controller in an interface-dependent method, to determine if the controller is currently functional. If a controller is not functional, a health check trap is sent indicating which interface failed.

Level 2 also tests the Fibre Channel link status registers (which monitor Fibre Channel link errors). A trap is sent if any change in these registers is detected.

Level 3: Simple Device Health Check,

Level 3 contains a level 1 and a level 2 health check, plus a device health check. Every attached device is polled to determine its status. A device is considered healthy if it responds to a simple SCSI inquiry command.

Level 4: Device Availability Health Check,

Level 4 contains a level 1, a level 2 and a level 3 health check, plus a device-functional health check. At this level, each target device receives a SCSI **Test Unit Ready** command. If the device reports a good status, it is considered healthy. If it is not ready, the analyzed sense data from the device is interpreted to determine if the device is in a normal not-ready state, or if it is in a failed state. For removable media devices, such as tape drives, level 4 is treated the same as level 3.

An SNMP trap is issued if a device is in a failed state.

After a successful health check, a trap is generated.

Health Check Interval

The health check interval controls how often the health check process runs. The interval may range from 1 to 65 535 minutes (about 45 days). In Figure 74, the default setting has been reset to 1 minute.

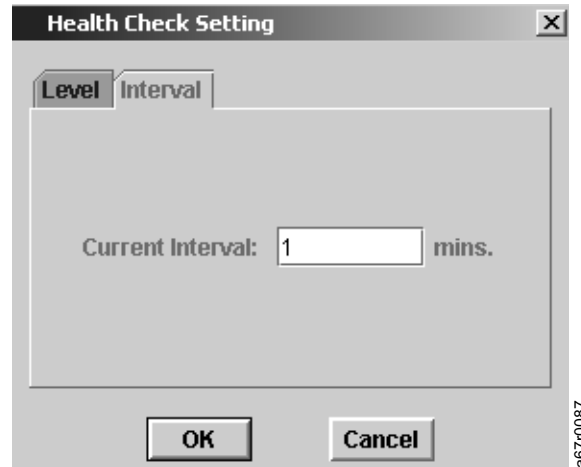


Figure 74. Setting the Health Check Interval

Performance Impact of Health Checks

At higher levels (3 or 4), the health check process may interfere with high-input/output (I/O) operations. For example, in a video delivery application, you may want to select a very low level, or even level 0 to disable health checks. A transaction-processing server may require a more rigorous periodic check.

If a device fails during normal I/O activity, the event is logged in the event log. Health check does not detect the failure or send a trap unless the health check level is set to 3 or 4.

A trap issued from a health check is sent each time the health check interval expires. This means that there will be repeated messages if the same conditions exist on successive checks.

Chapter 5. Maintenance Analysis Procedures

This chapter describes the maintenance analysis procedures for the SAN Data Gateway Module. The SAN Data Gateway Module will be referred to in the rest of this chapter by the name Gateway.

Maintenance Analysis Procedures will be referred to in this chapter by the acronym (MAPs).

Host Bus Adapter will be referred to in this chapter by the acronym HBA.

In this chapter when the phrase **service terminal** is used it refers to a PC or laptop connected to the service port on the Gateway.

MAPs analyze a failure and suggest fix or fixes for each failure. Several tools are available to assist in pinpointing the failing component. These tools and suggested fixes are listed below:

- Event codes
- Visual inspection
- Checking and verifying Fibre Channel operation
- Service Action Table
- Device Access
- SCSI MAP
- Fibre Channel MAP
- Gateway MAP
- Temperature MAP
- Power MAP
- Ethernet MAP
- Service Port MAP

Start MAP

Note: For the latest information on the Gateway, refer to the web site at:
www.ibm.com/storage/lto, click on **technical support**.

Always start problem determination here and review the following steps. Gather as much information as possible before performing a repair action. When gathering information, you might need to connect the service terminal to the service port (see “Connecting the Service Terminal” on page 119).

Checking Event Code or Error Symptom

Either an event code has been reported by the StorWatch Specialist or an error has been observed by other means. If the event code or error symptoms are known, go to Table 13 on page 85, check the event code or symptom, and perform the recommended action.

Inspecting LED Status Indicators

Find the front panel of the Gateway located at the back of the library. Observe LED status indicators. Check the display against Table 13 on page 85. For more information about the LED displays, see Table 12.

If the Ready LED is flashing as expected but the SCSI, Ethernet, and SAN Connection LEDs are off, the Gateway may have been left in diagnostic mode. The device drivers for SCSI, Fibre Channel, and Ethernet interfaces are disabled when in diagnostic mode. If the command prompt on the service terminal is **diagmode** →, return the Gateway to normal mode by entering the **normalBoot** command on the service terminal (see “Boot Modes” on page 196).

Table 12. Gateway LED Display Meaning

LED	ON SOLID	OFF	FLASHING
FC 1,2	Channel is Communicating	Channel Not Communicating	Channel is Active (processing data) ¹
SCSI 1–4	Target Found	No Device Detected	Channel is Active (processing data) ¹
Power	The Gateway has power	The Gateway does not have power	Missing or out of range voltage
Ready	Problem Exists	Problem Exists	Normal, shows Good Health ¹
ERR	Error Detected	No Errors Detected	N/A
Ethernet (Green) ²	Connection OK and able to communicate	If Ethernet cable is connected properly, problem exists	Suspect a loose cable connection
Ethernet (Yellow)	Connection OK and speed is correct	If Ethernet cable is connected properly, problem exists	Suspect a loose cable connection
¹ Flashes at one second intervals ² When running “Discovery”, green LED flickers; yellow LED stays on.			

Checking for Problems on Attached SCSI Devices

Check the following on the SCSI devices to determine if they are the source of the problem:

- LEDs
- Display panels
- Firmware levels
- Operability

Checking Fibre Channel Host Versions

For an updated list of supported Gateway host platforms and Fibre Channel HBAs, refer to the web site at:

www.ibm.com/storage/lto, click on **technical support**

Before contacting technical support determine the version of the following:

- Operating system
- Service pack
- Hot-fix
- HBA hardware
- HBA firmware
- HBA device driver

If an update is required, perform the update.

Checking Gateway Product Versions

For an updated list of required updates, see the web site at:

www.ibm.com/storage/lto

Use the following procedure to determine the firmware and hardware versions, and to perform updates if necessary.

1. If the StorWatch Specialist application is in use, see “Chapter 3. Using the IBM StorWatch SAN Data Gateway Specialist” on page 33. Check **Help —> About** in the StorWatch Specialist to determine its software version. Look for the FW rev. field in the Gateway product data to determine the firmware version. If an update to Gateway is required, download the update from the web site at: www.ibm.com/storage/lto and perform the update.
2. If the StorWatch Specialist application is not available, use the **snaVersion** command from the service terminal to determine the firmware version (see “version” on page 174). If an update is required, download the update from the web site. See the web site at: www.ibm.com/storage/lto and perform the update.
3. If an update is not required, go to “Checking the Event Log” on page 84.

Checking the Event Log

If the StorWatch Specialist application is in use, see “Chapter 3. Using the IBM StorWatch SAN Data Gateway Specialist” on page 33. Check the event log by selecting **Tools Menu → Events → View Event Log**.

When viewing the log, set the viewing level to Warning. Look for a message similar to the following in the list:

```
000001 0185 0d:00h:00m:05s:15t -- NOTICE: LOGGING STARTED
```

Note: Actual date and time will be substituted for 0d:00h:00m:

If the message is not in the list, continue viewing the event log until the start message can be found in the log. If the start message cannot be found, use the log message with the lowest sequence number (the first number on the display line) at the start of the current log.

Check the event codes against the Table 13 on page 85. If no action is required, go to “Performing a Health Check”.

If the client application is not available, use the **loggerDumpCurrent 2** command from the service terminal. Check the event codes against the “Service Reference Table” on page 85. To see additional log messages, follow the procedure in “Event Log Dump” on page 199. If no action is required, go to “Performing a Health Check”.

Quick Component Check

Enter the **showBox** command from the service terminal. If an installed component is not displayed, go to the map that corresponds to that component. For example, if a SCSI interface is missing, go to “SCSI MAP” on page 90. If a Fibre Channel card is missing, go to “Fibre Channel MAP” on page 96.

Performing a Health Check

If the StorWatch Specialist application is in use, see “Introduction to the IBM StorWatch Specialist” on page 14.

1. Click **Tools → Health Check → Setting Health Check**.
2. On the **Level** tab of the **Health Check Setting** dialog box, choose the **Device Ready** radio button
3. Click **Tools → Health Check → Setting Health Check → Perform Health Check**.
4. Write down the event codes reported by the health check procedure.
5. If health check cannot be performed using the client application, use the **hlthChkNow** command from the service terminal. See “Manual Health Check” on page 197.

Checking the Host Event Log

Check the event log on Fibre Channel hosts. Check the most recent entries for any Fibre Channel HBA driver errors. If errors are found, go to “Fibre Channel MAP” on page 96.

Service Reference Table

Review all visual observations and event codes against Table 13. Make a list of the recommended action numbers. Where multiple action numbers are shown, more than one action may be required to determine the problem. Go to “Action reference table” on page 88 and follow the appropriate action.

There are three viewing levels. 0 displays notices only, 1 displays warnings and notices, and 2 displays information, warnings, and notices. A threshold of 0 means that a trap will not be generated for the event (the event is logged in the event log but no trap occurs).

Note: On the Gateway front panel the READY LED is abbreviated RDY and ERROR LED is abbreviated ERR. In Table 13 RDY and ERR are used.

Table 13. Service reference table

Event code	Viewing Level	Default Trap Threshold	Description	Action
Visual observation descriptions				
-			All LEDs are off.	5
-			The RDY LED is not blinking once per second after power has been on for at least one minute.	3
-			ERR LED is on.	4
-			The Gateway is not responding.	3
-			Ethernet green or yellow LEDs flashing. Check for loose or cocked RJ-45 connector	3
-			Persistent reboots.	3
-			Host application error message or host log entry that indicates a SCSI target error.	12
-			Host cannot access attached devices.	11
-			Gateway Connection LED is off although cables are attached and the host systems are on and have fully started up.	2
-			Heartbeat failure.	6
-			fcShow command returns Firmware State=Sync Lost.	2, 0
-			StorWatch Specialist failure.	6
-			Service terminal connection failure.	7
Generic event descriptions				
8	2	0	Sense data was recorded following a check condition. Note: Normally, the host system requests and processes sense data and then performs error recovery.	0
9	1	0	LUN reports a unit attention condition on a device which has permanently mounted media.	1, 2
11	1	1	Gateway reports a temperature change; event message indicates the change was high, very high, reduced to high, or OK.	4
13	1	1	Gateway is shutting down as requested by the StorWatch Specialist (a restart was requested).	0
14	0	0	Additional status information used for diagnostics.	0
16	1	1	A SCSI bus reports an unexpected interrupt.	1

Table 13. Service reference table (continued)

Event code	Viewing Level	Default Trap Threshold	Description	Action
17	1	1	Fibre Channel interface reports a LIP reset was received from a host.	0, 2
18	0	0	Fibre Channel interface reports a system error.	2
19	1	1	Fibre Channel interface reports an error processing a request.	2
20	1	1	Fibre Channel interface reports an error processing a response.	2
21	1	1	A Gateway processor memory fault was detected.	6, 3, 2, 1
22	1	10	Fibre Channel interface detected an LIP.	2
23	2	0	Fibre Channel interface reports a loop up.	0
24	2	0	Fibre Channel interface reports a loop down.	0
25	1	1	A Gateway PCI bus parity error was detected.	6, 3, 2, 1
26	1	1	A Gateway PCI interface error was detected.	6, 3, 2, 1
27	2	1	A device has been added to a SCSI bus.	0
28	1	0	A SCSI bus reports a reset was detected.	1
29	1	1	The Gateway has added a device to its configuration table. Note: The trap is held off until the Gateway has been up for 60 seconds.	0
30	1	1	The Gateway has removed a device from its configuration.	0, 1, 2
31	2	0	The Gateway event logging service has started.	0
33 ¹	1	1	An interface has detected a bus fault (event message indicates the specific interface).	1, 2
34 ¹	1	1	An interface has detected a device fault (event message indicates the specific interface).	1, 2
35	1	1	A SCSI interface reported an unexpected disconnect by a device.	1
36	1	1	A parity error was detected on a SCSI bus.	1
37	2	0	A Fibre Channel port database change was detected.	0
39	1	1	The directory server on fabric has changed.	0
40	1	1	The maximum LUN limit has been exceeded (more than 255 devices connected).	10
41	1	0	A Fibre Channel transfer failure has occurred. Note: Error recovery may have succeeded.	0
42	1	1	The maximum device limit has been exceeded (the persistent Address Map database is full).	11
43	1	1	Fibre Channel interface driver has reported a debug file dump (event log contains more information).	13
58	1	1	Power has returned to nominal from alarm range	None
59	1	1	Power has entered alarm range	5
60	1	1	Power has entered alarm range	5

Table 13. Service reference table (continued)

Event code	Viewing Level	Default Trap Threshold	Description	Action
61 ²	1	1	Inlet air, outlet air and I/O Processor temperatures have entered nominal range from alarm range ² .	None
62 ²	1	1	Inlet air temperature has entered warning range from nominal range (heating up) or alarm range (cooling down) ² .	4
63	1	1	Inlet air temperature has entered alarm range.	4
64 ²	1	1	Outlet air or I/O processor temperature has entered warning range from nominal or alarm range ² .	4
65	1	1	Outlet air or I/O processor temperature has entered alarm range.	4
66	1	1	Fan is operating in nominal range after operating in a fault state.	None
67	1	1	Fan speed has entered warning range (tachometer fans only).	4
68	1	1	Fan speed has entered alarm range (tachometer fans only) or is stalled (rotor stall fans).	4
150	1	1	The event log is about to overwrite the earliest events.	0
Health check event descriptions				
100	1	1	The power supply is out of specification.	5
102	1		A temperature change was detected since the last report (event message indicates whether change is high, very high, reduced to high, or OK).	4, 0
106	1	1	Fibre Channel interface failed the health check.	2
107	1	1	The SCSI interface failed the health check.	1
109	1	1	The target device failed the health check.	1
110	1	1	Fibre Channel link status has changed.	0, 2
111	1	1	Fibre Channel transfer failures have been detected since the last report. Note: Error recovery may have succeeded.	0
112	1	1	Blower/fan is running in warning or alarm range.	4
113	1	1	Power is running in warning or alarm range.	5
114	1	1	Temperature is running in warning or alarm range.	4
115	1	1	Network is running at 10 Mbps/sec.	7

Table 13. Service reference table (continued)

Event code	Viewing Level	Default Trap Threshold	Description	Action
Heartbeat event descriptions				
Note: These event codes are not logged in the event log. Notification of these events occurs from the StorWatch Specialist.				
200 ³	1	1	The server could not verify the connection to a Gateway.	6, 3
201 ³	1	1	The client could not communicate with the server.	8
202 ^{3, 4}	1	1	The server could not communicate with the client.	8
¹ Check the Event Log to find out which interface (FCAL or SCSI) caused this event, then use the appropriate action number. ² This trap signals a change in state. A string sent with trap will indicate the nature of the previous state. ³ Events not logged in the Gateway event log. ⁴ Not reported; view the server log. ⁵ Health check information string returns the state value for each sensor which is in error state. Sensor identification is included. For example, "Inlet Air in Error".				

Action reference table

Table 14. Action reference table

Action number	Action
0	No action necessary.
1	Go to "SCSI MAP" on page 90.
2	Go to "Fibre Channel MAP" on page 96.
3	Go to "Gateway MAP" on page 99.
4	Go to "Temperature MAP" on page 100.
5	Go to "Power MAP" on page 101.
6	RESERVED
7	Go to "Ethernet MAP" on page 101.
8	Go to "Service Port MAP" on page 105.
9	Contact your network administrator.
10	Reduce the number of target devices attached to the Gateway.
11	Go to "Database Full MAP" on page 89.
12	Go to "Device Access MAP" on page 89.
13	Go to "Retrieving the Code 43 Dump File" on page 199.

Database Full MAP

Perform this procedure for event code 42. Event code 42 indicates that the persistent address map database is full (having more than 255 devices in the database). If the database has no room for a newly detected device, the new device is not mapped (assigned a LUN). The database can become full if there are more devices attached than there were previously or if devices were moved to different ports or channels. You can free up database entries that are no longer needed, but keep the devices that are currently attached at the same assigned LUNs.

Attention: Use this procedure only when you are sure that the devices you are interested in are connected and available to the Gateway. Devices that are not currently attached are removed from the database. You must restart the Gateway after performing this procedure for the changes to take effect.

1. Connect the service terminal to the service port (see “Appendix A. Connecting to the Service Port” on page 117).
2. Press the Enter key on the service terminal. If the prompt is not displayed, go to “Connecting the Service Terminal” on page 119 to determine whether the RS-232 cable and service terminal are working properly.
3. From the service terminal, enter the **mapShowDatabase** command to display the contents of the database (see “Appendix B. Service Port Command Reference” on page 123).
4. From the service terminal, enter the **mapShowDevs** command to display LUN assignments for the attached devices that have been mapped.
5. From the service terminal, enter the **mapWinnowDatabase** command to remove LUN assignments for devices that no longer need to be kept.
6. Restart the Gateway.
7. After the gateway has fully restarted, repeat steps 3 and 4 to verify that all the attached devices have been mapped.

Device Access MAP

Perform this procedure if a host is not able to access SCSI or Fibre Channel devices.

1. Connect the service terminal to the service port (see “Appendix A. Connecting to the Service Port” on page 117).
2. Press the Enter key on the service terminal. If the prompt is not displayed, go to “Service Port MAP” on page 105 to determine whether the RS-232 cable and service terminal are working properly.

Checking Fibre Channel Port Status

1. Enter the **fcShow** command from the service terminal (see “Appendix B. Service Port Command Reference” on page 123). If the **fcShow** command does not display a firmware state of Ready for the attached Fibre Channel SAN connections, go to “Fibre Channel MAP” on page 96.
2. The Gateway Fibre Channel port modes are set by default to target mode. If the port mode for the host connection was changed to initiator from the StorWatch Specialist, the host cannot see the SCSI devices. Verify that the port mode was not inadvertently changed using the **StorWatch Specialist Controls —> Fibre Channel** menu.
3. If the host attached to a SAN connection is not able to access a Fibre Channel device on another SAN connection, go to “Checking Fibre Channel Initiator Port Mode” on page 90.

Checking SCSI Channel Devices

Enter the **scsiShow** command from the service terminal. If all of the attached SCSI devices are not displayed, go to “SCSI MAP”.

Checking Channel Zoning Settings

1. Enter the **fcShowDevs** command from the service terminal. Look at the display for each Fibre Channel interface. If all of the SCSI devices are displayed under each Fibre Channel interface, then host access to SCSI devices is not being restricted by channel zoning. Go to “SCSI MAP”.
2. If the channel zoning settings are correct, go to “SCSI MAP”.
3. If you want to remove all channel zoning access restrictions, enter the **setFcNormal** command from the service terminal (see “Appendix B. Service Port Command Reference” on page 123).
4. If you want to modify channel zoning settings, use the **StorWatch Specialist Controls —> Access Options —> Channel Zoning** menu to change the settings. The StorWatch Specialist allows every combination of channel zoning settings. For an alternate channel zoning method, enter the **setFcSplit** command from the service terminal (see “Appendix B. Service Port Command Reference” on page 123). This alternate command method is not as flexible as the StorWatch Specialist because it only provides one combination of channel zoning settings.
5. Go to “SCSI MAP”.

Checking Fibre Channel Initiator Port Mode

The port mode of the Fibre Channel that the target devices are attached to must be set to initiator or target and initiator mode. If the port mode is set to target, the gateway cannot see the target devices. Verify the port mode using the **StorWatch Specialist Controls —> Fibre Channel** Gateway StorWatch Specialist menu.

SCSI MAP

These steps are performed if one or more of the following errors occur:

- Errors are reported on the SCSI bus
- SCSI I/O fails to operate
- Parity errors are detected on the SCSI bus
- SCSI device reports unit attention on a unremovable device
- Unexpected SCSI bus reset occurs
- Unexpected SCSI disconnect reported by a SCSI device
- Not all SCSI devices attached are displayed by SCSI Show

Getting SAN Data Gateway Module SCSI Information

1. Connect the service terminal to the service port (see “Appendix A. Connecting to the Service Port” on page 117).
2. If library main power is in the O position, turn library main power switch to the I position. Wait until the Gateway Ready LED is blinking once per second.
3. As the Gateway is starting up, several status messages should be displayed on the service terminal. If no status messages are displayed, go to “Service Port MAP” on page 105 to determine whether the RS-232 cable and service terminal are working properly. Otherwise, look for the last status message, “done executing startup script”.
4. Enter **showBox** from the service terminal (see “Appendix B. Service Port Command Reference” on page 123).
5. Write down the information for each Ultra SCSI channel (for example, “SCSI-4 requires Low Voltage Differential cable”).

6. If the SCSI interfaces are not all displayed, replace Gateway. Go to “Remove and Replace Gateway” on page 109.

Checking Attached SCSI Devices from the Service Port

Attention: The Gateway supports up to 256 LUNs. If more than 256 LUNs are attached this results in unreliable operation. Only 255 LUNs are available to the user. The Gateway utilizes LUN 0 as the command and control LUN.

1. Enter **scsiShow** from the service terminal to display a list of attached SCSI devices (see “Appendix A. Connecting to the Service Port” on page 117).
2. For each SCSI channel, make a list of attached devices (SCSI device ID, manufacturer, device status, flags). Go to “Comparing Listed Versus Physical Devices” .

Comparing Listed Versus Physical Devices

For each SCSI channel (starting with Ultra2 channel 1), perform the following:

1. Compare the list of attached devices with the physical devices. If all of the physical devices are not shown, go to “Checking SCSI Bus Termination”.
2. If all the physical devices are shown, go to “Comparing Listed Versus Supported Devices”.

Comparing Listed Versus Supported Devices

1. Only LTO drives and the 3583 Library are supported on the SCSI bus.

Note: Record any devices which are not supported. Report them to the system administrator for possible replacement.

2. If the attached SCSI devices are all supported devices, go to “SCSI Loopback Test” on page 94.

Checking SCSI Bus Termination

See Figure 75 on page 92 for following procedure.

Attention: If you remove a SCSI cable **1** or terminator **2** during this procedure, all I/O activity to the Gateway must be stopped. Toggle the library main power switch to the O position.

For each device attached to the questionable SCSI channel do the following steps:

1. Verify the Gateway termination.

The Gateway has internal terminators on its SCSI channels. The terminators are disabled from the StorWatch Specialist. Verify that the customer has not inadvertently disabled termination using the **Controls** → **SCSI Channel** menu.

2. The last physical device on a chain of SCSI devices needs to be terminated **2** .

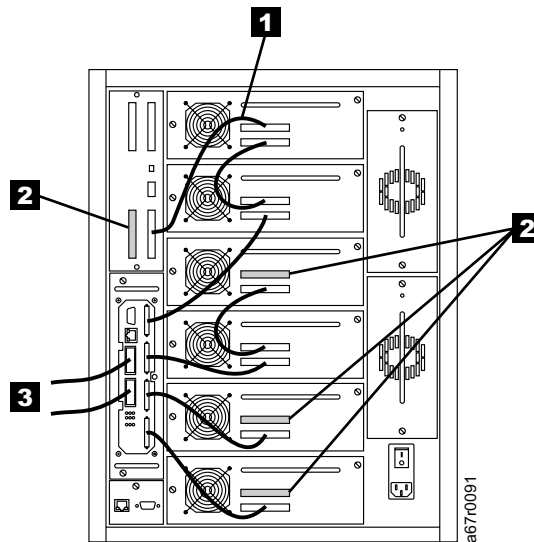


Figure 75. SCSI Cabling and Termination

- a. If the Gateway SCSI channel for this SCSI chain has internal termination enabled no external terminator is needed. Otherwise, check that an external terminator **2** is attached to the end device.
- b. A differential (DE) terminator on a single-ended (SE) bus or a SE terminator on a DE bus will cause the bus to be unusable. Verify the type of terminators for each SCSI channel.
3. Only the last device in a string must to be terminated. All other devices in the string must have internal termination disabled.
4. If SCSI termination is OK, go to “Checking for Multiple SCSI IDs”.
5. If you corrected a SCSI termination problem, toggle the library main power switch to the | position. Wait for the Gateway to complete start up. After Gateway starts up, enter the **scsiShow** command from the service terminal. Compare the list of attached devices with the physical devices. If not all of the physical devices are shown, go to “Checking for Multiple SCSI IDs”. Otherwise, go to “SCSI Health Check” on page 94.

Checking for Multiple SCSI IDs

Attention: If you need to correct any SCSI IDs during this procedure, all I/O activity to the Gateway must be stopped. Toggle the library main power switch to the O position.

If two or more devices on the same SCSI channel are configured at the same SCSI ID, only one of those devices is seen by the Gateway. Data transfers to that device are unreliable.

1. Write down the SCSI IDs of all devices connected to each SCSI channel.
2. Check that only one device is set to each ID for each SCSI channel.
3. If a target device is set to the same ID as the Gateway (ID 7), the bus is unstable and data corruption can result.
4. For each SCSI channel, check that no devices are set to ID 7 (except the channel ID of the Gateway).
5. If you do not need to correct any SCSI IDs, go to “Incorrect Device Type” on page 93.

6. Turn off the SCSI target device (if appropriate) which must have its SCSI ID reassigned.
7. Assign a new SCSI ID to the target device.
8. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
9. After it starts up, enter the **scsiShow** command from the service terminal. Compare the list of attached devices with the physical devices. If all of the physical devices are not shown, go to “Incorrect Device Type”. Otherwise, go to “SCSI Health Check” on page 94.

Incorrect Device Type

Attention: If you determine in this procedure you need to replace a SCSI device, all I/O to the SAN Gateway must be stopped. Toggle the library main power switch to the O position.

1. When a mix of Ultra2/3 SCSI and Ultra SCSI devices are connected to a single bus, the bus will run at the Ultra SCSI speed. Because the bus will auto-adjust to the slowest speed, it is not recommended that you run both Ultra2/3 SCSI and Ultra SCSI devices on the same bus.
2. If you do not have to replace an incorrect device, go to “Examining SCSI Cables”.
3. Replace the incorrect SCSI device with a correct device. Reconnect the SCSI cable and turn on the SCSI device.
4. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up. After it finishes starting up, enter the **scsiShow** command from the service terminal. Compare the list of attached devices with the physical devices. If all of the physical devices are not shown, go to “Examining SCSI Cables”. Otherwise, go to “SCSI Health Check” on page 94.

Examining SCSI Cables

Attention: If you need to remove a SCSI cable during this procedure, all I/O activity to the Gateway must be stopped. Toggle the library main power switch to the O position.

1. Look for damaged cables. Check for breaks in the cable jacket, exposed or frayed cable shield, and exposed or broken wires. Replace any damaged cables.
2. Check for inadequate cables. Older SCSI cables may not be suitable for running at Ultra2/3 speeds. Be sure all cables are rated for Ultra2/3. Replace any that are not.
3. Check for mixed cable types. If a SCSI bus has both round cables and flat ribbon cables, problems can occur when running at Ultra2/3 speeds. Use the same cable type consistently for all segments of the SCSI bus. Replace any cables that do not match.
4. Check for cables without shield. A SCSI cable without shield used outside a cabinet may cause reliability problems. This is due to interference from other electrical devices. Replace all cables which are not shielded.
5. Go to “Examining SCSI Connectors” on page 94.

Examining SCSI Connectors

Attention: Before removing a SCSI cable, all I/O activity to the Gateway must be stopped. Toggle the library main power switch to the O position.

1. The pins in the SCSI connectors are fragile. Carefully inspect each connector for bent pins. Replace any cables that have bent pins.
2. If you did not have to replace or tighten a SCSI cable, go to “SCSI Loopback Test”.
3. If you replaced or tightened a SCSI cable, toggle the library main power switch to the | position. Wait for the Gateway to complete start up. After it starts up, enter the **scsiShow** command from the service terminal. Compare the list of attached devices with the physical devices. If all of the physical devices are not shown, go to “SCSI Loopback Test”. Otherwise, go to “SCSI Health Check”.

SCSI Health Check

1. Perform a health check and check the event log for SCSI errors (see “Performing a Health Check” on page 84 and “Checking the Host Event Log” on page 84).
2. If errors persist, go to “SCSI Loopback Test”.
3. If no errors are reported, exit this MAP.

SCSI Loopback Test

Attention:

Before performing Diagnostics complete the following steps:

1. Stop all I/O activity on the Gateway.
2. Toggle the library main power switch to the O position.
3. Remove SCSI cables from the Gateway. See “Remove Gateway” on page 109 to remove SCSI cables.

Attention: Do *not* perform SCSI loopback tests on SCSI channels that are attached to SCSI target devices. If you do this, you will corrupt the customer's data.

1. If the Gateway command prompt on the terminal is not **diagmode =>**, enter the **diagBoot** command at the service terminal (see “Entering Diagnostic Mode” on page 196).
2. Connect the short SCSI cable (provided in the service tool kit) to two of the SCSI channels.
3. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
4. To test the SCSI connection, enter the **scsiChannelTest x,y** command from the service terminal to perform a loop back test. Substitute SCSI channel numbers for x, y in the command above.
5. If the Gateway returns a **passed** status and you have already encountered a failure on the other two channels go to “Chapter 6. Removal and Replacement Procedures” on page 107. Otherwise, go to “Testing SCSI Cables” on page 95
6. If the Gateway returns a **failed** status and you have already encountered a failure on the other two channels you may have a bad loop back cable. You must replace the loop back cable before continuing. If this is your first time

through here you may have a bad loop back cable or a SCSI connector on the Gateway may be bad. Go to step 4 on page 94 to test the other two SCSI channels

Testing SCSI Cables

The SCSI channels use a SCSI-3 68-pin connector with jackscrews. If the cables of the devices attached to a channel have a compatible pin layout on both sides, the Gateway can test the cable using the loopback test.

Note: For this procedure you will need SCSI Interposer cable P/N 19P0482 which is not provided in the ship group for this library or the Gateway.

1. Stop all I/O activity to the Gateway.
2. Connect the terminal to the service port. See "Appendix A. Connecting to the Service Port" on page 117.
3. If the Gateway command prompt on the terminal is not **diagmode >**, see "Entering Diagnostic Mode" on page 196 to enter diagnostic mode.
4. Toggle the library main power switch to the O position.
5. Draw a diagram of the devices and their connections to the SCSI channels.
6. Remove the cable from the attached SCSI device and attach interposer cable as a loopback cable to the Gateway.
7. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
8. When the Gateway finishes booting, enter the **scsiChannelTest x,y** command from the service terminal to perform a loop back test. Substitute the slot numbers connected by the loopback cable for "**x**" and "**y**".
9. If the Gateway returns a **failed** status, the cable is faulty and must be replaced.
10. If the Gateway returns a **passed** status, go to "Isolating SCSI Devices" to isolate bad devices on the SCSI bus.

Isolating SCSI Devices

1. Restore the Gateway to normal operations (go to "Restoring Normal Mode" on page 196).
2. Perform this procedure for each SCSI device that was missing in "Comparing Listed Versus Supported Devices" on page 91:
 - a. Toggle the library main power switch to the O position.
 - b. Remove all devices from the SCSI buses.
 - c. Attach *only* the device in question to the SCSI channel it was originally connected to (see the list made in "Checking for Multiple SCSI IDs" on page 92) using a known-good SCSI cable and terminators.
 - d. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
 - e. Enter the **scsiShow** command from the service terminal and verify that the device is active on the system.
 - f. If the device is missing, it needs to be replaced. Inform the system administrator of any suspected bad devices found in this procedure. Replace or remove any bad devices.
 - g. If the device is present, perform a health check (see "Performing a Health Check" on page 84).
 - h. Review the event log (go to "Checking the Host Event Log" on page 84).

- i. If SCSI errors are found, inform the system administrator that the connected device might be bad. Replace or remove any bad devices.
- j. After all possible device checks are performed, go to “Restoring SCSI Setup”.

Restoring SCSI Setup

1. Toggle the library main power switch to the O position.
2. Reconnect all available SCSI devices to their correct channel assignments (either their original configuration, or with any changes made during this MAP).
3. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
4. If the Gateway is in diagnostic mode (**command prompt = diagmode >**), enter the **normalBoot** command at the service terminal to restore normal operation (see “Restoring Normal Mode” on page 196).
5. Perform a health check (go to “Performing a Health Check” on page 84).
6. Review the event log (go to “Checking the Host Event Log” on page 84).
7. If all attached SCSI devices and cables are determined to be good but SCSI errors still persist, replace the Gateway, (go to “Remove and Replace Gateway” on page 109).
8. Exit this MAP.

Fibre Channel MAP

Perform these steps if any of the following occur:

- Fibre Channel interface reports a reset or system error.
- Fibre Channel interface reports an error processing a request or response.
- Fibre Channel interface reports an excess of 10 LIPs in a 10 minute interval.
- Other Fibre Channel errors are reported.
- See Figure 76. The Gateway Connection LED **1** is off.

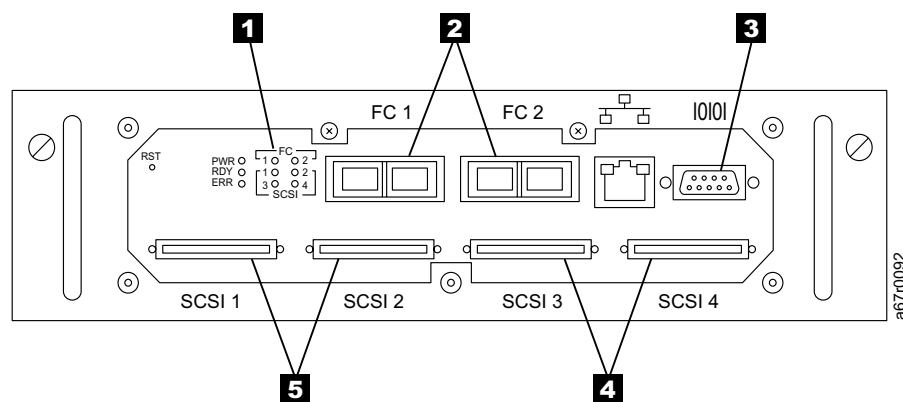


Figure 76. Gateway Panel

Verify Fibre Channel Connections

1. Connect the service terminal to the service port (see “Appendix A. Connecting to the Service Port” on page 117).

2. Press the enter key at the service terminal. If the prompt is not displayed, go to "Service Port MAP" on page 105 to determine whether the RS-232 cable and service terminal are working correctly.
3. Enter the **showBox** command from the service terminal (see "Appendix B. Service Port Command Reference" on page 123).
4. Confirm the Fibre Channel connections are correctly displayed. If **showBox** displays the Fibre Channel connections correctly, go to "Examining Cables".
5. If Fibre Channel connections do not display correctly in the **showBox** display, remove the GBIC and replace it with a known-good GBIC. Go to "Remove and Replace GBIC" on page 108 to remove and replace the suspected bad GBIC. After remove/replace of GBIC return to "Test GBIC".

Test GBIC

Attention: You must stop all I/O at the Fibre Channel host.

1. With the known-good GBIC installed confirm the Gateway Fibre Channel connections are correctly displayed. This is accomplished by issuing the **showBox** command from service terminal. If **showBox** displays the Fibre Channels correctly return the failing GBIC. Exit this MAP.
2. If the output of the **showBox** command still does not match the Fibre Channel configuration, remove the known-good GBIC and install the original GBIC. Go to "Examining Cables".

Examining Cables

Attention: If you determine that you need to remove or replace a Fibre Channel cable during this procedure, you must stop all I/O activity at Fibre Channel host.

1. Remove the cables.
2. If any cables are obviously damaged, replace them.
3. Use dusting spray (compressed gas) to dust off optical connectors on GBIC and cable ends.
4. Reconnect the cables.
5. Perform "Performing a Health Check" on page 84.
6. If errors persist, go to "Checking Optical Cable Type".

Checking Optical Cable Type

The optical cable diameter is important for longwave Fibre Channel optical transceivers. Shortwave GBICs will function with any cable diameter (though not necessarily all lengths). The cable diameter is expressed as the ratio of the diameter of its fiber core over the diameter of the protective cladding.

1. Record the core/cladding diameter printed on the cable jacket. Also record what Fibre Channel port it was plugged into.

Note: Only 50/125 microns are supported at the Gateway GBIC.

2. If the problem persists, go to "Fibre Channel Loopback Test".

Fibre Channel Loopback Test

Attention: Before performing diagnostics, Fibre Channel cables must be marked and removed from the Gateway. All I/O activity to the Gateway must be stopped.

See Figure 77 on page 98 for the following procedure:

1. Attach Fibre Channel loopback plug, provided in the service tool kit, to Fibre Channel port.
2. If front panel Fibre Channel connection status LED or LEDs **1** are not on, replace Gateway (go to “Remove and Replace Gateway” on page 109). Return the Gateway you removed.
3. If the Gateway command prompt on the service terminal is not **diagmode >**, enter the **diagBoot** command at the service terminal (see “Boot Modes” on page 196). Wait for the Gateway to finish booting.
4. From the service terminal, enter the **fcSlotTest x** command, substituting the port number for **x** (see “Appendix D. Diagnostic Command Reference” on page 195). If the test fails, replace Gateway (go to “Remove and Replace Gateway” on page 109).
5. If the test passes, Fibre Channel port is good. Remove the loopback plug and reconnect all Fibre Channel cables.
6. Exit diagnostic mode. enter the **normalBoot** command at the service terminal to return the Gateway to normal mode (see “Restoring Normal Mode” on page 196).
7. Inform the system administrator that an external component of Fibre Channel subsystem appears be bad. This may be the cables or the HBA.
8. If the optical cable is easy to remove, go to “Testing Fibre Channel Optical Cable” to test it.
If the optical cable is not easy to remove, go to “Replacing Fibre Channel Cable” on page 99 to replace the cable.

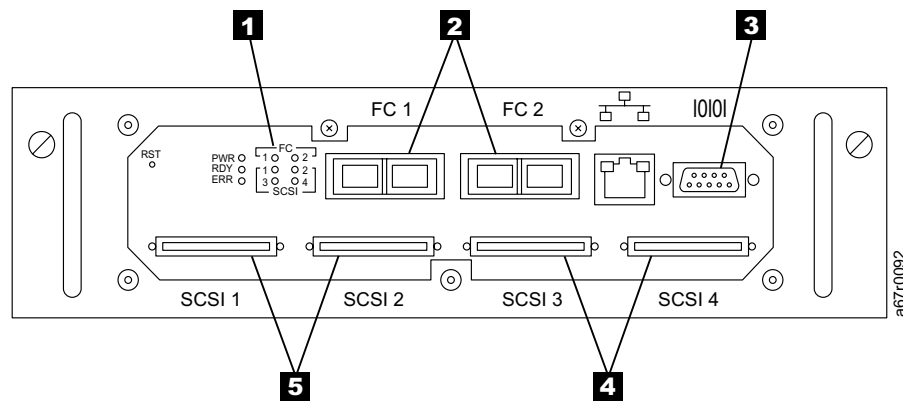


Figure 77. Fibre Channel LEDs

Testing Fibre Channel Optical Cable

Note: If Fibre Channel cable is extremely long, it may be more practical to replace Fibre Channel device first. If the problem persists, replace the cable.

See Figure 77 for the following procedure.

1. Remove the Fibre Channel optical cable end from the host or switch.
2. Obtain the SC-to-SC coupler from the service tool kit. Attach it to Fibre Channel optical cable end removed in step 1
3. Attach the Fibre Channel loopback plug into the other end of the SC-to-SC coupler

Note: If the Fibre Channel optical cable is longer than 150 meters the results of test will be unreliable. The total length of light travel will be over 300 meters.

4. Wait up to 1 minute for the FC Status LED **1** corresponding to Fibre Channel port **2** to light. If it does not light, go to “Replacing Fibre Channel Cable”.
5. If the FC Status LED **1** lights go to “Replacing Fibre Channel Device”.

Note: An alternative method of testing Fibre Channel cables up to 300 meters is to remove both ends of the Fibre Channel cable. Uncouple the cables at each end. Using these cables couple each strand together (A to A & B to B). Then plug each coupled strand into the Gateway GBIC watching for the FC LED indicator to light. If either or both strands fail to light the FC LED go to “Replacing Fibre Channel Cable”. If both strands light the FC LED indicator reconnect cable ends in the original configuration (A to B & A to B). Go to “Replacing Fibre Channel Device”

Replacing Fibre Channel Cable

Note: If Fibre Channel cable is extremely long, it may be more practical to replace Fibre Channel device first. If the problem persists, replace the cable.

1. Toggle the library main power switch to the O position.
2. Replace the cables to Fibre Channel ports with known-good cables.
3. Toggle the library main power switch to the I position. Wait for the Gateway to complete start up.
4. Perform a health check and view the log at viewing level 3.
5. If the problems persists, replace other external devices that are attached to Fibre Channel GBIC (go to “Replacing Fibre Channel Device”). Otherwise, exit this MAP.

Replacing Fibre Channel Device

If the device that needs to be replaced is one of the following:

- Fibre Channel HBA
- Fibre Channel switch
- Fibre Channel hub

Inform the system administrator that it is necessary to replace Fibre Channel device connected to the Gateway to resolve Fibre Channel errors. Repeat this MAP after replacing an external component.

Gateway MAP

Perform these steps if any of the following steps are true:

- **Ready** LED not blinking once per second after power has been on for one minute.
- Gateway is not responding.
- Gateway processor memory fault detected.
- You were directed here from the “Power MAP” on page 101 because all of the LEDs are off.
- You were directed here from the “Power MAP” on page 101 because the Power LED is on but the Ready LED is not blinking once per second.

- Gateway PCI bus parity error is detected.
- Gateway PCI interface error is detected.
- Server could not verify the connection to the Gateway.

Observing Operational LED Patterns

When the Gateway is first powered on, the front panel LEDs flash a variety of patterns. These patterns are generated by the Power On Self Test (POST) and the gateway start up. Within two minutes, the Gateway should have started successfully and the Ready LED should be blinking once per second. If the Ready LED is blinking as expected, go to “Start MAP” on page 82.

If LEDs are not blinking as expected go to “Remove and Replace Gateway” on page 109.

Temperature MAP

Perform this procedure if the following are true:

- Gateway generates trap event codes 62, 64, or 67.
- Gateway generates trap event codes 63, 65, or 68.
- Health Check generates trap event codes 112 or 114.

Notification of Problems in Temperature Subsystem

The Gateway is specified over an operational temperature of 10 to 40°C (50 to 104°F). If the immediate environment of the Gateway exceeds these limits, additional cooling or change of location is required.

If the ambient temperature is within specification, go to “Resolving Temperature Alarm”.

Resolving Temperature Alarm

System operators are normally notified of problems or potential problems in the Gateway subsystem. This is done by the event traps which appear in the “Received Event Trap” window of the StorWatch Specialist client. However, when sensors detect an Alarm condition in the temperature subsystem several things occur. Trap event codes 62, 63, 64, or 65 are generated and a pop up dialog box immediately alerts the user.

(go to “Remove and Replace Gateway” on page 109)

Trap Event Codes 62 to 65 or 67

Temperature problems in the Gateway due to a reduction in blower speed will have event codes 62, 63, 64, or 65 accompanied by event codes 67 or 68. The above event codes may be caused by an obstruction at the inlet or outlet cooling vents. Use the following steps to determine corrective action with these event codes.

1. Check inlet and outlet air vents for obstruction. If obstruction is found remove and allow Gateway to cool. Go to 4 on page 101
2. If trap event codes 61 or 66 are received the cooling problem is fixed. Exit this map.
3. If trap event code 67 is received go to “Remove and Replace Gateway” on page 109. Return to this MAP only if temperature problems occur with new Gateway.

4. If temperature in Gateway does not stabilize in 10 to 15 min and event code 62 or 63 are being generated go to "Remove and Replace Gateway" on page 109. Return to this MAP only if temperature problems occur with new Gateway.
5. If event codes 64, 65, or 67 are being generated go to "Remove and Replace Gateway" on page 109. Return to this MAP only if temperature problems occur with new Gateway.
6. If event code 68 is being generated go to "Remove and Replace Gateway" on page 109. Return to this MAP only if temperature problems occur with replacement Gateway.

Power MAP

You are here because of suspected power problems which are evident by one or more of the following items:

1. The Gateway generates trap event codes 59 or 60.
2. Health Check generates a trap event code 113.
3. The tape library and Gateway are not operational.
4. The Gateway does not respond to any method of management or control.
5. The Gateway fails to perform any I/O operation.
6. All LEDs are off. Go to step 3 following.
7. For step 1 and 2 go to step 1 following.
8. For step 3 through step 6 go to step 3 following.

A character string accompanying a trap event will indicate which power supply is involved.

1. If problem is with the 5 V dc or 12 V dc go to 3.
2. If problem is with the 3.3 V dc or 2.5 V dc go to "Remove and Replace Gateway" on page 109. Do not return to this map unless power problems occur with new Gateway.
3. See *3583 Ultrium Scalable Tape Library Maintenance Information* manual to resolve the power problem.

Ethernet MAP

The network administrator must provide the following information before you can perform this procedure:

- The IP address for the Gateway.
- The net mask for the Gateway in decimal and hex formats.
- The network gateway IP address for the Gateway, if assigned.
- The IP address of a computer on the same subnet as the Gateway for ping tests.
- The IP address of the StorWatch Specialist server.

After gathering the required network administration information, perform this Ethernet MAP procedure. See Figure 78 for the following procedure.

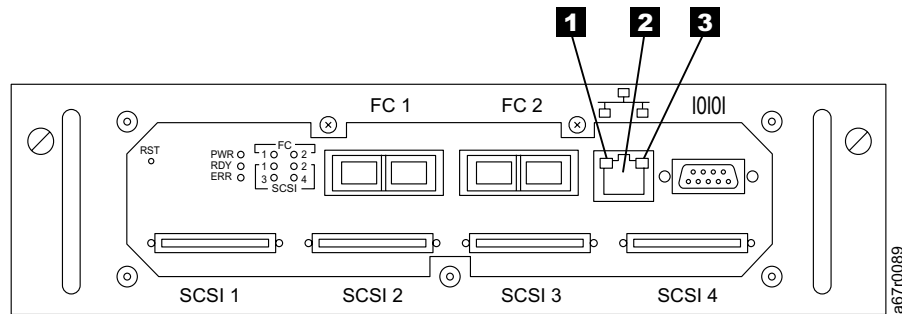


Figure 78. Ethernet LEDs

1. The Gateway must be on and its Ethernet port **2** must be attached to the LAN.
 2. Verify that the Ethernet link LED **1** is on solid. If the LED is on solid, go to step 3. If the LED is off or flashing, continue with step 6.
 3. Verify the yellow speed LED **3** is on solid. If it is flashing check cable connection. To determine the speed of the network go to "Performing a Health Check" on page 84. Return to step 4.
 4. If health check generated a trap event code of 115 the yellow speed LED **3** should be on solid. If yellow speed LED is on solid, go to step 6. If yellow speed LED is not on or is flashing, go to step 5.
 5. Inform the system administrator there may be a problem with Ethernet cable for one of the following reasons:
 - a. Cable quality.
 - b. Intermediate link speeds.
 - c. Interconnect speeds.
- If no problems can be found and Gateway yellow speed LED does not come on go to "Remove and Replace Gateway" on page 109. Exit this MAP.
6. Remove the Ethernet cable from the Gateway Ethernet port and attach the Ethernet loopback plug provided in the service tool kit.
 7. Verify that the Ethernet link LEDs **1** and **3** are on.
 8. If the LEDs are on solid, go to step 10.
 9. If the LEDs are not on or are flashing, replace cable, if still failing, replace the Gateway (go to "Remove and Replace Gateway" on page 109). Exit this MAP.
 10. Remove the Ethernet loopback plug. Obtain another Ethernet cable. Use this cable to attach the Gateway to the LAN.
 11. Verify that the Ethernet link LED **1** is on solid. If the LED is off or flashing inform the network administrator that there is a network problem on the net where the Gateway is attached. Then continue with step 12.
 12. Connect the service terminal to the service port (see "Connecting the Service Terminal" on page 119).
 13. Press the Enter key on the service terminal. If the prompt is not displayed, go to "Service Port MAP" on page 105 to determine whether the RS-232 cable and service terminal are working properly.
 14. Enter the **ifShow** command from the service terminal (see "Appendix A. Connecting to the Service Port" on page 117).

```

Gateway > ifShow
InPci (unit number 0):
  Flags: (0x63) UP BROADCAST ARP RUNNING
  Internet address: 192.168.1.64
  Broadcast address: 192.168.1.255
  Netmask 0xffffffff Subnetmask 0xffffffff
  Ethernet address is 00:60:45:0d:00:c1
  Metric is 0
  Maximum Transfer Unit size is 1500
  2 packets received; 4 packets sent
  0 input errors; 0 output errors
  0 collisions
lo (unit number 0):
  Flags: (0x69) UP LOOPBACK ARP RUNNING
  Internet address: 127.0.0.1
  Netmask 0xff000000 Subnetmask 0xff000000
  Metric is 0
  Maximum Transfer Unit size is 4096
  4 packets received; 4 packets sent
  0 input errors; 0 output errors
  0 collisions

```

15. If there is no entry for **InPci**, enter the **ethEnable** command. Obtain permission from the customer to restart the Gateway. All I/O activity must be stopped. enter the **reboot** command and wait for the Gateway to finish the restart process.
16. From the service terminal enter the **ifShow** command. From the **ifShow** display, write down the values of the internet address, netmask, and subnetmask.
17. Compare the internet address with the IP address supplied by the network administrator. Compare the netmask value with the netmask in hex format supplied by the network administrator. The subnetmask should be the same as the netmask. If these values are correct, go to step 19, otherwise continue with step 18.
18. Enter the **ethAddrSet** command to set the correct IP address and netmask values (see "Gateway Network Setup" on page 115). From the service terminal, enter the **reboot** command and wait for the Gateway to finish the start up. Go back to step 16.
19. Enter the **ping [host IP address],10** command, where [host IP address] is four decimal numbers separated by periods. This is the address provided by the network administrator for **ping** testing.

An example of a successful **ping** test follows

```

Gateway > ping "192.168.1.1", 10
PING 192.168.1.1: 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=1. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=2. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=3. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=4. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=5. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=6. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=7. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=8. time=0. ms
64 bytes from 192.168.1.1: icmp_seq=9. time=0. ms
----192.168.1.1 PING Statistics----
10 packets transmitted, 10 packets received, 0% packet loss
round-trip (ms) min/avg/max = 0/0/0
value = 0 = 0x0

```

Display of successful PING test

```
Gateway > ping "192.168.1.251",10
PING 192.168.1.251: 56 data bytes
no answer from 192.168.1.251
value = -1 = 0xffffffff
```

Display of typical PING test

20. If the ping test passed, go to step 25, if not, continue with step 21.
21. Remove the Ethernet cable from the Gateway and install the Ethernet loopback plug. Enter the **diagBoot** command from the service terminal. Wait for the Gateway to complete start up. Verify that the **diagmode >** prompt is displayed.
22. Enter the **elTest** command from the service terminal.

```
diagmode > elTest

==== Testing Ethernet ====
External loopback LANCE-0
Ethernet OK
value = 0 = 0x0
```

23. If the test failed, replace the Gateway. See "Remove and Replace Gateway" on page 109).
24. Remove the Ethernet loopback plug. Enter the **normalBoot** command from the service terminal, and wait for the Gateway to finish start up. Attach the Ethernet cable to the Gateway.
25. Enter the **gateAddrGet** command from the service terminal, and write down the network gateway address that is displayed. Compare this address to the one provided by the network administrator. If both addresses are the same, go to step 27. If they are not the same, continue with step 26.

```
Gateway > gateAddrGet
Gateway Address set to 192.168.1.1
value = 0 = 0x0
```

26. If the network Gateway address is incorrect, enter the **gateAddrSet** command to set address to the value provided by the network administrator.
27. Enter the **reboot** command from the service terminal, and wait until the Gateway has finished start up.
28. Enter the **ping** command from the service terminal, to test the connectivity of the StorWatch Specialist server IP address (see step 19 on page 103).
29. Enter the **ping** command from the StorWatch Specialist server to test the connectivity of the Gateway.
30. If both **ping** tests succeed, exit this MAP.
If the **ping** test fails, have the network administrator check and correct the network connection, route tables, and network gateway addresses for both the StorWatch Specialist server and the Gateway.
31. After performing the tasks in step 30, return to step 27 and repeat steps 27 through 30 until the **ping** test succeeds.

Service Port MAP

These steps are performed if the Gateway starts and responds to the StorWatch Specialist, but the service port does not respond.

Checking the RS-232 Cable

This test requires another laptop or desktop computer with a functioning RS-232 9-pin port. Terminal emulation software must be installed and running.

1. Remove the RS-232 null-modem cable from the service port and connect it to the compatible port on the other computer.
2. Connect the service terminal to the cable.
3. Set the service terminal and the other computer to the following:
 - 19 200 Baud
 - 8 data bits
 - no parity
 - one stop bit
 - X-on X-off
4. Enter test lines in the service terminal and the other computer. Confirm that they are displayed on both monitors. If this fails, replace the RS-232 cable.
5. If the cable is good, remove it from the other computer.
6. Go to “Checking the Connection with Boot Messages”.

Checking the Connection with Boot Messages

1. Reconnect the terminal to the Gateway with the RS-232 null modem cable.
2. Stop all I/O activity to the Gateway.
3. Toggle the library main power switch to the O position. Wait for 1 minute, then toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
4. If start messages fail to appear on the service terminal, replace the Gateway base (go to “Remove and Replace Gateway” on page 109).

Chapter 6. Removal and Replacement Procedures

This chapter describes remove and replacement procedures for the SAN Data Gateway Module and/or GBICs. The SAN Data Gateway Module will be referred to in the rest of this chapter by the name Gateway.

Items covered in this chapter are as follows:

- Handling ESD parts.
- Remove and replace GBIC.
- Remove and replace Gateway.
- Verify new Gateway.
- Fibre Channel tests.
- Test SCSI ports.
- Ethernet test.
- Updating Gateway.
- Gateway network setup

Handling Electrostatic Discharge Sensitive Parts

In the rest of this chapter electrostatic discharge will be referred to by ESD.

Attention: It is highly recommended you follow industry best practices when handling ESD sensitive parts.

- Keep the ESD sensitive part in a static protective bag until you are ready to install the part into Gateway.
- Make the slightest possible movements with your body to prevent buildup of static electricity on your body from clothing, carpets, and furniture.
- If instructed to do so, toggle the library main power switch to the O position.
- Just before touching the ESD sensitive part, discharge any static charge buildup on your body by touching the metal frame of the library. If possible, keep one hand on the frame while you install or remove an ESD sensitive part.
- If available wear an ESD wrist strap.
- As you remove the ESD sensitive part put it into an ESD protective bag.
- Be very careful when you work with ESD sensitive parts when the outside temperature is low. Combination of low outside temperature and inside heating provides ideal conditions for generating static electricity

Remove and Replace GBIC

Attention: Shut down the host systems to ensure all I/O through the Gateway has stopped. Toggle the library main power switch to the O position.

Remove GBIC

Attention: You must stop I/O at Fibre Channel host.

1. Review “Handling Electrostatic Discharge Sensitive Parts”.
2. Disconnect the Fibre Channel cable.
3. Slide GBIC out of the slot in Gateway.
4. Place GBIC in a static protective bag.

Note: If there will be a delay in plugging Fibre Channel cable into new GBIC install protective dust caps over the Fibre Channel end.

Replace GBIC

Attention: You must stop I/O at Fibre Channel host.

1. Review “Handling Electrostatic Discharge Sensitive Parts”.
2. Remove the dust caps from new GBIC.
3. Insert the new GBIC into the Gateway GBIC slot.
4. Insert Fibre Channel cables in new GBIC.

Remove and Replace Gateway

The remove, replace procedures are performed if a repair action is required for the Gateway. If you suspect the Fibre Channel cable or GBIC is the failing component go to “Remove and Replace GBIC” on page 108.

Remove Gateway

Attention: All I/O activity must be stopped at the Fibre Channel host.

1. Verify that you have saved the latest configuration of the Gateway. See “Startup and Configuration” on page 30.
2. Toggle the library main power switch to the O position.
3. Review “Handling Electrostatic Discharge Sensitive Parts” on page 108.
4. Perform the following steps for each cable attached to the Gateway:
 - a. Disconnect cable. Install dust covers on Fibre Channel cable ends.
 - b. Mark cable clearly so you can connect cable to correct connector on the new Gateway.
5. Remove all GBIC Modules from the Gateway observing instructions in “Handling Electrostatic Discharge Sensitive Parts” on page 108.
6. Set the GBIC aside. You will install it in the new Gateway.
7. See Figure 79. Loosen thumbscrews **2** and slide the Gateway **1** out of library.
8. Return the Gateway. Service representative will know procedure for returning the Gateway.

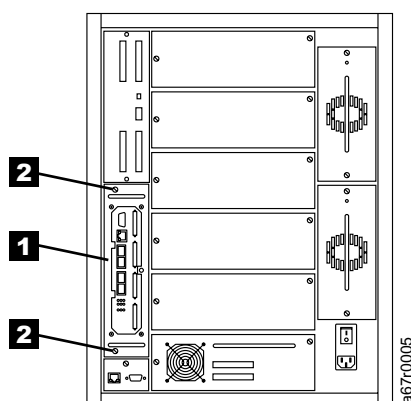


Figure 79. Gateway in tape library

Replace Gateway

See Figure 79 for following steps:

1. Review “Handling Electrostatic Discharge Sensitive Parts” on page 108.
2. Remove the Gateway from protective bag.
3. Insert the Gateway **3** into the empty bay in library **1** where you removed the failing Gateway.
4. Seat the Gateway firmly and tighten two thumbscrews **2**.
5. Install all GBIC modules which were removed in step 5 on page 109.
6. Go to “Verify New Gateway” on page 110.

Verify New Gateway

For more information about procedures and commands used in this section see “Appendix A. Connecting to the Service Port” on page 117 and “Appendix D. Diagnostic Command Reference” on page 195.

See Figure 80 for cabling in the following steps.

To verify the new Gateway you will need to do all the following steps:

1. Attach service terminal to serial port **3** on Gateway.
2. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
3. From the Service Terminal enter **diagboot** command.
4. Wait until Gateway has finished booting in diagnostic mode.
5. From the service terminal enter **showBox** command.
6. Verify that the Gateway accurately displays physical channel information.
7. If **showBox** display is accurate, go to “Fibre Channel Tests”. If not go to “Chapter 5. Maintenance Analysis Procedures” on page 81.

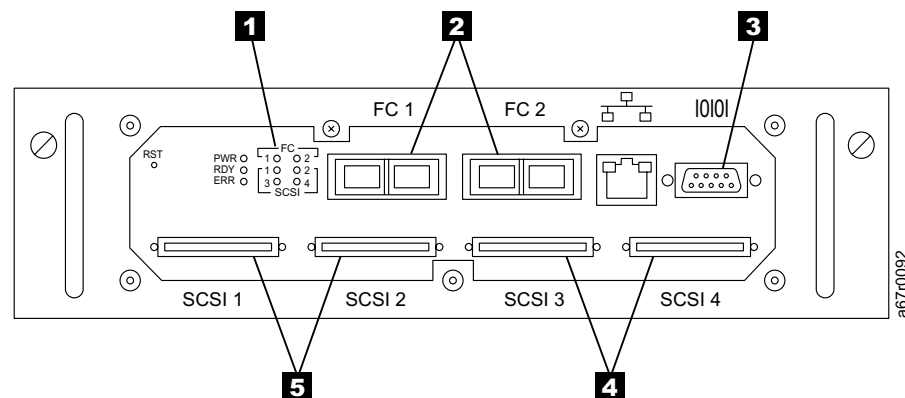


Figure 80. Gateway Cable Connections

Fibre Channel Tests

For following steps see Figure 80.

1. Insert the Fibre Channel wrap plug in one of the GBIC ports **2**.
2. From the service terminal enter the **fcSlotTest *** command.

Note: * to be replaced by the number 1 or 2 depending on which slot the wrap plug is in.

3. If the test passes and you have completed the test to both slots or the only slot, remove wrap plug. Install dust cover on wrap plug. Go to “Test SCSI Ports” on page 111.
4. If the test passes and you have another port to test, remove wrap plug. Insert wrap plug into the other port and go to step 2.
5. If the test failed, remove the wrap plug and go to “Chapter 5. Maintenance Analysis Procedures” on page 81.

Test SCSI Ports

See Figure 80 on page 110 for following steps:

1. Attach the appropriate VHDCI loop back cable between SCSI Ports 1 and 2 **5**.
2. From the service terminal enter the **scsiChannelTest x,y** command.

Note: For SCSI ports 1 and 2 **x,y is 1,2**. For SCSI ports 3 and 4 **x,y is 3,4**.

3. If test passes and you have not completed test on ports 3 and 4 move loop back cable to ports 3 and 4 **4**. Go to step 2.
4. If the test passes and you have completed ports 3 and 4 the SCSI test is complete. Go to "Ethernet Test".
5. If the test fails, go to "Chapter 5. Maintenance Analysis Procedures" on page 81.

Ethernet Test

Configure the Ethernet network or obtain the following Ethernet network parameters:

1. Ethernet port host name
2. Ethernet port host network address.
3. Ethernet port host network mask
4. Ethernet port host routes
5. See "Gateway Network Setup" on page 115.

See Figure 81. Proceed with the test:

1. Insert Ethernet wrap plug into Ethernet port **2**
2. From the service terminal enter **e!Test** command.
3. If the test fails go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
4. If the test passes proceed with step 5.
5. Remove the Ethernet wrap plug.
6. Go to "Updating Gateway" on page 112.

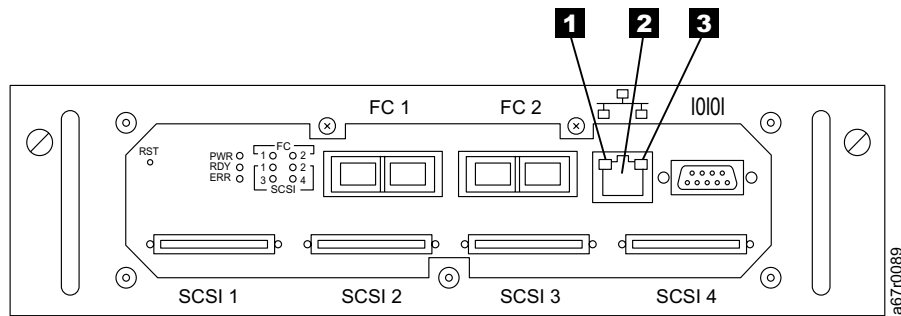


Figure 81. Gateway Ethernet Port

Updating Gateway

You must complete the following steps before loading the Gateway with configuration saved in step 1 on page 109.

1. At the service terminal enter the **hardwareConfig** command to update Gateway module's vital product data (VPD).
2. At the service terminal enter the **normalBoot** command.
3. Wait until Gateway has finished booting.
4. At the service terminal enter the **version** command. Record the operating software version number.
5. If an update is required, download the version to a storable media and do the following steps:
 - a. Start Gateway server and client.
 - b. Logon with administrator privileges and connect to Gateway.
 - c. If you downloaded new operating software in step 5 use **Controls —> Update Firmware** menu to update the operating system now.
 - d. Use menu item **Tools —> Load Gateway Configuration** to load the persistent address map into Gateway.
 - e. Use menu item **Controls —> Restart Gateway** to do a Gateway restart.
 - f. Use menu item **Tools —> Disconnect Gateway** to release Gateway.
6. Enter the **ridTag** command and type the identifier.
7. Toggle the library main power switch to the O position.
8. Disconnect the RS-232 cable from Gateway.
9. Toggle the library main power switch to the | position. Wait for the Gateway to complete start up.
10. Use the "After repair checklist" on page 113 Table 15 on page 113 to verify that all repair actions are complete.

After repair checklist

This table may be used as a checklist to confirm that the repair action is complete.

Table 15. Post Repair Checklist

Step	Actions	Comments and References
1	Reinstall the Gateway in its original location.	See "Replace Gateway" on page 109.
2	Ensure the FC hosts are turned off. If not, disconnect the FC cables now.	Although you just reconnected all cables, if you cannot turn off the FC hosts you must disconnect the FC hosts before applying power to the library. This is a safety precaution which ensures that the FC hosts cannot perform any I/O to the SCSI target devices prior to restoring the Gateway configuration.
3	Attach the service terminal to the Gateway	None
4	Toggle the library main power switch to the position. Wait for the Gateway to complete start up.	None
5	Gateway should finish booting within one minute.	Within one minute, the Ready LED should start flashing once per second and the "Done executing startup script" message should be displayed on the service terminal. If not, go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
6	From the service terminal enter the targets command.	See "Appendix B. Service Port Command Reference" on page 123. If all attached SCSI devices are not shown go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
7	If you replaced the Gateway, configure the network parameters.	Obtain the network parameters from customer. See "Gateway Network Setup" on page 115.
8	Perform the following steps: 1. Start the Gateway server and client. Logon with administrator privileges. Connect to Gateway. 2. If you downloaded new operating software in step 5 on page 112 use Controls → Update Firmware menu to update the operating system now. 3. Use menu item Tools → Load Gateway Configuration to load the persistent address map into Gateway. 4. Use menu item Controls → Restart Gateway to do a Gateway restart. 5. Use menu item Tools → Disconnect Gateway to release Gateway.	This step must be performed if you replaced Gateway.
9	1. If you disconnected Gateway cables at step 2 of this table, connect them now. 2. Ask customer to power on (or reboot) the FC hosts.	See Figure 82 on page 114. If the FC Connection Status LEDs 1 for the attached hosts are not on check FC cables. If FC cables are good go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
10	1. From service terminal enter the fcShow command. This command will display status of each FC interface installed and connected. 2. From service terminal enter the fcShowDevs command. This command will display SCSI target devices which are connected as seen by the Fibre Channel interface.	In the output of fcShow command look for Firmware State column. If the word Ready does not appear go to "Fibre Channel MAP" on page 96. Verify all SCSI target devices are seen by each FC interface. If not go to "SCSI MAP" on page 90.

Table 15. Post Repair Checklist (continued)

Step	Actions	Comments and References
11	Verify all (or designated) target devices are available to the host systems.	Use appropriate host system utilities for disk and tape. If "Access Control" is enabled (Channel Zoning, VPS or VPM) hosts will only see devices assigned to them. If designated devices are NOT available, reboot host and check again. If problem persists, go to "Chapter 5. Maintenance Analysis Procedures" on page 81.
12	Disconnect RS-232 cable from the Gateway and from the service terminal. Return it, the SCSI loop back cable, FC wrap plug, and Ethernet wrap plug to the service tool kit.	None
13	End of repair	

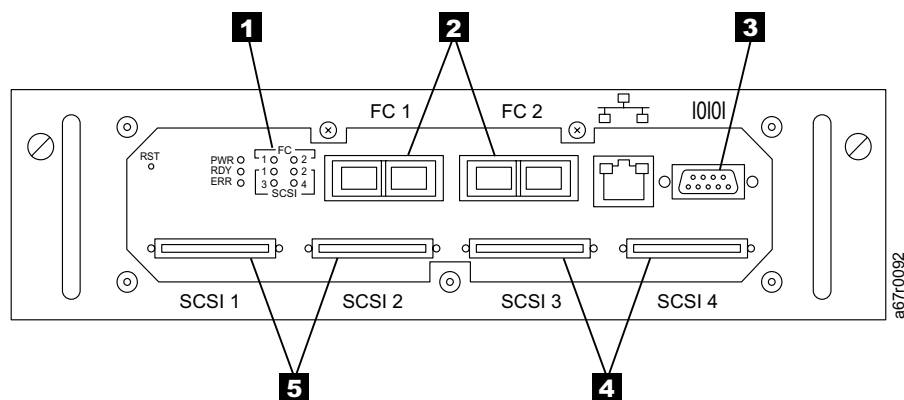


Figure 82. Gateway Panel

Gateway Network Setup

1. The Gateway must be connected to a 10/100 Base-T Ethernet network for use with the StorWatch Specialist software.
2. See Figure 81 on page 111 for this step. The RJ-45 Ethernet connector **2** is located on the panel of the Gateway.
3. See Figure 82 on page 114. You will need to configure first the IP address by connecting a terminal or terminal emulator to the service port **3** of the Gateway (see “Appendix A. Connecting to the Service Port” on page 117).

For all the following examples, substitute values you obtain from customer network administrator.

1. Set host name.
The host name is set using the **hostNameSet** command. In example shown the host name of GATEWAY was “GATEWAY”, being changed to “foster”. Shell prompt will change to reflect the new name.

```
GATEWAY > hostNameSet "foster"
Target hostname set to foster
value = 0 = 0x0
foster >
```

2. Set host network address.
If you need to set a netmask, specify it after the network address using the command **foster > ethAddrSet “10.0.0.2”, “255.0.0.0”**
The network address is set using the **ethAddrSet** command. IP address is specified as four decimal numbers separated by periods.
foster > ethAddrSet “192.168.1.54”
Host Address set to 192.168.1.54 for Ethernet interface
value = 0 = 0x0

3. Set network routes and/or default gateway.
If a network gateway is needed for the Gateway to communicate with other systems, you must specify one using the **gateAddrSet** command.

```
foster > gateAddrSet "192.168.1.1"
value = 0 = 0x0
```

When more complicated routing is required to reach StorWatch Specialist server, use the **route** command. Specify the destination address, as a full address (single host) or as an abbreviated subnet address. Specify the address of the gateway which is reachable on the local subnet.

```
foster > route "add", "192.168.1.1"
value = 0 = 0x0
```

4. Enable the Ethernet port.
By default, the Ethernet port on the Gateway is disabled. To enable the port, use the **ethEnable** command. Gateway must be rebooted to activate the Ethernet port.

```
foster > ethEnable
Ethernet will be enabled on the next boot
value = 0 = 0x0
foster >
```

5. Add user account for Telnet (optional).

If you want to access the Gateway command interface through its Ethernet port using a Telnet session you must add a user account. In the example below replace “username” with name your user will logon with. Replace “password” with password your user will logon with. The password you specify must be eight or more characters. The default username is “user”. The default password is “password”. For more information, see the **user** commands in “Appendix B. Service Port Command Reference” on page 123.

```
foster > userAdd "username", "password  
value = 0 = 0x0  
foster >
```

6. Reboot the Gateway to activate the Ethernet port. Use the **reboot** command to accomplish the reboot..

```
foster > reboot
```

Appendix A. Connecting to the Service Port

The service port is an RS-232C DTE port, configured at 19 200 Baud, with 8 data bits, no parity, and X-on and X-off flow control. The 9-pin connector is compatible with serial ports on PCs. A PC can be used to connect to the service port using the 9-pin null modem cable provided with the unit. For connection to another system, such as a UNIX workstation, a different cable or an adapter might be required.

This appendix provides information about the following:

- Service port connections
- SAN Data Gateway Module network setup (the SAN Data Gateway Module will be referred to in the rest of this appendix by the name Gateway)

Service Port Connections

Figure 83 shows the service port pin-out.

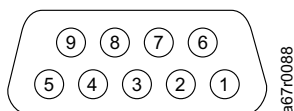


Figure 83. Service Port Pin-Out

Service port connector pin assignments are listed in Table 16.

Table 16. DB-9 RS-232 Connector Pin Assignments

Pin number	Signal name	Abbreviation	Direction relative to the Gateway
1	Carrier detect	CD	In
2	Receive data	RD	In
3	Transmit data	TD	Out
4	Data terminal ready	DTR	Out
5	Signal ground	SG	-
6	Data set ready	DSR	In
7	Request to send	RTS	Out
8	Clear to send	CTS	In
9	Ring indicator	RI	In

Table 17 lists the null-modem cable connections.

Table 17. Null-Modem Cable Connections

Service port pin number	Signal name	9-pin AT connector	25-pin (DB25) connector (DTE)
1	Carrier detect (not used)	N/C	N/C
2	Receive data <-> Transmit data	3	2
3	Transmit data <-> Receive data	2	3
4	Data terminal ready <-> Data set ready	6	6
5	Signal ground	5	7
6	Data set ready <-> Data terminal ready	4	20
7	Request to send <-> Clear to send	8	5
8	Clear to send <-> Request to send	7	4
9	Ring indicator (not used)	N/C	N/C

Connecting the Service Terminal

This section contains the hardware information needed to interconnect the service terminal.

Hardware Required

- RS-232 DB9F-to-DB9F null modem cable
- Desktop computer or laptop computer, or a 232 DTE terminal, or a desktop or laptop computer that runs terminal emulation software
- RS-232 DB9M to DB25F adaptor if the terminal uses a DB25M connector

Initial Setup of HyperTerminal

This section shows the steps to setup the HyperTerminal program. Other terminal emulation programs operate in a similar fashion.

1. Connect the null modem cable (and the 9- to 25-pin adapter if applicable) between the computer-serial (COM) port and the Gateway service port.
2. Turn on the service terminal.
3. On the service terminal, select the HyperTerminal icon and double-click on it.
4. For **New Connection** enter **Gateway** and click **OK**.
5. Select **Connect To**—>**Connect using** and the number of the COM port you have chosen. Click **OK**.
6. In **COM Properties** select:
 - Bits per second:19 200
 - Data bits:8
 - Parity:None
 - Stop bits:1
 - Flow Control:XON/XOFF
7. Click **OK**.

Verifying the Connection

If the Gateway is already on, then characters typed in the terminal should be visible to the operator. The simplest test is to press the Enter key. The Gateway will respond by displaying a command prompt like:

```
Gateway >
```

When the Gateway is rebooting, several messages are displayed on the service terminal. A successful boot is indicated by the last message: "Done executing startup script".

Updating Firmware and Configurations

Although the StorWatch Specialist is the simplest and most efficient tool for updating firmware and saving/loading configurations, you can use the service terminal as an alternate method to perform these operations.

The Gateway service port supports Zmodem file transfers. The procedures below are specific for using the HyperTerminal program on the service terminal to transfer files. Other terminal emulation programs operate in a similar fashion. The Zmodem send and receive functions in some terminal emulation programs automatically issue the command string "rz" before sending a file and the command string "sz" before receiving a file. However, even if the program you are using automatically sends the "rz" command, manually issuing the command string "rz" before starting the transfer has no negative effect on the transfer.

Updating Gateway Firmware

1. From the Hyper Terminal window, at the Gateway > command prompt, type rz and then press the Enter key.
2. From the HyperTerminal window select Transfer and Send File.
3. From the Send File dialog enter the path and filename where the firmware file (must be an image (.img) file) is located or click the Browse button and navigate to it. In the Protocol field, select Zmodem and click the Send button.
4. It will take several minutes for the file to be transferred. The Zmodem file send dialog will display the current status, and it will close automatically when the file transfer has completed.
5. Wait for the "Firmware Update Complete" status message to be displayed on the service terminal indicating successful completion. You must reboot the Gateway for the update to take effect.

If HyperTerminal reports an error, try to send the file again. If the Gateway reports an error, make a note of the error code and see "Zmodem Status Code Table" on page 121 for further information.

Saving a Configuration File

1. From the HyperTerminal window enter sz "config.cfg" **Enter**. The filename "config.cfg" is shown here as an example. You can specify a different filename, but it must be in quotes, 8 characters or less, and end in .cfg.
2. From the HyperTerminal window select Transfer and Receive File.
3. From the Receive File dialog enter the path to the folder where you want to save the file or click the Browse button and navigate to it. For the Receiving protocol, select Zmodem and press the Receive button.
4. Wait for the "Configuration Download Complete" status message to be displayed on the service terminal indicating successful completion.

If HyperTerminal reports an error, try to receive the file again. If the Gateway reports an error, make a note of the error code and see the "Zmodem Status Code Table" for further information.

Loading a Configuration File

1. From the Hyper Terminal window, at the Gateway > command prompt, type rz and then press the Enter key.
2. From the HyperTerminal window select Transfer and Send File.
3. From the Send File dialog enter the path and file name where the firmware file is located or click the Browse button and navigate to it. In the Protocol field, select Zmodem and click the Send button.
4. Wait for the "Configuration Update Complete" status message to be displayed on the service terminal indicating successful completion. You must reboot the Gateway for the update to take effect.

If HyperTerminal reports an error, try to send the file again. If the Gateway reports an error, make a note of the error code and see the "Zmodem Status Code Table" for further information.

Zmodem Status Code Table

The following table shows Zmodem status codes reported by the Gateway.

Table 18. Zmodem Status Codes

Status Code	Description
0	OK
-1	Error unwrapping file -bad file, or out of space
-2	Error opening file
-3	Error writing file
-4	Error closing file
-5	Service Port Function Only
-6	Can not create Debug file - only applicable under lab conditions
-7	Cancelled by host
-8	"Command" not supported
-9	Memory Buffer allocation failed - problem with Gateway memory allocation
-10	No file to send
-11	Garbage - degraded link
-12	CRC Error - degraded link
-13	Timeout Error
-14	File size error - file size is different than it was supposed to be
-15	Invalid file type
-16	Too many retries - degraded link
-17	Position Error - file data has been lost

Appendix B. Service Port Command Reference

A shell interface provides access to management and configuration commands. The shell can be accessed by connecting a terminal or a computer with terminal emulation software to the SAN Data Gateway Module service port.

The SAN Data Gateway Module will be referred to in the rest of this appendix by the name Gateway.

Use the StorWatch Specialist to manage the Gateways. When you use the specialist, most of the operations described in this reference are carried out through the client application.

Table 19 lists all the commands, grouped by their function, and the page numbers where you can find command descriptions.

Table 19. Management and Configuration Commands Grouped by Function

Group	Description	Page
Command and control		
disableCC	Disable command and control interface	129
enableCC	Enable command and control interface	130
setSnaCCLun	Change command and control interface LUN	164
Data mover		
sncFeatureEnable	Enable the optional data mover feature	166
Diagnostics		
elTest	Test Ethernet port with loop-back cable in diagnostic mode	130
scsiChannelTest	Test SCSI channels with loop-back cable in diagnostic mode	157
Environmental Sensors		
envMonShow	Display all environmental channel states	130
Ethernet Network		
arptabShow	Display a list of known ARP entries	127
ethAddrSet	Set Ethernet port address	132
ethDisable	Disable Ethernet port	133
ethEnable	Enable Ethernet port	133
gateAddrGet	Display network gateway address	140
gateAddrSet	Set network gateway address	141
host	Add, delete, or list network host table entries	144
host "add"	Add host table entries	144
host "delete"	Delete network host table entries	144
host "list"	List network host table entries	145
hostAdd	Add a timeserver to the system	145
hostNameSet	Change the Gateway network name	145
icmpstatShow	Display statistics for ICMP	146
ifShow	Display Ethernet port parameters and status	146
inetstatShow	Display all internet protocol sockets	147

Table 19. Management and Configuration Commands Grouped by Function (continued)

Group	Description	Page
ipstatShow	Display statistics for IP	147
macShow	Display Ethernet port media access control address	149
mbufShow	Display mbuf statistics	152
route	Add, delete, or list network route table entries	155
route "add"	Add network route table entries	155
route "delete"	Delete network route table entries	156
route "list"	List network route table entries	156
snmpCommunitiesShow	Display list of community names currently in use	166
snmpReadCommunityAdd	Add community name with read permission	167
snmpReadCommunityRemove	Remove community name read permission	167
snmpTrapCommunitySet	Set community name passed with traps	168
snmpWriteCommunityAdd	Add community name with write permission	168
snmpWriteCommunityRemove	Remove community name write permission	168
tcpstatShow	Display statistics for TCP	171
trapDestAdd	Add recipient IP address to trap destination table	172
trapDestRemove	Remove recipient IP address from trap destination table	172
trapDestShow	Display trap destination table	172
udpstatShow	Display statistics for UDP	173
userAdd	Add a user and password to the password file	173
userDelete	Delete a user from the password file	173
userList	Display the contents of the password file	173
Event logging		
cleShow	Display command log events for the specified LUN	128
cleShowAll	Display command log events for all LUNs	128
loggerDump	Display event log records	148
loggerDumpCurrent	Display event log records for current boot	148
supportDump	Display information used in troubleshooting	168
Fibre Channel		
fcConnTypeGet	Display the current setting of a Fibre Channel port connection type	133
fcConnTypeSet	Set the type of connection for a Fibre Channel port	133
fcFibreSpeedGet	Display maximum and current speeds of Fibre Channel port	134
fcFibreSpeedSet	Set Fibre Channel port speed	134
fcGbicShow	Display the GBIC information for each installed GBIC	135
fcPortModeGet	Display the mode for the specified Fibre Channel port	135
fcPortModeSet	Set the mode for the specified Fibre Channel port	136
fcRestart	Restart the specified Fibre Channel port	137
fcShow	Display Fibre Channel interface status	137
fcShowDevs	Display attached SCSI and Fibre Channel target devices from Fibre Channel port perspective	139
fcShowNames	Display node and port names for Fibre Channels	139

Table 19. Management and Configuration Commands Grouped by Function (continued)

Group	Description	Page
fcTxDisable	Disable a Fibre Channel port transmitter	140
fcTxEnable	Enable or reenable a Fibre Channel port transmitter	140
setFcFrameSize	Set frame size for specific Fibre Channel port	162
setFcHardId	Set loop ID for specific Fibre Channel port	163
setHost	Set host OS type for specific Fibre Channel port	163
sysNodeNameModeSet	Change the Fibre Channel node name mode	
sysNodeNameModeShow	Display the current Fibre Channel node name mode	
targets	Display attached SCSI and Fibre Channel target devices	171
Flash file system		
cd	Set current working path	127
ll	List directory contents in long format	149
ls	List directory contents	149
rm	Remove (delete) a file	155
rz	Initiate a receive Zmodem file transfer session	156
sz	Initiate a send Zmodem file transfer session	171
Health check		
hlthChkIntervalGet	Display health check interval	143
hlthChkIntervalSet	Set health check interval	143
hlthChkLevelGet	Display health check level	143
hlthChkLevelSet	Set health check level	144
hlthChkNow	Perform a health check now	144
Help		
clehelp	Display command log entry command information	128
diagHelp	Display diagnostic command information	129
help	Display information for all shell commands	142
hlthChkHelp	Display health check command information	143
mapHelp	Display device map command information	150
netHelp	Display network command information	153
snmpHelp	Display SNMP command information	167
userHelp	Display user account command information	174
Product data and maintenance		
clearReservation	Force-clear a reservation on the specified target LUN	127
dataScrubberDisable	Disable the data scrubber	128
dataScrubberEnable	Enable the data scrubber	128
hardwareConfig	Re-inventory FRUs and update vital product data (must be in diagnostic mode)	141
initializeBox	Restore factory defaults by deleting all configuration files including persistent address map, then restart	147
licenseShow	Display information about installed software license keys	147
mapCompressDatabase	Remove inactive device entries and reassign LUNS contiguously in persistent address map database	149

Table 19. Management and Configuration Commands Grouped by Function (continued)

Group	Description	Page
mapRebuildDatabase	Delete and reconstruct persistent address map database	150
mapShowDatabase	Display all persistent address map database entries	150
mapShowDevs	Display persistent address map database entries for attached devices only	151
mapWinnowDatabase	Remove inactive device entries from persistent address map database	152
shellLock	Lock or unlock the shell command interface	165
showBox	Display graphic of installed hardware modules	165
sysConfigShow	Display configuration settings	169
sysVpdShow	Display vital product data	169
sysVpdShowAll	Display vital product data for all subsystems	169
ridTag	Display and set serial number of replaced base	154
version	Display firmware version	174
uptime	Display time elapsed since last start	173
SCSI		
fcShowDevs	Display information about the devices that are accessible from each Fibre Channel interface	139
scsiAltIdGet	Display SCSI alternate IDs	157
scsiAltIdSet	Change SCSI alternate IDs	157
scsiHostChanGet	Display SCSI host channel modes	158
scsiHostChanSet	Set SCSI host channel modes	158
scsiHostIdGet	Display SCSI host ID numbers	158
scsiHostIdSet	Set SCSI host ID numbers	159
scsiRescan	Rescan for devices on one or all SCSI channels	159
scsiResetDisableGet	Display SCSI bus reset on startup setting	159
scsiResetDisableSet	Set the SCSI bus reset on startup setting	160
scsiShow	Display SCSI channels and attached devices	160
scsiTermGet	Display termination status information for SCSI channels	161
scsiTermSet	Set termination status for the selected channel	162
targets	Display attached SCSI and Fibre Channel target devices	171
xscsiAltIdGet	Display SCSI alternate IDs for Ultra2/3 channels	174
xscsiAltIdSet	Change SCSI alternate IDs for Ultra2/3 SCSI channels	175
xscsiHostChanGet	Display SCSI host channel modes for Ultra2/3 channels	175
xscsiHostChanSet	Set SCSI host channel modes for Ultra2/3 SCSI channels	175
xscsiHostIdGet	Display SCSI host ID numbers for Ultra2/3 channels	176
xscsiHostIdSet	Set SCSI host ID numbers for Ultra2/3 SCSI channels	176
xscsiResetDisableGet	Display SCSI bus reset on startup settings for Ultra2/3 SCSI channels	176
xscsiResetDisableSet	Set the SCSI bus reset on startup setting for Ultra2/3 SCSI channels	176
xscsiTermGet	Display termination status information for Ultra2/3 SCSI channels	177
xscsiTermSet	Set termination status for the selected Ultra2/3 SCSI channels	177
Startup		
diagBoot	Shutdown and restart in diagnostic mode	128

Table 19. Management and Configuration Commands Grouped by Function (continued)

Group	Description	Page
normalBoot	Shutdown and restart in normal mode	154
reset	Restart without shutdown	154
reboot	Shutdown and restart	154

Commands

This section describes the commands that are available to control, manage, and service the Gateway. The commands are listed in alphabetical order for easier reference. Examples of most commands are shown after the description.

Most commands display a status value in decimal and hexadecimal after execution and before a new prompt is displayed. Usually a value of 0 indicates success, but some commands can return a different value.

arptabShow

Use the **arptabShow** command to display the contents of the ARP table. The ARP table contains the current internet-to-Ethernet address mappings. This information can be useful to the LAN administrator.

```
Gateway > arptabShow
192.168.1.19 at 8:0:20:23:2f:db
value =0 =0x0
Gateway >
```

cd

Use the **cd** command to move to a different directory (usually in the flash file system).

```
Gateway > cd "MGMT"
value = 0 = 0x0
Gateway >
```

clearReservation [devId]

Use the **clearReservation** command to force-clear a reservation that is held by a host for the specified target device. It might be necessary to issue this command if a host that has a reservation for a shared device was disconnected from the Gateway without properly shutting down the application software that issued the reservation. If this is the case, other hosts that attempt to access the shared device will repeatedly receive reservation conflict status from the device. Issuing the **clearReservation** command may result in resetting the target device.

devId The index of the device (LUN)

```
Gateway > clearReservation 4
value =0 =0x0
Gateway >
```

In the example the **clearReservation** command clears a reservation on a target device at LUN 4.

cleHelp

Use the **cleHelp** command to display a list of the command log event facility commands.

```
Gateway > cleHelp
CLE - Command Log Event facility
cleShow <lun> - Displays Logged Events for a specific LUN
cleShowAll - Displays Logged Events for All LUNs
Gateway >
```

cleShow [lun]

Use the **cleShow** command to display the last 64 command log events for a device at the specified LUN. This log is not maintained for disk devices because the performance impact is significant. The manufacturer may request the contents of the command log for diagnostic purposes. Information about interpreting these events is not provided here.

cleShowAll

Use the **cleShowAll** command to display the last 64 command log events for all LUNs. The manufacturer may request the contents of the command log for diagnostic purposes. Information about interpreting these events is not provided here.

csEtimeShow

Use the **csEtimeShow** command to display the elapsed time since the last startup of the Gateway.

```
Gateway > csEtimeShow
Elapsed time since reset 4d:23h:12m:46s:10t
value = 10 = 0xa
Gateway >
```

The example indicates that 4 days, 23 hours, 12 minutes, 46 seconds and 10 clock ticks have elapsed since the Gateway was reset. There are 60 ticks per second.

dataScrubberDisable

Use the **dataScrubberDisable** command to disable the memory scrubber, an independent low-priority task that checks the full data buffer space approximately once per hour.

dataScrubberEnable

Use the **dataScrubberEnable** command to enable the memory scrubber, an independent low-priority task that checks the full data buffer space approximately once per hour.

diagBoot

Use the **diagBoot** command only to transition a Gateway from normal operations to the special diagnostic mode. The **diagBoot** command first ensures that the `ffs0:mt` directory exists. It then verifies that the files `diagnstk.o` and `diagnstk.rc` are in the flash file system. If they are in the root directory, they are moved to the `ffs0:mt` directory.

This command copies the existing bootline to a file in the ffs0:mt directory on the Gateway.

The **diagBoot** command installs a new bootline directing the Gateway to start, using a special diagnostic startup script ffs0:mt/diagnstk.rc. The persistent map file config/device.map is renamed config/device.bak (a new file is generated after restarting).

Finally, the **diagBoot** command issues a **reboot** command to apply the changes.

diagHelp

Use the **diagHelp** command to display a list of the diagnostic commands.

```
Gateway > diagHelp
** Diagnostic commands: Available in Diagnostic Mode Only **
elTest Test          Ethernet port w/loop-back cable
fcSlotTest<slotnum> Test specified Fibre Channel port w/loop-back cable
hardwareConfig       Re-inventory FRUs and update Vital Product Data
normalBoot           Shutdown and restart in normal mode
scsiChannelTest <x,y> Test specified SCSI Channels w/loop-back cable
Gateway >
```

disableCC [option number]

Use the **disableCC** command to disable the command and control interface (LUN 0). Specify one of two option parameters as follows:

Option numbers

Results

- 1 Hides the command and control interface and results in inquiry data returning the following message:

```
device not available for LUN 0
```

- 2 Completely disables all command and control functions.

The Gateway is addressed as a SCSI target device for command and control support. On a Fibre Channel interface, this device is seen as logical unit number 0 (LUN 0). The LUN 0 device returns a device type of 0Ch in an **inquiry** command, indicating it is a controller device.

In some cases, it might be desirable to disable this feature. If LUN 0 is disabled, then a device type of 2Ch is returned in an inquiry to LUN 0, indicating that the device is not presently available at this LUN. LUN 0 remains reserved for the command and control interface and is not allocated to another target device.

Other commands are available for re-enabling the command and control interface or reassigning it to a different LUN rather than hiding or disabling it. See the **enableCC** command and the **setSnaCCLun** command for more information.

Note: If you enter the **disableCC** command without specifying an option number, it has the same effect as entering a **disableCC 1** command.

```
Gateway > disableCC 1
value = 0 = 0x0
Gateway >
```

eITest

The Gateway must be in diagnostic mode to use this command, and a loopback plug must be installed on the Ethernet port. Use the **eITest** command to perform an Ethernet loopback test.

```
Gateway > eITest

==== Testing Ethernet ====
External loopback LANCE-0
Ethernet OK
value = 0 = 0x0
```

The first time the **eITest** command is issued it displays the message External loopback LANCE-0. This indicates that the Ethernet chip is in external loop-back mode. Do not connect it to the LAN while in this state. Perform a restart or **normalBoot** command before reconnecting the Gateway to the LAN.

The **eITest** command issues a series of loop-back tests. Test data is transferred and verified.

A good test ends with the following message: Ethernet OK.

Errors are displayed as they are detected.

If errors are detected, the test displays the number of bad test iterations as shown in the following example:

```
==== Testing Ethernet ====
interrupt: ln0: no carrier
Ethernet timeout error
interrupt: ln0: no carrier
Ethernet timeout error
interrupt: ln0: no carrier
Ethernet timeout error
interrupt: ln0: no carrier
Ethernet timeout error
Ethernet test reported 4 errors out of 12 iterations
value = 4 = 0x4
```

enableCC

Use the **enableCC** command to restore the capability to send commands to the command and control interface (LUN 0). The command is typically used to re-enable the interface after it was disabled by the **disableCC** command.

```
Gateway > enableCC
value = 0 = 0x0
Gateway >
```

envMonShow

The **envMonShow** command lists all of the environmental channel states and their current values. Use the command **envMonRangeShow** to restrict output to a display of the ranges relevant to each state. The following channels have been defined.

Table 20. Environmental Channels

Channel Name	Description
Air Inlet Temp	Temperature of the air as it enters the unit
Air Outlet Temp	Temperature of the air as it exits the unit
IO Processor Temperature	Temperature of the IO Processor
Input Power: ± 5 V dc	Voltage level of the ± 5 V dc input
Input Power: ± 12 V dc	Voltage level of the ± 12 V dc input
Local Power: ± 2.5 V dc	Voltage level of the local 2.5 V dc supply
Local Power: ± 3.3 V dc	Voltage level of the local ± 3.3 V dc supply
Local Power: ± 3.3 V dc Aux	Voltage level of the local auxiliary ± 3.3 V dc supply
Fan	Fan running (for tachometer fans: RPM of fan)

```

Gateway > envMonShow
Channel State Value
-----
Air Inlet Temperature Nominal 44 C
Air Outlet Temperature Nominal 51 C
IO Processor Temperature Warning 31 C
Input Power:  $\pm 5$  V dc Nominal 5.2 V dc
Input Power:  $\pm 12$  V dc Nominal 12 V dc
Local Power:  $\pm 2.5$  V dc Nominal 3.3 V dc
Local Power:  $\pm 3.3$  V dc Nominal 3.3 V dc
Local Power:  $\pm 3.3$  V dc Aux Nominal 3.29 V dc
All Power Nominal
All Temp Nominal
Sample Count 20
value =1 =0x1
Gateway >

```

envMonRangeShow

The **envMonRangeShow** command specifies operational ranges for the Gateway's environmental channels. It displays ranges of values associated with the nominal, warning, and alarm states for voltage, temperature, and fan/blower operation according to the channels defined in the envMonShow command:

```
Gateway >envMonRangeShow
INLET Temperature (Degrees C):
Nominal: 5 - 45
Warning: 4 - <5, >45 - 50
Alarm: <4 or >50
IOP Temperature (Degrees C):
Nominal: 5C - 80C
Warning: 4 - <5, >80 - 108
Alarm: <4 or >108
OutletTemperature (Degrees C):
Nominal: 5 - 50
Warning: 4 - <5, >50- 55
Alarm: <4 or >55
5 Volts:
Nominal: 4.83 - 5.20
Warning: 4.75 - <4.83 or >5.20 - 5.25
Alarm: <4.75 or >5.25
12 Volts:
Nominal: 11 - 12.93
Warning: 10.75 to < 11.00, >12.93 - 13.18
Alarm: <10.75 or >13.18
3.3 Volts:
Nominal: 3.20 - 3.39
Warning: 3.13 - <3.20, >3.39 - 3.436
Alarm: <3.13 or >3.46
3.3 Volts (Aux V):
Nominal: 3.20 - 3.39
Warning: 3.13 - <3.20, >3.39 - 3.436
Alarm: <3.13 or >3.46
2.5 Volts:
Nominal: 2.42 - 2.58
Warning: 2.36 - <2.42 or >2.58 to 2.62
Alarm: <2.36 or >2.62
Gateway >
```

ethAddrSet

Use the **ethAddrSet** command to change the IP address of the Gateway. An IP address is specified as four decimal numbers, separated by periods.

```
Gateway > ethAddrSet "192.168.1.54"
Host Address set to 192.168.1.54 for Ethernet interface
value = 0 = 0x0
Gateway >
```

If a netmask is required, specify it after the IP address in “dotted decimal” form, for example:

```
Gateway > ethAddrSet "10.0.0.2","255.255.0.0"
Inet Mask set to ffff0000 for Ethernet interface
Write complete
Host Address set to 10.0.0.2 for Ethernet interface
Gateway >
```

ethDisable

Use the **ethDisable** command to alter the startup parameters of the Gateway and disable the Ethernet port. This command does not take effect until the Gateway is restarted.

```
Gateway > ethDisable
Ethernet will be disabled on next boot
value = 0 = 0x0
Gateway >
```

ethEnable

Use the **ethEnable** command to alter the startup parameters of the Gateway and enable the Ethernet port. This command does not take effect until the Gateway is restarted.

```
Gateway > ethEnable
Ethernet will be enabled on next boot
value = 0 = 0x0
Gateway >
```

fcConnTypeGet [port]

Use the **fcConnTypeGet** command to display the current setting of a Fibre Channel port connection type. See also “fcConnTypeSet [port],[connection]” on page 134.

Table 21. Type of port connection

Parameter	Value	Meaning
Port	1 or 2	The SAN Connection Number

The following example shows how the connection type is displayed when Fibre Channel port 1 is specified and its connection type is loop.

```
Gateway > fcConnTypeGet 1
value =0 =0x0
```

The number displayed as a value indicates the connection type as follows:

Port Value	Connection Type
0	Indicates the connection type is loop.
1	Indicates the connection type is point to point.
2	Indicates the connection type is loop preferred.
3	Indicates the connection type is point to point preferred.

fcConnTypeSet [port],[connection]

Use the **fcConnTypeSet** command to set the type of connection for a Fibre Channel port. See also “fcConnTypeGet [port]” on page 133.

Table 22. Port numbering

Parameter	Value	Meaning
port	1,2	The SAN connection number
Connection	0	Sets the connection type to Loop
	1	Sets the connection type to point to point
	2	Sets the connection type to loop preferred

The following example shows how to set Fibre Channel port 1 connection type to point to point.

```
Gateway > fcConnTypeSet 1,1
value =0 =0x0
Gateway >
```

Attention: You must issue the **fcRestart** command or restart the gateway for the new setting to take affect. See the **fcRestart** command for further information.

fcFibreSpeedGet

The **fcFibreSpeedGet** command displays the potential maximum and the current speed of the Fibre Channel port.

```
Gateway > fcFibreSpeedGet
Possible Speed (Gb/sec)=1 & 2
Actual Speed (Gb/sec) = 1
value =1 =0x1
Gateway >
```

fcFibreSpeedSet

The **fcFibreSpeedSet** command sets the Fibre Channel port speed to 1 Gb/sec or 2 Gb/sec for a Fibre Channel port. The port can also be set to autorange. See Table 23.

Table 23. Meaning of Speed Settings

Parameter	Value	Meaning
Port	1,2	The SAN Connection number
Speed	0	1 Gb/sec
	1	2 Gb/sec
	2	Autorange

```
Gateway > fcFibreSpeedSet 1,1
value =0 =0x0
Gateway >
```

fcGbicShow

The **fcGbicShow** command displays the GBIC information for each installed GBIC. The information is presented in the following format:

```
SN600023 > fcGbicShow
-----
Ctlr : Module : Module
ID : Code : Information
-----
1 :4 :Serial Module Definition Protocol
: Connector Type ----- SC
: Nominal Speed ----- 2.5 Gb/sec
: Link length for 9/125 um ---- 0 meters
: Link length for 50/125 um ---- 5500 meters
: Link length for 62.5/125 um -- 2700 meters
: Vendor Name ----- FINISAR CORP.
: Vendor OUI ----- 009065
: Vendor Part Number ----- FTR-8519-3-2.5
: Vendor Revision ----- 1A
: Vendor Serial Number ----- B2557JC
: Vendor Mfg. Date ----- 10-26-2000
: RX LOS Implemented ----- Yes
: TX Fault Implemented ----- Yes
: TX Disable Implemented ----- Yes
2 :4 :Serial Module Definition Protocol
: Connector Type ----- SC
: Nominal Speed ----- 2.5 Gb/sec
: Link length for 9/125 um ---- 0 meters
: Link length for 50/125 um ---- 5500 meters
: Link length for 62.5/125 um -- 2700 meters
: Vendor Name ----- FINISAR CORP.
: Vendor OUI ----- 009065
: Vendor Part Number ----- FTR-8519-3-2.5
: Vendor Revision ----- 1A
: Vendor Serial Number ----- B2557K2
: Vendor Mfg. Date ----- 10-26-2000
: RX LOS Implemented ----- Yes
: TX Fault Implemented ----- Yes
: TX Disable Implemented ----- Yes
-----
```

fcPortModeGet [port]

Use the **fcPortModeGet** command to display the mode for a specified Fibre Channel port. The default port mode is public target. See also “fcPortModeSet [port],[mode]” on page 136.

Table 24. Port numbering

Parameter	Value	Meaning
Port	1, 2	The SAN Connection Number

The number displayed as a value indicates the port mode as follows:

Value Port Mode

- 1** Indicates the port mode is private target.
- 2** Indicates the port mode is private initiator.
- 3** Indicates the port mode is private target and initiator.
- 17** Indicates the port mode is public target.
- 18** Indicates the port mode is public initiator.
- 19** Indicates the port mode is public target and initiator.

The following example shows how the connection type is displayed when Fibre Channel port 1 is specified and the port mode is private target.

```
Gateway > fcPortModeGet 1
value =1 =0x1
Gateway >
```

fcPortModeSet [port],[mode]

Use the **fcPortModeSet** command to set the mode for a specified Fibre Channel port. See also “fcPortModeGet [port]” on page 135.

The default port mode is public target. This means that if attached to a fabric device the Gateway will register as a target with the name server. If the port mode is private target, the Gateway does not register with the name server and the fabric device will not recognize the Gateway as a target.

The port must be in initiator mode if you want the Gateway to scan for target devices on the port. When the port is in private initiator mode, the Gateway only scans for devices on the local loop.

If the port mode is in public initiator mode, the Gateway also scans for devices attached to a fabric.

Table 25. Port number and meaning

Parameter	Value	Meaning
Port	1,2	The SAN Connection number
Mode	1	Private Target
	2	Private Initiator
	3	Private Target and Initiator
	17	Public Target
	18	Public Initiator
	19	Public Target and Initiator

```
Gateway> fcPortModeSet 1,2
value =0 =0x0
Gateway>
```

fcRestart [port]

Use the **fcRestart** command to restart the specified Fibre Channel port. You typically use this command to restart the port after changing its configuration settings so that the changes take effect. Use this command as an alternative to restarting the Gateway in order to make the configuration changes take effect.

Attention: This command interrupts data flow.

Parameter	Value	Meaning
Port	1, 2	The SAN Connection Number

The following example shows the display when Fibre Channel port 1 is specified.

```
Gateway> fcRestart 1
value =0 =0x0
FCT Restart 1 :
Controller Restart Successful
Gateway >
```

fcShow [level]

Use the **fcShow** command to display the channel status for each Fibre Channel interface. The following example is for a Gateway that has three dual-port Fibre Channel PMCs installed for a total of six Fibre Channel ports.

```
Gateway > fcShow
-----
Fibre Channel Controllers
-----
Ctlr : PCI Addr : ISP : Firmware : Firmware: Loop : Fabric : Port
Id : Bs Dv Fn : Type : State : Version : ID : Attached : Mode
-----
1 : 00 06 00 : 2200 : Ready : 2.01.7 : 1 : No : Targ
2 : 00 07 00 : 2200 : Sync Lost : 2.01.7 : None : No : Targ
3 : 01 08 00 : 2100 : Ready : 2.01.7 : 1 : No : Init
4 : 00 18 00 : 2200 : Ready : 2.01.7 : 1 : No : Targ
5 : 00 18 00 : 2200 : Ready : 2.01.7 : 1 : No : Targ
6 : 00 19 00 : 2200 : Ready : 2.01.7 : PtoP : Yes : Targ
-----
value = 80 = 0x50 = 'P'
Gateway >
```

The column fields in the display provide the following information:

Table 26. Firmware states by function

Function	Firmware States	Results
Ctlr Id	—	Port number for this interface.
PCI Addr	—	PCI address of the interface, including the bus (Bs), device ID (Dv), and function number (Fn).
ISP Type	—	Type of Fibre Channel controller.
Firmware State	—	The current state of the interface as reported by the Fibre Channel PMC adapter firmware. Firmware states are listed below.
	Configuration Wait	Firmware is not initialized.
	Waiting for AL_PA	Firmware is performing or waiting to perform loop initialization.
	Waiting for login	Firmware is attempting port and process logins with all loop ports.
	Ready	The interface is connected, operational, and ready to process SCSI commands. Any other value indicates intermediate states or interface failure.
	Sync Lost	The firmware has detected a loss-of-sync condition and is resynchronizing the serial link receiver. This state is reported when the Fibre Channel link does not detect a connection to a Fibre Channel device.
	Error	The firmware has detected an unrecoverable error condition.
	Nonparticipating	The firmware is not participating on the loop since it did not acquire an AL_PA during initialization.
	Failed	The firmware is not responding to commands.
Firmware Version	—	The version of firmware on the Fibre Channel PMC adapter
Ctrl Addr	—	A pointer to an internal data structure that is used for some diagnostic operations.
Nvram Addr	—	The memory address of the parameter RAM for this interface.
Loop ID	—	The Fibre Channel loop ID for this interface. PtoP indicates a point-to-point connection.
Fabric Attached	—	Indicates whether the port is attached to a fabric.
Port Mode	—	Indicates whether the port is set to target or initiator mode.

fcShowDevs

Use the **fcShowDevs** command to display information about the devices that are accessible from each Fibre Channel interface. The display shows the LUN that the Gateway has assigned to each device, the SCSI channel that the device is attached to, the actual SCSI ID and LUN of the device, and the vendor, product, revision, and serial number of the device.

In the example, channel zoning was used for access control. Fibre Channel 1 has access to all of the attached SCSI tape and disk devices. For the other Fibre Channel interfaces, channel zoning has been set up to restrict access to certain devices.

```
Gateway : fcShowDevs
FC 1:

LUN Chan Id Lun Vendor    Product      Rev  SN
-----
 0   0   0   0 PATHLGHT Gateway      0338 00000060450d0080
17   3   0   0 IBM      03570C12    5346 000000000305
18   3   0   1 IBM      03570C12    5346 000000000305
19   3   1   0 IBM      03570C12    5346 000000000306
 6   1   1   0 IBM OEM   DCHS04X      6363      681F775B
 7   1   2   0 IBM OEM   DCHS04X      6363      682086D3
 8   2   3   0 IBM OEM   DCHS04X      6363      6820837B
 9   2   4   0 IBM OEM   DCHS04X      6363      682076AC

FC 2:

LUN Chan Id Lun Vendor    Product      Rev  SN
-----
 0   0   0   0 PATHLGHT Gateway      0338 00000060450d0080
 6   1   1   0 IBM OEM   DCHS04X      6363      681F775B

value = 2 = 0x2
Gateway >
```

fcShowNames

Use the **fcShowNames** command to display the node and port names (addresses) of the Fibre Channels.

```
Gateway > fcShowNames

-----
Ctlr : PCI Addr : ISP :      Node      :      Port
Id   : Bs Dv Fn : Type :      Name      :      Name
-----
 1   : 00 06 00 : 2200 : 10000060.451603bb : 20010060.451603bb
 2   : 00 07 00 : 2200 : 10000060.451603bb : 20020060.451603bb
 3   : 01 08 00 : 2200 : 10000060.451603bb : 20030060.451603bb
 4   : 00 18 00 : 2200 : 10000060.451603bb : 20040060.451603bb
 5   : 00 19 00 : 2200 : 10000060.451603bb : 20050060.451603bb
 6   : 01 20 00 : 2200 : 10000060.451603bb : 20060060.451603bb
-----

value = 64 = 0x40 = '@'
Gateway >
```

The column fields in the display provide the following information:

Ctlr Id	The channel number for the interface.
PCI Addr	The PCI address of the interface, including bus (Bs), device ID (Dv), and function number (Fn).
ISP Type	The type of Fibre Channel controller, ISP2200 or ISP2200A.
Node Name	The Fibre Channel node name for the Gateway.
Port Name	The Fibre Channel port name for the interface.

fcTxDisable

The **fcTxDisable** command disables a Fibre Channel port transmitter.

```
Gateway > fcTxDisable 1
value =0 =0x0
Gateway >
```

fcTxEnable

The **fcTxEnable** command enables or reenables a Fibre Channel port transmitter.

```
Gateway > fcTxenable 1
value =0 =0x0
Gateway >
```

gateAddrGet

Use the **gateAddrGet** command to display the default network gateway address if one has been set. This address is used when connections are made to a different subnet and there are no explicit routes defined for that subnet. Consult your network administrator for more information about the default gateway (sometimes referred to as default router) address.

```
GATEWAY > gateAddrGet
Write complete
Gateway Address set to 10.0.0.1 for Ethernet Interface
value = 0 = 0x0
Gateway >
```

gateAddrSet

Use the **gateAddrSet** command to change the default network gateway address. This address is used when connections are made to a different subnet and there are no explicit routes defined for that subnet. Consult your network administrator for more information about the default gateway (sometimes referred to as default router) address.

```
Gateway > gateAddrSet "10.0.0.1"
value = 0 = 0x0
Gateway >
```

hardwareConfig

Note: To use the **hardwareConfig** command, the gateway must be in diagnostic mode.

Use the **hardwareConfig** command to record the configurations of installed FRUs by copying them to the nonvolatile vital product data (VPD) stored on the Gateway base. The fields that are updated are the SCSI channel types and the PMC card type. Issue the **hardwareConfig** command after replacing any FRUs. This causes the Gateway to update the VPD.

```
Gateway > hardwareConfig

==== Recording Hardware Configuration ====
Scanning PMC options slots...
Scanning SCSI IO Modules...
Checking memory sizes...

MemSize PCI-0 is 64 Mbytes ...Done

value = 0 = 0x0
Gateway >
```

help

Use the **help** command to display a list of the shell commands.

```
Gateway > help
help                Print this list
cleHelp             Print Command Log Entry info
diagHelp            Print Diagnostic Help info
hlthChkHelp         Print Health Check Help info
mapHelp             Print Device Map Help info
netHelp             Print Network Help info
snmpHelp            Print SNMP Help info
userHelp            Print User account info
cd                  "path"      Set current working path
copy                "in"["out"] Copy in file to out file (0 = std in/out)
h                  [n]          Print (or set) shell history
ls                  ["path"[,long]] List contents of directory
ll                  ["path"]     List contents of directory - long format
pwd                 Print working path
rename              "old","new"  Change name of file
rm                  ["name"]     Remove (delete) a file
shellLock           Lock or unlock shell command interface
version             Print Version info
whoami              Print user name
clearReservation [devId] Clear reservation on a target (may reset target)
diagBoot            Shutdown and restart in diagnostic mode
initializeBox       Delete all device maps, restore factory defaults, reboot
ridTag ["value"]    Display and set serial number of replaced base unit
disableCC [option]  Disable Command and Control Interface
                    option 1 - Report as Invalid (AIX mode)
                    option 2 - Fully disabled
enableCC            Enable Command and Control Interface
scsiRescan [chan]   Rescan SCSI Channel (all if chan not specified)
scsiShow            Display info for SCSI Channels
fcShow             Display info for Fibre Channels
fcShowDevs         Display devices available on each Fibre Channel
fcShowNames        Display Node and Port names for Fibre Channels
hostTypeShow       Display Default Host Type settings
loggerDump [count] Display Logger Dump Records
loggerDumpCurrent [level] Display Logger Dump Records for current boot
reboot             Shut down and restart
reset              Restart without shut down
setFcScsiChanMask [chan],[scsi],[allow] Set Channel Access Control
setFcFrameSize [chan],[size] Set FC Frame Size
setFcHardId [chan],[id] Set FC Loop ID
setHost [chan],[OS] Set default host type for FC Channel
                    OS may be "aix", "nt", "solaris","hpux"
setSnaCCLun        Set LUN for Controller Device (typically zero)
showBox            Display graphic of current hardware configuration
sysConfigShow      Display System Config Parameters
sysVpdShow         Display Vital Product Data
sysVpdShowAll      Display Vital Product Data for all subsystems
targets            List all known target devices
uptime             Display time since last boot
Gateway >
```

hlthChkHelp

Use the **hlthChkHelp** command to display a list of the health check commands.

```
Gateway > hlthChkHelp

hlthChkIntervalGet          - Show Check Interval
hlthChkIntervalSet <interval> - Set Check Interval
hlthChkLevelGet             - Show Check Level
hlthChkLevelSet <level>     - Set Check Level
hlthChkNow                  - Run Health Check Now
Gateway >
```

hlthChkIntervalGet

Use the **hlthChkIntervalGet** command to view the existing health check interval. In the following example, the current interval is 60 minutes.

```
Gateway > hlthChkIntervalGet
value = 60 = 0x3c = '<'
Gateway >
```

hlthChkIntervalSet

Use the **hlthChkIntervalSet** command to set the health check interval. This controls how often the health check process runs. The interval can range from 1 to 65 535 minutes (about 45 days).

```
Gateway > hlthChkIntervalSet 60
value = 0 = 0x0
Gateway >
```

hlthChkLevelGet

Use the **hlthChkLevelGet** command to display the existing health check level. In the following example, the current health check level is 2.

```
Gateway > hlthChkLevelGet
value = 2 = 0x02
Gateway >
```

The following health check levels can be set:

Level number	Level name	Functionality
0	None	Health check disabled
1	Basic function	Power supply and temperature status
2	Interface test	Everything from level 1, plus check all interfaces
3	Device test	Everything from level 2, plus device inquiry on each target device
4	Device ready	Everything from level 3, plus test unit ready on each target device (non-removable media only)

hlthChkLevelSet

Use the **hlthChkLevelSet** command to set the health check level. In the following example the level is set to 3.

```
Gateway > hlthChkLevelSet 3
value = 0 = 0x0
Gateway >
```

hlthChkNow

Use the **hlthChkNow** command to cause the gateway to execute an immediate level 4 health check. Results are displayed that indicate what devices or subsystems failed the check.

```
Gateway > hlthChkNow
```

host

Use the **host** command to add, remove, and list known hosts and their IP addresses. Alias names are supported, allowing multiple names to a single host.

The **host** command creates and maintain a host file, `ffs0:/mgmt/hosts`, for use as a network hosts table. The table associates network names with IP addresses. Use of the hosts table is entirely optional, but can facilitate frequently needed connections.

Each host entry is a single line using the following format:

host add,[hostname],[ipaddress]

```
IP-address official_host_name nicknames ...
```

where

IP-address

is a text string in standard IP Address format (for example, 10.0.0.2)

official_host_name

is the first name selected for this host

nicknames

is an optional list of additional aliases for this host (separated by spaces)

The following is an example of host file contents:

```
192.168.1.90 bruno
200.0.0.42 socrates
200.0.0.45 plato
200.0.0.47 fred
```

Note: The host file does not exist until you enter the **host add** command.

host delete,[hostname]

You must have created the host file with **host add** command before the **host delete** command will execute.

host delete,[hostname]

Deletes the named host from the host table and host file. If the hostname is an alias, then only the alias is removed. If hostname is the official host name, the entry and all aliases are removed.

```
Gateway > host "delete","plato"
Gateway >
```

The command above would give the following results:

```
192.168.1.90 bruno
200.0.0.42 socrates
200.0.0.47 fred
```

host list

Command**Results****host list**

Displays the contents of the host file.

```
Gateway > host "list"
192.168.1.90 bruno
200.0.0.42 socrates
200.0.0.45 plato
200.0.0.47 fred
value = 0 = 0x0
Gateway >
```

hostAdd

The **hostAdd** command allows you to add an entry for a timeserver to your system's configuration, so that log entries are all made according to a single clock. It can be named anything, but in the example, it is named "timeserver". The "ipAddress" must be entered in standard dotted quad format and should be the address of a real timeserver.

```
Gateway > hostAdd "timeserver" "192.168.1.10"
value =0 =0x0
Gateway >
```

hostNameSet

Use the **hostNameSet** command to change the network name of the Gateway. The shell prompt is set to the new host name.

```
Gateway > hostNameSet "foster"
Target hostname set to foster
value = 0 = 0x0
foster >
```

hostTypeShow

Use the **hostTypeShow** command to display the host type setting for each Fibre Channel. The following example shows the possible host types.

```

Gateway > hostTypeShow
FC 1: Type 2 - aix
FC 2: Type 4 - hp-ux
FC 3: Type 1 - nt
FC 4: Type 1 - nt
FC 5: Type 3 - solaris
FC 6: Type 5 - netware
value =0 =0x0
Gateway >

```

icmpstatShow

Use the **icmpstatShow** command to display ICMP statistics for the Ethernet network. Interpreting these statistics requires detailed knowledge of internet networking protocols. This information can be useful to the LAN administrator.

```

Gateway > icmpstatShow
ICMP:
    0 call to icmp_error
    0 error not generated because old message was icmp
    0 message with bad code fields
    0 message < minimum length
    0 bad checksum
    0 message with bad length
    Input histogram:
        destination unreachable: 1
    0 message response generated
value = 30 = 0x1e
Gateway >

```

ifShow

Use the **ifShow** command to show the attached network interface parameters as shown in the example. The Gateway shows two devices. **lnPci** is the Ethernet port. **lo** is the local loop-back port. If **lnPci** is not shown in the output, the Ethernet port has been disabled (see “ethEnable” on page 133).

```

Gateway > ifShow
lnPci (unit number 0):
    Flags: (0x63) UP BROADCAST ARP RUNNING
    Internet address: 192.168.1.54
    Broadcast address: 192.168.1.255
    Netmask 0xffffffff Subnetmask 0xffffffff
    Ethernet address is 00:60:45:0d:00:c0
    Metric is 0
    Maximum Transfer Unit size is 1500
    13 packets received; 12 packets sent
    0 input errors; 0 output errors
    0 collisions
lo (unit number 0):
    Flags: (0x69) UP LOOPBACK ARP RUNNING
    Internet address: 127.0.0.1
    Netmask 0xff000000 Subnetmask 0xff000000
    Metric is 0
    Maximum Transfer Unit size is 4096
    4 packets received; 4 packets sent
    0 input errors; 0 output errors
    0 collisions
value = 18 = 0x12
Gateway >

```


inetstatShow

Use the **inetstatShow** command to display statistics about internet protocol sockets for the Ethernet network. Interpreting these statistics requires detailed knowledge of internet networking protocols. This information can be useful to the LAN administrator.

```
Gateway > inetstatShow
Active Internet connections (including servers)
PCB      Proto Recv-Q Send-Q Local Address Foreign Address (state)
-----
c1fee18c TCP      0      0 192.168.1.59.23 206.0.64.117.4239 ESTABLISHED
c1fee40c TCP      0      0 0.0.0.0.52787 0.0.0.0.0 LISTEN
c1fee58c TCP      0      0 0.0.0.0.21 0.0.0.0.0 LISTEN
c1fee68c TCP      0      0 0.0.0.0.23 0.0.0.0.0 LISTEN
c1feea0c TCP      0      0 0.0.0.0.513 0.0.0.0.0 LISTEN
c1fee48c UDP      0      0 0.0.0.0.161 0.0.0.0.0
value =1 =0x1
Gateway >
```

initializeBox

Use the **initializeBox** command to remove configuration files, such as management configuration and SCSI device maps, and then prompt to restart.

Attention: Use this function with care as data can be lost as a result of devices moving to different LUNs when the mapping database is removed. Make sure all I/O activity has been stopped.

ipstatShow

Use the **ipstatShow** command to display internet protocol statistics for the Ethernet network. Interpreting these statistics requires detailed knowledge of internet networking protocols. This information can be useful to the LAN administrator.

```
Gateway > ipstatShow
total 8380
badsum 0
tooshort 0
toosmall 0
badhlen 0
badlen 0
fragments 0
fragdropped 0
fragtimeout 0
forward 0
cantforward 0
redirectsent 0

value =1 =0x1
Gateway >
```

licenseShow

Use the **licenseShow** command to display information about software license keys that are installed and the corresponding features that are available. The following example shows a gateway that contains a license key for the data mover feature.

```

Gateway > licenseShowLicense "wsk96-sd59a": Valid
Feature:
Data Mover.
value =1 =0x1
Gateway >

```

loggerDump [number]

Use the **loggerDump** command to dump records from the system event log to the console. A numeric parameter can be used to indicate the number of events to display. With no parameter specified, all events in the log file are displayed starting with the most recent events. The following example shows a **loggerDump** display of events in the log file.

```

Gateway > loggerDump 5
*** Dumping 5 (1018 through 1022) of 1080 records ***
SEQUENCE ELAPSED TIME      CODE DESCRIPTION
0008      0d:00h:00m:07s:22t 28   SCSI 1: Bus RESET
0009      0d:00h:00m:07s:22t 28   SCSI 2: Bus RESET
0010      0d:00h:00m:08s:18t 29   SCSI 3: Bus RESET
0011      0d:00h:00m:08s:18t 28   SCSI 4: Bus RESET
0012      0d:00h:00m:08s:18t 29   Mapping 1: Target Device Added: index 10, handle
0xc0ad2590
value = 0 = 0x0
Gateway >

```

loggerDumpCurrent [level]

Use the **loggerDumpCurrent** command to dump records from the system event log to the console. Only records logged since the system was started are dumped. The level specifies the event log level for the events as shown in Table 27.

Table 27. Event viewing levels

Level	Name	Explanation
0	Private	Events that are never shown by the event viewer but are recorded in the gateway event log
1	Notice	Conditions that should always be reported, such as temperature alarms and device removals
2	Warning	Events that might result in a later problem
3	Information	Events that are not errors or warnings

The following example shows a dump after a typical startup sequence.

```

Gateway > loggerDumpCurrent 1
*** Dumping 5 current records (of 22 total) with level <= 1 ***
SEQUENCE ELAPSED TIME      CODE DESCRIPTION
0008      0d:00h:00m:07s:22t 28   SCSI 1: Bus RESET
0009      0d:00h:00m:07s:22t 28   SCSI 2: Bus RESET
0010      0d:00h:00m:08s:18t 29   SCSI 3: Bus RESET
0011      0d:00h:00m:08s:18t 28   SCSI 4: Bus RESET
0012      0d:00h:00m:08s:18t 29   Mapping 1: Target Device Added: index 10, handle
0xc0ad2590
value = 0 = 0x0
Gateway >

```

ls or ll

The Gateway contains a file system in its flash memory. Use the **ls** command to display the files as shown in the following example.

```
Gateway > ls
CONFIG
LOG
VXWORKST.Z
SNA.RC
MGMT
MT
value = 0 = 0x0
Gateway >
```

To obtain detailed information about the file, use the **ll** command instead.

macShow

Use the **macShow** command to display the media access control (MAC) address for the Ethernet interface.

```
Gateway > macShow
Enet MAC Address: 0.60.45.d.0.80
value = 33 = 0x21 = '!'
Gateway >
```

mapCompressDatabase

Attention: Compressing the map database causes device addresses to change unpredictably. Use this command only when no host systems are expecting devices to remain at their current addresses. You must restart the Gateway after issuing this command for the new setting to take effect.

The Gateway maintains a persistent device map database. Occasionally, it may be necessary to eliminate inactive entries and reorder the active entries in the persistent device map database. Use the **mapCompressDatabase** command to remove entries for devices that are no longer present and to reassign existing device entries to new addresses. The devices are assigned new addresses immediately and hosts must rescan for devices or be restarted.

Removing and reassigning device entries can be required when a host system has a limited number of LUNs that can be supported, and changing devices on the Gateway has caused the LUNs to increase beyond the supported level of the host.

```
Gateway > mapCompressDatabase

This command will compress the Persistent Device Map.

Do you want to compress the Device Map? (y or n) y
0xc1689ac0 (tShell): Wrote 23 device maps to file
'ffs0:config/device.map'

Device Map Compressed
value = 23 = 0x17
Gateway >
```

mapHelp

Use the **mapHelp** command to display a list of the persistent address map database commands.

```
Gateway > mapHelp

mapCompressDatabase - Compress Device Map Database (reboot required)
mapRebuildDatabase  - Rebuild Device Map Database (reboot required)
mapShowDatabase     - Show the Map Database
mapShowDevs         - Show currently attached devices
mapWinnowDatabase   - Remove unattached devices from database
Gateway >
```

mapRebuildDatabase

Attention: Clearing the map database causes device addresses to change unpredictably. Use this command only when no host systems are expecting devices to remain at their current addresses. The Gateway must be restarted after issuing this command for the new setting to take effect.

The Gateway maintains a persistent device map database. Occasionally, it may be necessary to entirely eliminate the persistent device map database. In order to assign new addresses to the existing devices use the **mapRebuildDatabase** command to delete the existing database. When the Gateway is next started, the devices found are assigned new addresses.

Eliminating the device map and assigning new addresses can be required when a host system has a limited number of logical units that are supported, and changing devices on the Gateway has caused the LUNs to increase beyond the supported level of the host.

```
Gateway > mapRebuildDatabase

This command will clear the Persistent Device Map.

These changes will take effect when the Gateway is rebooted.

Do you want to clear the Device Map? (y or n) y
Removing the Persistent Device Map

Device Map Cleared - Reboot Gateway? (y or n) y== reboot
Gateway
```

mapShowDatabase

Use the **mapShowDatabase** command to display the persistent device map database.

The Gateway maintains a persistent device map. The database ensures that each time a host attaches to the Gateway, the target devices are seen at a consistent address. The database lists not only the devices that are presently connected, but also devices that have previously been connected. If a previously attached device is later reattached, it is assigned its previous address.

```

Gateway > mapShowDatabase
devId  Type  Chan  tId  tLun  UID
-----
000    SNA   127   127  127   00000060:450d00c0
001    SCSI  002   003  000   00000060:450d00c0
002    SCSI  002   002  000   00000060:450d00c0
003    SCSI  002   001  000   00000060:450d00c0
004    SCSI  003   002  000   00000060:450d00c0
005    SCSI  003   000  000   00000060:450d00c0
006    SCSI  003   006  000   00000060:450d00c0
007    SCSI  003   009  000   00000060:450d00c0
008    SCSI  003   002  001   00000060:450d00c0
009    SCSI  003   005  000   00000060:450d00c0
010    SCSI  003   005  001   00000060:450d00c0
011    SCSI  002   000  000   00000060:450d00c0
012    SCSI  002   006  000   00000060:450d00c0
value = 0 = 0x0
Gateway >

```

The column fields in the display provide the following information:

devId	The index of the device in the database.
Type	The type of interface where the device is connected. SNA indicates an internal device. SCSI or Fibre Channel indicate I/O interfaces.
Chan	The channel number of the interface where the device is attached.
tId	Target ID mapping for SCSI initiators.
tLun	Target LUN mapping for SCSI initiators.
UID	For a Fibre Channel interface, the unique ID of the device. For a SCSI interface, the Gateway unique ID.

mapShowDevs

The Gateway maintains a cross-reference map of device addresses. Use the **mapShowDevs** command to display information about the presently attached and available devices in the map.

```

Gateway > mapShowDevs
devId  Type  Chan  iId  iLun  UID                      tId  tLun  Handle  Itl
-----
000    SNA   127   127  127   00000060.450d00c0  001  000   c0ec2600h  00000000h
009    SCSI  003   005  000   09000060.450d00c0  255  255   c1f9e090h  00000000h
010    SCSI  003   005  001   0a000060.450d00c0  255  255   c0ad2590h  00000000h
012    SCSI  002   006  000   0c000060.450d00c0  255  255   c1ffdf10h  c1ffdc80h
value = 0 = 0x0
Gateway >

```

The column fields in the display provide the following information:

devId	The index of the device in the database.
Type	The type of interface where the device is attached to the Gateway.
Chan	The channel number of the interface.
iId	For a SCSI interface only: the device ID of the device.
iLun	For a SCSI interface only: the logical unit number of the device.

UID	For a Fibre Channel interface: the unique ID of the device. For a SCSI interface: a constructed unique ID based on the Gateway unique ID.
tId	Target ID mapping for SCSI initiators.
tLun	Target LUN mapping for SCSI initiators.
Handle	An internal pointer used for some diagnostic operations.
Itl	An internal pointer used for some diagnostic operations.

mapWinnowDatabase

Attention: Using the **mapWinnowDatabase** command can cause unattached devices to change addresses unpredictably if they are reattached. Use this command only when you are sure that the devices you are interested in are connected and available to the Gateway.

Occasionally, you might want to eliminate inactive entries from a persistent device map database. Use the **mapWinnowDatabase** command to reduce the database to only the devices presently attached. The address mapping of the existing devices is not altered.

```
Gateway > mapWinnowDatabase
0xc0ac8340 (tShell): Wrote 4 device maps to file 'ffs0:config/device.map'
value = 4 = 0x4
Gateway >
```

mbufShow

Use the **mbufShow** command to display statistics about the distribution of mbufs on the Ethernet network. Interpreting these statistics requires detailed knowledge of internet networking protocols. This information can be useful to the LAN administrator.

```

Gateway > mbufShow
type          number
-----
FREE   :      23
DATA   :       0
HEADER :       1
SOCKET :       0
PCB    :      11
RTABLE :       3
HTABLE :       0
ATABLE :       0
SONAME :       0
ZOMBIE :       0
SOOPTS :       0
FTABLE :       0
RIGHTS :       0
IFADDR :       2
TOTAL  :      40
number of mbufs: 40
number of clusters: 4
number of interface pages: 0
number of free clusters: 4
number of times failed to find space: 0
number of times waited for space: 0
number of times drained protocols for space: 0
value = 47 = 0x2f = '/'
Gateway >

```

netHelp

Use the **netHelp** command to display a list of the Ethernet network commands.

```

Gateway > netHelp

arptabShow      - Display a list of known ARP entries
ethAddrSet "inetaddr","netmask" - set IP Address
ethDisable     - disable Ethernet port (reboot required)
ethEnable      - enable Ethernet port (reboot required)
gateAddrGet    - Display Default IP gateway
gateAddrSet "inetaddr" - set Default IP gateway
host "<func>","hostname","inetaddr"
    func - "add" - add to host table
          - "delete" - delete from host table
          - "list" - list host table
hostNameSet    - set host name
icmpstatShow   - Display statistics for ICMP
ifShow         - Display info about network interfaces
inetstatShow   - Display all Internet protocol sockets
ipstatShow     - Display statistics for IP
macShow        - Display Media Access Control Address
mbufShow       - Display mbuf statistics
route "<func>","destination","gateway"
    func - "add" - add route to route table
          - "delete" - delete route from route table
          - "list" - list route table
tcpstatShow    - Display statistics for TCP
udpstatShow    - Display statistics for UDP
Gateway >

```

normalBoot

Certain commands and tests are only available in diagnostic mode. Switching to diagnostic mode saves all configuration parameters so that they are restored before returning to normal operation. Use the **normalBoot** command to restore the Gateway to normal operating conditions.

This command is used only to transition a Gateway from the special diagnostic mode to normal operations. It restores the bootline that was copied by the **diagBoot** command. The new persistent device map is erased, and the original map file is renamed config/device.map. The original map file is restored to use when the Gateway is restarted.

The **NormalBoot** command then restarts the Gateway.

reboot

Use the **reboot** command to request that the Gateway shut down existing operations and then restart. This is the preferred method of restarting the Gateway. There are processes running within the Gateway that can have data-pending writes to files within the Gateway flash file system. Following a **reboot** command, these processes flush their data to the flash file system, and the flash file system writes all pending data out to the flash memory. The Gateway will only start a reset cycle after all pending data has successfully been written to flash.

```
Gateway > reboot
```

reset

Attention: Any pending data writes to the flash file system are lost when the **reset** command is initiated.

Use the **reset** command to immediately initiate a reset cycle. This command is not typically used. The **reboot** command should be used to shut down and restart the Gateway.

```
Gateway > reset
```

ridtag [value]

Use the **ridtag** command to change the replacement identifier (RID) tag for the Gateway when the base is replaced by the service representative. This should be the final step after replacing and verifying that the replacement unit is performing satisfactorily.

The **sysVpdShow** command displays the RID tag. Before replacing the Gateway base, the service representative must determine the existing RID tag, if there is one, or the original serial number if no replacement has been made.

If the **ridtag** command is entered with a string, that string becomes the RID tag recorded for the unit.

```
Gateway > ridtag "12D345677"  
*** value = 0 = 0x0
```


If a string is not entered, the existing RID tag is displayed.

```
Gateway > ridtag
RID Tag = 12D345677
value = 0 = 0x0
Gateway >
```

On original equipment, the RID tag is blank.

rm

Use the **rm** command to remove a file. Specify the file name in double quotes, for example:

```
Gateway > rm "file.ext"
```

route

Use the **route** command to add, remove, and list the route table. The **route** command maintains a route file, `hp1ffs0:/mgmt/route`, which is used at system startup to initialize the network routing table. Each route entry is a single line using the following format:

`destination:Gateway`

where

Description	Result
destination	is an IP address (for a subnet or host) or the name of a host that is described in the hosts file.
gateway	is an IP address or the name of a gateway to a host. The gateway must be a device on the local subnet.

An IP address is a text string in standard IP address format (that is, 10.0.0.2). A host or gateway name must be listed in the hosts file. The following is an example of the contents of the route file.

```
socrates:bruno
10.0.0:bruno
```

The first line instructs the system to reach the host *socrates* by directing the IP packets to the host *bruno*. The second example shows how all traffic for the subnet 10.0.0 (implied netmask is 255.255.255.0) is sent to the host *bruno* for forwarding. By default, no routes are defined in the route file.

The three **route** commands are described as follows:

route add,[destination],[gateway]

Adds a route to the destination through the gateway.

```
Gateway > route "add","200.0.0","bruno"
Gateway >
```

route delete,[destination],[gateway]

Removes a route

```
Gateway > route "delete","200.0.0","bruno"  
Gateway >
```

route "list"

Lists the existing routes through the destination Gateway.

```
Gateway > route "list"  
Destination          Gateway  
-----  
socrates             bruno  
Destination          Gateway  
-----  
200.0.0              bruno  
value = 0 = 0x0  
Gateway >
```

rz

Use the **rz** command to initiate a receive Zmodem file transfer session. Use this command to download a file from the service terminal to the Gateway. The file can be either a firmware or configuration file. After issuing this command, you start the file transfer from the service terminal by initiating a send file operation that uses Zmodem protocol.

The following example shows the **rz** command when it is used to receive a file that contains operational firmware. The Gateway extracts individual firmware modules from the file and saves them temporarily in memory. After the file transfer has completed, the Gateway copies the modules to nonvolatile flash memory. The Gateway must be restarted to use the updated firmware.

```
Gateway > rz  
**B000000023be50  
Firmware Update in Progress....  
Found Image File BOOTROM.IMG - loading  
.....Found Image File IPOST.IMG - loading  
.....Found Image File SPOST.IMG - loading  
Firmware Update Complete. Reboot for Update to Take Effect.  
value =0 =0x0  
Gateway >
```

The following example shows the **rz** command when it is used to receive a file that contains configuration parameters. See also the **sz** command for information about sending a configuration file.

```
Gateway > rz  
**B000000023be50  
Configuration Update in Progress....  
Configuration Update Complete. Reboot for Update to Take Effect.  
value =0 =0x0  
Gateway >
```

scsiAltIdGet [channel]

Use the **scsiAltIdGet** command to display the alternate ID number for a specified channel. If no channel is specified, alternate IDs are displayed for all Ultra SCSI channels.

```
Gateway > scsiAltIdGet
SCSibus AltId -----
SCSI 1 1
SCSI 2 6
SCSI 3 Auto
SCSI 4 Auto
value = -1 = 0xffffffff
Gateway >
```

For information about Ultra2/3 SCSI channels, see the **xscsiAltIdGet** command.

scsiAltIdSet [channel],[id]

Use the **scsiAltIdSet** command to set the alternate ID for the specified SCSI channel.

Channel numbers 1 - 4 (Ultra SCSI)

ID channel numbers 0 - 15

```
Gateway > scsiAltIdSet 3,6
Alternate Id set to 6 for SCSI 3
will take effect upon reboot
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new setting to take effect.

To set alternate ID numbers for Ultra2/3 SCSI channels, see the **xscsiAltIdSet** command.

scsiChannelTest [x,y]

The Gateway must be in diagnostic mode to use this command and a SCSI cable must be connected between two SCSI channels.

Use the **scsiChannelTest** command to perform a confidence test on a pair of SCSI channels. Substitute the SCSI channel numbers you want to test for x and y. Parenthesis are optional. This command can be used to test the SCSI interfaces or a SCSI cable.

The following example shows the display for a test on SCSI channels 3 and 4.

```
diagmode > scsiChannelTest 3,4
SCSI-3 -> SCSI-4 [#####] 101 iterations PASSED
SCSI-4 -> SCSI-3 [#####] 101 iterations PASSED
PASSED
value = 0 = 0x0
```

scsiHostChanGet [channel]

Use the **scsiHostChanGet** command to display host channel modes for a SCSI channel. If no channel is specified, host channel modes are displayed for all Ultra SCSI channels.

```
Gateway > scsiHostChanGet
SCSIbus HostChan -----
SCSI 1 Channel is Target
SCSI 2 Channel is Initiator
SCSI 3 Channel is Target
SCSI 4 Channel is Target
value = -1 = 0xffffffff
Gateway >
```

For information about Ultra2/3 SCSI channels, see the **xscsiHostChanGet** command.

scsiHostChanSet [channel],[mode]

Use the **scsiHostChanSet** command to set the channel mode to target or initiator for the specified SCSI channel.

Channel numbers 1 - 4 (Ultra SCSI)

Mode 0 Set to initiator

Mode 1 Set to target

```
Gateway > scsiHostChanSet 3,1
Host Chan set to TRUE for SCSI 3 will take effect upon reboot
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new settings to take effect.

To set host channel modes for Ultra2/3 SCSI channels only, see the **xscsiHostChanSet** command.

scsiHostIdGet [channel]

Use the **scsiHostIdGet** command to display the host ID number for a specified SCSI channel. If no channel is specified, host IDs are displayed for all SCSI channels, both Ultra and Ultra2/3.

```
Gateway > scsiHostIdGet
SCSIbus HostId -----
SCSI 1 7
SCSI 2 7
SCSI 3 7
SCSI 4 7
value = -1 = 0xffffffff
Gateway >
```

For information about Ultra2/3 SCSI channels, see the **xscsiHostIdGet** command.

scsiHostIdSet [channel],[id]

Use the **scsiHostIdSet** command to set the host ID for a specified SCSI channel.

Channel numbers 1 - 4 (Ultra SCSI)

ID numbers can be 0 - 15

```
Gateway > scsiHostIdSet 3,7
Host Id set to 7 for SCSI 3
will take effect upon reboot
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new settings to take effect.

To set host IDs for Ultra2/3 SCSI channels only, see the **xscsiHostIdSet** command.

scsiRescan [channel]

Use the **scsiRescan** command to request a SCSI rescan for new devices. If channel is specified (1, 2, 3 or 4), then only that channel is scanned. Otherwise, if the channel is not specified or if the channel is 0, then all channels are scanned.

```
Gateway > scsiRescan 4
Done
value =0 =0x0
Gateway >
```

Notes:

1. Rescanning a SCSI bus might delay I/O commands pending on that bus for several seconds. Do not rescan SCSI buses if this delay might not be tolerated. When possible, only scan the bus where a new device has been added.
2. If a channel is specified, that channel is scanned and the prompt is returned on completion. If no channel is specified (or channel 0 is specified), SCSI channels 1 through 4 are scanned in sequence and the prompt is returned on completion.
3. When a device is discovered, further device specific initialization may continue after the scan has completed, and the device may not show up immediately when you issue the **fcShowDevs** command. An example of this is a disk that requires a **start unit** command to become ready. (Tape and changer devices and disks that indicate Ready status are available on scan completion.)
4. If a SCSI target device should require replacement, remove the old device, set the new device to the same SCSI bus ID as the old device, and attach it to the same channel. Rescan the channel to update the configuration data. The new device should be available to host systems with the same LUN as the old device.

scsiResetDisableGet [channel]

Use the **scsiResetDisableGet** command to display the status of SCSI bus reset on power up. True means that SCSI bus reset on power up is enabled. False means that SCSI bus reset on power up is disabled.

```

Gateway > scsiResetDisableGet
SCSibus Reset Disable -----
SCSI 1 TRUE
SCSI 2 FALSE - default
SCSI 3 FALSE - default
SCSI 4 FALSE - default
value = -1 = 0xffffffff
Gateway >

```

For information about Ultra2/3 SCSI channels, see the **xscsiResetDisableGet** command.

scsiResetDisableSet [channel],[mode]

Use the **scsiResetDisableSet** command to set the SCSI bus reset on during a startup cycle for the specified SCSI channel. False is the default and enables a SCSI bus reset on power up. True disables the SCSI bus reset on power up.

Channel number 1 - 4 (Ultra SCSI)

Mode 0 Enable reset on start up

Mode 1 Disable reset on start up

```

Gateway > scsiResetDisableSet 1,1
Reset Disable set to TRUE for SCSI 1
will take effect upon reboot
value =0 =0x0
Gateway >

```

For information about bus reset settings for Ultra2/3 SCSI channels only, see the **xscsiResetDisableSet** command.

scsiShow

Use the **scsiShow** command to display all SCSI channels and information about the devices attached to each channel. The following example shows the display for two disk devices attached to SCSI channel 1, two disk devices attached to SCSI channel 2, a tape library attached to SCSI channel 3, and no devices attached to SCSI channel 4:

```

Gateway > scsiShow
SCSI Initiator Channel 1: 0xc08b5b60
ID  LUN  Vendor  Product  Rev  Sync/Off Width
-----
1    0    IBM OEM  DCHS04X  6363  12/15  16 S W  0/ 0  8 S W Q
2    0    IBM OEM  DCHS04X  6363  12/15  16 S W  0/ 0  8 S W Q
SCSI Initiator Channel 2: 0xc087c460
ID  LUN  Vendor  Product  Rev  Sync/Off Width
-----
3    0    IBM OEM  DCHS04X  6363  12/15  16 S W  0/ 0  8 S W Q
4    0    IBM OEM  DCHS04X  6363  12/15  16 S W  0/ 0  8 S W Q
SCSI Initiator Channel 3: 0xc08d26e0
ID  LUN  Vendor  Product  Rev  Sync/Off Width
-----
0    0    IBM      03570C12  5346  25/15  16 S W  0/ 0  8 S W
0    1    IBM      03570C12  5346
1    0    IBM      03570C12  5346  25/15  16 S W  0/ 0  8 S W
SCSI Initiator Channel 4: 0xc0898fe0
No Devices
value = 0 = 0x0
Gateway >

```

The column fields in the display provide the following information:

ID	The SCSI ID of the target device.
LUN	The SCSI LUN of the target device.
Vendor	The content of the vendor ID field from the SCSI inquiry data.
Product	The content of the product ID field from the SCSI inquiry data.
Rev	The content of the revision ID field from the SCSI inquiry data.
Sync/Off	The negotiated synchronous transfer period and offset. The period is the negotiated transfer period. Multiply the period times four nanoseconds (ns) to determine the actual period. (There is one exception: If the period is negotiated to 12, then 50 ns is used.) The offset indicates the REQ/ACK offset that was negotiated. A zero in these fields indicates that an asynchronous transfer is in use.
Width	The negotiated transfer width in bits, either 8 or 16.

scsiTermGet [channel]

Use the **scsiTermGet** command to display termination status information for the specified channel. If no channel is specified, status information is displayed for all SCSI channels, both Ultra and Ultra2/3.

For information about Ultra2/3 SCSI channels only, see the **xscsiTermGet** command.

```

Gateway> scsiTermGet
SCSibus Termination -----
SCSI 1 Enabled - default
SCSI 2 Enabled
SCSI 3 Enabled
SCSI 4 Disabled
XSCSI 2 Enabled
XSCSI 5 Enabled
value =0 =0x0
Gateway >

Gateway> scsiTermGet 2
SCSibus Termination -----
SCSI 2 Enabled - default
value =0 =0x0
Gateway >

Gateway> scsiTermGet 6
SCSibus Termination -----
XSCSI 2 Enabled
value =0 =0x0
Gateway>

```

scsiTermSet [channel],[termination]

Use the **scsiTermSet** command to enable or disable the termination for the SCSI channel.

Channel numbers 1 - 4 (Ultra2/3 SCSI)

Termination 0 Enable termination

Termination 1 Disable termination

```

Gateway > scsiTermSet 3,1
Termination Disabled for SCSI 3
will take effect upon channel reset
value =0 =0x0
Gateway >

```

Attention: You must restart the Gateway after issuing this command for the new settings to take effect.

For information about setting termination status for Ultra2/3 SCSI channels only, see the **xscsiTermSet** command.

setFcFrameSize [channel],[size]

Use the **setFcFrameSize** command to set the frame size for a channel.

channel The SAN connection number, 1, or 2

size The frame size, where 512, 1024, and 2048 are valid. If an invalid size is set, then the frame size of 2048 is used.

Attention: You must restart the Gateway after entering this command, to apply the new setting.

setFcHardId [channel],[id]

Use the **setFcHardId** command to set the hard AL_PA for a Fibre Channel.

The **setFcHardId** command parameters are described by the following information:

channel	The SAN connection number, 1, or 2.
id	The ID setting, where 0 - 125 are valid IDs. An ID of 255 requests the soft ID method. If an invalid number is requested, the soft ID method is used.

```
Gateway > setFcHardId 1,4  
value = 0 = 0x0  
Gateway >
```

Attention: You must restart the Gateway after entering this command to apply the new setting.

setFcNormal

Use the **setFcNormal** command to remove the restrictions implemented by the **setFcSplit** command, restoring access to all SCSI channels and to all SAN connections.

Attention: You must restart the Gateway after entering this command to apply the new setting.

setFcScsiChanMask [channel],[scsiChannel],[allow]

Use the **setFcScsiChanMask** command to divide the SCSI channels in any way between the available SAN connections.

The fields in the display provide the following information:

channel	The SAN connection slot number, 1, or 2.
scsiChannel	The SCSI channel number, 1, 2, 3, or 4.
allow	0 to deny, 1 to allow

For each Fibre Channel SAN connection, select a SCSI channel and set **allow** to the correct value. See also **setFcNormal** and **setFcSplit** commands.

Attention: You must restart the Gateway after entering this command to apply the new setting.

setFcSplit

Use the **setFcSplit** command to assign SCSI channels 1 and 3 for the exclusive use of the interface labeled "SAN connection 1". Channels 2 and 4 are reserved for "SAN connection 2".

Attention: You must restart the Gateway after entering this command to apply the new setting.

setHost [port] OS

Use the **setHost** command to set the operating system type for the specified Fibre Channel port. This setting ensures that the Gateway provides command responses

that are appropriate for the particular type of attached host. For example, some operating systems have different SCSI sense data requirements. See also the **hostTypeShow** command for information about how to display the current host type settings.

port The SAN connection number 1, or 2

If 0 is specified for port, the change applies to all SAN connections; otherwise, the host type is applied only to the SAN connection for the specified Fibre Channel port.

OS The host operating system. The default setting for OS is nt. Other values that can be specified with this command include the following.

- AIX
- AS400
- HP-UX
- NETWARE
- gateway
- generic
- SOLARIS
- Unisys

The following example shows how to set all SAN connections to host type AIX.

```
Gateway > setHost 0,"aix"  
value =0 =0x0  
Gateway >
```

Attention: You must restart the Gateway after entering this command to apply the new setting. See the **fcRestart** command for further information.

setSnaCCLun [newLUN]

Use the **setSnaCCLun** command to reassign the Gateway command and control LUN to the specified value.

newLUN The new value for the command and control LUN. Valid values are 0 to 255.

The new setting takes effect immediately. The previous value is removed from the device map and database, and a trap is generated indicating that the device has been removed.

If the new LUN is not currently in use, a new entry is added in the device map and database. A trap is generated indicating the new device has been added.

If the new LUN is already in use, the command and control LUN is disabled. It remains disabled until the device mapped at the requested LUN is removed and deleted from the database. In this case, you can use the **mapRebuildDatabase** command to remove the previous LUN assignment and to allow the new command and control LUN to be enabled.

Attention: Because AIX, Windows NT, and Windows 2000 use LUN 0 when they issue a **Report LUNs** command, you must make sure that a device is configured at LUN 0.

shellLock

Only one management interface can be in use at a time. If a network interface is opened, the service port interface is not available. Use the **shellLock** command to prevent a network protocol access to the shell.

A numeric parameter specifies if the shell is to be locked or unlocked. If the parameter is 0, the shell is unlocked. If the parameter is 1, the shell is locked.

```
Gateway > shellLock 1
value = 1 = 1x1
Gateway >
.. Shell is now locked
Gateway > shellLock 0
value = 0 = 0x0
```

showBox

Use the **showBox** command to display the components present in the Gateway using characters to form a picture of the unit. The view of Gateway is from the front. Gateway is positioned in the rear of library.

In Figure 84, the four Ultra2 SCSI I/O module channels are shown as a group of four “LVDs”, which stands for “SCSI low voltage differential terminated”, according to the legend immediately below them.

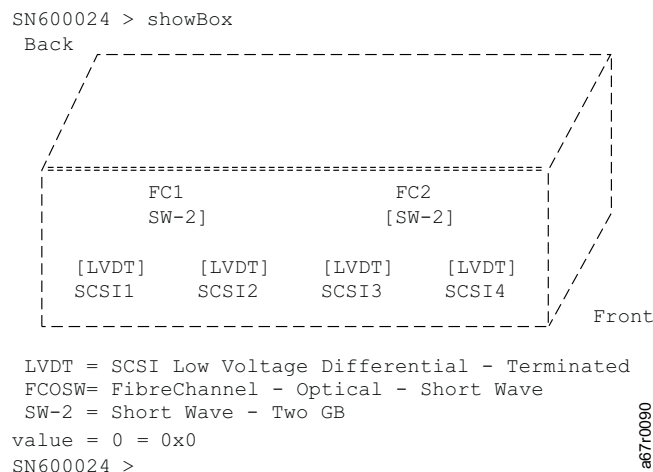


Figure 84. showBox Command Display of Gateway

```
LVD = SCSI Low Voltage Differential - Terminated
FC SW = FibreChannel Optical Short Wave
SCSI-1 requires Low Voltage Differential cable
SCSI-2 requires Low Voltage Differential cable
SCSI-3 requires Low Voltage Differential cable
SCSI-4 requires Low Voltage Differential cable
FC1 SW-1 slot-1 requires FibreChannel Multi-Mode (SW) cable
FC2 SW-2 slot-2 requires FibreChannel Multi-Mode (SW) cable
value =0 =0x0
Gateway >
```

Table 28 shows other possibilities for this area.

Table 28. *showBox Abbreviations for Ultra2 SCSI Channels*

Abbreviation in showBox diagram	Type of Ultra SCSI I/O channel
LVD	Low voltage differential - terminated
SET	Single-Ended-terminated

See Figure 84 on page 165. The two Fibre Channel ports shown are optical short wave Fibre Channels.

snaVersion

The Gateway contains software that controls all functions. Use the **snaVersion** command to display the current version of the operating software.

```
Gateway > snaVersion

IBM Gateway Version 0252 Built Feb 10 1999, 11:34:39
value = 594 = 0x252
Gateway >
```

sncFeatureEnable [licensekeystring]

Use the **sncFeatureEnable** command to enable the optional data mover feature. You enable the feature by entering the **unique license key**.

```
Gateway> sncFeatureEnable "BVRXC-G79DN"
value =0 =0x0
Gateway >
```

If the license key was factory-installed, you can enter the word **enable** rather than the actual license key.

```
Gateway> sncFeatureEnable "enable"
value =0 =0x0
Data Mover License is Valid
Gateway >
```

If the value =1 =0x1 message is displayed, it means the license is already installed and data mover is already enabled.

If the value = -1 =0xffffffff message is displayed, it means the license is not already installed and you do need to enter the license key.

snmpCommunitiesShow

Use the **snmpCommunitiesShow** command to display the list of SNMP community strings in use by the Gateway.

```

Gateway > snmpCommunitiesShow

ReadCommunity      ViewIndex
-----
pub                1
public             1
icmp               2

WriteCommunity      ViewIndex
-----
priv               1
private            1

TrapCommunity
-----
private
Gateway >

```

snmpHelp

Use the **snmpHelp** command to display a list of the SNMP commands.

```

Gateway > snmpHelp
snmpCommunitiesShow
snmpReadCommunityAdd "string"
snmpReadCommunityRemove "string"
snmpTrapCommunitySet "string"
snmpWriteCommunityAdd "string"
snmpWriteCommunityRemove "string"
trapDestAdd "ipaddress"
trapDestRemove "ipaddress"
trapDestShow
value =5 =0x5
Gateway >

```

snmpReadCommunityAdd [string],[view]

Use the **snmpReadCommunityAdd** command to add the specified string to the list of accepted strings for SNMP read operations (Get and GetNext). The **view** switch must be set to 1 to be accepted by the StorWatch Specialist.

```

Gateway > snmpReadCommunityAdd "ibm"
Success
value =4 =0x4
Gateway >

```

snmpReadCommunityRemove [string]

Use the **snmpReadCommunityRemove** command to remove the specified string from the list of accepted strings for SNMP read operations.

```

Gateway > snmpReadCommunityRemove "ibm"
Success
value =0 =0x0
Gateway >

```

snmpTrapCommunitySet [string],[view]

Use the **snmpTrapCommunitySet** command to set the community string passed with all SNMP traps. The **view** switch must be set to 1 to be accepted by the IBM StorWatch SAN Data Gateway Specialist.

```
Gateway > snmpTrapCommunitySet "ibm"
Success
value =8 =0x8
Gateway >
```

snmpWriteCommunityAdd [string],[view]

Use the **snmpWriteCommunityAdd** command to add the specified string to the list of accepted strings for SNMP write operations (Set). The **view** switch must be set to 1 to be accepted by the StorWatch Specialist

```
Gateway > snmpWriteCommunityAdd "xyzy654", 1
Success
value =0 =0x0
Gateway >
```

snmpWriteCommunityRemove [string]

Use the **snmpWriteCommunityRemove** command to remove the specified string to the list of accepted strings for SNMP write operations.

```
Gateway > snmpWriteCommunityRemove "xyzy654"
Success
value =3 =0x3
Gateway >
```

supportDump

The supportDump command outputs the result of a number of Service Port commands in a standard way and in a specific order. The resulting file is used for troubleshooting. The individual commands called by supportDump are:

```
envShow
version
showBox
sysVpdShowAll
sysConfigShow
licenseShow
hostTypeShow
targets
scsiShow
fcShow
fcShowDevs
mapShowDevs
mapShowDatabase
showScsiAssign
fctShowChan
cleShowAll
loggerDumpCurrent
envMonShow
dmva
reserveShow
```

sysConfigShow

Use the **sysConfigShow** command to display current system parameter settings. The display shows whether or not the Gateway command and control interface is enabled or disabled and the LUN that is assigned to it; whether or not enhanced tape performance features are enabled; the MAC address of the Ethernet port; the gateway Fibre Channel node address; and the state of the memory snooper.

```
Gateway > sysConfigShow
Current System Parameter Settings:
Command and Control Device (CC) : 0 Enabled
LUN : 0
Allow Early Write Status for Tape : 1 Enabled
Allow R/W Acceleration for Tape : 1 Enabled
Enet MAC Address: 0.60.45.16.1.4
FC Node WWN: 10000060.45160104
Memory Snooper: E
value =0 =0x0
Gateway >
```

sysVpdShow, sysVpdShowAll

Use the **sysVpdShow** or **sysVpdShowAll** command to display the vital product data for the Gateway. This includes such items as serial numbers and installed memory sizes, as shown in the following example:

```
Gateway > sysVpdShow
===== VPD =====
name      Gateway
uid       00:60:45:0D:00:00
s/n       0123456789
mfg       Pathlight
board     Gateway
s/n       100111
mfg       Pathlight Tech
board     Gateway
" s/n     08357659
flash     2Mbyte
dram      32Mbyte
slot1     10772100 FCOSW
slot2     10772100 FCOSW
slot3     10772100 FCOSW
ddf       64 Mbyte
scsi      1: DET 2: DET 3: DET 4: DET
EC        OTA08000H
RID       Tag
value = 0 = 0x01
Gateway >
```

The fields in the display provide the following information:

name	The product name, up to 16 characters.
uid	The unique Ethernet MAC address of the product, consisting of 32 characters that are displayed as hexadecimal bytes separated by colons.
s/n	The serial number of the product, up to 16 characters.
mfg	The manufacturer of the product, up to 16 characters.

board	The name of the system board contained in the base unit, up to 16 characters.
board s/n	The serial number of the system board, up to 16 characters.
flash	The size of the flash memory on the system board.
dram	The size of the DRAM on the system board.
slot1	The card type installed in SAN connection slot one.
slot2	The card type installed in SAN connection slot two.
slot3	The card type installed in SAN connection slot three.
scsi	The SCSI type for each of the four channels, typically DET for "differential, terminated".
EC	The engineering change request (ECR) level for the system board, up to 16 characters.
RID	The RID tag identifier, up to 16 characters.

The **sysVpdShowAll** command shows more information and includes product data for the Fibre Channel PMC cards and the DDF memory board.

```

Gateway > sysVpdshowAll

=== [ Vital Product Data ] ===

-- [ Base Assembly ] --
Name      Gateway
Mfg       Pathlight Tech
UID       00:60:45:16;01:04
S/N       100111
Assy HCO  OTA08000H
Board     Gateway
" S/N    08357659
Flash     2 Mbyte
Dram      32 Mbyte

RID Tag

-- [ Slot 1 ] -----
Type      10772100 FCOSW
S/N       123456
UID       0060.45160065
HCO       SC004120H

-- [ Slot 2 ] -----
Type      10772100 FCOSW
S/N       234567
UID       0060.45160066
HCO       SC004120H

-- [ Slot 3 ] -----
Type      10772100 FCOSW
S/N       345678
UID       0060.45160067
HCO       SC004120H
value = 0 = 0x0
Gateway >

```


sz [filename]

Use the **sz** command to initiate a send Zmodem file transfer session. Use this command when you want to save configuration information to a file in case the Gateway needs to be replaced. The Gateway uses Zmodem protocol to upload its persistent address map database and configuration parameter settings from its nonvolatile flash memory to a file on the service terminal. After issuing this command, start the file transfer from the service terminal by initiating a receive file operation that uses Zmodem protocol.

The filename config.cfg is shown in the following example. You can specify a different name for the file, but the name must not exceed eight characters and it must end in .cfg. See also the **rz** command for information about receiving a configuration file.

```
Gateway > sz "config.cfg"
Configuration Download Complete: config.cfg
value = 0 = 0x0
Gateway >
```

targets

The Gateway maintains a list of target devices that are attached to the I/O channels. Use the **targets** command to list each device that is attached, providing descriptions of the devices as shown in the following example.

```
Gateway > targets
Idx Tdev      Vendor    Product      Rev  ] Type Specific
-----]-----
0h 0xc194a400 IBM      Gateway      0252 ] Cmd/Cntrl Status 0h
2h 0xc1ffc390 IBM      03570C11     5324 ] Tape: Blk Size 32768 , flags 7h
3h 0xc1ffc290 IBM      03570C11     5324 ] Changer: flags 7h
value = 4 = 0x4
Gateway >
```

The column fields in the display provide the following information:

- Idx** Device index in the target list.
- Tdev** An internal pointer used for some diagnostic operations.
- Vendor** The content of the vendor ID field from the SCSI inquiry data.
- Product** The content of the product ID field from the SCSI inquiry data.
- Rev** The content of the revision ID field from the SCSI inquiry data.
- Type Specific** For each device type, information pertinent to the device.

tcpstatShow

Use the **tcpstatShow** command to display TCP statistics for the Ethernet network. Interpreting these statistics requires detailed knowledge of internet networking protocols. This information can be useful to the LAN administrator.

```

Gateway > tcpstatShow
TCP:

    301 packets sent
        278 data packets (18371 bytes)
        0 data packet (0 byte) retransmitted
        23 ack-only packets (22 delayed)
        0 URG only packet
        0 window probe packet
        0 window update packet
        0 control packet
    516 packets received
        272 acks (for 18372 bytes)
        1 duplicate ack
        0 ack for unsent data
        276 packets (322 bytes) received in-sequence
        0 completely duplicate packet (0 byte)
        0 packet with some dup. data (0 byte duped)
        0 out-of-order packet (0 byte)
        0 packet (0 byte) of data after window
        0 window probe
        0 window update packet
        0 packet received after close
        0 discarded for bad checksum
        0 discarded for bad header offset field
        0 discarded because packet too short
    0 connection request
    1 connection accept
    1 connection established (including accepts)
    1 connection closed (including 0 drop)
    0 embryonic connection dropped
    272 segments updated rtt (of 272 attempts)
    0 retransmit timeout
        0 connection dropped by rexmit timeout
    0 persist timeout
    1 keepalive timeout
        1 keepalive probe sent
        0 connection dropped by keepalive
value = 36 = 0x24 = '$'
Gateway >

```

trapDestAdd, trapDestRemove, trapDestShow

Use the **trapDestAdd**, **trapDestRemove**, and **trapDestShow** commands to view and manipulate the SNMP trap destination table maintained within the Gateway. When the StorWatch Specialist is running, it inserts its address into the table automatically. The broadcast address for the Ethernet port is also automatically included in the table.

trapDestAdd [ipAddress] Adds a specific IP address as a trap recipient.

```

Gateway > trapDestAdd "192.168.1.75"
value = 0 = 0x0
Gateway >

```

trapDestRemove [ipAddress]

Removes a specific IP address as a trap recipient.

```

Gateway > trapDestRemove "10.0.0.2"
value = 0 = 0x0
Gateway >

```

trapDestShow "ipAddress" Displays the entire trap destination table.

```
Gateway > trapDestShow
Trap Destination IP Address
-----
      192.168.30.255
      206.0.64.17
      206.0.64.25
      206.0.64.35
      206.0.64.255
value = 1 = 0x1
Gateway >
```

udpstatShow

Use the **udpstatShow** command to display UDP statistics for the Ethernet network. Interpreting these statistics requires detailed knowledge of internet networking protocols. This information can be useful to the LAN administrator.

```
Gateway > udpstatShow
UDP:
8514 total packets
8445 input packets
69 output packets
0 incomplete header
0 bad data length field
0 bad checksum
8383 broadcasts received with no ports
0 full socket
value = 15 = 0xf
Gateway >
```

uptime

Use the **uptime** command to display the elapsed time since the last startup of the Gateway.

```
Gateway > uptime
Elapsed time since reset 4d:23h:12m:46s:10t
value = 10 = 0xa
Gateway >
```

userAdd, userDelete, userList

Use the **userAdd**, **userDelete** and **userList** commands to control the user list. The persistent address map file can be sent to the Gateway or can be retrieved from it using FTP. If you need to use FTP, use the **user** commands to create a login and password so that you can access the gateway from the Ethernet network.

userAdd [username],[password] adds a user and password to the password file. The "username" must be 3 - 80 characters, and the "password" must be 8 - 40 characters.

```
Gateway > userAdd "nancy","password"
value =0 =0x0
Gateway >
```

userDelete [username],[password] deletes a user from the password file.

```
Gateway > userDelete "nancy","password"
value =0 =0x0
Gateway >
```

userList displays the contents of the password file. Passwords are encrypted.

```
Gateway > userList
Name : Password
nancy : SyecycRz
fred : b9dczebQbd
martha : RQQdRedb9d
admin : cScQRSQzzz
value =0 =0x0
Gateway >
```

It is not possible to remove a user without knowing the user's password. If the user's password is forgotten or unknown, you must delete the password file, restart the Gateway, and then add all user names and passwords again.

userHelp

Use the **userHelp** command to display a list of the **user** commands.

```
Gateway > userHelp

userAdd    "name","password" - Add user to user list
userDelete "name","password" - Delete user from user list
userList           - Show user list
```

version

The Gateway contains software that controls all functions. Use the **version** command to display the current version of the operating software. The first line displayed is the Gateway firmware version. The lines that follow pertain to the operating system software version.

```
Gateway > version
Gateway Version 0339.11 Built Dec 13 1999, 15:14:14
VxWorks (for Pathlight (i960RD)) version 5.3.1.
Kernel: WIND version 2.5.
value = 26 = 0x1a
Gateway >
```

xscsiAltIdGet [channel]

Use the **xscsiAltIdGet** command to display the alternate ID number for a specified Ultra2/3 SCSI channel.

```
Gateway > xscsiAltIdGet 5
SCSIbus      AltId      -----
XSCSI      5      Auto
value = -1 = 0xffffffff
Gateway >
```

For information about alternate ID numbers for Ultra SCSI channels, see “scsiAltIdGet [channel]” on page 157.

xscsiAltIdSet [channel],[id]

Use the **xscsiAltIdSet** command to set the alternate ID for an Ultra2/3 SCSI channel.

Channel numbers 5 - 10 (Ultra2/3 SCSI)

ID channel numbers 0 - 15

```
Gateway > xscsiAltIdSet 6,3
Alternate Id set to 3 for SCSI 6 will take effect upon reboot
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new setting to take effect.

To set alternate ID numbers for Ultra SCSI channels, see “scsiAltIdSet [channel],[id]” on page 157.

xscsiHostChanGet [channel]

Use the **xscsiHostChanGet** command to display host channel modes for a specified Ultra2/3 SCSI channel.

```
Gateway > xscsiHostChanGet 5
SCSIbus HostChan -----
XSCSI 5 Channel is Initiator
value = -1 = 0xffffffff
Gateway >
```

For information about host channel modes for Ultra SCSI channels, see “scsiHostChanGet [channel]” on page 158.

xscsiHostChanSet [channel],[mode]

Use the **xscsiHostChanSet** command to set the channel mode to target or initiator for an Ultra2/3 SCSI channel.

Channel numbers 1 through 4 (Ultra2/3 SCSI)

Mode 0 Initiator mode (false)

Mode 1 Target mode (true)

```
Gateway > xscsiHostChanSet 6,1
Host Chan set to TRUE for XSCSI 6 will take effect upon reboot
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new settings to take effect.

To set host channel modes for Ultra SCSI channels, see “scsiHostChanSet [channel],[mode]” on page 158.

xscsiHostIdGet [channel]

Use the **xscsiHostIdGet** command to display the host ID number for a specified Ultra2/3 SCSI channel.

```
Gateway > xscsiHostIdGet 5
SCSIbus      HostId -----
XSCSI 5      7
value = -1 = 0xffffffff
Gateway >
```

For information about host IDs for Ultra SCSI channels, see “scsiHostChanGet [channel]” on page 158.

xscsiHostIdSet [channel],[id]

Use the **xscsiHostIdSet** command to set the host ID for a specified Ultra2/3 SCSI channel.

Channel numbers 5 - 10 (Ultra2/3 SCSI)

ID numbers can be 0 - 15

```
Gateway > xscsiHostIdSet 5,9
Host Id set to 9 for XSCSI 5
will take effect upon reboot
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new settings to take effect.

To set host IDs for Ultra SCSI channels, see “scsiHostChanSet [channel],[mode]” on page 158.

xscsiResetDisableGet [channel]

Use the **xscsiResetDisableGet** command to display the SCSI bus reset during startup setting for a specified Ultra2/3 SCSI channel. False means that SCSI bus reset on startup is enabled. True means that SCSI bus reset on startup is disabled.

```
Gateway > xscsiResetDisableGet 5
SCSIbus      Reset Disable -----
XSCSI 5      FALSE – default
value = -1 = 0xffffffff
Gateway >
```

For information about bus reset settings for Ultra SCSI channels, see “scsiHostChanGet [channel]” on page 158.

xscsiResetDisableSet [channel],[mode]

Use the **xscsiResetDisableSet** command to set the SCSI bus reset during startup mode for an Ultra2/3 SCSI channel.

Channel numbers 1 through 4 (Ultra2-SCSI)

Mode 0 Enable bus reset on Power Up

Mode 1 Disable bus reset on Power Up

```
Gateway > xscsiResetDisableSet 5,1
Reset Disable set to TRUE for XSCSI 5
will take effect upon reboot
value =0 =0x0
Gateway >
```

For information about bus reset settings for Ultra SCSI channels, see “xscsiResetDisableSet [channel],[mode]” on page 160.

xscsiTermGet [channel]

Use the **xscsiTermGet** command to display termination status information for the specified Ultra2/3 SCSI channel.

```
Gateway> xscsiTermGet 6
SCSIbus      Termination  -----
XSCSI 6      Enabled
value = 0    = 0x0
Gateway >
```

For information about termination status for Ultra SCSI channels, see “xscsiTermGet [channel]” on page 161.

xscsiTermSet [channel],[termination]

Use the **xscsiTermSet** command to enable or disable the termination for an Ultra2/3 SCSI channel.

Channel numbers 5 - 10 (Ultra2/3 SCSI)

termination 0 = Enable termination

termination 1 = Disable termination

```
Gateway > xscsiTermSet 5,1
Termination for XSCSI 5
will take effect upon channel reset
value =0 =0x0
Gateway >
```

Attention: You must restart the Gateway after issuing this command for the new settings to take effect

For information about setting termination status for Ultra SCSI channels, see “xscsiTermSet [channel],[termination]” on page 162.

Appendix C. Application Notes

This appendix contains information on special procedures and configurations that may be useful for advanced users to know. Included topics are as follows:

- Fibre Channel loop addressing—hard versus soft IDs
- Understanding and modifying device maps
- Setting up a redundant dual SCSI configuration
- MS cluster server notes

The SAN Data Gateway Module will be referred to in the rest of this appendix by the name Gateway.

Fibre Channel Loop Addressing—Hard Versus Soft IDs

This application note concerns the use of hard and soft addresses on Fibre Channel arbitrated loops (FC-ALs) and is applicable to the Gateway and the StorWatch Specialist.

Address Numbering

FC-ALs support a maximum of 127 devices; 126 NL_port devices and one FL_port device. Device addresses are arbitrated loop-physical addresses (AL_PA), and address numbers derive from the 8B/10B encoding used in Fibre Channel transmissions. Loop ID numbers and AL_PA numbers are not the same; however, AL_PAs can be referred to by loop IDs. Loop IDs number from 1 to 125. Loop ID 0 corresponds to the highest AL_PA number. Loop ID 126 is reserved for the FL_port (0-125, with 0 corresponding to the highest AL_PA; 126 is reserved for the FL_port). Note that the loop ID is not the same as the AL_PA.

Loop ID Assignment

Loop IDs are assigned during loop initialization. Devices can be configured to hard ID (request a specific AL_PA), or soft ID (one is assigned after all the hard IDs are known). Unlike SCSI, even if the desired hard ID is in use, the device can still be configured into the loop. It is assigned a soft ID if there is a conflict with another device already assigned that hard ID, and if there is still an available AL_PA.

Benefits and Drawbacks

The obvious benefit of using soft IDs is that no scheme of numbering needs to be decided in advance. All devices (as long as there are no more than the maximum number supported) will get an ID. The drawback to this method is that as the loop changes, either by the adding or removing of devices, the loop ID of any particular device might change (for example, after a system is restarted). Since many host adapter drivers will assign a SCSI-like target ID, based on the loop ID, the target ID of a device can change. On many operating systems, such as Solaris, the device name is entirely determined by its SCSI ID, so devices will cease to function or data corruption will occur if the loop ID changes during operation (or when a system restarts). Other systems, such as NT, are more forgiving, at least in the restart phase, but devices can still disappear from the system and applications may not detect devices they were connected with prior to a loop ID change.

Planning for Persistence

To ensure that devices are always located at the same loop ID (and therefore, usually, the same SCSI ID), you can assign hard IDs. By carefully planning the use of IDs, you can be certain that a device will always reappear at the same address. Any time a new device is added, the hard IDs of other devices on the loop must be accounted for before assigning the new device an ID.

Assigning a Hard ID to a Gateway Fibre Channel Port

You can assign a hard ID to the Gateway using either the Gateway or by issuing a command from a terminal connected to the service port.

Attention: Changing the hard ID may result in devices not being recognized by the host systems or causing the device addresses to change. To prevent possible data corruption, shut down all hosts before you change the ID. You also may need to reconfigure certain devices, perform a reconfiguration restart on SOLARIS, change hard-assigned SCSI addresses such as those used by some backup applications.

Using the StorWatch Specialist to Set the ID

Select a Gateway, then choose the desired Fibre Channel and click **Controls** → **Fibre Channel**. Click on the hard ID window and select an ID from the drop-down list, making sure it is not in use by any other device on the loop. The change will not take effect until the Gateway and the host are restarted. The StorWatch Specialist display shows the exact loop ID that is assigned to the channel. If the loop ID shown does not match the selected hard ID, another device is using that address on the loop. When the loop is down (nothing connected or hosts turned off), the loop ID is not meaningful.

Setting the ID from the Service Port

Enter the **setFcHardId** command as follows:

```
Gateway> setFcHardId 1,5
```

This example shows setting SAN connection 1 to a hard ID of 5 and will take effect when the Gateway is restarted. See “setFcHardId [channel],[id]” on page 163.

Understanding and Modifying Devices

Gateway Discovery and Mapping

The Gateway provides the ability to connect target devices (SCSI and Fibre Channel) to host systems using any of the available heterogeneous interfaces.

The Gateway and all attached devices are displayed at a single target address (loop ID, for example, on Fibre Channel), with each device addressable at a unique logical unit number (LUN) at that target address.

When a target device is attached to the Gateway, the Gateway adds that device to its address map and assigns a permanent LUN to it. Since the map is persistent, the device is always displayed at the same LUN unless the map is modified by one of the following techniques.

As the Gateway starts up, it detects the attached devices on each of its channel interfaces. Any device that can be a target, such as a disk or tape drive, is assigned to a persistent LUN. This process varies depending on whether or not there is an existing device address map database. This database can contain up to 256 entries on the Gateway. There is only one persistent map database in the Gateway and all initiators that are attached to it use the same entries.

In addition to assigning LUNs to each attached device, the Gateway reserves LUN 0 for communication with its command and control functions. LUN0 can be hidden, reassigned, or disabled. See “Changing the Command and Control LUN” on page 183.

Initial Device Discovery and Mapping

The initial discovery of devices is performed if the address map is empty. The following sections describe what happens as devices are added and removed.

SCSI discovery is carried out in a specific order and devices attached on the SCSI buses are enumerated by their SCSI target IDs (usually settable by switches or under device control) and LUN. Each SCSI bus is scanned from ID 0 to ID 15, and from LUN 0 to LUN 32 for each ID. When a device is located, it is placed at the next available LUN entry in the address map (this LUN is called the assigned LUN to distinguish it from its actual SCSI LUN). The buses themselves are scanned in order from channel 1 to channel 4.

Fibre Channel devices are scanned in loop ID order at the initial discovery time. Fibre Channel controllers are scanned in order from port 1 to port 6.

When a mix of SCSI and Fibre Channel devices are attached to a Gateway, SCSI channels are scanned first. Fibre Channel ports are scanned after the scan of SCSI channels has completed.

Mapping New Devices

If a new device is added and there are empty addresses in the device address map database, the new device is assigned to the first free address entry (see “Mapping Tape Drives” for special considerations for tape devices). To free up entries that are no longer needed and keep existing devices at the same assigned LUNs, you can use the **mapWinnowDatabase** command from the service port. See “mapWinnowDatabase” on page 152.

If the device address database is full (>256 devices are assigned addresses in the database), or if more than the maximum allowed number of devices are attached to the Gateway, the Gateway will send an event code to the StorWatch Specialist. The new device will not be mapped (assigned a LUN).

If the device address map database does not map a new device even though fewer than the maximum number of devices are present, you can free an address entry space by using the **mapWinnowDatabase** command from the service port. See “mapWinnowDatabase” on page 152.

Mapping Tape Drives

Tape drives are always assigned an even LUN number. If a changer is attached, its LUN will be one higher than the tape drive LUN. The odd LUN numbers that follows tape drive even numbers are reserved for the changer. If even or odd mapping of tape drives and changers is not suitable for your environment, see “Compressing the Address Map Database” on page 184 and “Customizing the Address Map Database” on page 184.

Changing the Command and Control LUN

In some operating environments, it may be necessary to remove or reassign access to the Gateway command and control LUN. You can do this in one of three ways:

- Hide the device so that a SCSI inquiry command will report that the device is not available.
- Reassign the device to a different LUN.
- Completely remove the device from the address map.

Hiding the Command and Control LUN

To hide the command and control LUN (LUN 0), enter the **disableCC 1** service port command.

Hiding the command and control LUN usually makes it invisible to the host operating system. For some operating systems and host bus adapter combinations, this may also prevent certain operations, such as automatic host registration for firmware updates.

Reassigning the Command and Control LUN

Attention: For AIX, Windows NT, and Windows 2000, you must not reassign the command and control LUN. AIX, Windows NT, and Windows 2000 use LUN 0 when they issue a **Report LUNs** command. If a disk or tape device is configured at LUN 0, these devices will not respond to the command. The Gateway firmware will do nothing to correct this configuration error.

To reassign the command and control LUN, enter the **setSnaCCLun newLUN** service port command.

newLUN is the new value for the command and control LUN. Valid values are 0—255.

The new setting takes effect immediately. The previous value is removed from the device map and database, and a trap is generated indicating that the device was removed.

If the new LUN is not currently in use, a new entry is added in the device map and database. A trap is generated indicating that the new device was added.

If the new LUN is already in use, the command and control LUN is disabled. It remains disabled until the device mapped at the requested LUN is removed and deleted from the database. In this case, you can use the **mapRebuildDatabase** command to remove the previous LUN assignment and to allow the new command and control LUN to be enabled.

Completely Removing the Command and Control LUN

To completely remove the device, enter the **disableCC 2** service port command. After completely disabling it, LUN 0 is available for other devices. To re-enable the command and control LUN, use the **enableCC** service port command.

Note: The command and control functions represent an important capability of the Gateway. These functions are used to update firmware, save, and restore configurations. Therefore, it is not recommended that this LUN be completely disabled.

Compressing the Address Map Database

A service port command is available that removes the holes in the address map database. This command is **mapCompressDatabase**. After this command is issued, all attached devices are assigned to consecutive LUNs. If the Gateway command and control LUN has been disabled, the map starts at LUN 0, otherwise it starts at 1.

To use this command, perform the following steps in order at the service port. The hosts should be turned off during this procedure.

1. Attach all target devices to the Gateway and make sure that power is applied to them.
2. Start up the Gateway.
3. Disable the command and control LUN if necessary.
4. Issue a **mapRebuildDatabase** command and allow the Gateway to restart.
5. Issue a **mapCompressDatabase** command. If you want to remove the LUNs reserved for tape changers and restart the Gateway, otherwise, go to the next step.
6. Issue the **fcShowDevs** command to verify the LUN assignments.
7. Start up the hosts one at a time and verify access to devices.

Customizing the Address Map Database

The address map database is stored on the Gateway as a formatted text file. It is possible to read this file and even edit it and replace it to achieve customized address maps. Use of this capability is an advanced function and must be done carefully to prevent configuration issues that can even lead to loss of data.

IBM StorWatch SAN Data Gateway Specialist version 2.5 and higher allows you to edit the address map database from the client application. It is a simpler method than the one described below.

The database file, `device.map`, is stored on the flash file system in the `config` directory. The procedure to modify the file can be performed using File Transfer Protocol (FTP) or a terminal emulator program that supports Zmodem connected to the Gateway service port.

Perform the following steps to manipulate the address map. For details and examples of these steps, see the information in , “Retrieving the Address Map Using Zmodem” on page 185, and “Modifying the Address Map” on page 185, and “Sending the Device Map Back to the Gateway” on page 187.

1. Retrieve the address map from the Gateway.
2. Make a copy of the address map file for backup.
3. Modify the contents of the file and save it in text format.
4. Send the modified map to the Gateway.
5. Restart the Gateway.

Retrieving the Address Map Using FTP

To use file transfer protocol (FTP), first set up an account on the Gateway using the **userAdd** command from the service port. The quote marks in the following examples are required.

```
userAdd "username","password"
```

The following example shows how you can use FTP to retrieve the map from any system that has network access to the Gateway.

```
h:\>ftp 192.168.1.72
Connected to 192.168.1.72.
220 VxWorks (5.3.1) FTP server ready
User (192.168.1.72:(none)): username
331 Password required
Password: <not echoed>
230 User logged in
ftp> cd /config
250 Changed directory to "ffs0:/config"
ftp> get device.map
200 port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp: 222 bytes received in 0.04Seconds 5.55Kbytes/sec.
ftp> bye
221 Bye...see you later
```

Retrieving the Address Map Using Zmodem

To use Zmodem, you need a terminal emulation program that supports the protocol running on a computer (such as a laptop) connected by a serial cable to the service port. HyperTerminal and Terra Term all support this transfer method. Consult your user documentation for more details.

Note: If you use Zmodem, the file cannot be formatted as a DOS text file, and you should use WordPad to edit it rather than Notepad. If you use FTP and perform an ASCII (text) transfer, you can edit and view the file in Notepad correctly.

From the command prompt on the service port, enter the following. Include the quotation marks when you type on the command line.

```
Gateway > cd "/config"
value = 0 = 0x0
gateway > sz "device.map"
File Download Complete: device.map
value = 0 = 0x0
```

Modifying the Address Map

The following is an example of an address map file.

```
1 127 127 127 00000060 451601ec 000
4 001 000 000 00000060 451601ec 001
4 001 001 000 00000060 451601ec 002
4 002 002 000 00000060 451601ec 003
4 002 003 000 00000060 451601ec 004
4 003 008 000 00000060 451601ec 005
4 003 009 000 00000060 451601ec 006
4 004 000 000 00000060 451601ec 007
4 004 001 000 00000060 451601ec 008
```

Table 29 on page 186 shows an example of an annotated device map. Note that the column headings will not appear in displayed output.

Table 29. Annotated Device Map

Interface type	Channel or SAN connection	Target or loop ID (Fibre Channel)	LUN	Unique ID (High)	Unique ID (Low)	Assigned LUN
1	127	127	127	00000060	451601ec	000
4	001	000	000	00000060	451601ec	001
4	001	001	000	00000060	451601ec	002
4	002	002	000	00000060	451601ec	003
4	002	003	000	00000060	451601ec	004
4	003	008	000	00000060	451601ec	005
4	003	009	000	00000060	451601ec	006
4	004	000	000	00000060	451601ec	007
4	004	001	000	00000060	451601ec	008

The interface type describes the physical connection to the device. This field should not be changed. Table 30 lists interface type descriptions.

Table 30. Interface Type Descriptions

Interface type	Description
1	Command and control
2	Fibre Channel
3	SCSI

For Fibre Channel devices, the channel field corresponds to the SAN connection numbering. For SCSI devices, this is the SCSI channel number.

The target or loop ID field corresponds to the SCSI target ID for SCSI devices and the Fibre Channel loop ID for FC-AL devices.

The LUN field corresponds to the SCSI logical unit number of the target and is 0 unless the target is a multi-LUN device (such as tape drives with attached changers).

The unique ID fields represent the world-wide name (for Fibre Channel). For SCSI devices, this field is set to the world-wide name of the Gateway and should not be changed.

The assigned LUN field is the LUN as seen by the attached hosts.

Edit the map carefully. For SCSI devices, you will mostly be concerned with the channel, target, LUN and assigned LUN columns. If you add a new SCSI device to the map, use the same unique ID fields as the command and control LUN. If you intend to disable the command and control LUN, use the **ccDisable 2** command before retrieving the address map from the Gateway and before modifying it. Disabling the command and control interface will not interfere with FTP or Zmodem operation.

The following map is for eight tape drives (LUNs 0-7) distributed across each of the Gateway's four SCSI ports.


```
4 001 000 000 000000060 451601ec 000
4 001 001 000 000000060 451601ec 001
4 002 000 000 000000060 451601ec 002
4 002 001 000 000000060 451601ec 003
4 003 000 000 000000060 451601ec 004
4 003 001 000 000000060 451601ec 005
4 004 000 000 000000060 451601ec 006
4 004 001 000 000000060 451601ec 007
```

The tape drives are set to targets 0 and 1. Two tape drives are connected to each SCSI channel on the Gateway. The ID columns are unique to each Gateway.

Sending the Device Map Back to the Gateway

To send the map back to the Gateway, reverse the above procedure.

The following example shows what to type when you use file transfer protocol.

```
h:\>ftp 192.168.1.72
Connected to 192.168.1.72.
220 VxWorks (5.3.1) FTP server ready
User (192.168.1.72:(none)): username
331 Password required
Password:
230 User logged in
ftp> cd "/config"
250 Changed directory to "ffs0:/config"
ftp> send "device.map"
200 port set okay
150 Opening ASCII mode data connection
226 Transfer complete
ftp: 222 bytes received in 0.04Seconds 5.55Kbytes/sec.
ftp> bye
221 Bye...see you later
```

The following example shows what to type when you use Zmodem.

```
Gateway > cd "/config"
value = 0 = 0x0
```

Then initiate a send operation, using the Zmodem option of the terminal emulator software.

Setting Up a Redundant Dual SCSI Configuration

This section describes the procedure for setting up a fully redundant dual SCSI configuration.

Introduction

Redundant dual SCSI configurations require a host software application that can take advantage of redundant paths to a device. Functions such as fail-over and load balancing are enabled with this combination of redundancy and the appropriate host software. For this configuration to be a practical solution, software on the hosts must be able to resolve issues such as both hosts seeing the same SCSI devices twice.

To create a fully redundant SAN configuration, two access paths must exist between the host and target devices. This redundancy requires dual paths from two independent HBAs in the host through separate cables and interconnections to a port on two Gateways. The redundancy can be extended to include dual paths from SCSI channels of both Gateways to the same SCSI devices. To accomplish this, the SCSI bus must be shared between two Gateways. For example, SCSI channel 1 of Gateway number 1 is connected to multiple devices and then to SCSI channel 1 of Gateway number 2. In other words, create a daisy chain that starts with one Gateway and ends at the other with SCSI devices between them. SCSI bus termination must be disabled on the SCSI devices because the Gateways provide termination for each end of the SCSI bus. If one of the Gateways is turned off, its internal terminators receive power from the external SCSI bus.

The steps required to create a redundant configuration are summarized below. Further detail is provided in the sections that follow. This procedure assumes prior installation of both Gateways. See “Pre-Installation Checklist” on page 24, “Installation Checklist” on page 25, and “StorWatch Specialist Installation Checklist” on page 27.

Perform the following steps for all shared SCSI channels on both Gateways and all shared devices.

1. Set SCSI IDs of Gateway SCSI channels and target devices.
2. Disable reset on power up for every shared SCSI channel.
3. Create identical persistent address maps for both Gateways.

Setting SCSI IDs of Gateways and Target Devices

Only one device, either a host (initiator) or a target (disk or tape), can use a SCSI ID. Each Gateway SCSI channel uses two SCSI IDs for its SCSI host (initiator) functions, referred to as SCSI host ID and SCSI alternate ID. To allow communication with narrow SCSI devices, the host ID and alternate ID for each Gateway must be a number from 0 to 7.

Each shared target device must have a unique SCSI ID that does not conflict with the host ID and alternate ID of the two Gateways.

Table 31 shows the recommended SCSI ID assignments.

Table 31. Recommended SCSI ID Assignments

SCSI ID	Device
0	Target
1	Target
2	Target
3	Target
4	Gateway 2 - alternate ID
5	Gateway 1 - alternate ID
6	Gateway 2 - host ID
7	Gateway 1 - host ID
8	Wide target
9	Wide target
10	Wide target
11	Wide target
12	Wide target
13	Wide target
14	Wide target
15	Wide target

Note: For information about how to set the host ID and alternate ID for Gateway SCSI channels, see Figure 55 on page 62.

Step 1. Set SCSI IDs for Gateway SCSI channels and target devices.

For every shared SCSI channel of Gateway number 1:

- a. Set host ID to 7.
- b. Set alternate ID to 5.

For every shared SCSI channel of Gateway number 2:

- a. Set host ID to 6.
- b. Set alternate ID to 4.

Set the SCSI IDs of your target devices:

- a. For narrow devices use SCSI IDs 0 to 3.
- b. For wide devices use SCSI IDs 8 to 15 or 0 to 3.

Make sure that SCSI termination is disabled on the target devices.

Disabling SCSI Channel Reset During Startup

A SCSI bus should only be reset when it is absolutely necessary for continuing the operations on the bus. The SCSI channels of the Gateway can be configured to not reset the SCSI bus at startup. This will minimize bus interruptions when a Gateway is started up on a shared bus.

- Step 2. Disable the SCSI channel reset during power up for every channel of the two Gateways:
- For every shared SCSI channel of Gateway number 1, disable the SCSI channel reset during power up.
 - For every shared SCSI channel of Gateway number 2, disable the SCSI channel reset during power up.

Note: For information about how to disable reset during power up for Gateway SCSI channels, see Figure 55 on page 62.

Creating Identical Persistent Address Maps

Some procedures like “Setting Up a Redundant Dual SCSI Configuration” on page 188, require that devices share identical addresses.

Note: The SCSI bus must have termination at both bus endpoints and at no other location. The Gateway, by default, provides termination on the SCSI bus. It is recommended that you connect the cables so that the Gateways are positioned at each end of the SCSI bus. If a Gateway is connected to the midpoint of the SCSI bus, rather than the endpoint, you must disable the termination of those specific SCSI channels. For instructions on how to enable or disable the SCSI termination of the Gateway SCSI channels, see Figure 55 on page 62.

It is important that you perform the following steps in the specified order. The hosts must not be started up at this time. Identical connections must exist between the two Gateways. For example, SCSI channel 1 of Gateway number 1 is connected to devices and then to SCSI channel 1 of Gateway number 2. The identical connections must exist for all SCSI channels that are being shared by both Gateways.

- Step 3. Create identical persistent address maps for both Gateways.
- Attach SCSI devices to the Gateways and turn them on.
 - Turn on Gateway number 1.
 - If you do not want to reassign the command and control LUN, go to step 3d. Otherwise, reassign the command and control LUN. For further information, see “Understanding and Modifying Devices” on page 181.
 - Enter the **mapRebuildDatabase** command from the service port and wait for the Gateway to restart. This creates a new address map for the devices that are currently attached to the Gateway.
 - If you do not want to remove the LUNs reserved for tape changers, go to step 3f. Otherwise, enter the **mapCompressDatabase** command from the service port and then restart the Gateway. For further information, see “Understanding and Modifying Devices” on page 181.
 - Verify the LUN assignments by using the **fcShowDevs** command from the service port.
 - Repeat steps 3b through 3f for Gateway number 2.

- h. Compare the address map of Gateway number 1 and number 2 and make sure that they are identical.
- i. Start up the hosts one at a time and verify access to devices.

Adding Devices to an Existing Redundant Configuration

To add new devices to an existing redundant dual SCSI configuration, you may need to manipulate the address maps to ensure that they are identical on both Gateways.

The address map database is stored on the Gateway as a text file. You can edit or replace it to achieve a customized address map. If you need to alter the map, edit it carefully to prevent configuration problems.

Note: It is important that you perform the following steps in the specified order. The hosts must not be started up at this time. Identical device connections must exist between the two Gateways and the SCSI devices must have the power turned on.

Perform the following steps to manipulate the address map:

1. Retrieve the address map from Gateway number 1. For information about how to retrieve, manipulate, and send the address map, see "Customizing the Address Map Database" on page 184.
2. Make a copy of the address map file for backup purposes.
3. If necessary, modify the address map and save it to a file. You do not have to modify the device map if both Gateways are to have access to all of the same devices.
4. Send the modified address map from Gateway 1 to Gateway 2.
5. Restart Gateway 2.
6. Compare the address maps of Gateways 1 and 2 and make sure that they are as desired.
7. Start up the hosts one at a time and verify access to the SCSI devices.

Microsoft Cluster Server Notes

This section provides implementation details for setting up the Gateway for use with Microsoft Cluster Server (MSCS) under Windows NT 4.0 or Windows 2000.

It is extremely important to follow the specified procedure for installing MSCS. In particular, you should verify that each host has an identical view of the shared device LUNs, (that is, individually, with only one host turned on at a time), before you begin the installation. Once this has been verified, make sure that only one host is turned on when you start the cluster installation.

Finally, the service pack must be reinstalled after the MSCS is installed on each node.

Relevant Knowledge Base Articles

Microsoft publishes knowledge base articles when problems are identified or when additional information is available about products. You should regularly check the Microsoft web site at:

www.microsoft.com/technet/support

Table 32 lists some knowledge base articles about MSCS:

Table 32. Knowledge Base Articles

Q251007	Some cluster disks are not available after installing SP6
Q252974	Error message: System process - Lost or delayed-write data
Q256326	Cluster server cannot use disk beyond device number 25
Q245605	Clusdisk.sys may corrupt pool memory
Q248633	Booting node may prevent running node from accessing the quorum disk

Requirements and Settings

Table 33 lists the minimum recommended levels for supported configurations using the Gateway with Microsoft Cluster Server. Configurations must meet the minimum requirements.

Table 33. Supported Configuration Requirements

Item	Minimum recommended version
Microsoft, Windows NT, Windows 2000	4.0 (Enterprise edition)
Service pack	5 for NT
BIOS	1.37, 1.44
QLogic 2200 HBA driver	7.02.05 or 7.02.07 (7.04.02 is not supported)
Gateway firmware	3.40.08 or later

In addition to the driver levels, certain parameters (non-default) must be set in the QLogic NVRAM. This is done using the Fast!UTIL application, which is entered by pressing Alt+Q when the system is starting up and the QLogic banner is shown. There are two windows that control these settings on the 2100 adapters: Host Adapter Settings and Advanced Adapter Settings. The 2200 adapter provides one additional window, Extended Firmware Settings. These windows are not discussed here.

Table 34. QLogic Host Adapter Settings

Parameter	Value
Host adapter BIOS	Disabled
Frame size	2048
Loop reset delay	5 (minimum)
Adapter hard loop ID	Disabled
Hard loop ID	See Note
Note: Some configurations may require the use of hard IDs. Refer to “Fibre Channel Loop Addressing—Hard Versus Soft IDs” on page 180 for more information.	

Table 35. QLogic Advanced Adapter Settings

Parameter	Value
Execution throttle	240
Fast command posting	Enabled
>4 GB addressing	Disabled for 32-bit systems
LUNs per target	0

Table 35. QLogic Advanced Adapter Settings (continued)

Parameter	Value
Enable LIP reset	No
Enable LIP full login	No
Enable target reset	Yes
Login retry count	20 (minimum)
Port down retry count	20 (minimum)
Drivers load RISC code	Enabled
Enable database updates	No
IOCB allocation	256
Extended error logging	Disabled (may be enabled for debugging purposes)

Three of these parameters (shown in *italics*) control behavior of the adapter when Windows NT or Windows 2000 attempts to do a SCSI bus reset (since this must be emulated on Fibre Channel). Target resets are essential to making cluster failovers work; SCSI bus device reset (target reset) is used to clear SCSI reservations. (The Gateway does not support LIP reset and the full login is not necessary after the target reset.)

The adapter driver must be configured for largeLuns support. If you obtained the driver from the compact disc or from the web site at:

www.ibm.com/storage/lto

this is included as part of the setup information file. Otherwise, you should enable largeLuns by adding a largeLuns value to the HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\QL2100\Parameters\Device registry key and setting the value to 1. You must restart the system for this to take effect.

Appendix D. Diagnostic Command Reference

This appendix describes procedures that should be used when diagnostics are required.

Boot Modes

The SAN Data Gateway Module has two modes of operation: normal mode and diagmode. The SAN Data Gateway Module will be referred to in the rest of this appendix by the name Gateway. Two commands are available from the service terminal to restart the Gateway in the desired mode. The Gateway remains in the existing mode until directed to restart in the other mode.

Attention: Before entering diagmode, disconnect the SCSI cables from the Gateway. If this is not done, data will be corrupted.

When you start the Gateway in diagmode, the command prompt displayed on the service terminal is `diagmode >`. While in diagmode, a limited command set is available for testing the Gateway memory and interfaces. In addition, the device drivers for the Ethernet, Fibre Channel, and SCSI interfaces are disabled so that loopback tests can be performed on them.

Entering Diagnostic Mode

Use the **diagBoot** command when you need the special features of the Gateway diagnostic module. (See “diagBoot” on page 200). Perform the following steps:

1. Stop all input/output (I/O) activity.
2. Turn off the Gateway.
3. Remove the Ethernet cable, if installed.
4. Connect the terminal to the service port.
5. Turn on the Gateway and wait for it to finish the startup.
6. If the command prompt displayed on the service terminal is `diagmode >`, then return the procedure from which you came.
7. From the service terminal, type `diagBoot`.
8. Wait for the Gateway to restart.
9. If the command prompt displayed on the service terminal is `diagmode >`, return the procedure from which you came .

Restoring Normal Mode

normalBoot runs if the Gateway is in diagnostic mode. You must restore it to normal mode. See “normalBoot” on page 200. Perform the following steps:

1. If the Gateway is on, turn it off.
2. Connect the terminal to the service port.
3. Turn on the Gateway and wait for it to finish the startup.
4. If the command prompt displayed on the service terminal is not `diagmode >`, then return the procedure from which you came .
5. From the service terminal, type `normalBoot`.
6. Wait for the Gateway to finish the startup.
7. If the command prompt displayed on the service terminal is not `diagmode >`, then return the procedure from which you came .

Special Procedures

This section contains information about special procedures.

Health Check

The health check function provides a method to periodically determine the operational state of a Gateway and its attached interfaces and devices.

Manual Health Check

Health check runs manually from the service terminal *only* if the Gateway is in normal mode. This procedure uses the **hlthChkNow** command that performs a level 4 health check and includes a SCSI device availability. You must connect and turn on the SCSI target devices so that health check can determine the operational status. Four other commands, which are not used in this procedure, allow you to view or specify the health check interval and level. See the commands with the prefix **hlthCk** in “Appendix B. Service Port Command Reference” on page 123.

Perform the following procedure:

1. Stop all I/O activity.
2. Remove the Ethernet cable, if installed.
3. Connect the terminal to the service port.
4. Type **hlthChkNow** from the service terminal.
5. Check the results displayed on the service terminal to determine the status of the interfaces and attached devices. If a failure occurs, perform the appropriate maintenance analysis procedure (MAP). If a failure does not occur, return the procedure from which you came .

Periodic Health Checks

Health checks run periodically at the programmed interval and level. If health check detects a failure in the Gateway or one of its interfaces, a trap or event code is logged in the event log. To receive the trap or event code, monitor the Gateway from the IBM StorWatch Specialist clients.

When health check is disabled, the Gateway performs no periodic checks beyond monitoring environmental status lines that indicate power supply and temperature conditions. The health check adds additional status checks.

The health check function posts Simple Network Management Protocol (SNMP) traps, when required, to convey status information to management applications. The Gateway broadcasts SNMP traps on the local internet protocol (IP) network segment. In addition, you can configure specific addresses to send directed SNMP traps to host systems that are located on other subnets. The routing information must be set up for directed traps to a different subnet to operate. The server automatically registers itself as a trap recipient when it connects to a Gateway.

Health check failures are recorded in the event log. The trap is sent on each occurrence. Each health check event has an associated health check level. The trap is not issued unless the Gateway health check level is set to that level or greater.

Setting Up the Health Check

The health check enables when the level sets to a value greater than 0. This is set from the client application or from the service port. See “Health Check Level Control” on page 198.

Health Check Level Control

You can set the health check levels to those described below when you use the management application. For more information on the traps sent from the health check facility, see “Service Reference Table” on page 85. You can store the health check level in the Gateway configuration tables and it is persistent between restarts.

0—no health check

Although no health check is performed based on a resettable interval, the Gateway monitors the power and temperature and records variations in the event log. Traps for events listed in “Service Reference Table” on page 85 are still generated based on the threshold settings regardless of the health check level.

1—system health check

When set to level 1, the Gateway periodically scans the system resources to locate problems. The health check status sets if any of the following conditions are true:

- Temperature sensors detect warning or alarm status
- Power supply sensors detect a change in status since the last report on primary or auxiliary supplies.

2—interface health check (default)

The interface health check provides an active poll to the interface device, such as a Fibre Channel or SCSI controller. The controller is queried in an interface-dependent method to determine if it is currently functional. If a controller is not functional, a health check trap is sent to indicate which interface failed.

Also enabled at level 2 is a test of the Fibre Channel link status registers, which monitor Fibre Channel link errors. A trap is sent if any change in these registers is found.

3—simple device health check

The device health check polls every attached device to determine its status. A device is healthy if it responds to a simple SCSI inquiry command.

4—device availability health check

At this level, each target device is sent a SCSI **Test Unit Ready** command when the interval expires. If the device reports Good Status, it is healthy. If the device is not ready, the sense data from the device is interpreted to determine if the device is in a “normal” not ready state, or if the device is in a failed state. A “normal” not ready state can be a tape drive without a mounted tape.

If a device is determined to be in a “failed” state, a SNMP trap is issued.

Health Check Interval

The health check interval controls how often the health check process runs. The interval ranges from 1 to 65 535 minutes (about 45 days). The default setting is 60 minutes.

Performance Impact of Health Checks

At higher levels (3 or 4), the health check process can interfere with high-demand I/O operations. For example, in a video delivery application, you might want to select a very low level of health check, or none at all. A transaction processing server can require more rigorous periodic checks.

If a device fails during normal I/O activity, the event is logged in the event log. Health check does not detect the failure or send a trap unless the health check level is set to 3 or 4.

Any trap based on the health check is sent each time the health check interval expires. This means that there are repeated messages if the same conditions exist on successive checks.

Event Log Dump

The events that are logged in the Gateway event log are displayed on the service terminal or viewed from the StorWatch Specialist. This information is useful because you can see normal events or abnormal events that can lead to the source of an internal or external failure.

1. Each entry contains a sequence number, date, and time-stamp (relative to start-time), the event code, event source (interface name or system process), an index, and a description of the event.
2. The event log holds more than 2000 events. The most recent events overwrite the oldest events.
3. You can choose to view only the events logged since the Gateway was last started, or you can view a longer list of events that accumulate from previous starts.
4. You can choose to view events by severity level. If you specify level 1, you see all high-severity events, less severe events, including warnings, and informational events. If you specify level 2, you see warnings and information events. Level 3 shows informational events only.

See the **loggerDump** and **loggerDumpCurrent** commands in “Appendix B. Service Port Command Reference” on page 123.

Retrieving the Code 43 Dump File

If an event code 43 was reported to the StorWatch Specialist client, it is an indication that the Gateway performed an error recovery operation and had to reset the Fibre Channel interface to clear a lockup condition.

This event is also recorded in the Gateway event log along with the name of a file that was saved to the flash file system. The file contains information about the state of the Fibre Channel interface prior to the reset. Use this procedure to retrieve the file:

1. Connect the service terminal to the service port (see “Appendix A. Connecting to the Service Port” on page 117).
2. Press the Enter key on the service terminal. If the prompt is not displayed, go to “Service Port MAP” on page 105 to determine whether the RS-232 cable and service terminal are working properly.
3. From the service terminal, navigate to the DUMP directory by typing `cd dump`.

4. From the service terminal, type `ls` to produce a listing of files in the directory. There can be multiple dump files if the error condition has repeatedly occurred.

Note: Dump file names have the

`.dmp`

extension. These files are automatically deleted whenever you update the Gateway firmware.

5. Refer to “Saving a Configuration File” on page 120. Substitute the name of the dump file and use that procedure to save the file to the service terminal. Repeat this step if there is more than one file to save to the service terminal.

Boot Mode Commands

This section contains the **boot mode** commands.

diagBoot

1. Use the **diagBoot** command to transition a Gateway from normal operations to the special diagnostic mode.
2. The **diagBoot** ensures that the `ffs0:mt` directory exists.
3. It verifies that the files `diagnstk.o` and `diagnstk.rc` are in the flash file system. If they are in the root directory, they are moved to the `ffs0:mt` directory.
4. This command copies the existing bootline to a file in the `ffs0:mt` directory on the Gateway.
5. The **diagBoot** command installs a new bootline, directing the Gateway to start, using a special diagnostic startup script `ffs0:mt/diagnstk.rc`.
6. The persistent map file `config/device.map` is renamed `config/device.bak` (a new file is generated after restarting).
7. Finally, **diagBoot** issues a **reboot** command to apply the changes.

normalBoot

1. The **normalBoot** command is used only to transition a Gateway from the special diagnostic mode to normal operations.
2. It restores the boot parameters that were copied by **diagBoot**.
3. The new persistent device map is erased. The original map file is renamed `config/device.map`, restoring its use when the Gateway restarts.
4. The **NormalBoot** command restarts the Gateway.

Diagnostic Commands

This section is a reference for the commands that are available when the Gateway is started in diagmode.

1. The command set is limited while in diagmode. Use the **showBox** command and four commands (with suffix: Test) when testing the Ethernet, Fibre Channel, and SCSI interfaces.
2. The Ethernet loopback plug, Fibre Channel loopback plug, and SCSI cable, provided in the service tool kit, are required for the corresponding loopback test.

Attention: Disconnect the SCSI cables from the Gateway. If this is not done, the data will be corrupted.

elTest

The **elTest** command is the Ethernet loopback test. The Gateway must be in diagnostic mode, and a loopback cable must be installed on the Ethernet port.

```
Gateway > elTest

=== Testing Ethernet ===
External loopback LANCE-0 Ethernet OK
value = 0 = 0x0
```

The first time the **elTest** command is issued, it displays the message External loopback Lances. This indicates that the Ethernet chip is in external loopback mode. Do not connect it to the LAN while in this state. Perform a **reboot** or **normalBoot** command before reconnecting the Gateway to the LAN.

The test issues a series of loopback tests. Test data is transferred and verified. A good test ends with the message Ethernet OK.

Errors are displayed as they are detected.

If errors are detected, the test displays the number of bad test iterations as shown in the following example:

```
=== Testing Ethernet ===
interrupt: 1n0: no carrier
Ethernet timeout error
interrupt: 1n0: no carrier
Ethernet timeout error
interrupt: 1n0: no carrier
Ethernet timeout error
interrupt: 1n0: no carrier
Ethernet timeout error
Ethernet test reported 4 errors out of 12 iterations
value = 4 = 0x4
```

fcSlotTest [x]

The Gateway must be in diagnostic mode to use this command and a loopback plug must be connected to the PMC card.

The **fcSlotTest** command performs a confidence test on a Fibre Channel. Substitute for x the port number you want to test. This command can be used to test a Fibre Channel port or a Fibre Channel cable. The slot and port numbering convention is shown in Table 36:

Table 36. Single-Port Fibre Channel Optical Interfaces

SAN Connection Port Number Assignments	
<div><div>2</div><div>■ ■</div><div>PMC 2</div></div>	<div><div>1</div><div>■ ■</div><div>PMC 1</div></div>

a67r0103

The following example shows the display for a test on a single-port Fibre Channel PMC card in slot 1:

```
diagmode > fcSlotTest 1
Fibre Channel in slot 1 returns PASSED
value = 0 = 0x0
```

scsiChannelTest [x,y]

The Gateway must be in diagnostic mode to use this command and a SCSI cable must be connected between the two SCSI channels.

The **scsiChannelTest** command performs a confidence test on a pair of SCSI channels. Substitute the SCSI channel numbers you want to test for x and y. This command is used to test the SCSI interfaces or a SCSI cable.

The following example shows the display for a test on SCSI channels 3 and 4.

```
diagmode > scsiChannelTest 3,4
SCSI-3 -> SCSI-4 [#####] 101 iterations PASSED
SCSI-4 -> SCSI-3 [#####] 101 iterations PASSED
PASSED
value = 0 = 0x0
```

For Ultra2/3 SCSI channels, use the **xscsiChannelTest** command.

xscsiChannelTest [x,y]

The Gateway must be in diagnostic mode to use this command and you must have the appropriate short VHDCI offset cable with 68-pin connectors, LVD/SE.

The **xscsiChannelTest** command performs a confidence test on a pair of Ultra2/3 SCSI channels. Substitute for *x* and *y* the Ultra2/3 SCSI channel numbers you want to test. Parenthesis are optional. This command can be used to test the Ultra2/3 SCSI interface or an Ultra2/3 SCSI cable.

The following example shows the display for a test on Ultra2/3 SCSI channels 1 and 4.

```
diagmode > xscsiChannelTest 1,4
XSCSI-1 -> XSCSI-4 [#####] 101 iterations PASSED
XSCSI-4 -> XSCSI-1 [#####] 101 iterations PASSED
PASSED
value =0 =0x0
```

For Ultra SCSI channels, use the **scsiChannelTest** command.

Appendix E. Startup Message Reference

This appendix covers the startup messages sent by the SAN Data Gateway Module. The SAN Data Gateway Module will be referred to in the rest of this appendix by the name Gateway.

Boot Rom Messages

After the Gateway completes its power-on self-test, it will attempt to find, load, and run the real-time LIC boot loader. See the sample code below.

```
Press any key to stop auto-boot...
0
auto-booting...
boot device : ibmEmac
unit number : 0
processor number : 0
file name : //ffs/vxWorks.st
inet on ethernet (e) : 192.168.1.183
flags (f) : 0x8
target name (tn) : SN600030
startup script (s) : //ffs/sna.rc
Attaching to TFFS... done.
Loading /ffs/vxWorks.st...2697865
Done
Starting at 0x10000...
```

LIC Initialization Messages

After the BootLoader finds and loads the licensed internal code (LIC), the BootLoader will transfer control and start Gateway operations. See the sample code below.

```
Host Name: bootHost
User: anyone
Attached TCP/IP interface to ibmEmac unit 0
Attaching network interface lo0... done.
NFS client support not included.
Adding 8123 symbols for standalone.
SDRAM DIMM: 128 Meg - 1 banks detected
Enabling MMU Data Translation
/nvfs/ - disk check in progress ...
/nvfs/ - Volume is OK
total # of clusters: 1,008
# of free clusters: 935
# of bad clusters: 0
total free space: 478,720
max contiguous free space: 478,720 bytes
# of files: 5
# of folders: 10
total bytes in files: 29,785
# of lost chains: 0
total bytes in lost chains: 0
Executing startup script /ffs/sna.rc ...
#! /bin/csh -f
CNFinit
value =0 =0x0
csSrvInit
SN600030
Clock set from RTC
value =0 =0x0
```

```
amemInit
SDRAM DIMM: 128 Meg - 1 banks detected
value =0 =0x0
appInit
```

Final Startup Messages

In the final stage of the boot process, information is displayed about the firmware version, Gateway name, optional features that are enabled or disabled, SCSI channels, and the IP address. In the example below, after the Gateway command prompt, a message is displayed as a result of a response from a host.

```
Data Mover Enabled, License is Valid
USCSI 4 -LVDTerm Enabled
USCSI 3 -LVDTerm Enabled
USCSI 2 -LVDTerm Enabled
USCSI 1 -LVDTerm Enabled
SN600030
value = 28051936 = 0x1ac09e0
Done executing startup script /ffs/sna.rc
SN600030 >
```

Appendix F. POST Error Codes

The power-on self-test (POST) is responsible for testing the integrity of the processor's SDRAM. After testing SDRAM POST will attempt to transfer control to either the default bootrom image or an alternate image. POST can also download binary images over the service port and write them to flash memory. This enables POST to perform a minimal amount of emergency recovery from FLASH errors.

POST Boot Behavior

ROM Init

Power-on

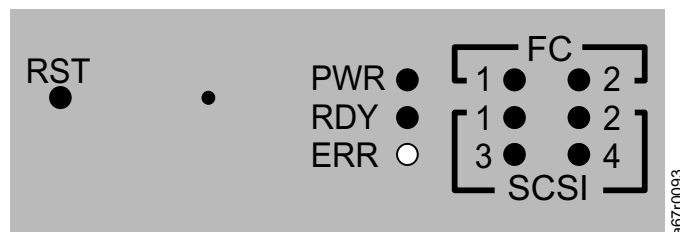


Figure 85. ROM Init

After applying power the ERR LED will illuminate. See Figure 85. At this time postInit code initializes the processor's internal registers and subsystems, including the SDRAM controller. The processor's internal RAM is used as a tiny-stack for this stage of POST. Control is then passed to the "ipostmain" routine for the SDRAM memory.

Initial POST

PLD and Service Port Initialization

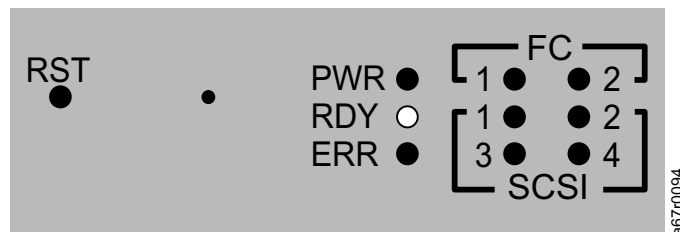


Figure 86. Initial POST

ipostMain starts by initializing the service-port and the system PLD(s). The ERR LED will extinguish and the RDY LED will turn on. See Figure 86. POST will display the following message on the service port:

```
== POST Version nnn ==
```

Simple Access Test



Figure 87. Simple Access

The simple access test verifies that the processor can perform basic writes and reads to the SDRAM. This test is identified by the flash of the Fibre Channel 1 LED. See Figure 87.

Bitwalk Test



Figure 88. Bitwalk Test

This test first walks a one-bit then a zero-bit through the base of each bank of SDRAM. This test is identified by the flash of the Fibre Channel 2 LED. See Figure 88.

Memory Size

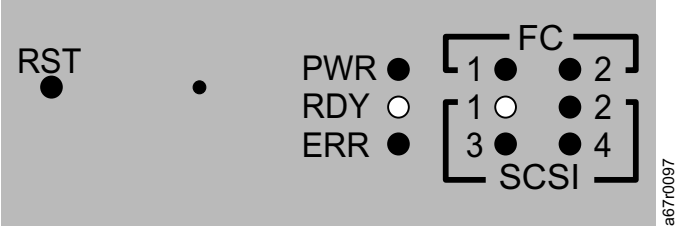


Figure 89. Memory Size

This test verifies that the apparent size of SDRAM meets the minimum and maximum sizes specified for the product. This test is identified by the flash of the SCSI1 LED. See Figure 89.

Pattern Test

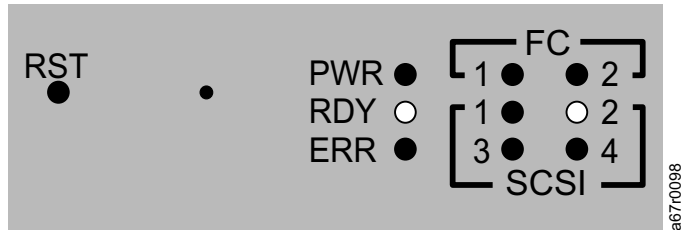


Figure 90. Pattern Test

This test writes and reads a series of diagnostic patterns to each memory location in SDRAM. This test is identified by the repeated flash of the SCSI2 LED. See Figure 90. This test can take several seconds to complete.

Address Test

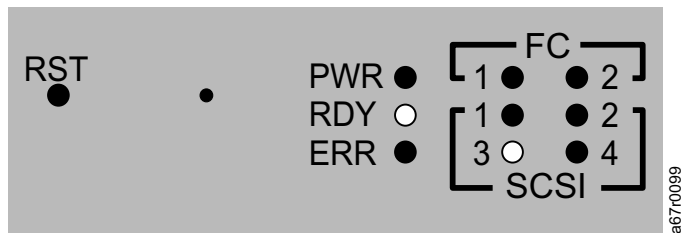


Figure 91. Address Test

This test writes and reads address tags to memory to test for bad SDRAM address lines. This test is identified by the flash of the SCSI3 LED. See Figure 91. POST then relocates itself to SDRAM and moves its stack from processor internal RAM to SDRAM. Control is then transferred to the SDRAM based Secondary POST.

Secondary POST

This stage of POST attempts to locate and execute the intermediate loader, or “bootrom.” If the operator presses the interrupt button then POST will enter into the service menu. See the section “POST Service Menu” for details.

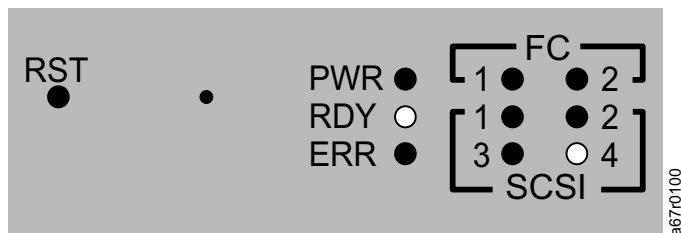


Figure 92. Identify and Execute

POST will examine the FLASH memory primary bootrom locations to determine whether or not it contains a viable bootrom. If the bootrom appears valid then POST will transfer control to it. If the bootrom image is considered invalid then POST will repeat the bootrom checks at the location of the secondary bootrom. This step is indicated by the flash of the SCSI4 LED. Figure 92.

Start of Bootrom

When POST starts a bootrom image it will display a line like:

Bootrom (*FFF00100) (2)

The number in the first parenthesis is the address of the bootrom's startup code. The number in the second parenthesis is flag to the operating system to determine what type of boot it has – warm or cold. Bootrom code will set the ERR LED when it reconfigures the PLD.

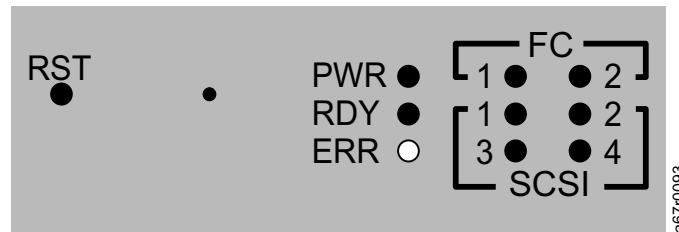


Figure 93. Start of Bootrom

POST Service Menu

The POST Service Menu is enabled by using a slim tool to depress the unlabeled button between the RST button and PWR LED. See **1** in Figure 94.

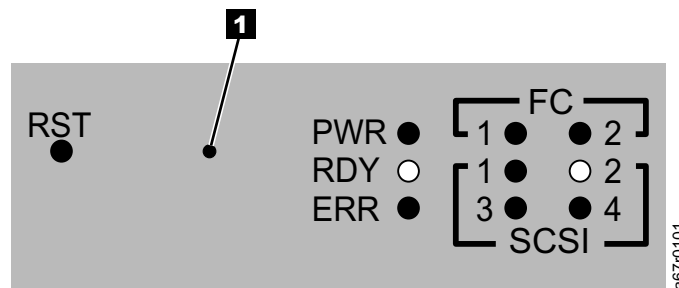


Figure 94. NMI 1

The button may be depressed any time during the memory tests. See **1** in Figure 95.

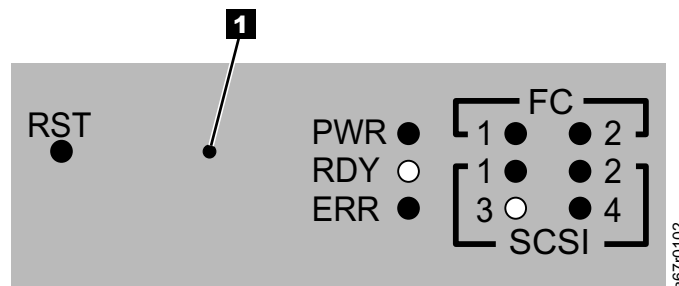


Figure 95. NMI 2

After completing the memory tests POST will display:

== POST Version nnn ==

== POST MENU ==

A - Cold boot from [A]lternate bootrom

B - Cold [B]oot from primary bootrom

R - [R]eceive new boot image from serial port

V - full [V]ersion information

A - Cold Boot from [A]lternate Bootrom

This option causes POST to transfer control to the alternate bootrom image at address 0xFFE00100 and to treat it as a cold boot.

B - Cold [B]oot from Primary Bootrom

This option causes POST to transfer control to the default, or primary, bootrom image at address 0xFFFF00100 and to treat it as a cold boot.

Notices

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

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

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

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

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

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

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

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

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

Read Before Using
IMPORTANT

YOU ACCEPT THE TERMS OF THIS IBM LICENSE AGREEMENT FOR MACHINE CODE BY YOUR USE OF THE HARDWARE PRODUCT OR MACHINE CODE. PLEASE READ THE AGREEMENT CONTAINED IN THIS BOOK BEFORE USING THE HARDWARE PRODUCT. SEE "IBM Agreement for Licensed Internal Code" on page 216.

Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries (or regions), or both:

AIX
IBM
StorWatch

Microsoft and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries (or regions), or both.

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

Intel is a registered trademark of Intel Corporation in the United States, other countries (or regions), or both.

UNIX is a registered trademark of The Open Group in the United States and other countries or regions.

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

Electronic Emission Statements

This section gives the electronic emission notices or statements for the United States and other countries or regions.

Federal Communications Commission (FCC) Class B Statement

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.

- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM authorized dealer or service representative for help.

IBM is not responsible for any radio or television interference caused by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Industry Canada Class B Emission Compliance Statement

This Class B digital apparatus complies with Canadian ICES-003.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

European Union (EU) Electromagnetic Compatibility Directive

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Germany Electromagnetic Compatibility Directive

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) vom 30. August 1995 (bzw. der EMC EG Richtlinie 89/336).

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Konformitätserklärung nach Paragraph 5 des EMVG ist die IBM Deutschland Informationssysteme GmbH, 70548 Stuttgart.

Informationen in Hinsicht EMVG Paragraph 3 Abs. (2) 2: Das Gerät erfüllt die Schutzanforderungen nach EN 50082-1 und EN 55022 Klasse B.

EN 50082-1 Hinweis: "Wird dieses Gerät in einer industriellen Umgebung betrieben (wie in EN 50082-2 festgelegt), dann kann es dabei eventuell gestört werden. In solch einem Fall ist der Abstand bzw. die Abschirmung zu der industriellen Störquelle zu vergrößern."

Anmerkung: Um die Einhaltung des EMVG sicherzustellen, sind die Geräte wie in den IBM Handbüchern angegeben zu installieren und zu betreiben.

Japan VCCI Class A ITE Electronic Emission Statement

この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づきクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

vcci

Taiwan Class A Electronic Emission Statement

警告使用者：
這是甲類的資訊產品，在
居住的環境中使用時，可
能會造成射頻干擾，在這
種情況下，使用者會被要
求採取某些適當的對策。

taitemi

Korean Government Ministry of Communication Statement

Please note that this device has been approved for business purposes with regard to electromagnetic interference. If you find this is not suitable for your use, you may exchange it for one with a non-business purpose.

IBM Agreement for Licensed Internal Code

You accept the terms of this Agreement (Form Z125-4144) by your initial use of a machine that contains IBM Licensed Internal Code (called "Code"). These terms apply to Code used by certain machines IBM or your reseller specifies (called "Specific Machines"). International Business Machines Corporation or one of its subsidiaries ("IBM") owns copyrights in Code or has the right to license Code. IBM or a third party owns all copies of Code, including all copies made from them.

If you are the rightful possessor of a Specific Machine, IBM grants you a license to use the Code (or any replacement IBM provides) on, or in conjunction with, only the Specific Machine for which the Code is provided. IBM licenses the Code to only one rightful possessor at a time.

Under each license, IBM authorizes you to do only the following:

1. execute the Code to enable the Specific Machine to function according to its Official Published Specifications (called "Specifications");
2. make a backup or archival copy of the Code (unless IBM makes one available for your use), provided you reproduce the copyright notice and any other legend of ownership on the copy. You may use the copy only to replace the original, when necessary; and
3. execute and display the Code as necessary to maintain the Specific Machine.

You agree to acquire any replacement for, or additional copy of, Code directly from IBM in accordance with IBM's standard policies and practices. You also agree to use that Code under these terms.

You may transfer possession of the Code to another party only with the transfer of the Specific Machine. If you do so, you must 1) destroy all your copies of the Code that were not provided by IBM, 2) either give the other party all your IBM-provided copies of the Code or destroy them, and 3) notify the other party of these terms. IBM licenses the other party when it accepts these terms. These terms apply to all Code you acquire from any source.

Your license terminates when you no longer rightfully possess the Specific Machine.

Actions You Must Not Take

You agree to use the Code only as authorized above. You must not do, for example, any of the following:

1. Otherwise copy, display, transfer, adapt, modify, or distribute the Code (electronically or otherwise), except as IBM may authorize in the Specific Machine's Specifications or in writing to you;
2. Reverse assemble, reverse compile, or otherwise translate the Code unless expressly permitted by applicable law without the possibility of contractual waiver;
3. Sublicense or assign the license for the Code; or
4. Lease the Code or any copy of it.

IBM License Agreement for Machine Code

Regardless of how you acquire (electronically, preloaded, on media or otherwise) BIOS, Utilities, Diagnostics, Device Drivers, firmware, or Microcode (collectively called "Machine Code"), you accept the terms of this Agreement by your initial use of a Machine or Machine Code. The term "Machine" means an IBM Machine, its features, conversions, upgrades, elements or accessories, or any combination of them. Acceptance of these license terms authorizes you to use Machine Code with the specific product for which it is provided.

International Business Machines Corporation or one of its subsidiaries ("IBM"), or an IBM supplier, owns copyrights in Machine Code.

IBM grants you a nonexclusive license to use Machine Code only in conjunction with a Machine. As the rightful possessor of a Machine, you may make a reasonable number of copies of Machine Code as necessary for backup, configuration, and restoration of the Machine. You must reproduce the copyright notice and any other legend of ownership on each copy of Machine Code you make.

You may transfer possession of Machine Code and its media to another party only with the transfer of the Machine on which the Machine Code is used. If you do so, you must give the other party a copy of these terms and provide all user documentation to that party. When you do so, you must destroy all your copies of Machine Code.

Your license for Machine Code terminates when you no longer rightfully possess the Machine.

No other rights under this license are granted.

You may not, for example, do any of the following:

1. Otherwise copy, display, transfer, adapt, modify, or distribute in any form, Machine Code, except as IBM may authorize in a Machine's user documentation.
2. Reverse assemble, reverse compile, or otherwise translate the Machine Code, unless expressly permitted by applicable law without the possibility of contractual waiver;
3. Sublicense or assign the license for the Machine Code; or
4. Lease the Machine Code or any copy of it.

The terms of IBM's Machine warranty, which is incorporated into this Agreement by reference, apply to Machine Code. Please refer to that warranty for any questions or claims regarding performance or liability for Machine Code.

Statement of Limited Warranty

International Business Machines Corporation
Armonk, New York, 10504

The warranties provided by IBM in this Statement of Limited Warranty¹ apply only to Machines you originally purchase for your use, and not for resale, from IBM or your reseller. The term "Machine" means an IBM machine, its features, conversions, upgrades, elements, or accessories, or any combination of them.

Unless IBM specifies otherwise, the following warranties apply only in the country or region where you acquire the Machine. If you have any questions, contact IBM or your reseller.

Machine: SAN Data Gateway Module

Warranty Period: One Year *

**Contact your place of purchase for warranty service information.*

Production Status

Each Machine is manufactured from new parts, or new and used parts. In some cases, the Machine may not be new and may have been previously installed. Regardless of the Machine's production status, IBM's warranty terms apply.

IBM Warranty for Machines

IBM warrants that each Machine 1) is free from defects in materials and workmanship and 2) conforms to IBM's Official Published Specifications. The warranty period for a Machine is a specified, fixed period commencing on its Date of Installation. The date on your receipt is the Date of Installation, unless IBM or your reseller informs you otherwise.

During the warranty period IBM or your reseller, if authorized by IBM, will provide warranty service under the type of service designated for the Machine and will manage and install engineering changes that apply to the Machine.

1. Form Z125-4753

For IBM or your reseller to provide warranty service for a feature, conversion, or upgrade, IBM or your reseller may require that the Machine on which it is installed be 1) for certain Machines, the designated, serial-numbered Machine and 2) at an engineering-change level compatible with the feature, conversion, or upgrade. Many of these transactions involve the removal of parts and their return to IBM. You represent that all removed parts are genuine and unaltered. A part that replaces a removed part will assume the warranty service status of the replaced part.

If a Machine does not function as warranted during the warranty period, IBM or your reseller will repair it or replace it with one that is at least functionally equivalent, without charge. The replacement may not be new, but will be in good working order. If IBM or your reseller is unable to repair or replace the Machine, you may return it to your place of purchase and your money will be refunded.

If you transfer a Machine to another user, warranty service is available to that user for the remainder of the warranty period. You should give your proof of purchase and this Statement to that user. However, for Machines which have a lifetime warranty, this warranty is not transferable.

Warranty Service

To obtain warranty service for the Machine, you should contact your reseller or call IBM. In the United States, call IBM at **1-800-IBM-SERV (426-7378)**. In Canada, call IBM at **1-800-465-6666**. You might be required to present proof of purchase.

IBM or your reseller will provide certain types of repair and exchange service, either at your location or at IBM's or your reseller's service center, to restore a Machine to good working order.

When a type of service involves the exchange of a Machine or part, the item IBM or your reseller replaces becomes its property and the replacement becomes yours. You represent that all removed items are genuine and unaltered. The replacement may not be new, but will be in good working order and at least functionally equivalent to the item replaced. The replacement assumes the warranty service status of the replaced item. Before IBM or your reseller exchanges a Machine or part, you agree to remove all features, parts, options, alterations, and attachments not under warranty service. You also agree to ensure that the Machine is free of any legal obligations or restrictions that prevent its exchange.

You agree to:

1. Obtain authorization from the owner to have IBM or your reseller service a Machine that you do not own; and
2. Where applicable, before service is provided:
 - a. Follow the problem determination, problem analysis, and service request procedures that IBM or your reseller provide,
 - b. Secure all programs, data, and funds contained in a Machine, and
 - c. Inform IBM or your reseller of changes in a Machine's location.

IBM is responsible for loss of, or damage to, your Machine while it is 1) in IBM's possession or 2) in transit in those cases where IBM is responsible for the transportation charges.

Extent of Warranty

IBM does not warrant uninterrupted or error-free operation of a Machine.

The warranties might be voided by misuse, accident, modification, unsuitable physical or operating environment, improper maintenance by you, removal or alteration of Machine or parts identification labels, or failure caused by a product for which IBM is not responsible.

THESE WARRANTIES REPLACE ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THESE WARRANTIES GIVE YOU SPECIFIC LEGAL RIGHTS AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF EXPRESS OR IMPLIED WARRANTIES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU. IN THAT EVENT SUCH WARRANTIES ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. NO WARRANTIES APPLY AFTER THAT PERIOD.

Limitation of Liability

Circumstances might arise where, because of a default on IBM's part or other liability, you are entitled to recover damages from IBM. In each such instance, regardless of the basis on which you are entitled to claim damages from IBM (including fundamental breach, negligence, misrepresentation, or other contract or tort claim), IBM is liable only for:

1. Damages for bodily injury (including death) and damage to real property and tangible personal property; and
2. The amount of any other actual direct damages or loss, up to the greater of U.S. \$100,000 or the charges (if recurring, 12 months' charges apply) for the Machine that is the subject of the claim.

UNDER NO CIRCUMSTANCES IS IBM LIABLE FOR ANY OF THE FOLLOWING: 1) THIRD-PARTY CLAIMS AGAINST YOU FOR LOSSES OR DAMAGES (OTHER THAN THOSE UNDER THE FIRST ITEM LISTED ABOVE); 2) LOSS OF, OR DAMAGE TO, YOUR RECORDS OR DATA; OR 3) SPECIAL, INCIDENTAL, OR INDIRECT DAMAGES OR FOR ANY ECONOMIC CONSEQUENTIAL DAMAGES (INCLUDING LOST PROFITS OR SAVINGS), EVEN IF IBM OR YOUR RESELLER IS INFORMED OF THEIR POSSIBILITY. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE EXCLUSION OR LIMITATION MAY NOT APPLY TO YOU.

Glossary

This glossary includes terms for the Installation and User's Guide 2108 Model G07.

agent. A server program that receives virtual connections from the network manager (the client program) in an SNMP-TCP/IP network managing environment.

AIX. Advanced interactive executive.

AL_PA . Arbitrated loop physical address.

ARP. Address resolution protocol.

ASCII. American standard code for informational interchange.

BIOS. Basic input/output system.

bootline. An ASCII string of boot parameters.

Bs. Bus

CD. Change directory.

channel zoning. An access control method. Zones can be created between specific SAN Data Gateway interface channels (fibre channel and SCSI), as a means to either allow or restrict access between devices that are connected to these channels.

client. A functional unit that receives shared resources from a server unit on the computer network.

CTS. Clear to send.

DE. Differential ended.

DRAM. Dynamic random access memory.

DSR. Data set ready.

DTE. Data terminal equipment.

DTR. Data terminal ready.

dV. Device ID

EMI. Electromagnetic interference.

ESD. Electrostatic discharge.

fabric. Fibre channel switch and node connections in a fibre channel network.

FC. Fibre Channel.

Fn. Function number

FRU. Field replaceable unit.

FTP. File transfer protocol.

FW. Firmware.

GUI. Graphical user interface.

HBA. Host bus adapter.

heartbeat. The communication paths between the client-server components of the SAN Data Gateway are periodically checked to ensure that interconnection is constantly maintained.

HOP. A single transmission group connecting adjacent nodes.

HSM. Hierarchical storage management.

HTTP. Hypertext transfer protocol.

input/output. Pertaining to input or output activity, or both.

I/O. See also *input/output*.

IP. Internet protocol.

ITL. Initiator target LUN.

JMAPI. Java management application programming interface.

JRE. Java runtime environment.

LED. Light emitting diode.

LIC. Licensed internal code.

LIP. Loop initialization primitive.

LUN. Logical unit number.

LVD. Low voltage differential.

LW. Long wavelength.

MAC. Media access control.

MAC address. Media access control address.

MAP. Maintenance action plan.

Mbps. Megabits per second.

Mbitps. Megabytes per second.

MIB. Management information base.

n/c. Not connected or no connection.

PCI. Programmed control interruption.

PMC. PCI mezzanine card. See also *PCI*.

PPP. Point-to-point protocol.

RAID. Redundant array of inexpensive (or independent) disks.

RD. Receive data.

Registered clients. Clients that are actively monitoring the gateway.

RFI. Radio frequency interference.

RI. Ring indicator.

RID. Replacement identification, replacement identifier.

RMI. Remote method invocation.

router. A computer algorithm that determines the path of least resistance for traffic on a computer network.

RPC. Remote procedure call.

RTS. Request to send.

RTOS. Real time operating system.

SAN. Storage area network.

SC. Standard connector.

SCSI. Small computer system interface.

SCSI/TCP. Small computer system interface/transmission control protocol.

SDG Router. SAN Data Gateway router.

SDRAM. Static dynamic random access memory.

SE. Single-ended.

server. A functional hardware and software unit that delivers shared resources to workstation client units on a computer network.

SG. Signal ground.

SIMMS. Single in-line memory modules.

SNIA. Storage network industry association.

SNMP. Simple network management protocol.

SSA. Segment search argument.

subnet. A part of a network that is identified by a portion of an IP address.

SW. Short wavelength.

TCP. Transmission control protocol.

TR. Transmit data.

trap. An unprogrammed conditional jump to a specified address that is automatically activated by hardware.

U. Unit of measure for rack mounted equipment.

UID. Unique identifier.

VPD. Vital product data.

VPS. Virtual private storage area network.

WWN. Worldwide name.

X-on/X-off. Transmitter on, transmitter off.

Index

A

- about this book xix
- access control
 - options 58
 - setting up 21
 - single host access to the same target devices 57
- action
 - plans 81
 - reference table 88
- actions you must not take 217
- adding
 - a new user 46
 - devices to an existing redundant configuration 191
- additions, subsequent device, assignment of LUN numbers 182
- address map
 - creating identical persistent 190
 - database, compressing 184
 - database, customizing 184
 - modifying 185
 - using FTP, retrieving 184
- address numbering schemes 180
- administrative menu group 44
- administrator privilege 33
- After Repair Checklist 113
- agent
 - SNMP and SCSI/TCP 14
- agent (definition of) 221
- agreement for licensed internal code 216
- AIX (advanced interactive executive) 221
- AL_PA (arbitrated loop physical address) 221
- alternate SCSI IDs 20
 - changing 20
 - default 20
- application notes 179
- ARP 127
 - ARP (address resolution protocol) 221
 - arptabShow command 127
- ASCII (description of) 221
- assigning
 - a hard ID to a gateway fibre channel port 180
 - tape drives 182
- audience xix

B

- benefits and drawbacks of using soft IDs 180
- BIOS 24
 - BIOS (basic input/output system) 221
 - BIOS, Host adapter 192
 - BIOS Settings 192
- book, about this xix
- boot
 - mode commands 200
 - modes 196
- boot rom messages 205

- bootline
 - new 200
- Bs (bus) 221

C

- cable connections, null-modem 118
- cables
 - examining 97
 - optical, type 97
 - testing SCSI 95
- cd command 127
 - CD (change directory) 221
- changing
 - a password 45
 - the alternate SCSI ID 20
 - the command and control LUN 183
- channel
 - status for fibre channel interface 137
 - zoning settings, checking 90
- channel zoning
 - menu option 59
 - restrictions 139
- channel zoning (description of) 221
- check health, definition of 16
- checking
 - attached SCSI devices from the service port 91
 - channel zoning settings 90
 - connection with boot messages 105
 - event log 84
 - Fibre Channel initiator port mode 90
 - Fibre Channel port status 89
 - for problems on attached SCSI devices 83
 - Gateway product versions 83
 - multiple SCSI IDs 92
 - optical cable type 97
 - RS-232 cable 105
 - SCSI
 - bus termination 91
 - channel devices 90
 - service reference table 85
 - the host event log 84
 - versions of Gateway products 83
- checking heartbeats 76
- checklist
 - installation 25
 - post-installation 27
 - pre-installation 24
- clearReservation [devId] command 127
- cleHelp command 128
- cleShow [lun] command 128
- cleShowAll command 128
- client
 - install of JRE 29
 - system requirements 30
- client (description of) 221
- client-server model 14
- code 43 dump file, retrieving 199

- command and control LUN
 - changing 183
 - hiding 183
 - reassigning 183
 - removing 183
- command log for diagnostic purposes 128
- commands 123, 127, 195
 - arptabShow 127
 - boot mode 200
 - cd 127
 - clearReservation [devId] 127
 - cleHelp 128
 - cleShow [lun] 128
 - cleShowAll 128
 - csEtimeShow 128
 - dataScrubberDisable 128
 - dataScrubberEnable 128
 - diagBoot 128, 200
 - diagHelp 129
 - disableCC 129
 - elTest 130
 - enableCC 130
 - ethAddrSet 132
 - ethDisable 133
 - ethEnable 133
 - fcPortModeSet [port],[mode] 136
 - fcRestart [port] 137
 - fcShow [level] 137
 - fcShowDevs 139
 - fcShowNames 139
 - fcSlotTest 202
 - gateAddrGet 140
 - gateAddrSet 141
 - hardwareConfig 141
 - help 142
 - hlthChkHelp 143
 - hlthChkIntervalGet 143
 - hlthChkIntervalSet 143
 - hlthChkLevelGet 143
 - hlthChkLevelSet 144
 - hlthChkNow 144
 - hostNameSet 145
 - hostTypeShow 145
 - icmpstatShow 146
 - ifShow 146
 - inetstatShow 147
 - initializeBox 147
 - ipstatShow 147
 - licenseShow 147
 - loggerDump [number] 148
 - loggerDumpCurrent [level] 148
 - ls, ll 149
 - macShow 149
 - mapCompressDatabase 149
 - mapHelp 150
 - mapRebuildDatabase 150
 - mapShowDatabase 150
 - mapShowDevs 151
 - mapWinnowDatabase 152
 - mbufShow 152
 - netHelp 153

- commands (*continued*)
 - normalBoot 154, 200
 - reboot 154
 - reset 154
 - ridtag ["value"] 154
 - rm 155
 - rz 156
 - scsiAltIdGet [channel] 157
 - scsiAltIdSet [channel],[id] 157
 - scsiChannelTest(x,y) 157
 - scsiHostChanGet [channel] 158
 - scsiHostChanSet [channel],[mode] 158
 - scsiHostIdGet [channel] 158
 - scsiHostIdSet [channel],[id] 159
 - scsiRescan [channel] 159
 - scsiResetDisableGet [channel] 159
 - scsiResetDisableSet [channel],[mode] 160
 - scsiShow 160
 - scsiTermGet [channel] 161
 - scsiTermSet [channel],[termination] 162
 - setFcFrameSize [channel],[size] 162
 - setFcHardId [channel],[id] 163
 - setFcNormal 163
 - setFcScsiChanMask 163
 - setFcSplit 163
 - setHost [port] OS 163
 - setSnaCCLun [newLUN] 164
 - shellLock 165
 - showBox 165
 - snaVersion 166
 - sncFeatureEnable "licensekeysting" 166
 - snmpCommunitiesShow 166
 - snmpHelp 167
 - snmpReadCommunityAdd 167
 - snmpReadCommunityRemove 167
 - snmpTrapCommunitySet 168
 - snmpWriteCommunityAdd 168
 - snmpWriteCommunityRemove 168
 - sysConfigShow 169
 - sysVpdShow 169
 - sysVpdShowAll 169
 - sz [filename] 171
 - targets 171
 - tcpstatShow 171
 - trapDestAdd 172
 - trapDestRemove 172
 - trapDestShow 172
 - udpstatShow 173
 - uptime 173
 - userAdd 173
 - userDelete 173
 - userHelp 174
 - userList 173
 - version 174
 - xscsiAltIdGet [channel] 174
 - xscsiAltIdSet [channel],[id] 175
 - xscsiHostChanGet [channel] 175
 - xscsiHostChanSet [channel],[mode] 175
 - xscsiHostIdGet [channel] 176
 - xscsiHostIdSet [channel],[id] 176
 - xscsiResetDisableGet [channel] 176

- commands (*continued*)
 - xscsiResetDisableSet [channel], [mode] 176
 - xscsiTermGet [channel] 177
 - xscsiTermSet [channel], [termination] 177
- commands, diagnostic 201
 - diagBoot 200
 - elTest
 - loopback test 201
 - fcSlotTest 202
 - scsiChannelTest [x,y] 202
 - xscsiChannelTest [x,y] 203
- comparing
 - list versus physical devices 91
 - listed versus supported devices 91
- compliance statement
 - Korean Government Ministry of Communication (MOC) 216
- component check, quick 84
- compressing the address map database 184
- config directory 184
- configuration
 - how to 30
 - loading a SAN Data Gateway Module 56
 - SAN Data Gateway Module 16
 - saving the SAN Data Gateway Module 55
- configurations
 - preserving the SAN Data Gateway Module 22
- connecting
 - service terminal
 - hardware required 119
 - to the server 44
 - to the service port 117
- connection options, fibre channel port modes 21
- connection type options
 - loop preferred 22
 - point-to-point 22
- connection types
 - loop 22, 133
 - loop preferred 133
 - point to point 133
 - point to point preferred 133
- connections to the service port 118
- connector pin assignments, RS-232, DB-9 118
- controllers, ISP2200 21
- controls menu group, description of 57
- creating identical persistent address maps 190
- csEtimeShow command 128
- CTS (clear to send) 221
- customizing the address map database 184

D

- data mover
 - applications 58
 - license key 147
- data terminal equipment 117
- database
 - commands, persistent address map 150
 - compressing the address map 184
 - customizing the address map 184
- database full MAP 89
- dataScrubberDisable command 128
- dataScrubberEnable command 128
- DB-9 RS-232 connector pin assignments 118
- DE (differential ended) 221
- default gateway (information about) 141
- delete inactive entries from a database 152
- description
 - of the controls menu group 57
 - of the discover net 48
 - of the tools menu group 47
- description of Commands 127
- determining a problem 82
- device
 - access MAP 89
 - additions, subsequent, assignment of LUN numbers 182
 - isolating SCSI 95
 - mapping 64
 - specific mapping 182
 - type, incorrect 93
- devices
 - adding to an existing redundant configuration 191
 - understanding and modifying 181
- devices allowed
 - 256 for the SAN Data Gateway Module 182
- diagBoot command 128, 200
- diagHelp command 129
- diagnostic
 - command reference 195
 - mode
 - diagBoot 196
 - normal boot 196
 - of operation 196
- diagnostic, commands 201
- diagBoot 200
- elTest
 - loopback test 201
- fcSlotTest 202
- scsiChannelTest [x,y] 202
- xscsiChannelTest [x,y] 203
- diagnostic commands, reference 195
- diagnostic mode 154
- dimensions, SAN Data Gateway Module 10
- directory ffs0:mt 200
- disableCC [option number] 129
- discover net, description of 48
- discovery of devices, initial 181
- displaying
 - a list of the command log event facility
 - commands 128
 - alternate ID numbers for a specified channel 157
 - health check commands 143
 - vital product data 169
- DRAM (dynamic random access memory) 221
- DSR (data set ready) 221
- DTE (data terminal equipment) 221
- DTR (data terminal ready) 221
- dump, event log 199
- dV (device ID) 221

E

- edition notice ii
- electronic emission
 - statement 214
- eliminating inactive entries
 - from a database 152
- elTest command 130
- EMI (electromagnetic interference) 221
- enableCC command 130
- entering diagnostic mode, diagBoot 196
- entry, route 155
- envMonRangeShow 132
- envMonShow 130
- error codes
 - post 207
- ESD (electrostatic discharge) 221
- Ethernet
 - commands 132
 - ethAddrSet 132
 - ethDisable 133
 - ethEnable 133
 - Ethernet test 111
 - loopback test 130, 201
 - MAP 101
 - network commands 153
- event
 - assigned viewing levels 74
 - code 42 89
 - code or obvious symptom 82
 - codes, meaning of 74
 - log
 - checking 84
 - dump 199
 - logging 16, 74
 - remote notification 73
 - viewing 74
 - viewing levels 148
- event log
 - description of 51
 - saving 53
 - viewing 52
- event trap
 - receiving 54
 - setting the threshold 54
- events and traps 75
- examining
 - cables 97
 - SCSI cables 93
 - SCSI connectors 94
- extent of warranty 220

F

- fabric (definition of) 221
- FC (Fibre Channel) 221
- fc commands
 - diagnostic
 - fcSlotTest 202
 - fcConnTypeGet [port] 133
 - fcConnTypeSet [port],[connection] 134

- fc commands (*continued*)
 - fcFibreSpeedGet 134
 - fcFibreSpeedSet 134
 - fcGbicShow 135
 - fcPortModeGet [port] 135
 - fcPortModeSet [port],[mode] 136
 - fcRestart [port] 137
 - fcShow [level] 137
 - fcShowDevs 139
 - fcShowDevs command display 139
 - fcShowNames 139
 - fcTxDisable 140
 - fcTxEnable 140
 - setFcFrameSize [channel], [size] 162
 - setFcHardId [channel], [id] 163
 - setFcNorma 163
 - setFcScsiChanMask
 - [channel],[scsiChannel],[allow] 163
 - setFcSplit 163
- features
 - simple network management protocol 15
- ffs0:mt directory 200
- Fibre Channel 110
 - address numbering schemes 180
 - assigning a hard ID to a Gateway Fibre Channel port 180
 - benefits and drawbacks
 - hard ID 180
 - soft IDs 180
 - cable, replacing 99
 - connections, Verify 96
 - host adapter, replacing 99
 - host versions 83
 - initiator port mode, checking 90
 - loop addressing 179
 - description of 180
 - loop ID assignments 180
 - loopback test 97
 - MAP 96
 - optical cable, testing 98
 - parameters 63
 - frame size 64
 - settings 63
 - planning for persistence 180
 - port modes and connection options 21
 - port status, checking 89
 - setting ID from service port 181
 - setting the ID port 181
 - switch 99
 - tests 110
- file
 - persistent map 200
- file menu 36
- file removal 155
- files, route 155
- firmware
 - updating the SAN Data Gateway Module 9
- flash file system 127, 184
- Fn (function number) 221
- front panel view of the SAN Data Gateway Module 43
- FRU (field replaceable unit) 221

FTP (file transfer protocol) 221
FW (firmware) 221

G

gateAddrGet command 140
gateAddrSet command 141
Gateway, remove and replace 109
 network setup 115
 product versions, Checking 83
 remove 109
 replace 109
 test, Ethernet 111
 test, SCSI ports 111
 tests, Fibre Channel 110
 updating 112
 verify new 110
GBIC, Remove and Replace 108
 Remove 108
 Replace 108
 Test 97
gray menu options 33
grouped by function, commands 123
GUI (graphical user interface) 221
guidelines, startup sequence 28

H

Handling Electrostatic Discharge Sensitive Parts 108
hardware
 required to connect the service terminal 119
hardwareConfig command 141
HBA (host bus adapter) 221
health check
 commands, displaying 143
 definition of 16
 determining the operational state of an Gateway 76
 device availability 78
 for testing controllers 50
 for testing target devices 50
 interface 78
 interval 79
 interval procedure 198
 level control 78
 level control procedure 198
 not checking 78
 performance impact of 79
 performing 84
 periodic 197
 procedure 197
 pull-down menu 50
 checking SAN Data Gateway Module
 heartbeat 51
 performing health check 50
 setting health check interval 50
 setting health check level 51
SCSI 94
setting up 77
simple device 78
system 78

heartbeat
 checks 76
 description of 16
help command 142
hiding the command and control LUN 183
hierarchical tree, viewing 38
hlthChkHelp command 143
hlthChkIntervalGet command 143
hlthChkIntervalSet command 143
hlthChkLevelGet command 143
hlthChkLevelSet command 144
hlthChkNow command 144
HOP (definition of) 221
hop count 182
host
 add host 144
 bus adapters (HBAs)
 setup 28
 command 144
 delete host 144
 event log, checking 84
 Fibre Channel, versions 83
 file contents 144
 host list 145
 hostAdd 145
 table 144
 utility 144
hostNameSet command 145
hostTypeShow command 145
how to
 add a new user 46
 change the password 45
 connect the SAN Data Gateway Module 49
 disconnect the SAN Data Gateway Module 49
 disconnect 49
 identify the SAN Data Gateway Module 71
 log on 45
 prevent host from accessing the same target 57
 remove a user 46
 restart the SAN Data Gateway Module 70
HSM (hierarchical storage management) 221
HTTP (hypertext transfer protocol) 221
HyperTerminal 185

I

I/O (input/output) 221
IBM
 agreement for licensed internal code 216
 license agreement for machine code 217
 StorWatch Specialist
 installation 29
 warranty for machines 218
icmpstatShow command 146
ID, changing the alternate SCSI 20
IDs (hard versus soft) 180
IDs, SCSI 92
ifShow command 146
inactive entries, deleting from a database 152
incorrect device type 93
indicators, LED 9

- inetstatShow command 147
- initial discovery of devices 181
- initializeBox command 147
- initiator (port modes) 21
- Inspecting LED Status Indicators 82
- installation
 - checklist 25
 - IBM StorWatch Specialist 29
 - prerequisites 28
 - SAN Data Gateway Module 23
- insufficient user privileges 33
- internal
 - code, agreement 216
- introduction
 - SAN Data Gateway Module 1
 - to setting up a redundant dual SCSI configuration 188
 - to the IBM StorWatch Specialist 14
- IP (internet protocol) 221
- ipstatShow command 147
- isolating
 - SCSI devices 95
- ISP2200 initiator port mode options
 - private 22
 - public 21
- ITL (initiator target LUN) 221

J

- JMAPI (Java management application programming interface) 221
- JRE (Java runtime environment) 221

K

- knowledge-base articles, relevant 191
- Korean Government Ministry of Communication (MOC) Statement 216

L

- LED (light emitting diode) 221
- LED indicators
 - amber, meaning of 10
 - description of 9
 - flashing green, meaning of 9
 - green activity 9
 - patterns 100
 - solid green, meaning of 10
- levels, event viewing 148
- liability, limit of 220
- LIC (licensed internal code) 221
- lic initialization messages 205
- license agreement for machine code, IBM 217
- licensed internal code, agreement 216
- licenseShow command 147
- limitation of liability 220
- limited warranty statement (SOLW) 218
- LIP (loop initialization primitive) 221
- list
 - versus physical devices 91

- list of shell commands 142
- log
 - event, checking 84
 - event, dump 199
- log on
 - to server 34
- loggerDump [number] command 148
- loggerDump display 148
- loggerDumpCurrent [level] command 148
- logging on
 - how to 45
- logging on to the server 34
- loop
 - ID assignment 180
 - ID order 182
 - option 22
 - preferred option 22
- loopback
 - test, Fibre Channel 97
 - test, SCSI 94
- ls, ll command 149
- LUNs (logical unit number) 221
- LVD (low voltage differential) 221
- LW (long wavelength) 221

M

- MAC (media access control) 221
- MAC address (media access control address) 221
- machine code, IBM license agreement for 217
- macShow command 149
- maintaining the SAN Data Gateway Module 73
- manual health check 197
- MAP
 - database full 89
 - device access 89
- MAP (maintenance action plan) 221
- mapCompressDatabase command 149
- mapHelp command 150
- mapping
 - device specific 182
 - discovery of the SAN Data Gateway Module 181
- mapRebuildDatabase command 150
- maps
 - address, creating identical persistent 190
 - SCSI 90
- MAPs
 - Ethernet 101
 - Fibre Channel 96
 - Gateway MAP 99
 - maintenance action plans 81
 - MAP, Gateway 99
 - power 101
 - SAN Appliance Module web site 82
 - service port 105
 - temperature 100
- mapShowDatabase command 150
- mapShowDevs command 151
- mapWinnowDatabase command 152
- Mbps (megabits per second) 221
- MBps (megabytes per second) 221

- mbufShow command 152
- menu group, administrative 44
- menu options, gray 33
- menus to view the SAN Data Gateway Module and devices 33
- messages
 - boot rom 205
 - connection with boot messages 105
 - final startup 206
 - lic 205
 - startup, reference 205
- MIB (management information base) 221
- mode options, port 21
- modes, boot 196
- modifying
 - devices, understanding 181
 - the address map 185
 - the SNMP community strings 60
- multiple SCSI IDs 92

N

- n/c (not connected or no connection) 221
- netHelp command 153
- NetTerm 185
- network discovery 16
- network setup, Gateway 115
- new bootline 200
- new user, how to add 46
- normal
 - mode, restoring 196
 - mode of operation 196
 - operating conditions 154
 - operation 200
- normalBoot command 154, 200
- notes, application 179
- notices 213
- null-modem cable connections 118

O

- observing
 - operational LED patterns 100
- obvious symptom or event code 82
- operating
 - conditions, normal 154
 - specifications
 - electrical 10
 - environmental 10
 - physical 10
- operational LED patterns 100
- options, access 58
- options, port mode 21

P

- Parts, Handling Electrostatic Discharge Sensitive 108
- password
 - how to change 44, 45
- PCI (programmed control interruption) 221
- performance impact of health checks 79

- performance impact of health checks procedure 198
- performing
 - a health check 84
- periodic health checks 197
- persistent address map database commands 150
- persistent map file 200
- physical
 - devices 91
- pin connections for the service port 118
- planning for persistence 180
- PMC (PCI mezzanine card) 221
- point-to-point
 - option 22
- port modes 21
 - initiator 21
 - target 21
 - target and initiator 21
- port status, Fibre Channel 89
- post error codes 207
- post-installation checklist 27
- power
 - MAP 101
- power consumption ratings 10
- PPP (point-to-point protocol) 221
- pre-installation checklist 24
- preserving the SAN Data Gateway Module
 - configurations 22
- privilege, user 33
- problem determination 82
- procedures
 - health check
 - function 197
 - interval 198
 - level control 198
 - manual health check 197
 - performance impact of health checks 198
 - periodic health checks 197
 - setting up the health check 197
- Procedures, Removal and Replacement 107
- product versions, Checking Gateway 83
- production status 218
- protocol sockets for the Ethernet network 147
- publications, related xix

Q

- quick component check 84

R

- RAID (redundant array of inexpensive (or independent) disks) 222
- ratings, power consumption 10
- reassigning the command and control LUN 183
- reboot command 154
- receive (receive data) 222
- redundant dual SCSI configuration 179
- reference
 - diagnostic 195
 - startup 205
 - table reference, action 88

- registered clients 75
- registered clients (clients that are actively monitoring the gateway) 222
- related publications xix
- relevant knowledge-base articles 191
- remote event notification 73
- Removal and Replacement Procedures 107
- remove and replace Gateway 109
 - remove Gateway 109
 - verify new Gateway 110
- Remove and Replace GBIC 108
 - Remove 108
 - Replace 108
- removing
 - a file 155
 - a user 46
 - the command and control LUN 183
- Repair Checklist, After 113
- Replace Gateway, Remove and 109
 - replace Gateway 109
 - SCSI ports, test 111
- Replacement Procedures, Removal and 107
- replacing
 - Fibre Channel
 - cable 99
 - host adapter or Fibre Channel switch 99
- required hardware 119
- reset command 154
- resetting a SCSI channel 62
- Resolving temperature warning or alarm 100
- restarting the SAN Data Gateway Module 70
- restoring
 - normal boot 196
 - normal mode 196
 - SCSI setup 96
- retrieving the address map
 - using FTP 184
 - using Zmodem 185
- retrieving the code 43 dump file 199
- RFI (radio frequency interference) 222
- RI (ring indicator) 222
- RID (replacement identification, replacement identifier) 222
- ridtag ["value"] command 154
- rm command 155
- RMI (remote method invocation) 222
- route commands 155
 - add route 155
 - delete route 156
 - listing the routes 156
 - route, delete 156
- route utilities 155
- router (definition of) 222
- RPC (remote procedure call) 222
- RS-232 cable, checking 105
- RS-232 connector pin assignments, DB-9 118
- RS-232C data terminal equipment (DTE) port 117
- RST (request to send) 222
- RTOS (real time operating system) 222
- rz command 156

S

- safety xv
- SAN
 - access control 16
- SAN (storage area network) 222
- SAN data Gateway module
 - checking the heartbeat 51
 - configuration 16
 - description 1
 - discovery and mapping 181
 - event logging 16
 - Fibre Channel 2
 - connectivity 2
 - point to point 2
 - front panel view 43
 - health checks 16
 - heartbeats 16
 - how to 70
 - connect 49
 - identify 71
 - restart 70
 - update firmware 70
 - installing 23
 - introduction 1
 - LED indicators, meaning of 9, 10
 - loading a configuration 56
 - network discovery 16
 - operating specifications 10
 - overview 2
 - physical dimensions 10
 - preserving the configurations 22
 - refresh view 43
 - saved views 16
 - SCSI 90
 - security 16
 - shutting down 154
 - software updates 16
 - updating the firmware 9
 - views 16
 - web site xix
- SC (standard connector) 222
- SCSI
 - bus termination 91
 - channel 190
 - reset on start up 190
 - channel devices, checking 90
 - channel parameters 61
 - channel mode 61
 - host ID 61
 - identify channel 61
 - max IDs per bus 61
 - max IDs per ID 61
 - max speed 61
 - rescan SCSI bus 61
 - reset 62
 - termination 62
 - channels and attached devices 160
 - check attached devices from service port 91
 - commands 202
 - scsiAltIdGet [channel] 157
 - scsiAltIdSet [channel],[id] 157

SCSI (*continued*)

- commands (*continued*)
 - scsiChannelTest [x,y] 202
 - scsiChannelTest(x,y) 157
 - scsiHostChanGet [channel] 158
 - scsiHostChanSet [channel], [mode] 158
 - scsiHostIdGet [channel] 158
 - scsiHostIdSet [channel], [id] 159
 - scsiRescan [channel] 159
 - scsiResetDisableGet [channel] 159
 - scsiResetDisableSet [channel], [mode] 160
 - scsiShow 160
 - scsiTermGet [channel] 161
 - scsiTermSet [channel], [termination] 162
 - xscsiChannelTest (x,y) 203
- configuration, setting up a redundant dual 188
- connectors, examining 94
- device
 - from the service port, checking 91
 - problems 83
- diagnostic commands 202
 - scsiChannelTest [x,y] 202
 - xscsiChannelTest (x,y) 203
- examining cables 93
- health check 94
- ID
 - alternate 20
 - assignments, recommended 189
 - changing the alternate 20
 - default alternate 20
 - of SAN Data Gateway Modules and target devices, setting 188
- isolating devices 95
- loopback test 94
- maps 90
- multiple IDs 92
- restoring setup 96
- SAN Data Gateway Module SCSI 90
- testing cables 95
- SCSI (small computer system interface) 222
- SDG router 222
- SDRAM (static dynamic random access memory) 222
- SE (single-ended) 222
- security for the SAN Data Gateway Module 16
- selecting an access control option 58
- send operation using Zmodem option 187
- sending the device map back to the SAN Data Gateway Module 187
- server
 - as a Java component 14
 - how to connect to 44
 - system requirements 30
- server (definition of) 222
- service
 - reference table, checking 85
 - terminal, connecting 119
- service port
 - command reference 123
 - connections 118
 - MAP 105
 - pin-outs 118
- service port (*continued*)
 - using 117
- setHost [port] OS command 163
- setSnaCCLun [newLUN] command 164
- setting
 - advanced SCSI channel controls 62
 - SCSI IDs of SAN Data Gateway Modules and target devices 188
 - the ID from the service port 181
- setting up
 - a redundant dual SCSI configuration 188
 - access control 21
 - the health check 77
 - the health check procedure 197
- settings, fibre channel 63
- setup
 - host bus adapters (HBAs) 28
- setup, Gateway network 115
- SG (signal ground) 222
- shell commands, listing of 142
- shell interface 123
- shellLock command 165
- showBox command 165
- shutting down the SAN data Gateway module 154
- SIMMS (single in-line memory modules) 222
- simple network management protocol (SNMP)
 - community support 15
 - modifying community strings 60
 - standard SNMP v1 protocol 15
 - using to communicate with agent 14
- snaVersion command 166
- sncFeatureEnable "licensekeystring" command 166
- SNIA (storage network industry association) 222
- SNMP
 - community strings 60
 - community support 15
 - simple network management protocol 14
 - standards 15
- SNMP (simple network management protocol) 222
- snmpCommunitiesShow command 166
- snmpHelp command 167
- snmpReadCommunityAdd command 167
- snmpReadCommunityRemove command 167
- snmpTrapCommunitySet command 168
- snmpWriteCommunityAdd command 168
- snmpWriteCommunityRemove command 168
- software
 - updates 16
- SOLW (limited warranty statement) 218
- special
 - diagnostic mode 128, 200
 - procedures 197
 - procedures for advanced users 179
- special procedures
 - event log dump 199
 - health check 197
 - health check interval 198
 - health check level control 198
 - manual health check 197
 - performance impact of health checks 198
 - periodic health checks 197

- special procedures *(continued)*
 - retrieving the code 43 dump file 199
 - setting up the health check 197
- specific mapping, device 182
- SSA (segment search argument) 222
- start MAP 82
- starting the StorWatch Specialist 34
- startup
 - how to 30
 - message reference 205
 - sequence guidelines 28
- startup messages, final 206
- statement
 - electronic emission 214
 - Korean government ministry of communication (MOC) 216
 - of limited warranty 218
- StorWatch Specialist
 - client-server model 14
 - agent 14
 - client 15
 - server 14
 - connect to server 34
 - file menu 36
 - exit 37
 - opening a previous view 37
 - save current view 36
 - save current view as 36
 - installation
 - client 29
 - installing, Windows NT 30
 - requirements, Windows NT 29
 - server 29
 - introduction 14
 - starting 34
 - using 33
 - view menu
 - tree view 38
 - viewing 33
- subnet (definition of) 222
- subsequent device additions, assignment of LUN numbers 182
- Subsystem, Temperature
 - notification 100
- supportDump 168
- supported
 - devices 91
- SW (short wavelength) 222
- symptoms, obvious, or event code 82
- sysConfigShow command 169
- system requirements
 - client 30
 - server 30
- sysVpdShow command 169
- sysVpdShowAll command 169
- sz "filename" command 171

T

- table
 - reference action 88

- table *(continued)*
 - service reference 85
- tape drives 182
- target
 - and initiator 21
 - command 171
 - port modes 21
- TCP (transmission control protocol) 222
- tcpstatShow command 171
- telnet 115
- temperature
 - MAP 100
 - warning or alarm 100
- Temperature Subsystem
 - problems 100
- terminal, service, connecting 119
- termination
 - for SCSI busses 91
- Terra Term 185
- Test GBIC 97
- testing
 - Fibre Channel optical cable 98
 - SCSI cables 95
- tests, diagnostic
 - elTest 201
 - fcSlotTest [x] 202
 - scsiChannelTest [x,y] 202
 - xscsiChannelTest [x,y] 203
- tools menu group, description of 47
- TR (transmit data) 222
- trademarks 214
- trap (definition of) 222
- trap symbol 75
- trapDestAdd command 172
- trapDestRemove command 172
- trapDestShow command 172
- traps and events 75
- types of connections 133

U

- U (unit of measure for rack mounted equipment) 222
- udpstatShow command 173
- UID (unique identifier) 222
- understanding
 - and modifying devices 181
- updates
 - software 16
- updating
 - firmware, selecting 70
- updating Gateway 112
- uptime command 173
- user privilege 33
- user privileges, insufficient 33
- userAdd command 173
- userDelete command 173
- userHelp command 174
- userList command 173
- using
 - FTP 184
 - WordPad 185

V

- Verify
 - Fibre Channel connections 96
- version command 174
- versions, Checking Gateway product 83
- view menu 38
- viewing
 - the event 74
 - the hierarchical tree 38
- views 16
- views, saved 16
- VPD (vital product data) 222
- VPS (description of) 222

W

- warranty
 - extent of 220
 - for IBM machines 218
 - service
 - IBM machines 219
 - phone number 219
 - statement, limited 218
- web site xix
 - Fibre Channel host bus adapters 83
 - required updates 83
 - SAN Appliance Module 82
 - supported SAN Appliance Module host platforms 83
- who should use this book xix
- WordPad, using 185
- WWN (world-wide name) 222

X

- X-on/X-off (transmitter on, transmitter off) 222
- xscsiAltIdGet [channel] command 174
- xscsiAltIdSet [channel], [id] command 175
- xscsiChannelTest (x,y) command 203
- xscsiHostChanGet [channel] command 175
- xscsiHostChanSet [channel], [mode] command 175
- xscsiHostIdGet [channel] command 176
- xscsiHostIdSet [channel], [id] command 176
- xscsiResetDisableGet [channel] command 176
- xscsiResetDisableSet [channel], [mode] command 176
- xscsiTermGet [channel] command 177
- xscsiTermSet [channel], [termination] command 177

Z

- Zmodem, retrieving the address map 185
- zoning
 - channel 59

Readers' comments—we would like to hear from you

IBM Storage Area Network Data Gateway Module
Setup, Operator, and Service Guide

Publication No. GA32-0436-01

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Complete	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to find	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Easy to understand	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Well organized	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Applicable to your tasks	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? ☐ Yes ☐ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape



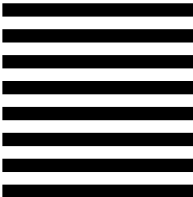
NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department GZW
9032 S Rita Road
Tucson, AZ 85775-4706



Fold and Tape

Please do not staple

Fold and Tape

Cut or Fold
Along Line



Part Number: 19P4544



Printed in the United States of America
on recycled paper containing 10%
recovered post-consumer fiber.

GA32-0436-01



(1P) P/N: 19P4544



Spine information:



IBM Storage Area Network Data
Gateway Module

**Storage Area Network Data Gateway Module: Setup,
Operator, and Service Guide**