



RPC-693xx Series Setup Guide

P/N 83-00004641-12-02
Revision A
November 2011

Copyright Protected Material 2011. The material in this document is for information only and is subject to change without notice. While reasonable efforts have been made in the preparation of this document to assure its accuracy, changes in the product design can be made without reservation and without notification to its users.



Adobe PostScript

Contents

Preface	11
Intended audience	11
Prerequisites.....	11
Related documentation	11
Document conventions and symbols.....	12
1 Components	13
12-drive enclosure front panel components	13
12-drive enclosure disk drive slot numbers	13
Rear panel views — controller module(s).....	13
693x6 controller module face plate — hybrid (FC/iSCSI).....	13
693x1 controller module face plate — Fibre Channel.....	14
693x4 controller module face plate — Serial Attached SCSI.....	14
693x5 controller module face plate — 10GbE Internet SCSI.....	14
693x6 controller enclosure rear panel components.....	15
693x1 controller enclosure rear panel components.....	16
693x4 controller enclosure rear panel components.....	16
693x5 controller enclosure rear panel components.....	17
693x2 enclosure rear panel components.....	17
695x2/697x2 12-drive enclosure rear panel components	17
Cache	18
CompactFlash	18
Super-capacitor pack.....	18
2 Installing the enclosures	19
Installation checklist.....	19
Connecting controller and drive enclosures.....	19
Cable requirements for drive enclosures	20
Testing enclosure connections.....	27
Powering on/powering off	27
AC PSU.....	28
DC and AC PSUs with power switch	29
Power Cords	29
AC model	29
DC model.....	29
Power cycle	30
3 Connecting hosts	31
Host system requirements	31
Cabling considerations.....	31
Connecting the enclosure to hosts	31
FC host ports	32
SAS host ports	32
iSCSI host ports (1Gb)	32
iSCSI host ports (10GbE)	32
Connecting direct attach configurations.....	32
Single-controller configurations.....	34
One server/one HBA/single path	34
Dual-controller configurations	35
One server/one HBA/dual path	35
Two servers/one HBA per server/dual path.....	36
Four servers/one HBA per server/dual path.....	36
Connecting switch attach configurations	37
Multiple servers/multiple switches	37
Connecting a management host on the network.....	38
Connecting two storage systems to replicate volumes	38
Single-controller configuration	40

One server/one switch/two storage systems	40
Dual-controller configuration	41
Two servers/one switch/two storage systems	41
Multiple servers/SAN fabric/Ethernet WAN/two storage systems	42
Multiple servers/FC SAN fabric/two storage systems	43
Updating firmware	43
Obtaining IP values	43
Setting network port IP addresses using DHCP	43
Setting network port IP addresses using the CLI	44
4 Basic operation	47
Accessing RAIDar	47
Configuring and provisioning the storage system	47
5 Troubleshooting	49
USB CLI port connection	49
Fault isolation methodology	49
Gather fault information.	49
Determine where the fault is occurring	49
Review the event logs	49
Isolate the fault	50
If the enclosure does not initialize	50
Correcting enclosure IDs.	50
Diagnostic steps	50
Is the front panel Fault/Service Required LED amber?	50
Is the controller back panel FRU OK LED off?	51
Is the controller back panel Fault/Service Required LED amber?	51
Are both disk drive module LEDs off?	51
Is the disk drive module Power/Activity/Fault LED blinking amber?	51
Is a connected host port's Host Link Status LED off?	52
Is a connected port's Expansion Port Status LED off?	52
Is a connected port's Network Port link status LED off?	52
Is the power supply's Input Power Source LED off?	53
Is the drive enclosure rear panel OK LED off?	53
Is the drive enclosure Fault/Service Required LED amber?	53
Controller failure in a single-controller configuration	54
If the controller has failed or does not start, is the Cache Status LED on/blinking?	54
Transporting cache via professional services	55
Isolating a host-side connection fault.	55
Host-side connection troubleshooting featuring FC or 10GbE iSCSI host ports	55
Host-side connection troubleshooting featuring SAS or iSCSI host ports	56
Isolating a controller module expansion port connection fault.	57
Isolating AssuredRemote replication faults	58
Cabling for replication	58
Replication setup and verification	58
Diagnostic steps for replication setup.	59
Can you access the AssuredRemote feature?	59
Can you view information about remote links?	59
Can you create a replication set, or select an existing one?	59
Can you replicate a volume?	60
Can you view a replication image?	61
Can you view remote systems?	61
Resolving voltage and temperature warnings.	61
Sensor locations	62
Power supply sensors	62
Cooling fan sensors.	62
Temperature sensors.	62
Power supply module voltage sensors	63
A LED descriptions	65
12-drive enclosure front panel LEDs	65

Disk drive LEDs	65
693x6 rear panel LEDs	66
693x1 rear panel LEDs	67
693x4 rear panel LEDs	68
693x5 rear panel LEDs	69
693x2 drive enclosure rear panel LEDs	70
695x2/697x2 12-drive enclosure rear panel LEDs	71
Power supply LEDs	72
B Environmental requirements and specifications.	73
Safety requirements	73
Site requirements and guidelines	73
Site wiring and AC power requirements	73
Site wiring and DC power requirements	73
Weight and placement guidelines	74
Electrical guidelines	74
Ventilation requirements	74
Cabling requirements	75
Management host requirements	75
Physical requirements	75
Environmental requirements	76
Electrical requirements	76
Site wiring and power requirements	76
Power cord requirements	76
C Electrostatic discharge	79
Preventing electrostatic discharge	79
Grounding methods to prevent electrostatic discharge	79
D USB device connection	81
Rear panel USB ports	81
USB CLI port	81
Emulated serial port	81
Supported host applications	82
Command Line Interface	82
Device driver/special operation mode	82
Microsoft Windows	82
Linux	82
Setting parameters for the device driver	82
Index	83

Figures

1	CompactFlash	18
2	Cabling connections between a single-controller enclosure and one drive enclosure	21
3	Cabling connections between a dual-controller enclosure and a single drive enclosure	22
4	Non-fault-tolerant cabling between a dual-controller enclosure and three LFF drive enclosures	22
5	Fault-tolerant cabling between a dual-controller enclosure and four LFF drive enclosures	23
6	Fault-tolerant cabling between a dual-controller enclosure and three drive enclosures	24
7	Fault-tolerant cabling between a dual-controller enclosure and four drive enclosures	25
8	Fault-tolerant cabling between a dual-controller enclosure and seven drive enclosures	26
9	AC PSU	28
10	AC power cord	28
11	DC and AC PSUs with power switch	29
12	DC power cable featuring D-shell and lug connectors	29
13	Connecting hosts – one server/one HBA/single path	34
14	Connecting hosts – one server/one HBA/dual path	35
15	Connecting hosts – two servers/one HBA per server/dual path	36
16	Connecting hosts – four servers/one HBA per server/dual path	37
17	Connecting hosts – switch attach: two servers/two switches	38
18	Connecting two storage systems for replication – single-controller module	40
19	Connecting two storage systems for replication – dual-controller module	41
20	Connecting two systems for AssuredRemote – 693x6 example	42
21	Connecting two systems for AssuredRemote – 693x1 example	43
22	Connecting an RS-232 cable to the CLI port	45
23	Connecting a USB cable to the CLI port	45
24	USB device connection – CLI port	81

Tables

1	Document conventions	12
2	Installation checklist	19
3	SAS cable type requirements	21
4	Maximum cable lengths for 850nm Fibre Channel SFP transceivers	33
5	Terminal emulator display settings	45
6	Terminal emulator connection settings	45
7	Diagnostics LED status – Front panel Fault/Service Required	50
8	Diagnostics LED status – Rear panel FRU OK	51
9	Diagnostics LED status – Rear panel Fault/Service Required	51
10	Diagnostics LED status – Disk drives	51
11	Diagnostics LED status – Disk drive Power/Activity/Fault	51
12	Diagnostics LED status – Rear panel Host Link Status	52
13	Diagnostics LED status – Rear panel Expansion Port Status	52
14	Diagnostics LED status – Rear panel Network Port Link Status	52
15	Diagnostics LED status – Power supply Input Power Source	53
16	Diagnostics LED status – Drive enclosure rear panel OK	53
17	Diagnostics LED status – Drive enclosure front panel Fault/Service Required	53
18	Diagnostics LED status – Rear panel Cache Status	54
19	Diagnostics for replication setup – Accessing AssuredRemote feature	59
20	Diagnostics for replication setup – Viewing information about remote links	59
21	Diagnostics for replication setup – Creating or selecting a replication set	59
22	Diagnostics for replication setup – Replicating a volume	60
23	Diagnostics for replication setup – Viewing a replication image	61
24	Diagnostics for replication setup – Viewing a remote system	61
25	Power supply sensors	62
26	Cooling fan sensor descriptions	62
27	Controller module temperature sensors	63
28	Power supply temperature sensors	63
29	Voltage sensor descriptions	63
30	LEDs – 3U12 enclosure front panel	65
32	LEDs – 693x6 rear panel	66
33	LEDs – 693x1 rear panel	67
34	LEDs – 693x4 rear panel	68
35	LEDs – 693x5 rear panel	69
36	LEDs – 693x2 rear panel	70
37	LEDs – 695x2/697x2 rear panel	71
38	LEDs – power supply units – rear panel	72
39	Power requirements - AC Input	73
40	Power requirements - DC Input	73
41	Rackmount enclosure dimensions	76
42	Rackmount enclosure weights	76
43	Operating environmental specifications	76
44	Supported terminal emulator applications	82
45	USB vendor and product identification codes	82

Preface

This guide provides information about the Phoenix™ RPC12 series storage management products:

Hybrid FC/iSCSI Controller Enclosure:

- 693x6

Fibre Channel Controller Enclosure:

- 693x1

Serial Attached SCSI Controller Enclosure:

- 693x4

Internet SCSI (10GbE) Controller Enclosure:

- 693x5

RPC12 series enclosures are MIL-STD-compliant — supporting large form factor (LFF 12-disk) 3U drive enclosures — using either AC or DC power supplies.

 **NOTE:** See [Components](#) on page 13 for details regarding enclosure components.

Intended audience

This guide is intended for use by system administrators and technicians who are experienced with the following:

- Direct attach storage (DAS) or storage area network (SAN) management
- Network administration
- Network installation
- Storage system installation and configuration

Prerequisites

Prerequisites for installing and configuring this product include familiarity with:

- Servers and computer networks
- Fibre Channel (FC), Serial Attached SCSI (SAS), Internet SCSI (iSCSI), and Ethernet protocols

Related documentation

In addition to this guide, please refer to other documents for this product line:

- Phoenix RPC12 series RAIDar User Guide
- Phoenix RPC12 series CLI Reference Guide
- Phoenix Event Descriptions Reference Guide

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Navy blue text	Cross-reference links and e-mail addresses
<code>Navy blue text</code>	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

 **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

 **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

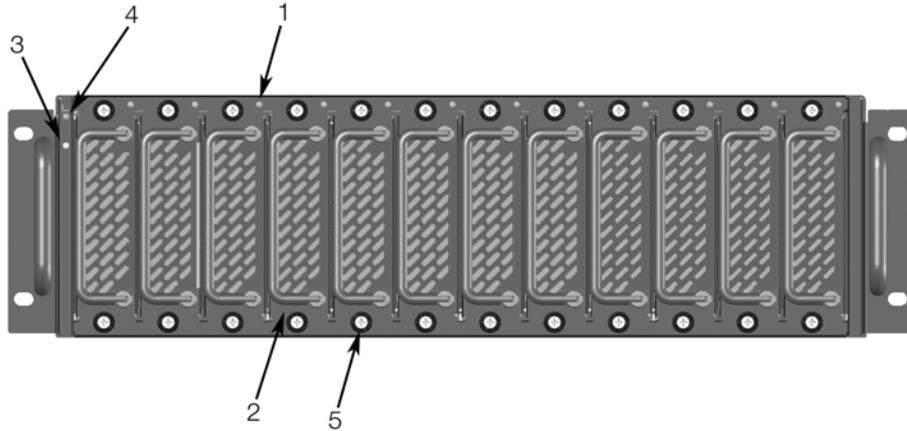
 **IMPORTANT:** Provides clarifying information or specific instructions.

 **NOTE:** Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

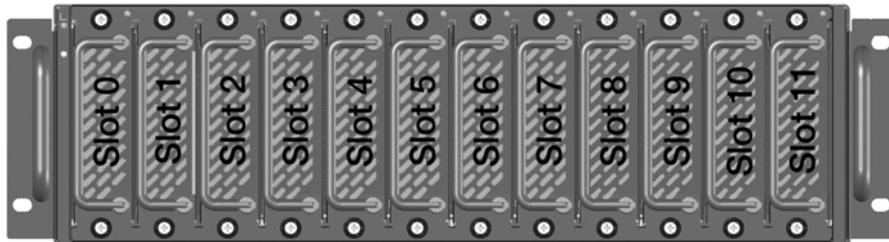
1 Components

12-drive enclosure front panel components



- 1 Disk drive status LED: Power/Activity/Fault
- 2 3.5" disk or drive blank (typical 12 slots)
- 3 Enclosure status LED: Fault/Service Required
- 4 Enclosure status LED: Power Indicator
- 5 Disk drive lock/thumb-screw

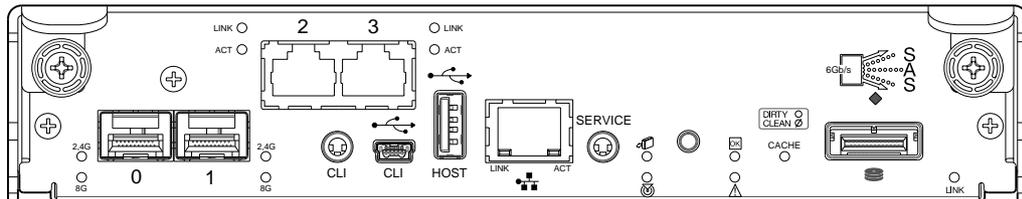
12-drive enclosure disk drive slot numbers



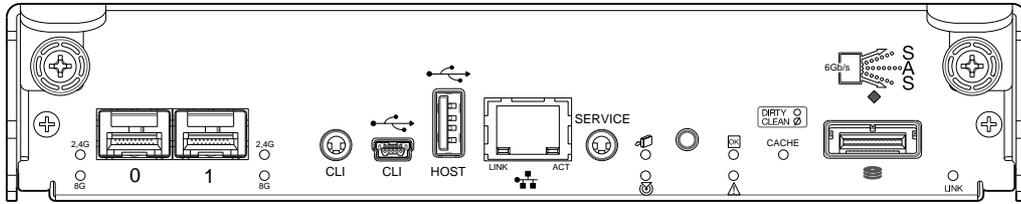
Rear panel views — controller module(s)

The Phoenix RPC12 series controller module(s) shown below are not proportionately sized relative to preceding controller enclosure views. Controller module face plates are enlarged to show relevant detail.

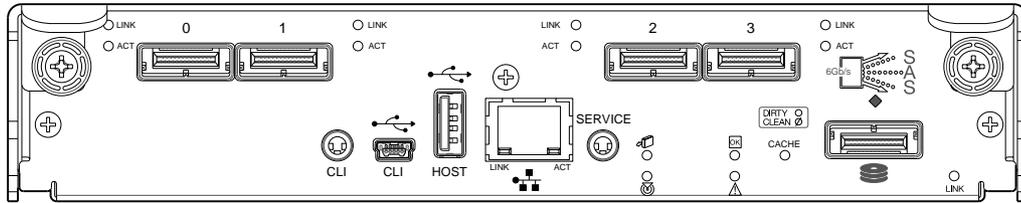
693x6 controller module face plate — hybrid (FC/iSCSI)



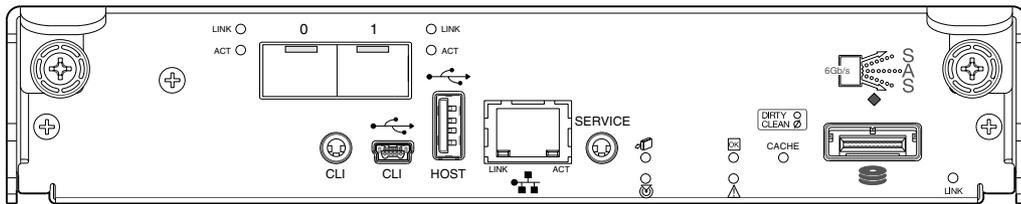
693x1 controller module face plate — Fibre Channel



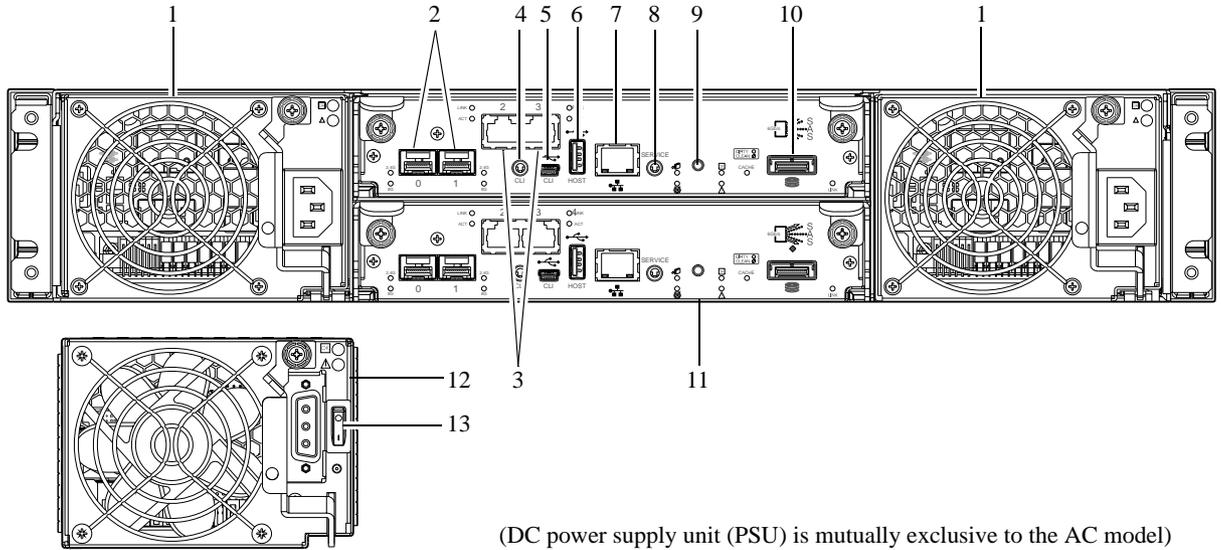
693x4 controller module face plate — Serial Attached SCSI



693x5 controller module face plate — 10GbE Internet SCSI



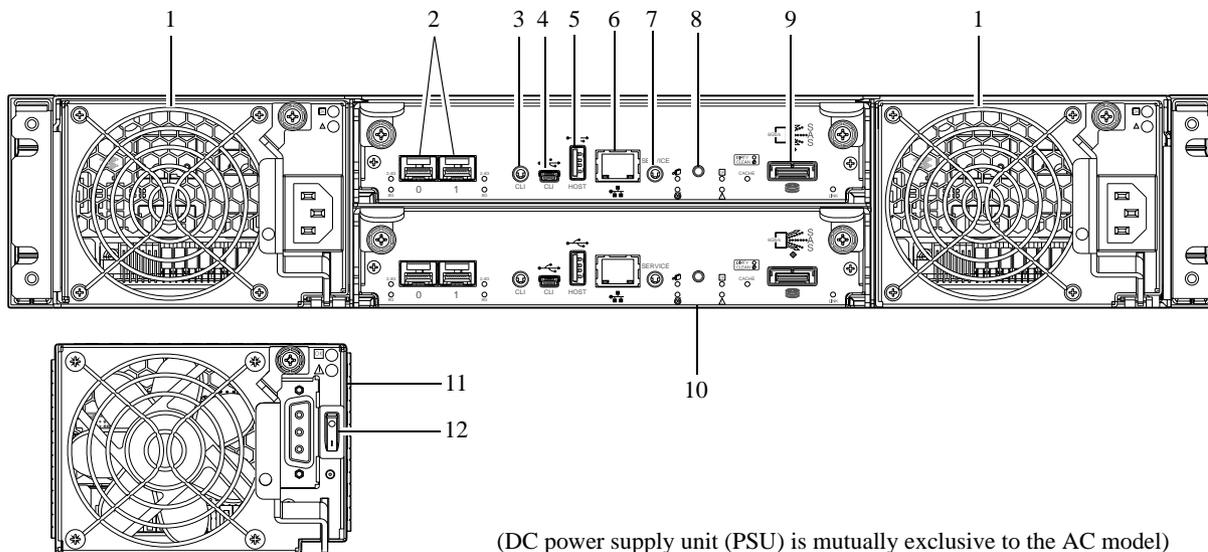
693x6 controller enclosure rear panel components



(DC power supply unit (PSU) is mutually exclusive to the AC model)

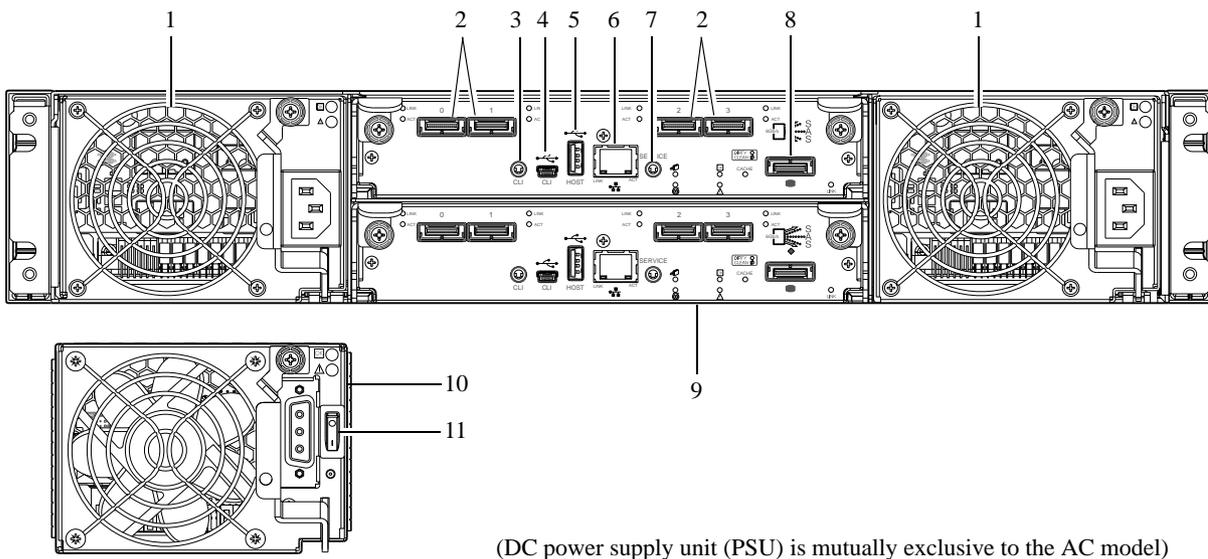
- | | |
|---|---|
| 1 AC power supplies | 8 Service port (used by service personnel only) |
| 2 Host interface ports (FC) | 9 Disabled button (used by engineering/test only) |
| 3 iSCSI ports: remote replication; or host ports | 10 Expansion port |
| 4 CLI port (RS-232) | 11 Controller module B |
| 5 CLI port (USB - Type B) [see Appendix D] | 12 DC Power supply (2) — (DC model only) |
| 6 Host port (USB - Type A; reserved for future use) | 13 DC Power switch |
| 7 Network port | |

693x1 controller enclosure rear panel components



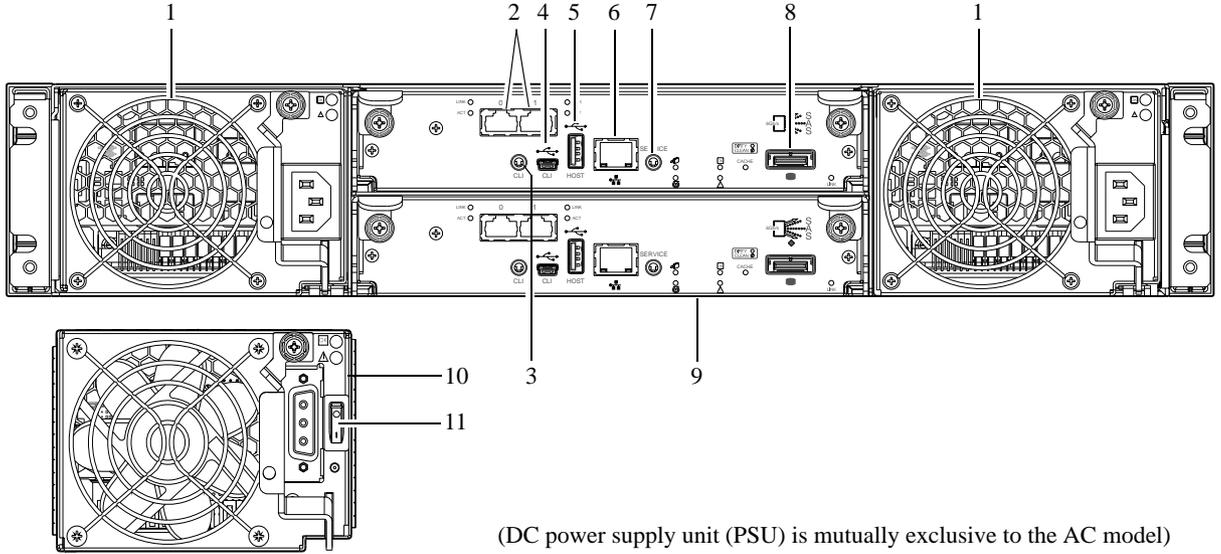
- | | |
|---|---|
| 1 AC power supplies | 7 Service port (used by service personnel only) |
| 2 Host interface ports (FC) | 8 Disabled button (used by engineering/test only) |
| 3 CLI port (RS-232) | 9 Expansion port |
| 4 CLI port (USB - Type B) [see Appendix D] | 10 Controller module B |
| 5 Host port (USB - Type A; reserved for future use) | 11 DC Power supply (2) — (DC model only) |
| 6 Network port | 12 DC Power switch |

693x4 controller enclosure rear panel components



- | | |
|---|---|
| 1 AC Power supplies | 7 Service port (used by service personnel only) |
| 2 Host interface ports (SAS) | 8 Expansion port |
| 3 CLI port (RS-232; reserved for future use) | 9 Controller module B |
| 4 CLI port (USB - Type B) [see Appendix D] | 10 DC Power supply (2) — (DC model only) |
| 5 Host port (USB - Type A; reserved for future use) | 11 DC Power switch |
| 6 Network port | |

693x5 controller enclosure rear panel components

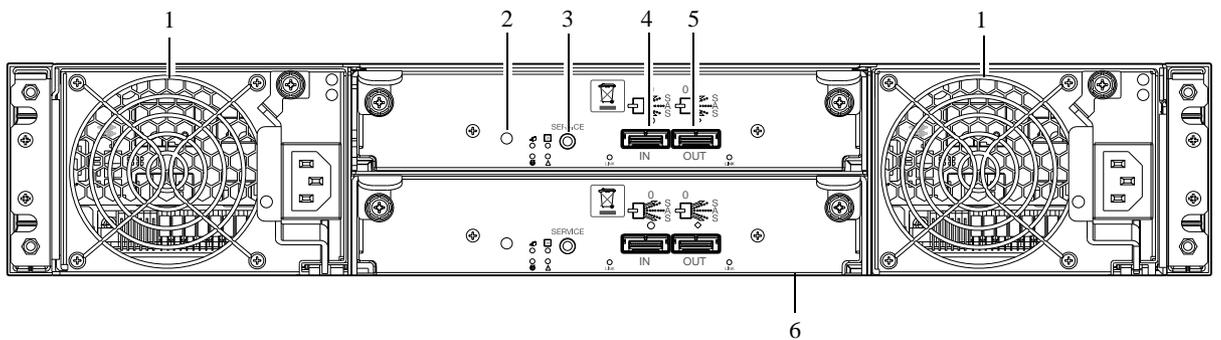


(DC power supply unit (PSU) is mutually exclusive to the AC model)

- | | |
|---|---|
| 1 AC Power supplies | 7 Service port (used by service personnel only) |
| 2 Host interface ports | 8 Expansion port |
| 3 CLI port (RS-232; reserved for future use) | 9 Controller module B |
| 4 CLI port (USB - Type B) [see Appendix D] | 10 DC Power supply (2) — (DC model only) |
| 5 Host port (USB - Type A; reserved for future use) | 11 DC Power switch |
| 6 Network port | |

693x2 enclosure rear panel components

Phoenix RPC12 series controller enclosures support the 693x2 drive enclosure for expansion of storage capacity. These three drive enclosures use mini-SAS (SFF-8088) connectors to facilitate backend SAS expansion. See [Cable requirements for drive enclosures](#) on page 20, or the installation instruction sheet for your controller enclosure product, regarding cabling information.

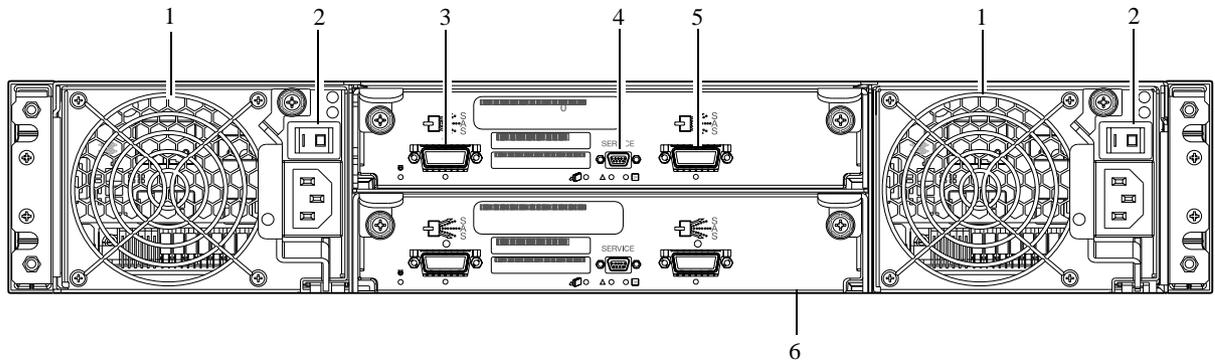


- | | |
|---|--|
| 1 Power supplies | 4 SAS In port (connects to controller enclosure) |
| 2 Disabled button (used by engineering/test only) | 5 SAS Out port (connects to another drive enclosure) |
| 3 Service port (used by service personnel only) | 6 Expansion module B |

695x2/697x2 12-drive enclosure rear panel components

Phoenix RPC12 series controller enclosures support 2130 and 5130 drive enclosures for expansion of storage capacity. These two drive enclosures use SAS 8470 connectors to facilitate backend SAS

expansion. See [Cable requirements for drive enclosures](#) on page 20, or the installation instruction sheet for your controller enclosure product, regarding cabling information.



- | | | | |
|---|--|---|--|
| 1 | Power supplies | 4 | Service port (used by service personnel only) |
| 2 | Power switches (not available on newer models) | 5 | SAS Out port (connects to another drive enclosure) |
| 3 | SAS In port (connects to a controller enclosure) | 6 | Expansion module B |

Cache

To enable faster data access from disk storage, the following types of caching are performed:

- Write-back or write-through caching. The controller writes user data into the cache memory in the controller module rather than directly to the disks. Later, when the storage system is either idle or aging — and continuing to receive new I/O data — the controller writes the data to the disks.
- Read-ahead caching. The controller detects sequential data access, reads ahead into the next sequence of data — based upon settings — and stores the data in the read-ahead cache. Then, if the next read access is for cached data, the controller immediately loads the data into the system memory, avoiding the latency of a disk access.

CompactFlash

During a power loss, data stored in cache are saved off to non-volatile memory (CompactFlash). These data are restored to cache, and then written to disk after the issue is corrected. CompactFlash provides unlimited cache memory backup time. To protect against writing incomplete data to disk, the image stored on the CompactFlash is verified before committing to disk.

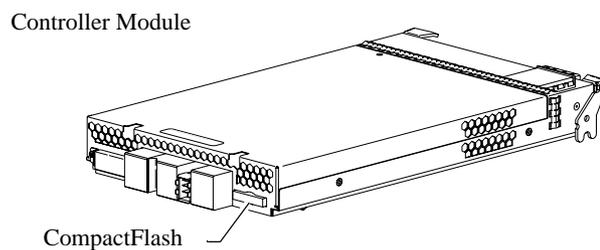


Figure 1 CompactFlash

Super-capacitor pack

To protect controller module cache in case of power failure, each controller enclosure model is equipped with super-capacitor technology, in conjunction with CompactFlash memory, built into each controller module to provide unlimited cache memory backup time. The super-capacitor pack provides energy for backing up unwritten data in the write cache to the CompactFlash, in the event of a power failure. Unwritten data in CompactFlash memory are automatically committed to disk media when power is restored. In the event of power failure, while cache is maintained by the super-capacitor pack, the Cache Status LED flashes at a rate of 1/10 second on and 9/10 second off.

2 Installing the enclosures

Installation checklist

The following table outlines the steps required to install the enclosures, and initially configure and provision the storage system. To ensure successful installation, perform the tasks in the order presented.

Table 2 Installation checklist

Step	Task	Where to find procedure
1.	Install the controller enclosure and optional drive enclosures in the rack, and attach ear caps. ¹	See the rack-mount bracket kit installation instructions pertaining to your enclosure.
2.	Connect controller enclosure and drive enclosures.	See Connecting controller and drive enclosures on page 19.
3.	Connect power cords.	See the installation sheet for your RPC12 series controller enclosure.
4.	Test enclosure connectivity.	See Testing enclosure connections on page 27.
5.	Install required host software.	See Host system requirements on page 31.
6.	Connect hosts. ²	See Connecting the enclosure to hosts on page 31.
7.	Connect remote management hosts. ²	See Connecting a management host on the network , page 38.
8.	Obtain IP values and set network port IP properties on the controller enclosure.	See Obtaining IP values on page 43. For USB CLI port and cable use, see Appendix D. Also see the ship kit CD.
9.	Perform initial configuration tasks ³ :	
	<ul style="list-style-type: none">Sign in to the web-based storage management application (RAIDar).	See “Getting Started” in the web-posted Phoenix RPC12 series RAIDar User Guide.
	<ul style="list-style-type: none">Initially configure and provision the system using RAIDar.	See “Configuring the System” and “Provisioning the System” topics in the RAIDar user guide or online help.

¹Also see Phoenix RPC12 series FRU Installation and Replacement Guide for illustrations showing installation of ear caps.

²For more about hosts, see the Phoenix RPC12 series RAIDar User Guide.

³RAIDar is introduced in [Accessing RAIDar](#) on page 47. See the RAIDar user guide or online help for additional information.

NOTE: Additional installation notes:

- Controller modules within the same enclosure must be of the same type.
- For optimal performance, do not mix 6Gb and 3Gb disk drives within the enclosure.

Connecting controller and drive enclosures

Phoenix RPC12 series controller enclosures — available in 12-drive (3u) chassis — support up to eight enclosures (including the controller enclosure), or 144 disk drives. You can also configure drive enclosures of mixed type as shown in [Figure 9](#) on page 28. The firmware supports both *straight-through* and *reverse* SAS cabling. Reverse (fault-tolerant) cabling allows any drive enclosure to fail — or be removed — while maintaining access to other enclosures. Fault tolerance and performance requirements determine whether to optimize the configuration for high availability or high

performance when cabling. Phoenix RPC12 series controller modules support both 3-Gbps and 6-Gbps internal disk drive speeds together with 3-Gbps and 6-Gbps expander link speeds.

Some 6-Gbps disks might not consistently support a 6-Gbps transfer rate. If this happens, the system automatically adjusts transfers to those disks to 3 Gbps, increasing reliability and reducing error messages with little impact on system performance. This rate adjustment persists until the controller is restarted or power-cycled.

Most cabling diagrams in this section show recommended fault-tolerant cabling patterns. Controller and expansion modules are identified by <enclosure-ID><controller-ID>. When connecting multiple drive enclosures, use reverse cabling to ensure the highest level of fault tolerance, enabling controllers to access remaining drive enclosures if a drive enclosure fails.

For example, [Figure 5](#) on page 23 shows fault tolerant cabling wherein controller 0A is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller 0B is connected to the lower expansion module (B) of the last drive enclosure in the chain, with connections moving in the opposite direction (green). Several cabling examples are provided on the following pages.

Cable requirements for drive enclosures

Dot Hill provides storage systems using 6-Gbps or 3-Gbps expansion port data rates. Observe the following guidelines when installing SAS cables (see [Table 3](#) below):

- Use only Phoenix or OEM-qualified SAS cables appropriate for the target drive enclosure:
 - For 6-Gbps drive enclosures, use cables providing 6-Gbps data rate per lane with four lanes (4x) per SAS connector:
 - When connecting a controller enclosure to a drive enclosure, the cable length should not exceed 2.0 meters
 - When connecting drive enclosures to one another, cable lengths should not exceed 2.0 meters
 - For 3-Gbps expansion modules, use cables providing 3-Gbps data rate per lane with four lanes per SAS connector:
 - When connecting a controller enclosure to a drive enclosure, the cable length should not exceed 2.0 meters
 - When connecting drive enclosures to one another, or when connecting a drive enclosure to an HBA directly, cable lengths should not exceed 2.0 meters
 - Newer cables provide SAS connectors supporting *both* 6-Gb and 3-Gb data rates
 - Qualified cables of 0.6 meter length may be used for cabling stacked components

 **NOTE:** If you connect a 3-Gbps drive enclosure to a 6-Gbps RPC12 series controller enclosure, data throughput occurs at the drive enclosure's 3-Gbps data rate.

- Refer to the [Table 3](#) on page 21 when cabling storage system components. The following terms supplement those defined in the table footer.
 - Mini-SAS to mini-SAS cables denote SFF-8088 to SFF-8088
 - Mini-SAS to SAS cables denote SFF-8088 to 8470
 - SAS to SAS cables denote 8470 to 8470
- You may need to order additional or longer cables when cabling a fault-tolerant configuration (see [Figure 5](#) on page 23).
- Cables required, if not included, must be purchased separately.

Table 3 SAS cable type requirements

Model	3U12 controller enclosure	3120/3130/2122 drive enclosure	2130/5130 drive enclosure
693x6	Not applicable	mini-SAS to mini-SAS	mini-SAS to SAS
693x1	Not applicable	mini-SAS to mini-SAS	mini-SAS to SAS
693x4	Not applicable	mini-SAS to mini-SAS	mini-SAS to SAS
693x5	Not applicable	mini-SAS to mini-SAS	mini-SAS to SAS
695x2	mini-SAS to SAS	mini-SAS to SAS	SAS to SAS
693x2	mini-SAS to mini-SAS	mini-SAS to mini-SAS	mini-SAS to SAS
697x2	mini-SAS to SAS	mini-SAS to SAS	SAS to SAS

Controller enclosure/chassis designators:
 3U12 = Enclosure measuring three rack units high, providing 12-drives.

Product models (6-Gbps SAS expansion data transmission rate unless noted otherwise):
 693x6 = RPC12 series controller enclosure (3.5" disks in 2U12 chassis)
 693x1 = RPC12 series controller enclosure (3.5" disks in 2U12 chassis)
 693x4 = RPC12 series controller enclosure (3.5" disks in 2U12 chassis)
 693x5 = RPC12 series controller enclosure (3.5" disks in 2U12 chassis)
 695x2 = 12-drive expansion enclosure (3.5" disks in 2U12 chassis) [3-Gbps SAS expansion]
 693x2 = 12-drive expansion enclosure (3.5" disks in 2U12 chassis)
 697x2 = 12-drive expansion enclosure (3.5" disks in 2U12 chassis) [3-Gbps SAS expansion]

NOTE: For clarity, the schematic diagrams show only relevant details such as face plate outlines and expansion ports. For detailed illustrations, see [Rear panel views – controller module\(s\)](#) on page 13.

The following illustrations show both *straight-through* and *reverse* cabling examples using different drive enclosures supported by Phoenix RPC12 series controller enclosures.

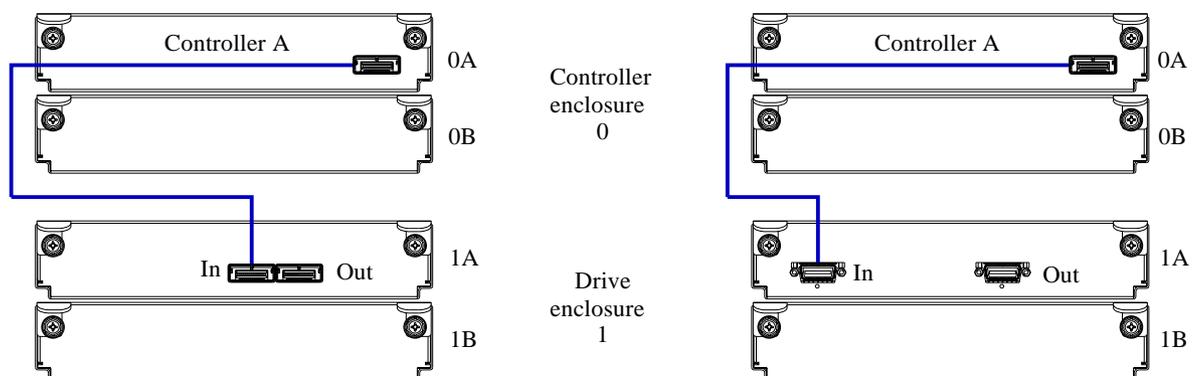


Figure 2 Cabling connections between a single-controller enclosure and one drive enclosure

The diagram at left (above) shows a single-controller enclosure connected to a 693x2 (single expansion module); whereas the diagram at right shows the controller enclosure connected to a 695x2 or 697x2 (single expansion module).

NOTE: Some enclosures use a SFF-8088 connector interface for drive expansion, whereas other enclosures use SAS 8470. Refer to [Table 3](#) on page 21 for SAS cable requirements.

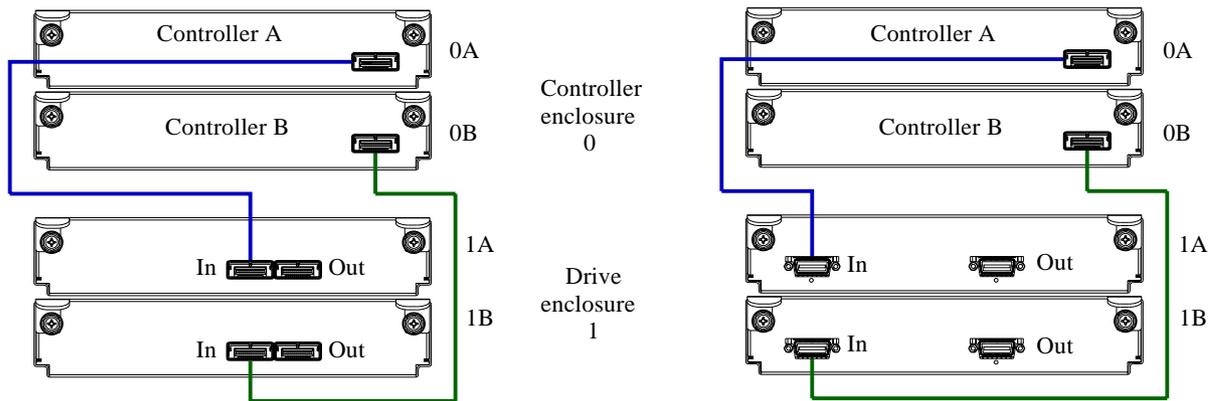


Figure 3 Cabling connections between a dual-controller enclosure and a single drive enclosure

The diagram at left (above) shows a dual-controller enclosure connected to a 693x2 (two expansion modules); whereas the diagram at right shows the dual-controller enclosure connected to a 695x2 or 697x2 (two expansion modules).

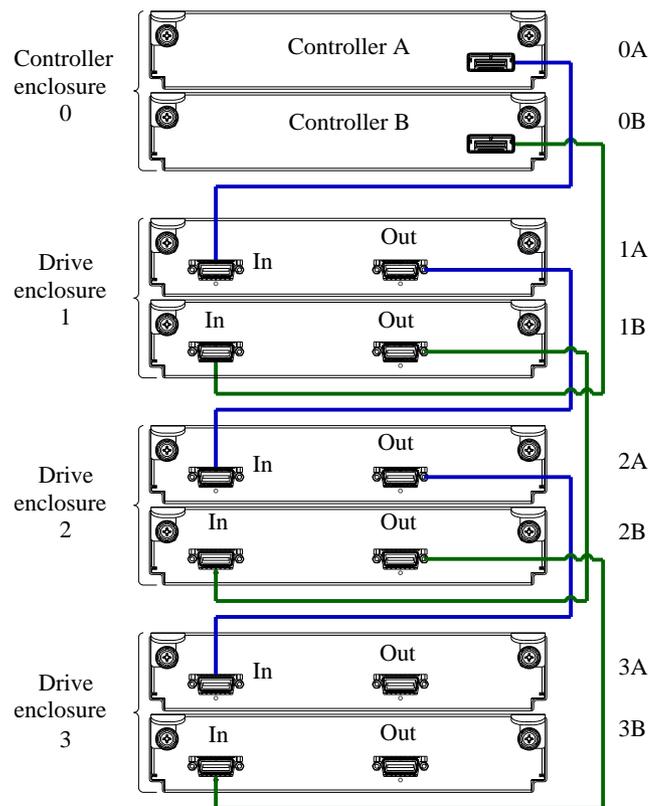


Figure 4 Non-fault-tolerant cabling between a dual-controller enclosure and three LFF drive enclosures

The diagram above shows a dual-controller enclosure cabled to 695x2 or 697x2 drive enclosures, featuring dual-expansion modules. Controller enclosure ID number 0, featuring dual controllers, is attached to three drive enclosures in straight-through fashion.

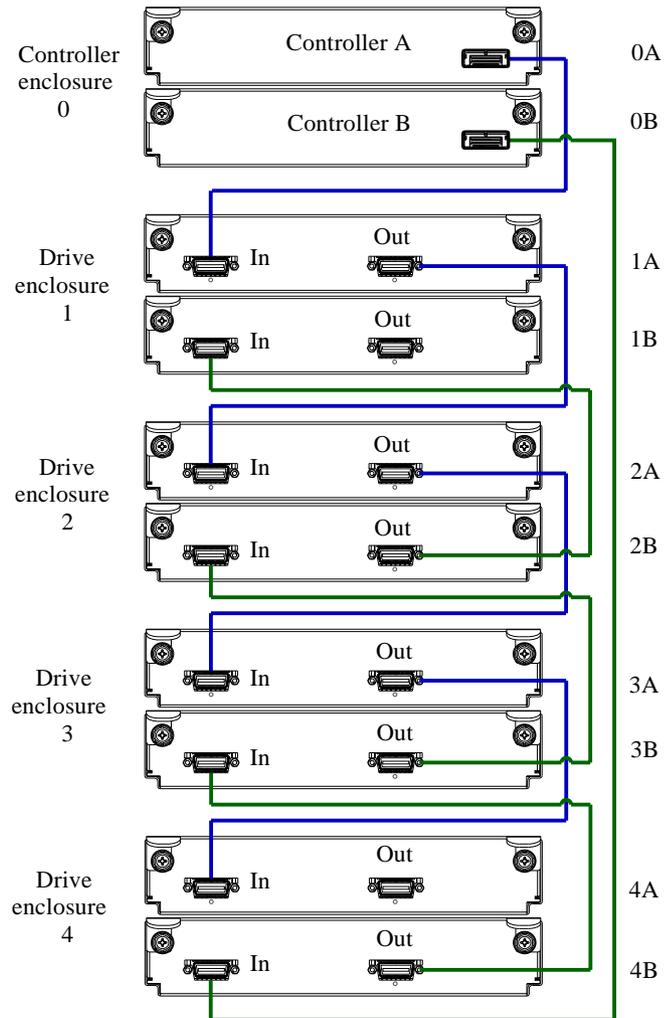


Figure 5 Fault-tolerant cabling between a dual-controller enclosure and four LFF drive enclosures

The diagram above shows a dual-controller enclosure cabled to 695x2 or 697x2 drive enclosures, featuring dual-expansion modules. Controller module 0A is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller module 0B is connected to the lower expansion module (4B), of the last drive enclosure, with connections flowing in the opposite direction (green).

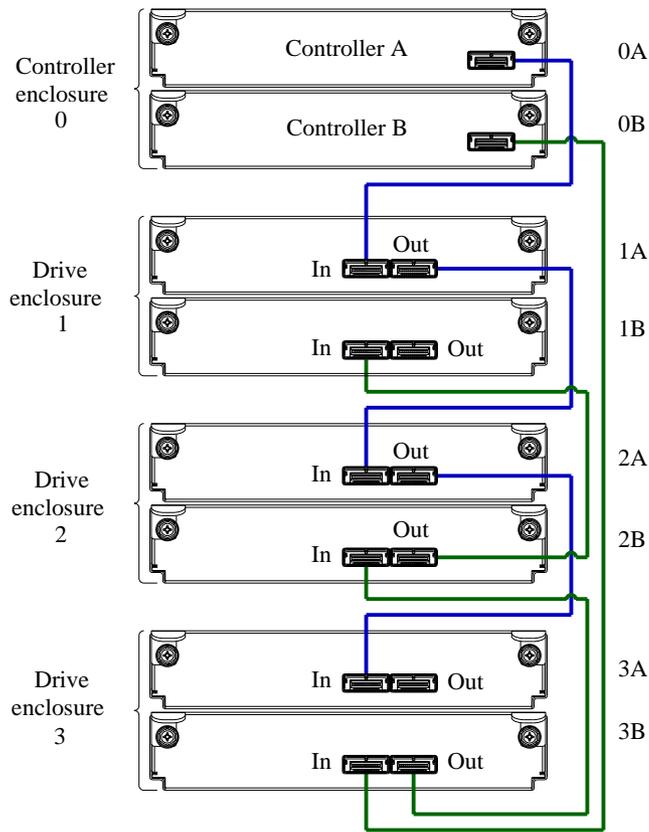


Figure 6 Fault-tolerant cabling between a dual-controller enclosure and three drive enclosures

The diagram above shows a dual-controller enclosure cabled to a 693x2 drive enclosure featuring dual-expansion modules. Controller module 0A is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller module 0B is connected to the lower expansion module (3B), of the last drive enclosure, with connections moving in the opposite direction (green).

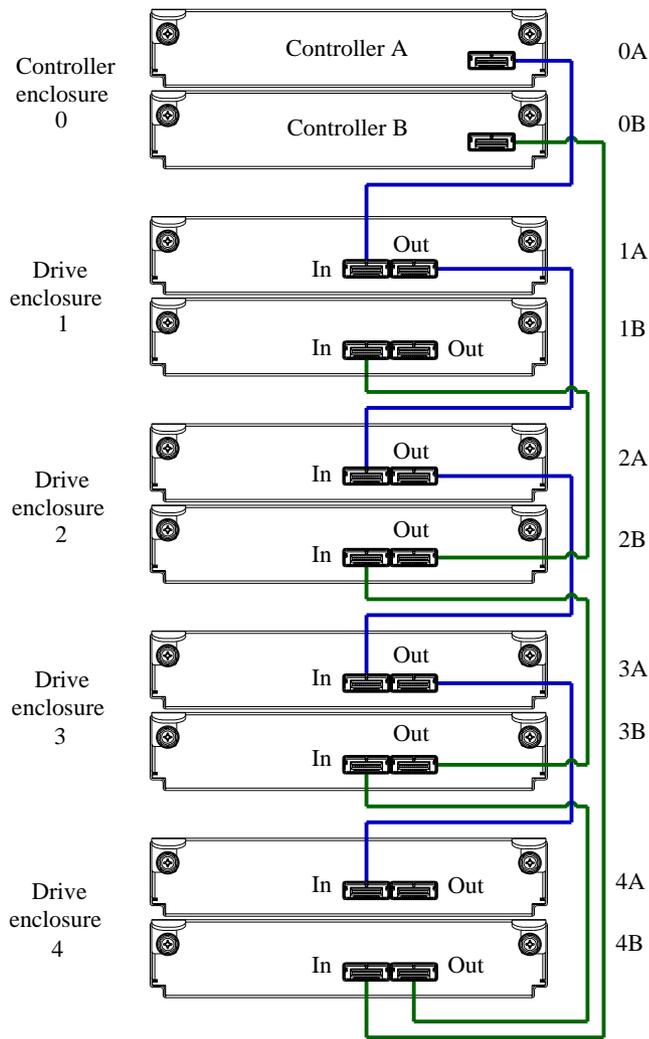


Figure 7 Fault-tolerant cabling between a dual-controller enclosure and four drive enclosures

The diagram above shows a dual-controller enclosure cabled to a 693x2 drive enclosure featuring dual-expansion modules. Controller module 0A is connected to expansion module 1A, with a chain of connections continuing down (blue). Controller module 0B is connected to the lower expansion module (4B), of the last drive enclosure, with connections moving in the opposite direction (green).

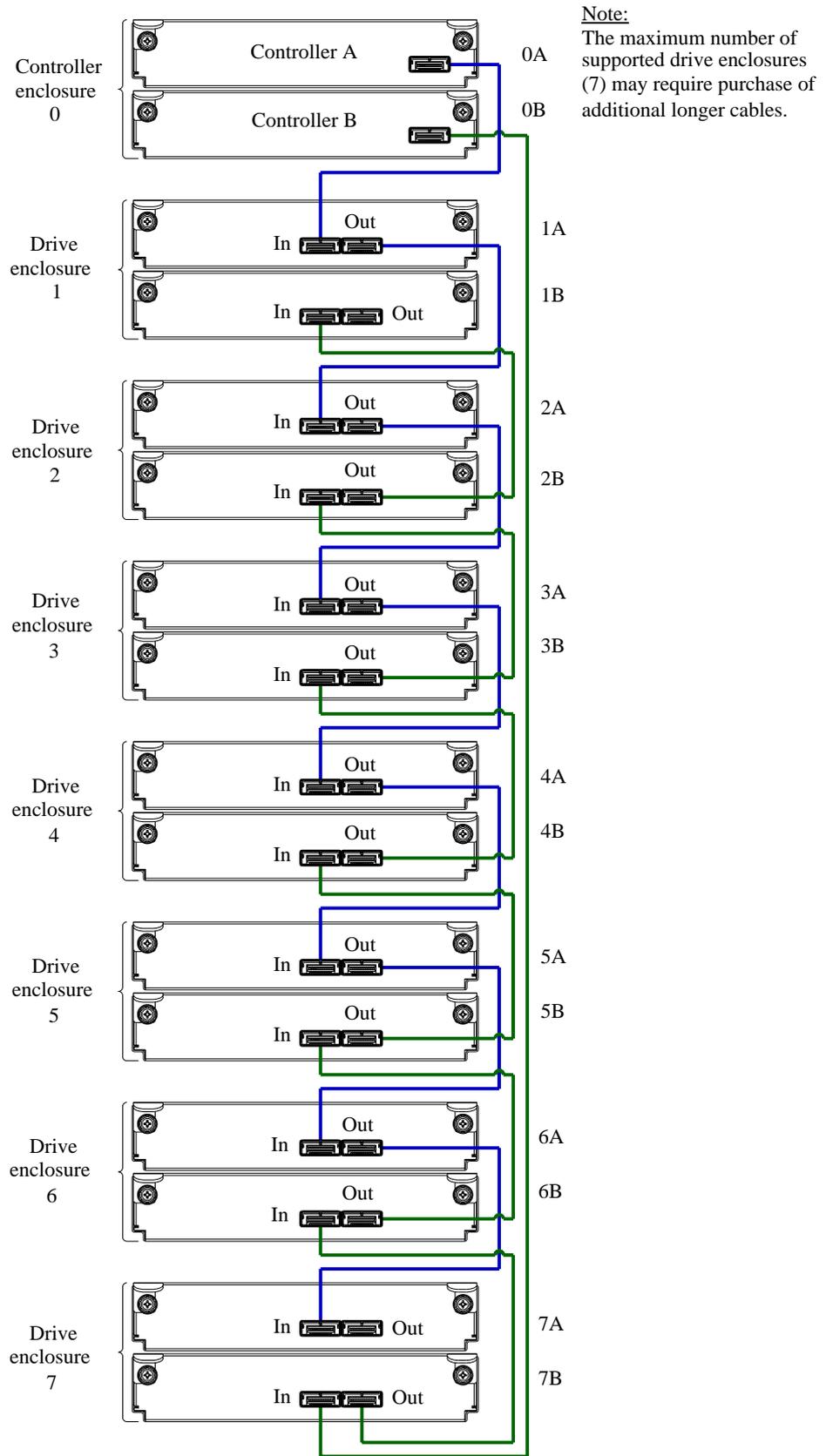


Figure 8 Fault-tolerant cabling between a dual-controller enclosure and seven drive enclosures

The diagram above shows a 693x1 dual-controller enclosure cabled to 693x2 drive enclosures featuring dual-expansion modules. Controller module 0A is connected to expansion module 1A, with a chain of connections cascading down (blue). Controller module 0B is connected to the lower

expansion module (7B), of the last drive enclosure, with connections moving in the opposite direction (green).

Testing enclosure connections

Power cycling procedures vary according to the type of power supply unit (PSU) provided with the enclosure. Some enclosure models are equipped with PSUs possessing power switches; whereas other enclosures use PSUs that have no power switch.

The following section, [Powering on/powering off](#), describes power cycling procedures relative to different types of PSUs installed within enclosures. Once the enclosures' power-on sequence succeeds, the storage system is ready to be connected to hosts as described in [Connecting the enclosure to hosts](#) on page 31.

Powering on/powering off

Before powering on the enclosure for the first time:

- Install all disk drives in the enclosure so the controller can identify and configure them at power-up.
- Connect the cables and power cords to the enclosure as explained in the installation sheet.

 **NOTE:** Newer AC power supply units (PSUs) do not have power switches. *Switchless* PSUs power on when connected to a power source, and power off when disconnected.

- Generally, when powering up, make sure to power up the enclosures and associated data host in the following order:
 - Drive enclosures *first*
This ensures that the disks in the drive enclosure have enough time to completely spin up before being scanned by the controller modules within the controller enclosure.
While enclosures power up, their LEDs blink. After the LEDs stop blinking — if no LEDs on the front and back of the enclosure are amber — the power-on sequence is complete, and no faults have been detected. See [LED descriptions](#) on page 65 for descriptions of LED behavior.
 - Controller enclosure *next*
Depending upon the number and type of disks in the system, it may take several minutes for the system to become ready.
 - Data host *last* (if powered down for maintenance purposes).

 **TIP:** Generally, when powering off, you will reverse the order of steps used for powering on.

Power cycling procedures vary according to the type of power supply unit included within the enclosure. For controller and drive enclosures configured with switchless AC PSUs, refer to the procedure described under [AC PSU](#) below. For procedures pertaining to a) controller enclosures configured with DC PSUs, or b) previously installed expansion enclosures featuring power switches, see [DC and AC PSUs with power switch](#) on page 29.

AC PSU

Controller and drive enclosures configured with switchless PSUs rely on the power cord for power cycling. Connecting the cord from the PSU power cord connector to the appropriate power source facilitates power on; whereas disconnecting the cord from the power source facilitates power off.

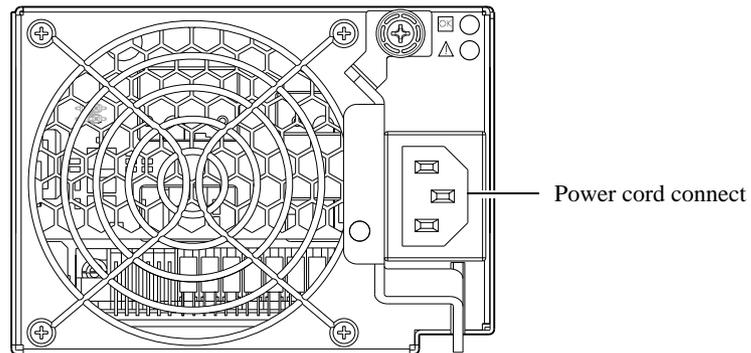


Figure 9 AC PSU

To power on the system:

1. Plug the power cord into the power cord connector on the back of the drive enclosure. Plug the other end of the power cord into the rack power source (see Figure 9 and Figure 10). Wait several seconds to allow the disks to spin up.

Repeat this sequence for each switchless PSU within each drive enclosure.

2. Plug the power cord into the power cord connector on the back of the controller enclosure. Plug the other end of the power cord into the rack power source (see Figure 9 and Figure 10).

Repeat the sequence for the controller enclosure's other switchless PSU.

Power cord facilitates
power on/power off

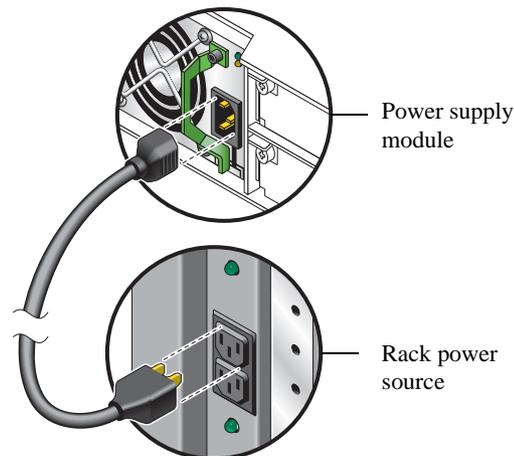


Figure 10 AC power cord

To power off the system:

1. Stop all I/O from hosts to the system.
2. Shut down both controllers using *either* method described below:
 - Use RAIDar to shut down both controllers, as described in the online help and Phoenix RPC12 series RAIDar User Guide.
Proceed to [step 3](#)
 - Use the command line interface (CLI) to shut down both controllers, as described in the Phoenix RPC12 series CLI Reference Guide.
3. Disconnect the power cord's male plug from the power source.
4. Disconnect the power cord's female plug from the power cord connector on the PSU.

DC and AC PSUs with power switch

DC and legacy AC power supplies — each equipped with a power switch — are shown below.

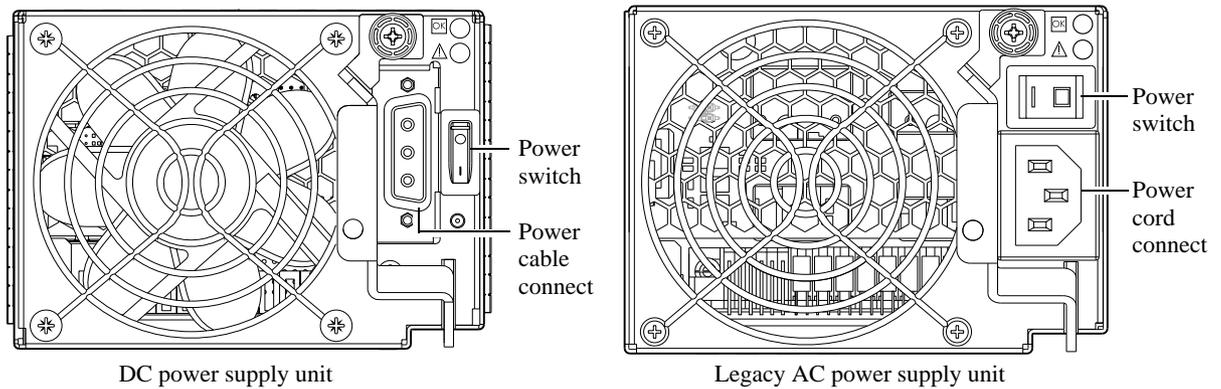


Figure 11 DC and AC PSUs with power switch

Power Cords

IMPORTANT: See [Environmental requirements and specifications](#) for additional information.

AC model

See [Figure 10](#) and the illustration at right (in [Figure 11](#)) when performing the following steps:

1. Verify that the enclosure's power switches are in the Off position.
2. Identify the power cord connector on the PSU, and locate the target power source.
3. Using the AC power cords provided, plug one end of the cord into the power cord connector on the PSU. Plug the other end of the power cord into the rack power source.
4. Verify connection of primary power cords from the rack to separate external power sources.
See [Power cycle](#).

DC model

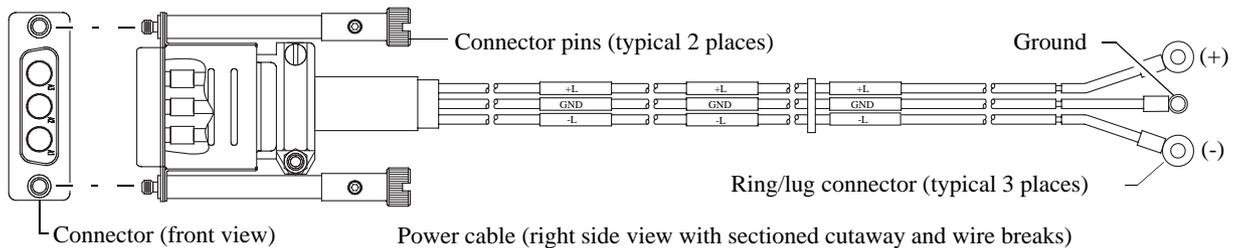
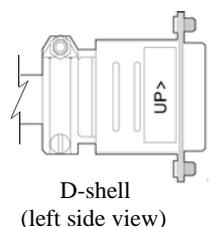


Figure 12 DC power cable featuring D-shell and lug connectors

See [Figure 12](#) and the illustration at left (in [Figure 11](#)) when performing the following steps:

1. Locate and use the provided DC power cables.
2. Verify that the enclosure's power switches are in the Off position.
3. Connect a DC power cable to each DC power supply using the D-shell connector. Use the **UP>** arrow on the connector shell to ensure proper positioning (see adjacent left side view of D-shell connector).
4. Tighten the screws at the top and bottom of the shell, applying a torque between 1.7 N-m (15 in-lb) and 2.3 N-m (20 in-lb), to securely attach the cable to the DC power supply module.



5. To complete the DC connection, secure the other end of each cable wire component of the DC power cable to the target DC power source.

Check the three individual DC cable wire labels before connecting each cable wire lug to its power source. One cable wire is labeled *ground* (GND), and the other two are labeled *positive* (+L) and *negative* (-L), respectively (shown in [Figure 12](#) above).

△ **CAUTION:** Connecting to a DC power source outside the designated -48VDC nominal range (-36VDC to -72VDC) may damage the enclosure.

See [Power cycle](#).

Power cycle

To power on the system:

1. Power up drive enclosure(s). Allow several seconds for disks to spin up.
Press the power switches at the back of each drive enclosure to the On position.
2. Power up the controller enclosure next.
Press the power switches at the back of the controller enclosure to the On position.

To power off the system:

1. Stop all I/O from hosts to the system.
2. Shut down both controllers using *either* method described below:
 - Use RAIDar to shut down both controllers, as described in the online help and Phoenix RPC12 series RAIDar User Guide.
Proceed to [step 3](#)
 - Use the command line interface (CLI) to shut down both controllers, as described in the Phoenix RPC12 series CLI Reference Guide.
3. Press the power switches at the back of the controller enclosure to the Off position.
4. Press the power switches at the back of each drive enclosure to the Off position.

3 Connecting hosts

Host system requirements

Hosts connected to a RPC12 series controller enclosure must meet the following requirements:

- Depending on your system configuration, host operating systems may require that multipathing is supported.

 **TIP:** See the web-posted Phoenix Installing Optional Software for Microsoft Windows® Server to aid in planning and implementing your MPIO DSM installation.

If fault tolerance is required, then multipathing software may be required. Host-based multipath software should be used in any configuration where two logical paths between the host and any storage volume may exist at the same time. This would include most configurations where there are multiple connections to the host or multiple connections between a switch and the storage.

- Use Phoenix MPIO DSM with **Windows Server 2003**.
- Use native Microsoft MPIO DSM support with **Windows Server 2008**. Use either the Server Manager or the command line interface (*mpclaim* CLI tool) to perform the installation.

See Phoenix Installing Optional Software for Microsoft Windows® Server and the following web sites for information about using native Microsoft MPIO DSM:

<http://support.microsoft.com/gp/assistsupport>

<http://technet.microsoft.com> (search the site for “multipath I/O overview”)

- To prevent **Microsoft Windows 2003** hosts from displaying the Found New Hardware Wizard when the storage system is discovered, install the Phoenix SCSI Enclosure Services driver.

 **NOTE:** The Phoenix SCSI Enclosure Services driver is *required* for Windows Server 2003.

Cabling considerations

Common cabling configurations address hosts, controller enclosures, drive enclosures, and switches. Cabling systems to enable use of the licensed AssuredRemote™ feature — to replicate volumes — is yet another important cabling consideration. See [Connecting two storage systems to replicate volumes](#) on page 38 for more information.

Fibre Channel ports can connect to Fibre Channel hosts; or be used with AssuredRemote for replication (licensed option). Similarly, iSCSI ports on the 693x6 can connect to iSCSI hosts; or be used with AssuredRemote for replication.

 **NOTE:** 693x6 and 693x1 models support AssuredRemote replication; whereas 693x4 and 693x5 models do not.

Connecting the enclosure to hosts

A *host* identifies an external port to which the storage system is attached. Cable connections vary depending on configuration. This section describes host interface protocols supported by RPC12 series controller enclosures, while showing a few common cable configurations.

 **NOTE:** RPC12 series controllers use Unified LUN Presentation (ULP) — a controller firmware feature enabling hosts to access mapped volumes via host ports — without the need for internal or external switches.

FC host ports

The RPC12 series controller enclosures use Fibre Channel (FC) interface protocol for host port connection, featuring either one or two controller modules. Each controller module provides two host ports configured with a Fibre Channel small form-factor pluggable (SFP transceiver) connector, supporting data rates up to 8-Gbps.

The 693x6 (FC/iSCSI) and 693x1 (FC) models support Fibre Channel Arbitrated Loop (FC-AL or “loop”) topology by default. Connection mode can be set to loop or point-to-point. Loop protocol can be used in a physical loop or in a direct connection between two devices. Point-to-point protocol is used to connect to a fabric switch. The RPC12 series controller enclosures can alternatively be cabled to support replication via the FC host interface ports. A 693x6 or 693x1 employs FC ports in one of two capacities:

- To connect two storage systems through a Fibre Channel switch for use of AssuredRemote replication; or
- For attachment to FC hosts directly, or through a Fibre Channel switch.

The first option requires a valid license for AssuredRemote replication features, whereas the second option requires that the host computer supports FC and multipath I/O. These two uses of FC ports are mutually exclusive to one another at any given point in time.

SAS host ports

The 693x4 uses Serial Attached SCSI (Small Computer System Interface — SAS) interface protocol for host port connection, featuring either one or two controller modules. Each controller module provides two dual SFF-8088 mini-SAS host ports supporting data rates up to 6-Gbps per lane — and 4-lanes per SAS connector.

iSCSI host ports (1Gb)

The 693x6 FC/iSCSI model supports Internet SCSI interface protocol as an alternative to FC host port connection. A 693x6 provides two iSCSI ports — each supporting data rates up to 1-Gbps — using either one-way or mutual CHAP (Challenge-Handshake Authentication Protocol). A 693x6 employs iSCSI ports in one of two capacities:

- To connect two storage systems through a switch for use of AssuredRemote replication; or
- For attachment to iSCSI hosts directly, or through an iSCSI switch.

The first option requires a valid license for AssuredRemote replication features, whereas the second option requires that the host computer supports Ethernet, iSCSI, and multipath I/O. These two uses of iSCSI ports are mutually exclusive to one another at any given point in time.

iSCSI host ports (10GbE)

The 693x5 models use Internet SCSI interface protocol for host port connection, featuring either one or two controller modules. Each controller module provides two iSCSI host ports configured with a small form pluggable (10GbE SFP+ transceiver) connector — each supporting data rates up to 10-Gbps — using either one-way or mutual CHAP (Challenge-Handshake Authentication Protocol).

Connecting direct attach configurations

The 693x5 and 693x1 each support up to four direct-connect server connections, two per controller module. The 693x6 and 693x4 each support up to eight server connections, four per controller. Connect appropriate cables from the server’s HBAs to the controller module’s host ports as described below, and shown in the following illustrations.

- To connect the RPC12 series controller enclosure to a server HBA or switch — using the controller’s FC host ports — select Fibre Channel cables supporting 2/4/8 Gb data rates, that are compatible with the controller module’s host port SFP connector. Such cables are also used for connecting a local storage system to a remote storage system via a switch, to facilitate use of the optional AssuredRemote replication feature.

The table below maps SFP transceiver data rates to relative fiber optic cable characteristics (i.e., cable length, multimode fiber type (MMF), and ISO/IEC optical multimode cable performance

standards). When transferring data through FC connections, cable lengths should not exceed the lengths listed for each given fiber type and performance code within the applicable data rate (2/4/8 Gb) class.

Table 4 Maximum cable lengths for 850nm Fibre Channel SFP transceivers

SFP data	Representative	Cable performance code		
		OM1	OM2	OM3
Data rate	MMF FC cable length designators			
8-Gbps	21m with 62.5µm fiber type	X		
	50m with 50µm fiber type		X	
	150m with 50µm fiber type			X
4-Gbps	70m with 62.5µm fiber type	X		
	150m with 50µm fiber type		X	
	380m with 50µm fiber type			X
2-Gbps	150m with 62.5µm fiber type	X		
	300m with 50µm fiber type		X	
	500m with 50µm fiber type			X

- To connect RPC12 series iSCSI controller modules to a server or switch — using the controller’s iSCSI ports — select (CAT5-E minimum) Ethernet cables supporting the 1 Gb RJ-45 copper host port iSCSI connector. Minimum cable length is 0.5 meters; maximum cable length is 7 meters. With the 693x6 model, such cables are also used for connecting a primary storage system to a secondary storage system via a switch, to facilitate use of the optional volume replication feature.
- To connect the 693x4 to a server HBA or switch, use Phoenix or OEM-qualified mini-SAS 4x cables. SAS cables connecting to host ports must support the SFF-8088 host port connector using 0.5 meter, 1 meter, 2 meter, 4 meter or 6 meter (maximum) cable lengths.
- To connect the 693x5 to a server or switch — using the controller’s iSCSI host ports — select the appropriate qualified 10GbE SFP+ option. The maximum supported cable length is 7.0 meters.

Single-controller configurations

One server/one HBA/single path

Model-specific illustrations show single-controller configurations for RPC12 series controller enclosures supporting pertinent host interface protocols.

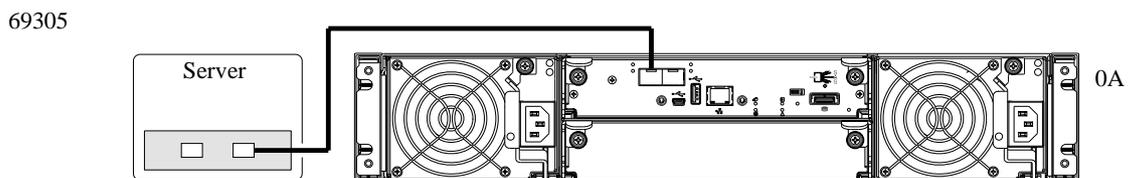
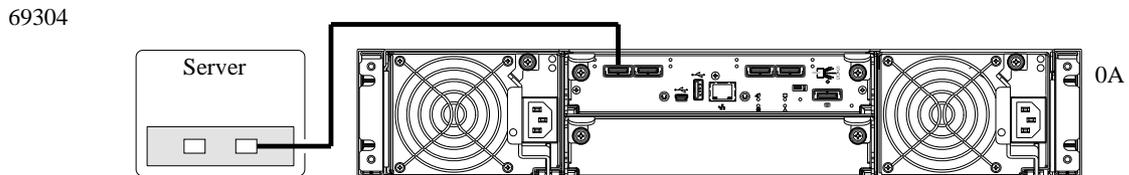
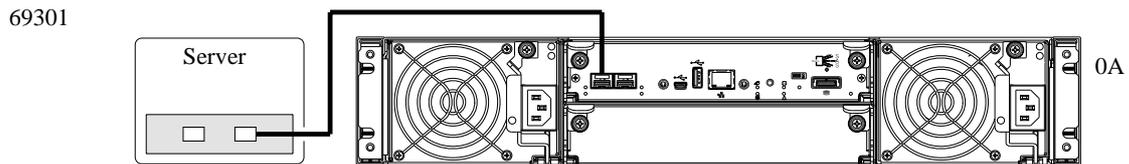
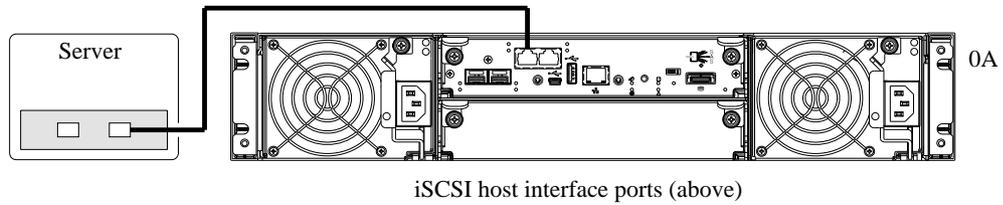
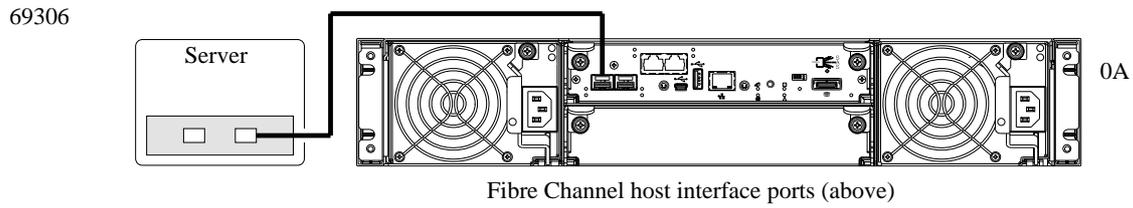


Figure 13 Connecting hosts — one server/one HBA/single path

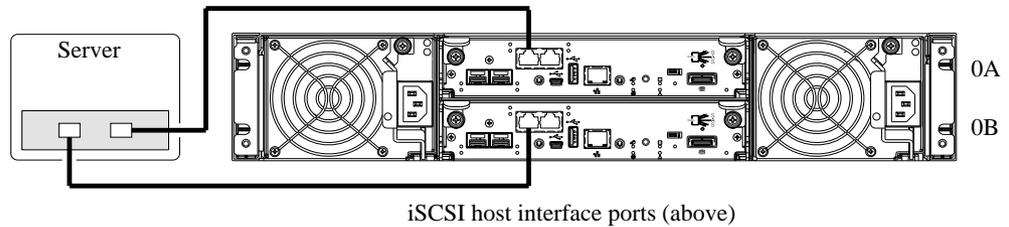
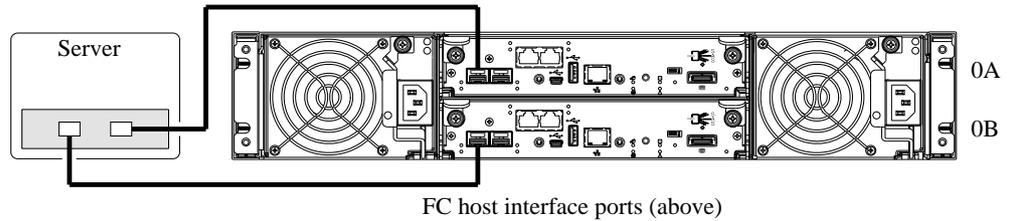
Dual-controller configurations

In a dual-controller system, hosts use LUN-identifying information from both controllers to determine that up to four paths are available to a given storage volume. A host can use any available data path to access a volume owned by either controller. The path providing the best performance is through host ports on the volume's owning controller. Controllers share one set of 512 LUNs (0-511) for use in mapping volumes to hosts (see "ULP" in the Phoenix RPC12 series RAIDar User Guide).

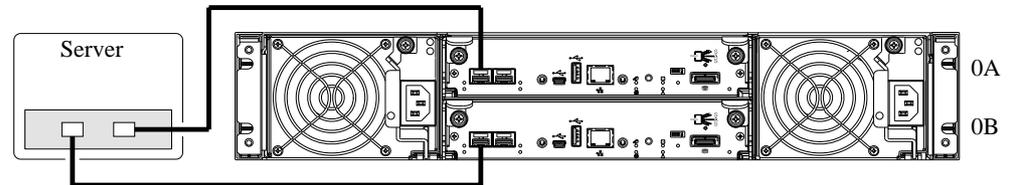
One server/one HBA/dual path

Model-specific illustrations (below) show dual-controller configurations for RPC12 series controller enclosures supporting pertinent host interface protocols.

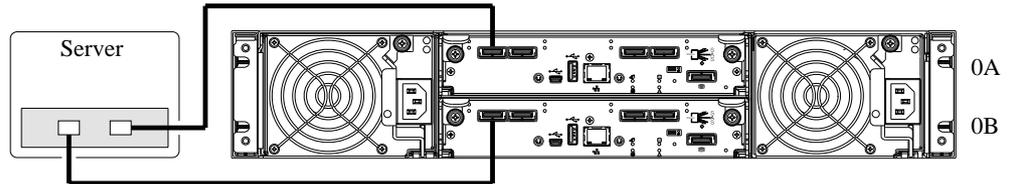
69326



69321



69324



69325

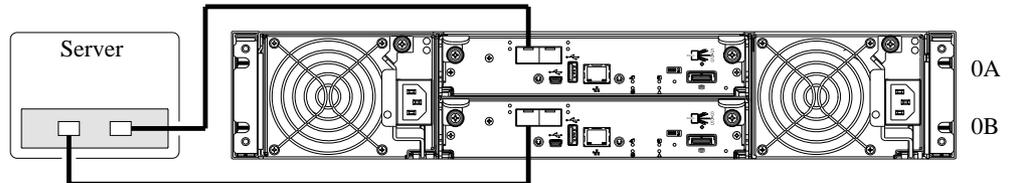


Figure 14 Connecting hosts — one server/one HBA/dual path

Two servers/one HBA per server/dual path

Model-specific illustrations show two-server/dual-controller configurations for RPC12 series controller enclosures supporting pertinent host interface protocols.

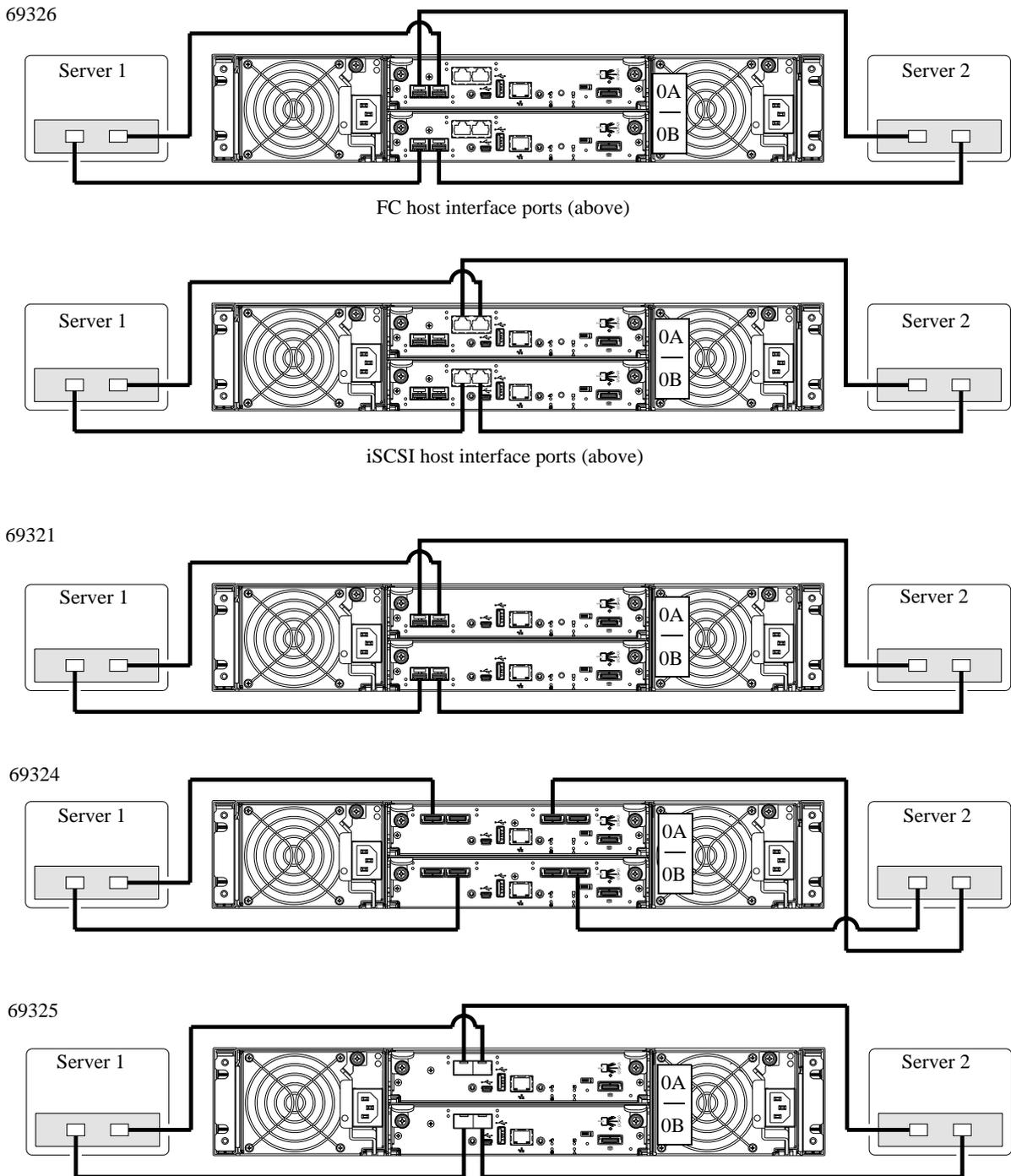


Figure 15 Connecting hosts — two servers/one HBA per server/dual path

Four servers/one HBA per server/dual path

Model-specific illustrations show two-server/dual-controller configurations for RPC12 series controller enclosures supporting pertinent host interface protocols.

69324

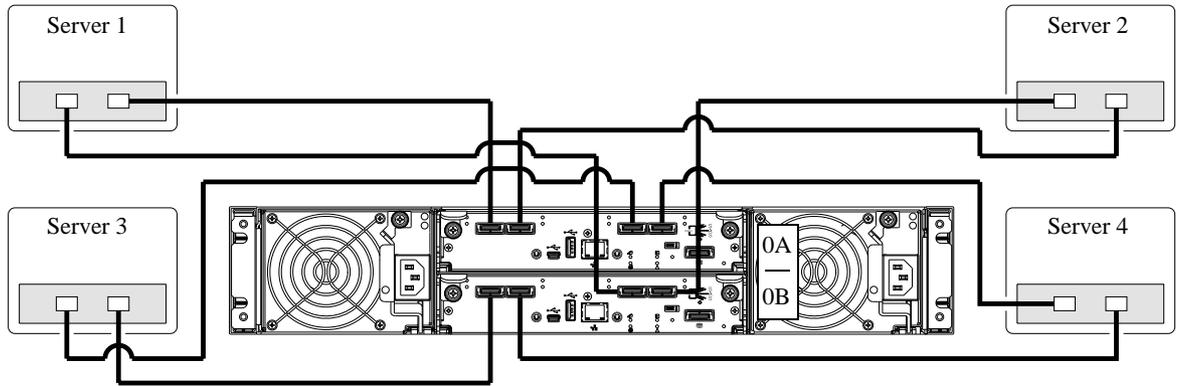


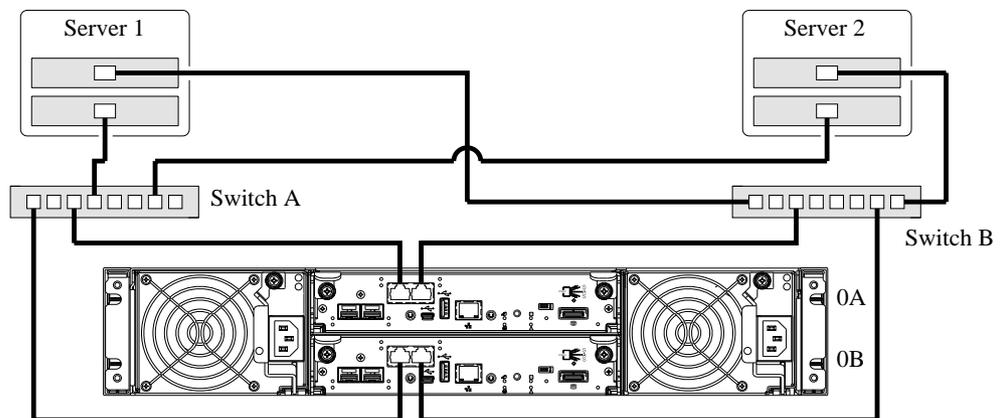
Figure 16 Connecting hosts — four servers/one HBA per server/dual path

Connecting switch attach configurations

Multiple servers/multiple switches

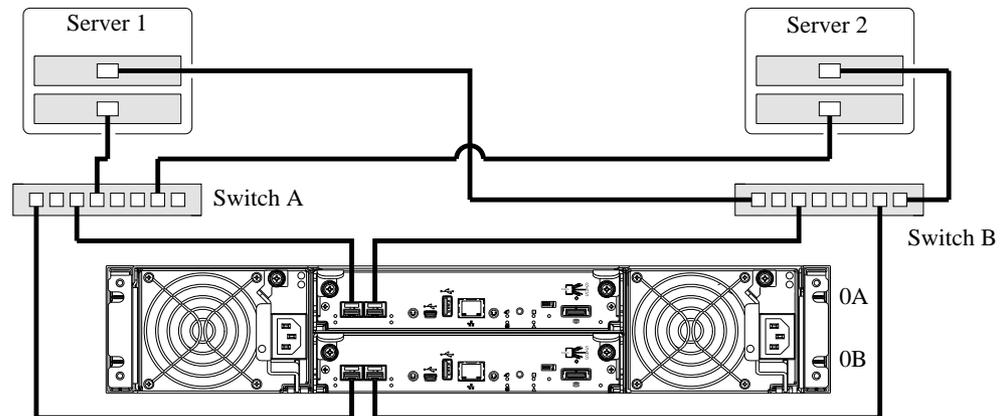
Model-specific dual-controller illustrations show switch-connect configurations for RPC12 series controller enclosures supporting pertinent host interface protocols. Connect appropriate cables from controller host ports to switch ports, and from switch ports to hosts.

69326



Note: FC host interface cabling is identical to that shown for 3720/3730 (below)

69321



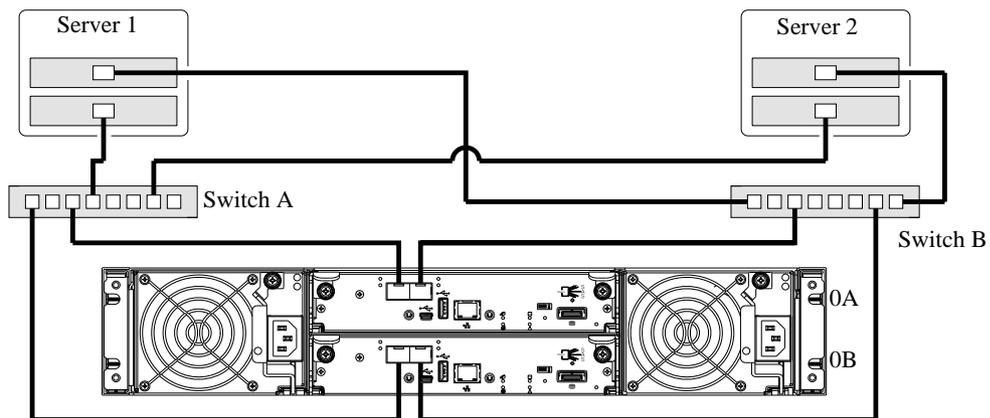
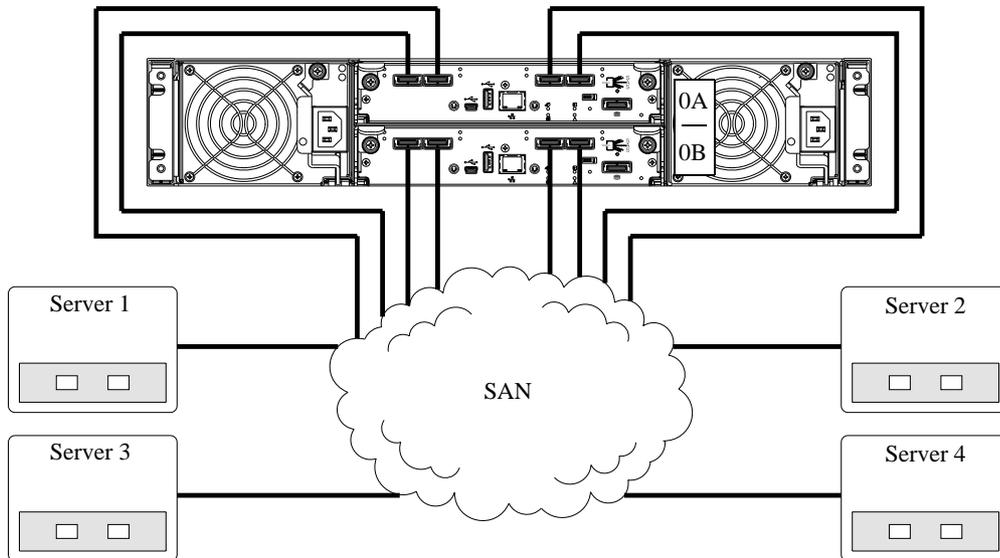


Figure 17 Connecting hosts — switch attach: two servers/two switches

Connecting a management host on the network

The management host directly manages storage systems out-of-band over an Ethernet network.

1. Connect an RJ-45 Ethernet cable to the network port on each controller.
2. Connect the other end of each Ethernet cable to a network that your management host can access (preferably on the same subnet).

NOTE: Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Connecting two storage systems to replicate volumes

AssuredRemote replication is a licensed feature for disaster-recovery. This feature performs asynchronous (batch) replication of block-level data from a volume on a local storage system to a secondary volume on the same system or on a second, independent system. The second system can be located at the same site as the first system, or at a different site.

The two volumes form a *replication set*, and only the primary volume can be mapped for access by a server. Both systems must be licensed to use replication, and must be connected through switches to the same fabric or network (i.e., no direct attach). The server accessing the replication set need only be

connected to the primary system. If the primary system goes offline, the server can access the replicated data from the secondary system.

A typical replication configuration includes a host — connected to a local storage system — and networked via FC or iSCSI ports to a remote storage system. The following RPC12 series controller enclosure configurations are required for the replication to be fault tolerant:

- Two FC-only systems, each with both ports on each of the four controller modules connected to an FC switch (see [Figure 21](#) on page 43).
- Two FC/iSCSI systems, each with both iSCSI ports on each of the four controller modules connected to an iSCSI switch (see [Figure 19](#) on page 41 and [Figure 20](#) on page 42).
- Two FC/iSCSI systems, each with both FC ports on each of the four controller modules connected to an FC switch.

Both single and dual-controller environments support replication, provided you connect like systems. A single-controller system can replicate data to another single-controller system, and a dual-controller system can replicate data to another dual-controller system. Replication services do not support mixed single and dual-controller environments.

Single-controller configuration

One server/one switch/two storage systems

The Illustration below shows the rear-panel of two 693x6 controller enclosures with FC host interface connection and iSCSI-based replication.

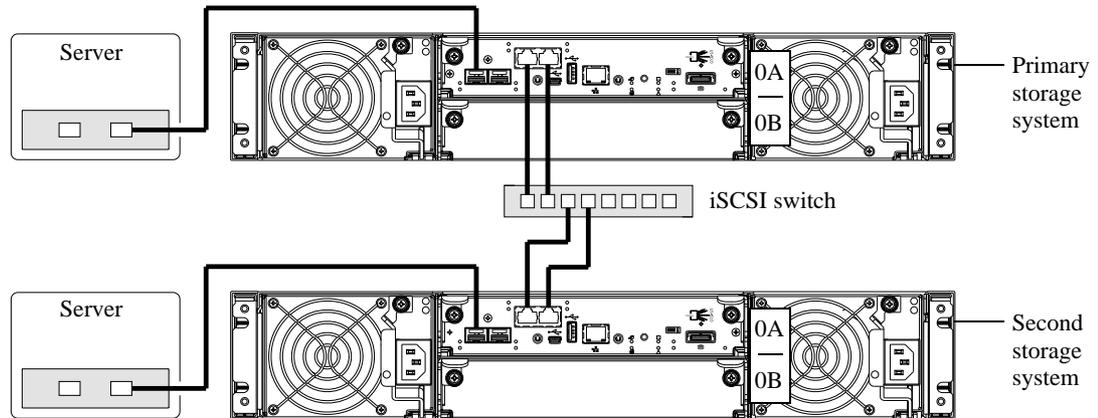


Figure 18 Connecting two storage systems for replication — single-controller module

Although not explicitly shown, the replication port-to-switch cabling logic illustrated in [Figure 18](#) (above) and [Figure 19](#) on page 41 applies to FC-based replication, albeit using FC ports instead of iSCSI ports, and FC switches in lieu of Ethernet switches.

Dual-controller configuration

Two servers/one switch/two storage systems

The illustration below shows the rear panel of two 693x6 controller enclosures with FC host interface connection and iSCSI-based replication.

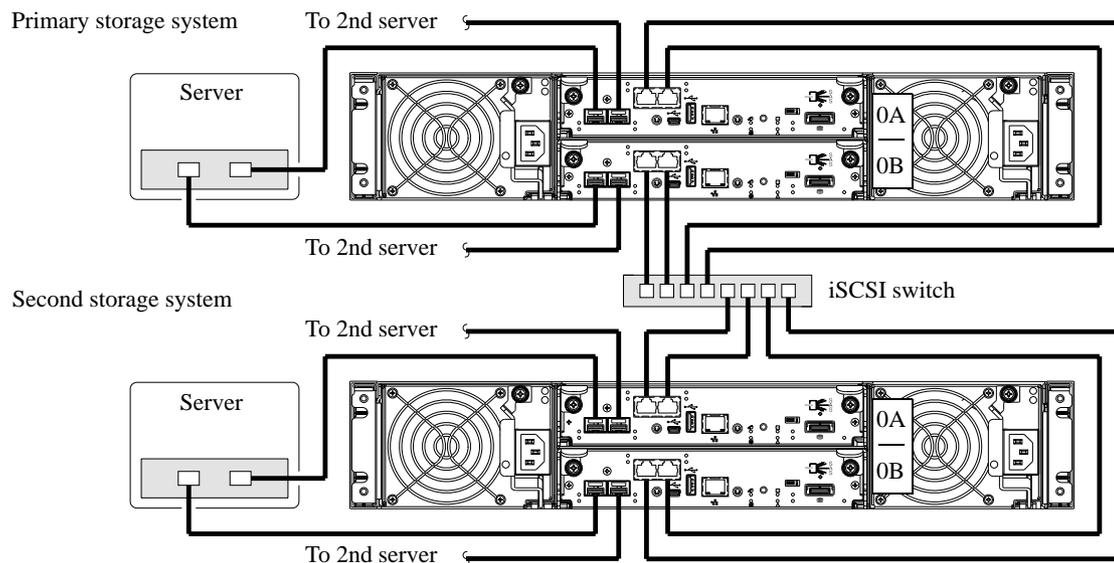


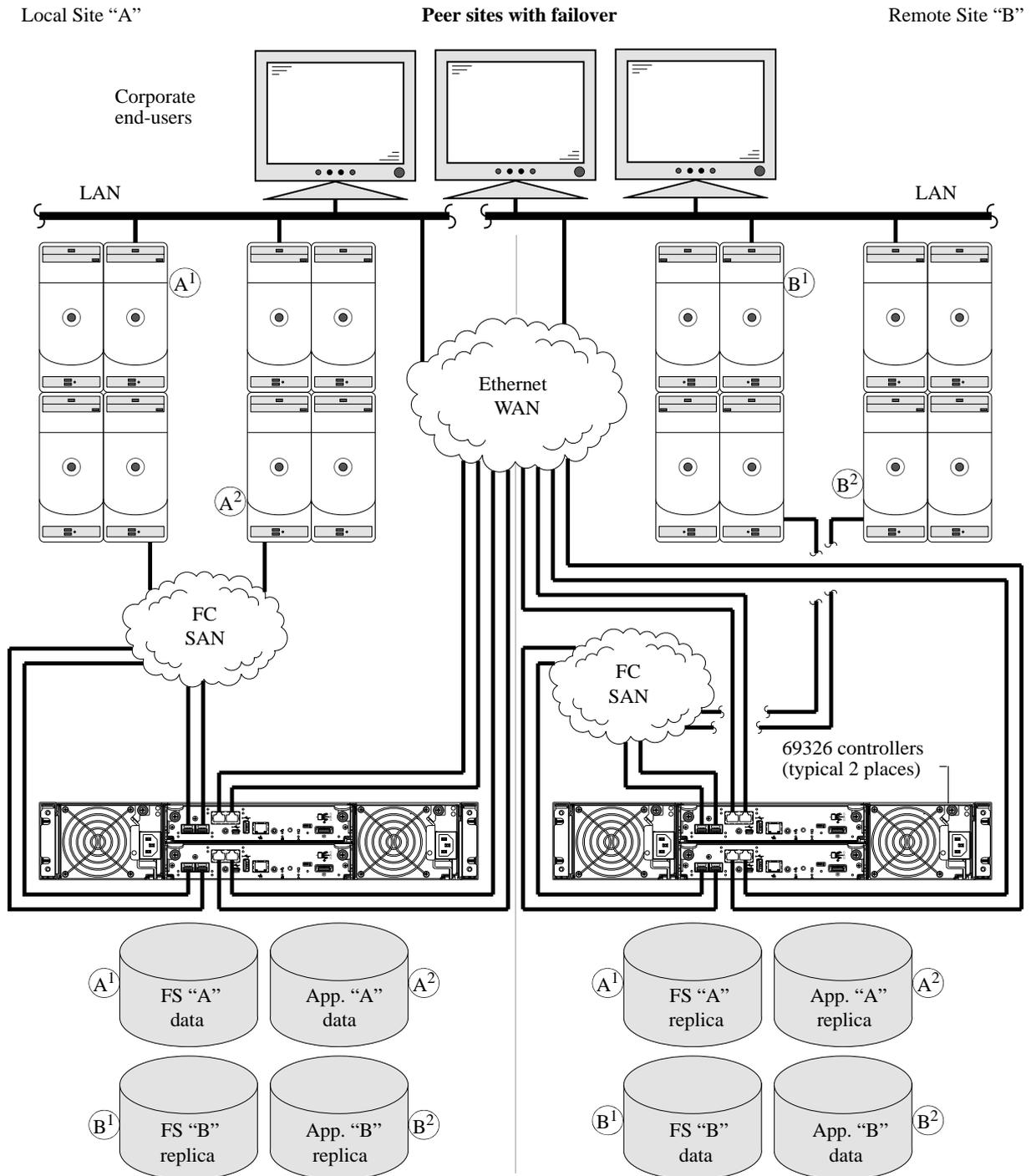
Figure 19 Connecting two storage systems for replication – dual-controller module

Additional dual-controller replication configurations follow herein.

 **NOTE:** See Phoenix RPC12 series RAIDar User Guide for more information about using AssuredRemote to perform replication actions. Systems must be cabled *before* performing replication.

Multiple servers/SAN fabric/Ethernet WAN/two storage systems

The illustration shows two 693x6 controller enclosures with FC host interface connection and iSCSI-based replication.



Key: Servers Codes:

- A¹ = "A" File Servers
- A² = "A" Application Servers
- B¹ = "B" File Servers
- B² = "B" Application Servers

Figure 20 Connecting two systems for AssuredRemote – 693x6 example

Multiple servers/FC SAN fabric/two storage systems

The illustration shows two 3720 or 693x1 controller enclosures with FC host interface connection and replication.

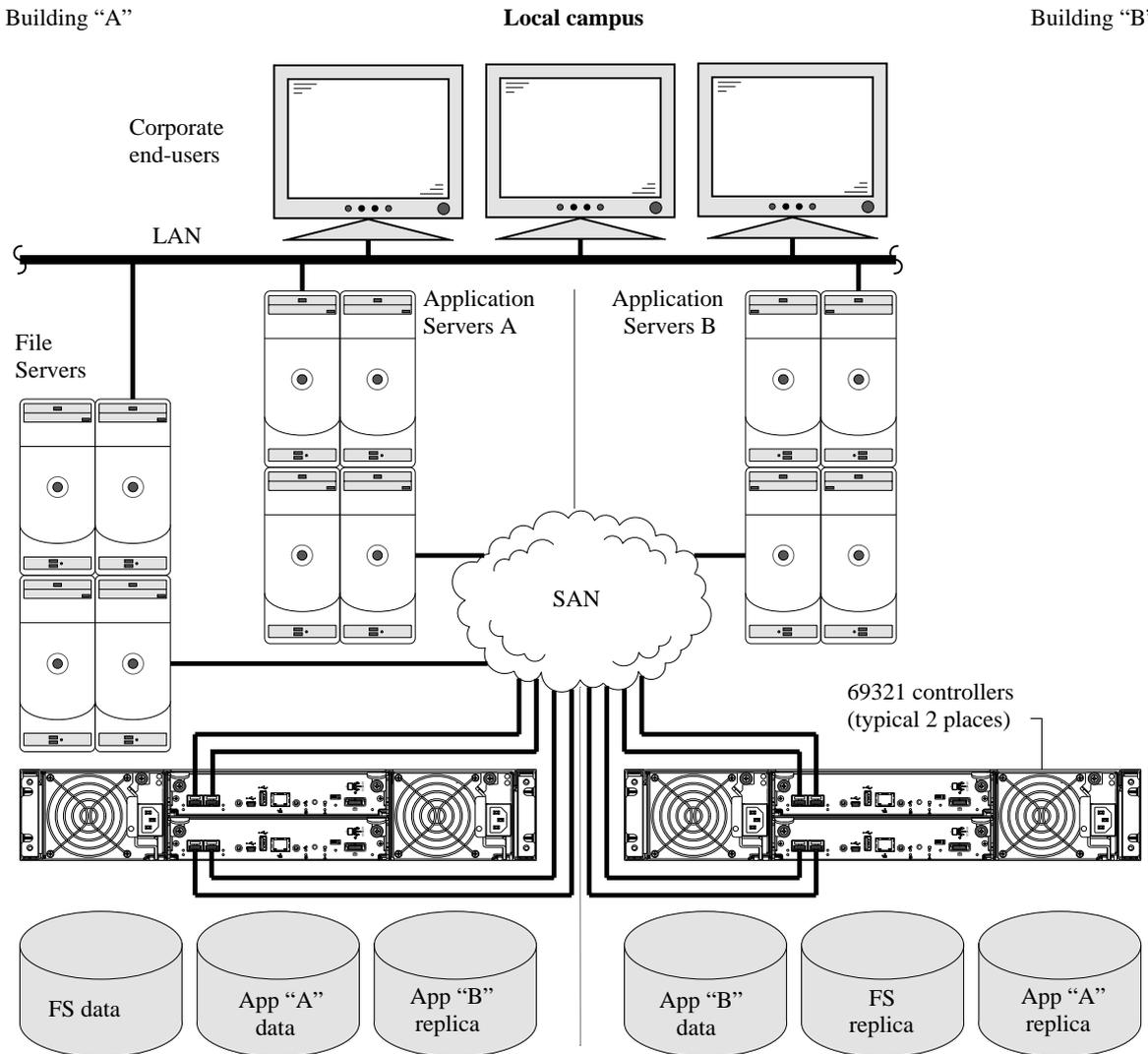


Figure 21 Connecting two systems for AssuredRemote — 693x1 example

Updating firmware

After installing the hardware and powering on the storage system components for the first time, verify that the controller modules, drive modules, and disk drives are using the current firmware release. Using RAIDar, right-click the system in the Configuration View panel, and select **Tools > Update Firmware**. The Update Firmware panel displays the currently installed firmware versions, and allows you to update them.

Obtaining IP values

You can configure addressing parameters for each controller module's network port. You can set static IP values or use DHCP.

Setting network port IP addresses using DHCP

In DHCP mode, network port IP address, subnet mask, and gateway values are obtained from a DHCP server if one is available. If a DHCP server is unavailable, current addressing is unchanged. You must

have some means of determining what addresses have been assigned, such as the list of bindings on the DHCP sever.

Because DHCP is disabled by default in RPC12 series systems, you must either use the CLI (Command Line Interface) to change controller IP address settings, or use RAIDar's Configuration Wizard as described in the Using the Configuration Wizard topic in the RAIDar user guide or online help.

Setting network port IP addresses using the CLI

If you did not use DHCP to set network port IP values, set them manually (default method) as described below. If you are using the USB CLI port and cable, you will need to enable the port for communication.

Network ports on controller module A and controller module B are configured with the following default values:

- **Network port IP address:** 10.0.0.1 (controller A), 10.0.0.2 (controller B)
- **IP subnet mask:** 255.255.255.0
- **Gateway IP address:** 0.0.0.0

If the default IP addresses are not compatible with your network, you must set an IP address for each network port using the command-line interface (CLI) embedded in each controller module. The CLI enables you to access the system using either the RS-232 or USB (universal serial bus) communication interfaces, and terminal emulation software.

 **NOTE:** If you are using the mini USB CLI port and cable, see Appendix D - [USB device connection](#):

- Windows customers should download and install the device driver as described in [Obtaining the software download](#) on page 86
 - Linux customers should prepare the USB port as described in [Setting parameters for the device driver](#) on page 82
-

Use the CLI commands described in the steps below to set the IP address for the Network port on each controller module.

Once new IP addresses are set, you can change them as needed using RAIDar. Be sure to change the IP address via RAIDar before changing the network configuration. See [Accessing RAIDar](#) on page 47 for more information concerning the web-based storage management application.

1. From your network administrator, obtain an IP address, subnet mask, and gateway address for controller A and another for controller B.
Record these IP addresses so you can specify them whenever you manage the controllers using RAIDar or the CLI.
2. Refer to the appropriate figure (below) corresponding to your CLI port's cable type (generic RPC12 series controller module shown).
 - [Figure 22](#) — Use the RS-232 (35mm jack) cable to connect controller A to a serial port on a host computer. The cable plugs into the controller's CLI port as shown.
Proceed to [step 3](#) below.
 - [Figure 23](#) — Use the USB cable to connect controller A to a USB port on a host computer. The USB mini 5 male connector plugs into the controller's CLI port as shown in [Figure 22](#).

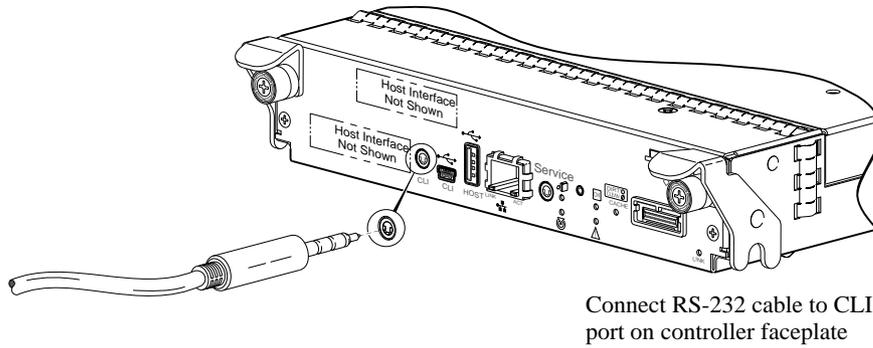


Figure 22 Connecting an RS-232 cable to the CLI port

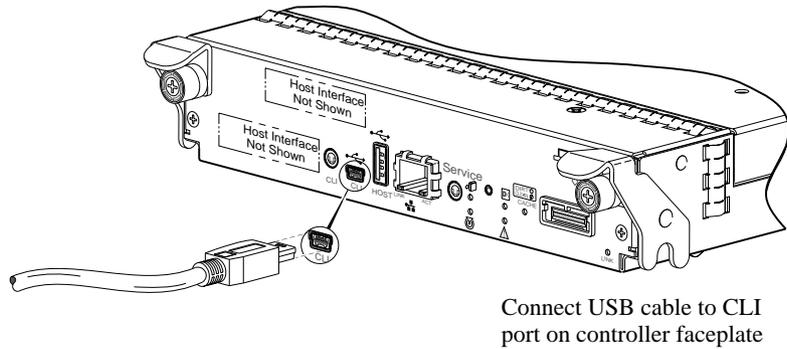


Figure 23 Connecting a USB cable to the CLI port

3. Start and configure a terminal emulator, such as HyperTerminal or VT-100, using the display settings in [Table 5](#) and the connection settings in [Table 6](#) (also, see the note following this procedure).

Table 5 Terminal emulator display settings

Parameter	Value
Terminal emulation mode	VT-100 or ANSI (for color support)
Font	Terminal
Translations	None
Columns	80

Table 6 Terminal emulator connection settings

Parameter	Value
Connector	COM1 (typically)
Baud rate	115,200
Data bits	8
Parity	None
Stop bits	1
Flow control	None

4. In the terminal emulator, connect to controller A.
5. Press Enter to display the CLI prompt (#).
The CLI displays the system version, MC version, and login prompt:

- a. At the login prompt, enter the default user `manage`.
- b. Enter the default password `!manage`.

If the default user or password — or both — have been changed for security reasons, enter the secure login code instead of the defaults shown above.

6. At the prompt, enter the following command to set the values you obtained in [step 1](#) for each Network port, first for controller A, and then for controller B:

```
set network-parameters ip address netmask netmask gateway gateway controller a|b
```

where:

- *address* is the IP address of the controller
- *netmask* is the subnet mask
- *gateway* is the IP address of the subnet router
- a|b specifies the controller whose network parameters you are setting

For example:

```
# set network-parameters ip 192.168.0.10 netmask 255.255.255.0 gateway
192.168.0.1 controller a

# set network-parameters ip 192.168.0.11 netmask 255.255.255.0 gateway
193.168.0.1 controller b
```

7. Type the following command to verify the new IP addresses:

```
show network-parameters
```

Network parameters, including the IP address, subnet mask, and gateway address are displayed for each controller.

8. Use the `ping` command to verify network connectivity.

For example:

```
# ping 192.168.0.10 (gateway)
Info: Pinging 192.168.0.10 with 4 packets.
Success: Command completed successfully. - The remote computer responded with 4
packets.
```

9. In the host computer's command window, type the following command to verify connectivity, first for controller A and then for controller B:

```
ping controller-IP-address
```

If you cannot access your system for at least three minutes after changing the IP address, you might have to restart the Management Controller(s) using the serial CLI.

When you restart a Management Controller, communication with it is temporarily lost until it successfully restarts.

Type the following command to restart the Management Controller in both controllers:

```
restart mc both
```

10. When you are done using the CLI, exit the emulator.

11. Retain the IP addresses (recorded in step 1) for accessing and managing the controllers using either RAIDar or the CLI.

 **NOTE:** Using HyperTerminal with the CLI on a **Microsoft Windows** host:

On a host computer connected to a controller module's mini-USB CLI port, incorrect command syntax in a HyperTerminal session can cause the CLI to hang. To avoid this problem, use correct syntax, use a different terminal emulator, or connect to the CLI using telnet rather than the mini-USB cable.

Be sure to close the HyperTerminal session before shutting down the controller or restarting its Management Controller. Otherwise the host's CPU cycles may rise unacceptably.

4 Basic operation

Verify that you have completed the sequential “Installation Checklist” instructions in [Table 2](#) on page 19. Once you have successfully completed steps 1 through 8 therein, you can access the management interfaces using your web-browser.

Accessing RAIDar

Upon completing the hardware installation, you can access the controller module’s web-based management interface, RAIDar, to monitor and manage the storage system. Invoke your web browser, and enter the IP address of the controller module’s network port in the address field (obtained during completion of “Installation Checklist” step 8), then press **Enter**. To sign in to RAIDar, use the default user name **manage** and password **!manage**. This brief Sign In discussion assumes proper web browser setup.

 **IMPORTANT:** For detailed information on accessing and using RAIDar, see the “Getting Started” section in the web-posted Phoenix RPC12 series RAIDar User Guide.

In addition to summarizing the process to configure and provision a new system for the first time — using the wizards — the Getting Started section provides instructions for signing in to RAIDar, introduces key system concepts, addresses browser setup, and provides tips for using the main window and the help window.

 **TIP:** After signing into RAIDar, you can use online help as an alternative to consulting the user guide.

Configuring and provisioning the storage system

Once you have familiarized yourself with RAIDar, use it to configure and provision the storage system. If you are licensed to use the optional AssuredRemote feature, you may also need to set up the storage systems for replication. Refer to the following chapters within the RAIDar user guide or online help:

- Getting started
- Configuring the system
- Provisioning the system
- Using AssuredRemote to replicate volumes

5 Troubleshooting

USB CLI port connection

Phoenix RPC12 series controllers feature a CLI port employing a mini-USB Type B form factor. If you encounter problems communicating with the port after cabling your computer to the USB device, you may need to either download a device driver (Windows), or set appropriate parameters via an operating system command (Linux). See Appendix D for more information.

Fault isolation methodology

Phoenix RPC12 series storage systems provide many ways to isolate faults. This section presents the basic methodology used to locate faults within a storage system, and to identify the pertinent FRUs (Field Replaceable Units) affected.

The basic fault isolation steps are:

- Gather fault information, including using system LEDs
- Determine where in the system the fault is occurring
- Review event logs
- If required, isolate the fault to a data path component or configuration

Cabling systems to enable use of the licensed AssuredRemote feature — to replicate volumes — is another important fault isolation consideration pertaining to initial system installation. See [Isolating AssuredRemote replication faults](#) on page 58 for more information.

Gather fault information

When a fault occurs, it is important to gather as much information as possible. Doing so will help you determine the correct action needed to remedy the fault.

Begin by reviewing the reported fault:

- *Is the fault related to an internal data path or an external data path?*
- *Is the fault related to a hardware component such as a drive module, controller module, or power supply?*

By isolating the fault to *one* of the components within the storage system, you will be able to determine the necessary corrective action more quickly.

Determine where the fault is occurring

Once you have an understanding of the reported fault, review the enclosure LEDs. The enclosure LEDs are designed to alert users of any system faults, and might be what alerted the user to a fault in the first place.

When a fault occurs, the Fault ID status LED on an enclosure's right ear illuminates (see the diagram pertaining to your product's front panel components on [page 13](#)). Check the LEDs on the back of the enclosure to narrow the fault to a FRU, connection, or both. The LEDs also help you identify the location of a FRU reporting a fault.

Use RAIDar to verify any faults found while viewing the LEDs. RAIDar is also a good tool to use in determining where the fault is occurring, if the LEDs cannot be viewed due to the location of the system. RAIDar provides you with a visual representation of the system and where the fault is occurring. It can also provide more detailed information about FRUs, data, and faults.

Review the event logs

The event logs record all system events. It is very important to review the logs, not only to identify the fault, but also to search for events that might have caused the fault to occur. For example, a host could lose connectivity to a virtual disk if a user changes channel settings without taking the storage resources assigned to it into consideration. In addition, the type of fault can help you isolate the problem to either hardware or software.

Isolate the fault

Occasionally, it might become necessary to isolate a fault. This is particularly true with data paths, due to the number of components comprising the data path. For example, if a host-side data error occurs, it could be caused by any of the components in the data path: controller module, cable, or data host.

If the enclosure does not initialize

It may take up to two minutes for the enclosures to initialize. If the enclosure does not initialize:

- Perform a rescan
- Power cycle the system
- Make sure the power cord is properly connected, and check the power source to which it is connected
- Check the event log for errors

Correcting enclosure IDs

When installing a system with drive enclosures attached, the enclosure IDs might not agree with the physical cabling order. This is because the controller might have been previously attached to some of the same enclosures during factory testing, and it attempts to preserve the previous enclosure IDs if possible. To correct this condition, make sure that both controllers are up, and perform a rescan using RAIDar or the CLI. This will reorder the enclosures, but can take up to two minutes for the enclosure IDs to be corrected.

To perform a rescan using the CLI, type the following command:

```
rescan
```

To rescan using RAIDar:

1. Verify that controllers are operating normally
2. In the Configuration View panel, right-click the system and select **Tools > Rescan Disk Channels**
3. Click **Rescan**

 **NOTE:** The reordering enclosure IDs action only applies to Dual Controller mode. If only one controller is available, due to either Single Controller configuration or controller failure, a manual rescan will not reorder the drive enclosure IDs.

Diagnostic steps

This section describes possible reasons and actions to take when an LED indicates a fault condition. See Appendix A – [LED descriptions](#) for descriptions of all LED statuses.

Is the front panel Fault/Service Required LED amber?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	A fault condition exists.	<ul style="list-style-type: none">• Check the LEDs on the back of the controller to narrow the fault to a FRU, connection, or both.• Check the event log for specific information regarding the fault.

Table 7 Diagnostics LED status — Front panel Fault/Service Required

Is the controller back panel FRU OK LED off?

Answer	Possible reasons	Actions
No (blinking)	System functioning properly. System is booting.	No action required. Wait for system to boot.
Yes	The controller module is not powered on. The controller module has failed.	<ul style="list-style-type: none"> Check that the controller module is fully inserted and latched in place, and that the enclosure is powered on. Check the event log for specific information regarding the failure.

Table 8 Diagnostics LED status — Rear panel FRU OK

Is the controller back panel Fault/Service Required LED amber?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes (blinking)	One of the following errors occurred: <ul style="list-style-type: none"> Hardware-controlled power-up error Cache flush error Cache self-refresh error 	<ul style="list-style-type: none"> Restart this controller from the other controller using RAIDar or the CLI. Remove the controller and reinsert it. Contact an authorized service provider for assistance. Replace the controller.

Table 9 Diagnostics LED status — Rear panel Fault/Service Required

Are both disk drive module LEDs off?

Answer	Possible reasons	Actions
Yes	<ul style="list-style-type: none"> There is no power The drive is offline The drive is not configured 	<ul style="list-style-type: none"> Check that the drive is fully inserted and latched in place, and that the enclosure is powered on.

Table 10 Diagnostics LED status — Disk drives

Is the disk drive module Power/Activity/Fault LED blinking amber?

Answer	Possible reasons	Actions
Yes, and the Online/Activity LED is off.	The drive is offline. A predictive failure alert may have been received for this device.	<ul style="list-style-type: none"> Check the event log for specific information regarding the fault. Isolate the fault. Contact an authorized service provider for assistance.
Yes, and the Online/Activity LED is blinking.	The drive is active, but a predictive failure alert may have been received for this device.	<ul style="list-style-type: none"> Check the event log for specific information regarding the fault. Isolate the fault. Contact an authorized service provider for assistance.

Table 11 Diagnostics LED status — Disk drive Power/Activity/Fault

Is a connected host port's Host Link Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required (see Link LED note: page 70).
Yes	The link is down.	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary • Inspect cable for damage. • Swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. • Verify that the switch, if any, is operating properly. If possible, test with another port. • Verify that the HBA is fully seated, and that the PCI slot is powered on and operational. • In RAIDar, review event logs for indicators of a specific fault in a host data path component. • Contact an authorized service provider for assistance. • See Isolating a host-side connection fault on page 55.

Table 12 Diagnostics LED status — Rear panel Host Link Status

Is a connected port's Expansion Port Status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • Inspect cable for damage. • Swap cables to determine if fault is caused by a defective cable. Replace cable if necessary. • In RAIDar, review the event logs for indicators of a specific fault in a host data path component. • Contact an authorized service provider for assistance. • See Isolating a controller module expansion port connection fault on page 57.

Table 13 Diagnostics LED status — Rear panel Expansion Port Status

Is a connected port's Network Port link status LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The link is down.	Use standard networking troubleshooting procedures to isolate faults on the network.

Table 14 Diagnostics LED status — Rear panel Network Port Link Status

Is the power supply's Input Power Source LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The power supply is not receiving adequate power.	<ul style="list-style-type: none"> • Verify that the power cord is properly connected, and check the power source to which it connects. • Check that the power supply FRU is firmly locked into position. • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance.

Table 15 Diagnostics LED status — Power supply Input Power Source

Is the drive enclosure rear panel OK LED off?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.
Yes	The power supply unit or a fan is operating at an unacceptable voltage/RPM level, or has failed.	<p>When isolating faults in the power supply, remember that the fans in both modules receive power through a common bus on the midplane, so if a power supply unit fails, the fans continue to operate normally.</p> <ul style="list-style-type: none"> • Verify that the power supply FRU is firmly locked into position. • Verify that the AC cord is connected to a power source. • Verify that the AC cord is connected to the enclosure's power supply unit.

Table 16 Diagnostics LED status — Drive enclosure rear panel OK

Is the drive enclosure Fault/Service Required LED amber?

Answer	Possible reasons	Actions
No	System functioning properly.	No action required.

Table 17 Diagnostics LED status — Drive enclosure front panel Fault/Service Required

Answer	Possible reasons	Actions
Yes (blinking)	One of the following errors occurred: <ul style="list-style-type: none"> • Hardware-controlled power-up error • Cache flush error • Cache self-refresh error 	<ul style="list-style-type: none"> • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance. • Replace if necessary.
Yes	A fault occurred. If installing an I/O module FRU, the module has not gone online and likely failed its self-test.	<ul style="list-style-type: none"> • Check the event log for specific information regarding the fault. • Isolate the fault. • Contact an authorized service provider for assistance. • Replace if necessary. • If installing an I/O module FRU, try removing and reinstalling the new I/O module, and check the event log for errors.

Table 17 Diagnostics LED status — Drive enclosure front panel Fault/Service Required

Controller failure in a single-controller configuration

Cache memory is flushed to CompactFlash in the case of a controller failure or power loss. During the write to CompactFlash process, only the components needed to write the cache to the CompactFlash are powered by the super-capacitor. This process typically takes 60 seconds per 1 Gbyte of cache. After the cache is copied to CompactFlash, the remaining power left in the super-capacitor is used to refresh the cache memory. While the cache is being maintained by the super-capacitor, the Cache Status LED flashes at a rate of 1/10 second off and 9/10 second on.

If the controller has failed or does not start, is the Cache Status LED on/blinking?

Answer	Actions
No, the Cache LED status is off, and the controller does not boot.	If valid data is thought to be in Flash, see Transporting cache via professional services ; otherwise, replace the controller.
No, the Cache Status LED is off, and the controller boots.	The system is flushing data to disks. If the problem persists, replace the controller.
Yes, at a strobe 1:10 rate - 1 Hz, and the controller does not boot.	See Transporting cache via professional services .
Yes, at a strobe 1:10 rate - 1 Hz, and the controller boots.	The system is flushing data to disks. If the problem persists, replace the controller.
Yes, at a blink 1:1 rate - 1 Hz, and the controller does not boot.	See Transporting cache via professional services .
Yes, at a blink 1:1 rate - 1 Hz, and the controller boots.	The system is flushing data to disks. If the problem persists, replace the controller.

Table 18 Diagnostics LED status — Rear panel Cache Status

Transporting cache via professional services

 **IMPORTANT:** Transportable cache only applies to single-controller configurations. In dual-controller configurations, there is no need to transport a failed controller's cache to a replacement controller because the cache is duplicated between the controllers.

To preserve the existing data stored in the CompactFlash, you must transport the CompactFlash from the failed controller to a replacement controller. To transport cache, you must return the controller module to a maintenance depot, for servicing by qualified personnel.

 **CAUTION:** Transporting of cache must be performed by a qualified service technician.

Isolating a host-side connection fault

During normal operation, when a controller module host port is connected to a data host, the port's host link status LED and host link activity LED are green. If there is I/O activity, the host activity LED blinks green. If data hosts are having trouble accessing the storage system, and you cannot locate a specific fault or cannot access the event logs, use the following procedure. This procedure requires scheduled downtime.

 **IMPORTANT:** Do not perform more than one step at a time. Changing more than one variable at a time can complicate the troubleshooting process.

Host-side connection troubleshooting featuring FC or 10GbE iSCSI host ports

The procedure below pertains to Phoenix RPC12 series controller enclosures employing small form factor pluggable (SFP) transceiver connectors in either 2/4/8Gb Fibre Channel or 10GbE iSCSI host interface ports. In the following procedure, *SFP* and *host cable* are used to refer to either an SFP with FC cable or a qualified 10GbE SFP+ option.

1. Halt all I/O to the storage system.
2. Check the host activity LED.
If there is activity, halt all applications that access the storage system.
3. Check the Cache Status LED to verify that the controller's cached data are flushed to the disk drives.
 - Blinking – Data are still being written to disk.
 - Off – Cache is clean (no unwritten data).
4. Inspect the cable for damage.
5. Reseat the SFP and host cable.
Is the host link status LED on?
 - Yes – Monitor the status to ensure that there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
 - No – Proceed to the next step.
6. Move the SFP and host cable to a port with a known good link status.
This step isolates the problem to the external data path (SFP, host cable, and host-side devices) or to the controller module port.
Is the host link status LED on?
 - Yes – You now know that the SFP, host cable, and host-side devices are functioning properly. Return the SFP and cable to the original port. If the link status LED remains off, you have isolated the fault to the controller module's port. Replace the controller module.

- No – Proceed to the next step.
7. Swap the SFP with the known good one.
Is the host link status LED on?
 - Yes – You have isolated the fault to the SFP. Replace the SFP.
 - No – Proceed to the next step.
 8. Re-insert the original SFP and swap the cable with a known good one.
Is the host link status LED on?
 - Yes – You have isolated the fault to the cable. Replace the cable.
 - No – Proceed to the next step.
 9. Verify that the switch, if any, is operating properly. If possible, test with another port.
 10. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
 11. Replace the HBA with a known good HBA, or move the host side cable and SFP to a known good HBA.
Is the host link status LED on?
 - Yes – You have isolated the fault to the HBA. Replace the HBA.
 - No – It is likely that the controller module needs to be replaced.
 12. Move the cable and SFP back to its original port.
Is the host link status LED on?
 - No – The controller module's port has failed. Replace the controller module.
 - Yes – Monitor the connection for a period of time. It may be an intermittent problem, which can occur with SFPs, damaged cables, and HBAs.

Host-side connection troubleshooting featuring SAS or iSCSI host ports

The procedure below applies to Phoenix RPC12 series controller enclosures configured with either 6Gb SFF miniSAS or 1Gb iSCSI host interface ports.

1. Halt all I/O to the storage system.
2. Check the host activity LED.
If there is activity, halt all applications that access the storage system.
3. Check the Cache Status LED to verify that the controller's cached data are flushed to the disk drives.
 - Blinking – Data are still being written to disk.
 - Off – Cache is clean (no unwritten data).
4. Inspect the cable for damage.
5. Reseat the cable.
Is the host link status LED on?
 - Yes – Monitor the status to ensure that there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
 - No – Proceed to the next step.
6. Move the cable to a port with a known good link status.
This step isolates the problem to the external data path (host cable and host-side devices) or to the controller module port.
Is the host link status LED on?
 - Yes – You now know that the host cable and host-side devices are functioning properly. Return the cable to the original port. If the link status LED remains off, you have isolated the fault to the controller module's port. Replace the controller module.
 - No – Proceed to the next step.
7. Verify that the switch, if any, is operating properly. If possible, test with another port.
8. Verify that the HBA is fully seated, and that the PCI slot is powered on and operational.
9. Replace the HBA with a known good HBA, or move the host side cable to a known good HBA.

Is the host link status LED on?

- Yes – You have isolated the fault to the HBA. Replace the HBA.
- No – It is likely that the controller module needs to be replaced.

10. Move the cable back to its original port.

Is the host link status LED on?

- No – The controller module's port has failed. Replace the controller module.
- Yes – Monitor the connection for a period of time. It may be an intermittent problem, which can occur with damaged cables and HBAs.

Isolating a controller module expansion port connection fault

During normal operation, when a controller module's expansion port is connected to a drive enclosure, the expansion port status LED is green. If the connected port's expansion port LED is off, the link is down. Use the following procedure to isolate the fault.

This procedure requires scheduled downtime.

 **NOTE:** Do not perform more than one step at a time. Changing more than one variable at a time can complicate the troubleshooting process.

1. Halt all I/O to the storage system.

2. Check the host activity LED.

If there is activity, halt all applications that access the storage system.

3. Check the Cache Status LED to verify that the controller's cached data are flushed to the disk drives.

- Blinking – Data are still being written to disk.
- Off – Cache is clean (no unwritten data).

4. Reseat the expansion cable, and inspect it for damage.

Is the expansion port status LED on?

- Yes – Monitor the status to ensure there is no intermittent error present. If the fault occurs again, clean the connections to ensure that a dirty connector is not interfering with the data path.
- No – Proceed to [step 5](#).

5. Move the expansion cable to a port on the controller enclosure with a known good link status.

This step isolates the problem to the expansion cable or to the controller module's expansion port.

Is the expansion port status LED on?

- Yes – You now know that the expansion cable is good. Return the cable to the original port. If the expansion port status LED remains off, you have isolated the fault to the controller module's expansion port. Replace the controller module.
- No – Proceed to the next step.

6. Move the expansion cable back to the original port on the controller enclosure.

7. Move the expansion cable on the drive enclosure to a known good expansion port on the drive enclosure.

Is the expansion port status LED on?

- Yes – You have isolated the problem to the drive enclosure's port. Replace the expansion module.
- No – Proceed to [step 8](#).

8. Replace the cable with a known good cable, ensuring the cable is attached to the original ports used by the previous cable.

Is the host link status LED on?

- Yes – Replace the original cable. The fault has been isolated.
- No – It is likely that the controller module must be replaced.

Isolating AssuredRemote replication faults

Cabling for replication

AssuredRemote replication is a disaster-recovery feature that performs batch replication of block-level data from a primary volume in one RPC12 series controller enclosure to a secondary volume on the same system, or on a second, independent RPC12 series controller enclosure. The second system can be located at the same site as the first system, or at a different site. See [Connecting two storage systems to replicate volumes](#) on page 38 for host connection information concerning AssuredRemote.

 **NOTE:** See the AssuredRemote topic within the RAIDar guide or online help for additional information. 3920/3930 and 3720/693x1 models support AssuredRemote replication; whereas 3520/69704 and 3420/3430 models do not.

 **CAUTION:** When replacing a RPC12 series controller set supporting AssuredRemote with a RPC12 series controller set that does not support this licensed feature (e.g., 69704), you must first delete all replication sets before swapping the controller modules. Not doing so will lead to unexpected results, and there is no way to delete replication sets after the installation. See the upgrade document supporting your product for additional information.

Replication setup and verification

After storage systems and hosts are cabled for replication, you can prepare to replicate a volume or snapshot. Optionally, you can telnet to access the IP address of the controller module and access the AssuredRemote feature using the CLI.

 **NOTE:** Refer to the following manuals for more information on replication setup:

- See Phoenix RPC12 series RAIDar User Guide for procedures to setup and manage replications.
 - See Phoenix RPC12 series CLI Reference Guide for replication commands and syntax.
 - See Phoenix RPC12 series Event Descriptions Reference Guide for replication event reporting.
-

Basic information for enabling the RPC12 series controller enclosures for replication supplements the troubleshooting procedures that follow.

1. Familiarize yourself with AssuredRemote by reviewing the Getting started and Using AssuredRemote to replicate volumes chapters in the RAIDar User Guide.
2. See descriptions and recommendations for replication-related events in the Event Descriptions Reference Guide.
3. Within the RAIDar User Guide's Using AssuredRemote to replicate volumes chapter, follow the procedure entitled Setting up Replication.

This procedure will help you to prepare to replicate an existing volume to another vdisk in the local system or to a remote system. Once setup is successfully completed, you can initiate replication from RAIDar's Configuration View panel. Alternatively, you can use CLI commands.

Diagnostic steps for replication setup

Can you access the AssuredRemote feature?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Invalid cabling connection. (If multiple controller enclosures are used, check the cabling for each system.)	Verify controller enclosure cabling: <ul style="list-style-type: none"> • Verify use of proper cables. • Verify proper cabling paths for host connections. • Verify cabling paths between replication ports and switches on the same fabric or network. • Verify that cable connections are securely fastened. • Inspect cables for damage and replace if necessary.
No	AssuredRemote is not licensed on each controller enclosure used for replication.	Verify licensing of the optional feature per system: <ul style="list-style-type: none"> • In RAIDar's Configuration View panel, right-click on the system, and select View > Overview. Within the System Overview table, select the Licensed Features component to display the status of licensed features. • If the Replication property is not enabled, obtain and install a valid license.

Table 19 Diagnostics for replication setup – Accessing AssuredRemote feature

Can you view information about remote links?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Communication link is down	<ul style="list-style-type: none"> • Check cable connections and reseal if necessary. • Inspect cable for damage. • Swap cables to determine if fault is caused by a defective cable; replace cable if necessary. • In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. • In RAIDar's Configuration View panel, right-click the remote system, and select Tools > Check Remote System Link. Click Check Links.

Table 20 Diagnostics for replication setup – Viewing information about remote links

Can you create a replication set, or select an existing one?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Unable to select the primary volume that contains the data to replicate?	<ul style="list-style-type: none"> • In RAIDar's Configuration View panel, expand vdisk entries to show secondary volumes. • In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component.

Table 21 Diagnostics for replication setup – Creating or selecting a replication set

Answer	Possible reasons	Actions
No	Unable to select the replication mode? ¹	<ul style="list-style-type: none"> In RAIDar, review event logs for indicators of a specific fault in a host or replication data path component. In RAIDar's Configuration View panel, right-click a subordinate volume, and select View > Overview to view links. Local Replication mode replicates to a secondary volume residing in the local storage system. Verify selection of a valid local volume on disk. Remote Replication mode replicates to a secondary volume residing in an independent storage system: <ul style="list-style-type: none"> Verify selection of valid remote volume on disk. Verify valid IP address of remote system's network port. Verify user name with Manage role on remote system. Verify that user's password.
No	Unable to select the secondary volume (the destination volume on the vdisk to which you will replicate data from the primary volume)? ¹	<ul style="list-style-type: none"> In RAIDar, review event logs for indicators of a specific fault in a replication data path component. Verify valid specification of the secondary volume according to either of the following criteria: <ul style="list-style-type: none"> Creation of the new volume on disk Selection of replication-prepared volume In RAIDar's Configuration View panel, right-click the secondary volume, and select View > Overview to display the Replication Volume Overview table. <ul style="list-style-type: none"> Verify the type and numbering of ports used for the inter-system link. Verify that the vdisk volume has sufficient space to accommodate replicated data.
No	Communication link is down.	<ul style="list-style-type: none"> See actions described in Can you view information about remote links? on page 59.
¹ After ensuring valid licensing, valid cabling connections, and network availability, create the replication set as described in the Setting up replication topic within the RAIDar user guide.		

Table 21 Diagnostics for replication setup — Creating or selecting a replication set

Can you replicate a volume?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Nonexistent replication set.	<ul style="list-style-type: none"> Determine existence of primary or secondary volumes. If a replication set has not been successfully created, use RAIDar to create one as described in the Setting up replication topic in the RAIDar user guide. In RAIDar, review event logs for indicators of a specific fault in a replication data path component.

Table 22 Diagnostics for replication setup — Replicating a volume

Answer	Possible reasons	Actions
No	Network error occurred during in-progress replication.	<ul style="list-style-type: none"> In RAIDar, review event logs for indicators of a specific fault in a replication data path component. In RAIDar's Configuration View panel, right-click the secondary volume, and select View > Overview to display the Replication Volume Overview table: <ul style="list-style-type: none"> Check for replication interruption suspended status. Check for inconsistent status. Check for offline status. Replications that enter the suspended state must be resumed manually.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 59.

Table 22 Diagnostics for replication setup — Replicating a volume

Can you view a replication image?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Nonexistent replication image.	<ul style="list-style-type: none"> In RAIDar's Configuration View panel, expand vdisks and subordinate volumes to reveal the existence of a replication image. If a replication image has not been successfully created, use RAIDar to create one as described in the Setting up Replication topic in the RAIDar user guide.
No	Communication link is down.	See actions described in Can you view information about remote links? on page 59.

Table 23 Diagnostics for replication setup — Viewing a replication image

Can you view remote systems?

Answer	Possible reasons	Actions
Yes	System functioning properly.	No action required.
No	Non-existent replication set.	See actions described in Can you replicate a volume? on page 60.
	Communication link is down.	See actions described in Can you view information about remote links? on page 59.

Table 24 Diagnostics for replication setup — Viewing a remote system

Resolving voltage and temperature warnings

1. Check that all of the fans are working by making sure each power supply's Voltage/Fan Fault/Service Required LED is off, or by using RAIDar to check for yellow yield icon hardware warnings. (In the Configuration View panel, right click the enclosure and click **View > Overview**.)
2. Make sure that all modules are fully seated in their slots and that their latches are locked.
3. Make sure that no slots are left open for more than two minutes.

If you need to replace a module, leave the old module in place until you have the replacement or use a blank module to fill the slot. Leaving a slot open negatively affects the airflow and can cause the enclosure to overheat.

4. Try replacing each power supply one at a time.
5. Replace the controller modules one at a time.

Sensor locations

The storage system monitors conditions at different points within each enclosure to alert you to problems. Power, cooling fan, temperature, and voltage sensors are located at key points in the enclosure. In each controller module and expansion module, the enclosure management processor (EMP) monitors the status of these sensors to perform SCSI enclosure services (SES) functions.

The following sections describe each element and its sensors.

Power supply sensors

Each enclosure has two fully redundant power supplies with load-sharing capabilities. The power supply sensors described in the following table monitor the voltage, current, temperature, and fans in each power supply. If the power supply sensors report a voltage that is under or over the threshold, check the input voltage.

Table 25 Power supply sensors

Description	Event/Fault ID LED condition
Power supply 1	Voltage, current, temperature, or fan fault
Power supply 2	Voltage, current, temperature, or fan fault

Cooling fan sensors

Each power supply includes two fans. The normal range for fan speed is 4,000 to 6,000 RPM. When a fan's speed drops below 4,000 RPM, the EMP considers it a failure and posts an alarm in the storage system's event log. The following table lists the description, location, and alarm condition for each fan. If the fan speed remains under the 4,000 RPM threshold, the internal enclosure temperature may continue to rise. Replace the power supply reporting the fault.

Table 26 Cooling fan sensor descriptions

Description	Location	Event/Fault ID LED condition
Fan 1	Power supply 1	< 4,000 RPM
Fan 2	Power supply 1	< 4,000 RPM
Fan 3	Power supply 2	< 4,000 RPM
Fan 4	Power supply 2	< 4,000 RPM

During a shutdown, the cooling fans do not shut off. This allows the enclosure to continue cooling.

Temperature sensors

Extreme high and low temperatures can cause significant damage if they go unnoticed. Each controller module has six temperature sensors. Of these, if the CPU or FPGA (Field-programmable Gate Array) temperature reaches a shutdown value, the controller module is automatically shut down. Each power supply has one temperature sensor.

When a temperature fault is reported, it must be remedied as quickly as possible to avoid system damage. This can be done by warming or cooling the installation location.

Table 27 Controller module temperature sensors

Description	Normal operating range	Warning operating range	Critical operating range	Shutdown values
CPU temperature	3–88°C	0–3°C, 88–90°C	> 90°C	0°C 100°C
FPGA temperature	3–97°C	0–3°C, 97–100°C	None	0°C 100°C
Onboard temperature 1	0–70°C	None	None	None
Onboard temperature 2	0–70°C	None	None	None
Onboard temperature 3 (Capacitor temperature)	0–70°C	None	None	None
CM temperature	5–50°C	≤ 5°C, ≥ 50°C	≤ 0°C, ≥ 55°C	None

When a power supply sensor goes out of range, the Fault/ID LED illuminates amber and an event is logged to the event log.

Table 28 Power supply temperature sensors

Description	Normal operating range
Power Supply 1 temperature	–10–80°C
Power Supply 2 temperature	–10–80°C

Power supply module voltage sensors

Power supply voltage sensors ensure that an enclosure's power supply voltage is within normal ranges. There are three voltage sensors per power supply.

Table 29 Voltage sensor descriptions

Sensor	Event/Fault LED condition
Power supply 1 voltage, 12V	< 11.00V > 13.00V
Power supply 1 voltage, 5V	< 4.00V > 6.00V
Power supply 1 voltage, 3.3V	< 3.00V > 3.80V

A LED descriptions

12-drive enclosure front panel LEDs

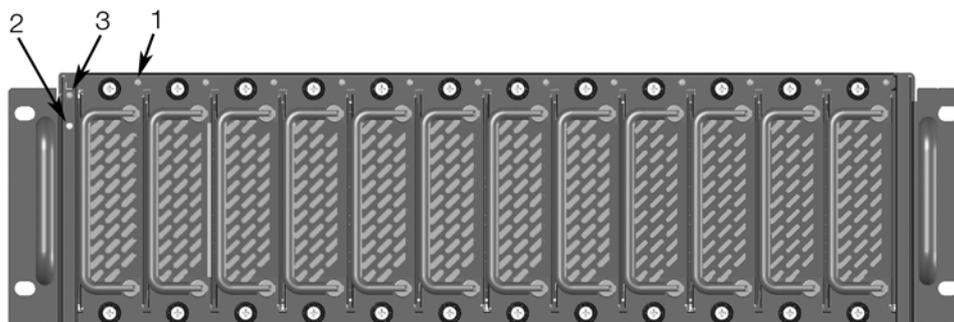


Table 30 LEDs — 3U12 enclosure front panel

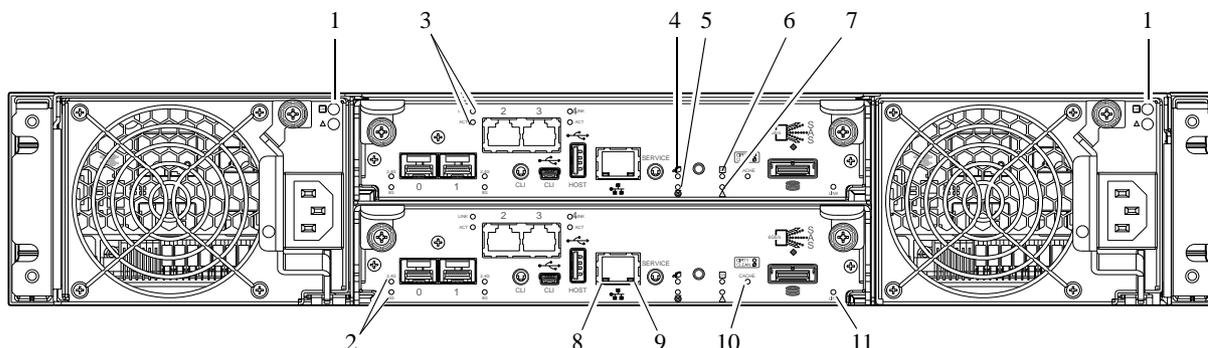
LED	Description	Definition
1	Disk drive — LED	See Table 31 below , Disk drive LEDs.
2	Fault/Service Required ID	Yellow — On Enclosure-level fault condition exists. The event has been acknowledged but the problem needs attention. Off — No fault condition exists.
3	FRU OK	Green — On The enclosure is powered on with at least one power supply operating normally. Off — Both power supplies are off; the system is powered off.

Disk drive LEDs

Table 31

LED No./Description	Color	State	Definition
Power/Activity/Fault	Green	On	The disk drive module is operating normally.
		Blink	The disk drive module is initializing; active and processing I/O; is performing a media scan; or the vdisk is initializing or rebuilding.
		Off	If neither green nor amber, the disk drive module is not powered on.
	Amber	On	The disk has failed; experienced a fault; is a leftover; or the vdisk is down or critical.
		Blink	Physically identifies the drive module.
		Off	If neither green nor amber, the disk drive module is not powered on.

693x6 rear panel LEDs



Note: Callouts do not tag multiple instances of an identified LED

Table 32 LEDs — 693x6 rear panel

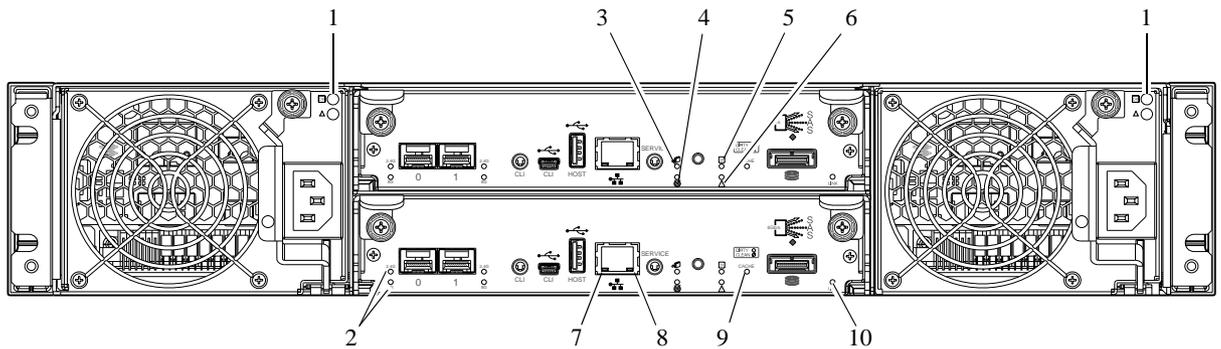
LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 72.
2 — Link Status/ Link Activity (Host 2/4/8 Gb FC)	Green	On	2,4G LED illuminates — link speed is 2 or 4-Gbps 8G LED illuminates — link speed is 8-Gbps
		Off	Both LEDs off — link speed is 1-Gbps ¹
		Blink	1Hz — no link detected
3 — Host 1 Gb iSCSI Link Status	Green	On	The port is connected and the link is up.
Link Activity	Green	Off	The port is empty or the link is down.
		Blink	Link has I/O activity. Link is idle.
4 — OK to Remove	Blue	On	The controller module can be removed.
		Off	The controller module is not prepared for removal.
5 — Unit Locator	White	Off	Normal operation.
		Blink	Physically identifies the controller module.
6 — FRU OK	Green	On	Controller module is operating normally.
		Off	Controller module is not OK.
		Blink	System is booting.
7 — Fault/Service Required	Yellow	On	A fault is detected or a service action is required.
		Blink	Hardware-controlled power-up, or a cache flush or restore error.
8 — Network Port Link Status	Green	On	The Ethernet link is up.
		Off	Ethernet port is not connected or the link is down.
9 — Network Port Activity	Green	Off	Ethernet link has no I/O activity.
		Blink	Ethernet link has I/O activity.

Table 32 LEDs — 693x6 rear panel

LED No./Description	Color	State	Definition
10 — Cache Status	Green	On Off Blink	Cache is dirty and operation is normal. Cache is clean (contains no unwritten data). CompactFlash flush or cache self-refresh is in progress, indicating cache activity.
11 — Expansion Port Status	Green	On Off	Port is connected and the link is up. Port is empty or link is down.

¹The 8 Gb SFP modules do not support 1 Gb link speeds.

693x1 rear panel LEDs



Note: Callouts do not tag multiple instances of an identified LED

Table 33 LEDs — 693x1 rear panel

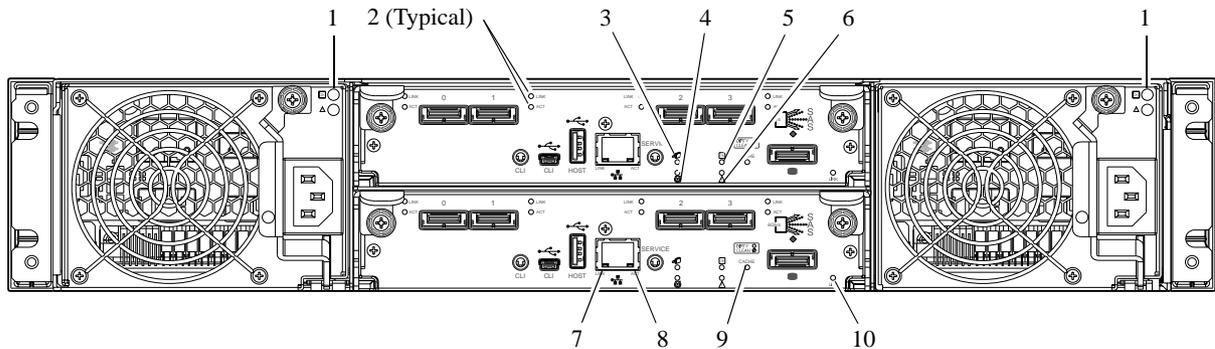
LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 72.
2 — Link Status/ Link Activity (Host 2/4/8 Gb FC)	Green	On Off Blink	2,4G LED illuminates — link speed is 2 or 4-Gbps 8G LED illuminates — link speed is 8-Gbps Both LEDs off — link speed is 1-Gbps ¹ 1Hz — no link detected
3 — OK to Remove	Blue	On Off	The controller module can be removed. The controller module is not prepared for removal.
4 — Unit Locator	White	Off Blink	Normal operation. Physically identifies the controller module.
5 — FRU OK	Green	On Off Blink	Controller module is operating normally. Controller module is not OK. System is booting.
6 — Fault/Service Required	Yellow	On Blink	A fault is detected or a service action is required. Hardware-controlled power-up, or a cache flush or restore error.
7 — Network Port Link Status	Green	On Off	The Ethernet link is up. Ethernet port is not connected or the link is down.

Table 33 LEDs — 693x1 rear panel

LED No./Description	Color	State	Definition
8 — Network Port Activity	Green	Off Blink	Ethernet link has no I/O activity. Ethernet link has I/O activity.
9 — Cache Status	Green	On Off Blink	Cache is dirty and operation is normal. Cache is clean (contains no unwritten data). CompactFlash flush or cache self-refresh is in progress, indicating cache activity.
10 — Expansion Port Status	Green	On Off	Port is connected and the link is up. Port is empty or link is down.

¹The 8 Gb SFP modules do not support 1 Gb link speeds.

693x4 rear panel LEDs



Note: Callouts do not tag multiple instances of an identified LED

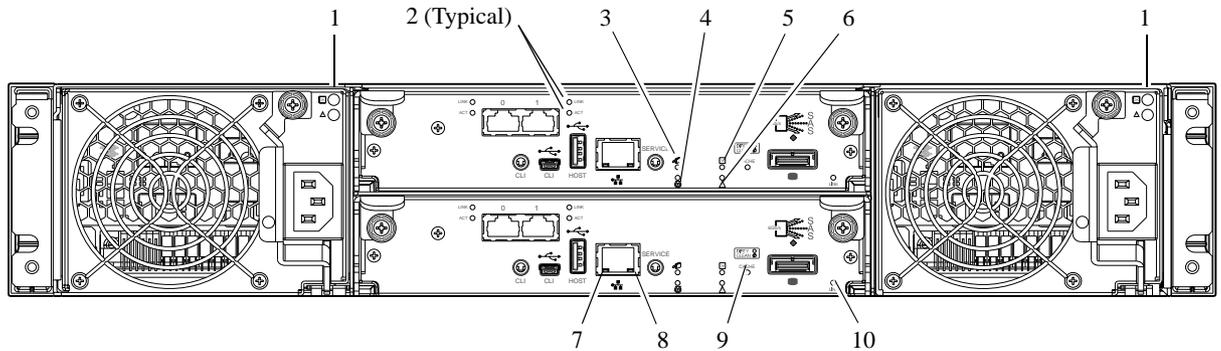
Table 34 LEDs — 693x4 rear panel

LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 72.
2 — 6Gb SAS Link Status 6Gb SAS Link Activity (ports 0-3)	Green	On Off Blink Off	The port is connected and the link is up. The port is empty or the link is down. Link has I/O activity. Link is idle.
3 — OK to Remove	Blue	On Off	The controller module can be removed. The controller module is not prepared for removal.
4 — Unit Locator	White	Off Blink	Normal operation. Physically identifies the controller module.
5 — FRU OK	Green	On Off Blink	Controller module is operating normally. Controller module is not OK. System is booting.
6 — Fault/Service Required	Yellow	On Blink	A fault is detected or a service action is required. Hardware-controlled power-up, or a cache flush or restore error.

Table 34 LEDs — 693x4 rear panel

LED No./Description	Color	State	Definition
7 — Network Port Link Status	Green	On Off	Ethernet link is up. Ethernet port is not connected or the link is down.
8 — Network Port Activity	Green	Off Blink	Ethernet link has no I/O activity. Ethernet link has I/O activity.
9 — Cache Status	Green	On Off Blink	Cache is dirty and operation is normal. Cache is clean (contains no unwritten data). CompactFlash flush or cache self-refresh is in progress, indicating cache activity.
10 — Expansion Port Status	Green	On Off	The port is connected and the link is up. The port is empty or the link is down.

693x5 rear panel LEDs



Note: Callouts do not tag multiple instances of an identified LED

Table 35 LEDs — 693x5 rear panel

LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 72.
2 — 10Gb iSCSI Link Status 10Gb iSCSI Activity (ports 0-1)	Green	On Off Blink Off	The port is connected and the link is up. The port is empty or the link is down. Link has I/O activity. Link is idle.
3 — OK to Remove	Blue	On Off	The controller module can be removed. The controller module is not prepared for removal.
4 — Unit Locator	White	Off Blink	Normal operation. Physically identifies the controller module.
5 — FRU OK	Green	On Off Blink	Controller module is operating normally. Controller module is not OK. System is booting.
6 — Fault/Service Required	Yellow	On Blink	A fault is detected or a service action is required. Hardware-controlled power-up, or a cache flush or restore error.

Table 35 LEDs — 693x5 rear panel

LED No./Description	Color	State	Definition
7 — Network Port Link Status	Green	On Off	Ethernet link is up. Ethernet port is not connected or the link is down.
8 — Network Port Activity	Green	Off Blink	Ethernet link has no I/O activity. Ethernet link has I/O activity.
9 — Cache Status	Green	On Off Blink	Cache is dirty and operation is normal. Cache is clean (contains no unwritten data). CompactFlash flush or cache self-refresh is in progress, indicating cache activity.
10 — Expansion Port Status	Green	On Off	The port is connected and the link is up. The port is empty or the link is down.

 **NOTE:** Once a Link Status LED is lit, it remains so, even if the controller is shut down via RAIDar or CLI.

When a controller is shut down or otherwise rendered inactive — its Link Status LED remains illuminated— falsely indicating that the controller can communicate with the host. Though a link exists between the host and the chip on the controller, the controller is not communicating with the chip. To reset the LED, the controller must be power-cycled (see [Powering on/powering off](#) on page 27).

693x2 drive enclosure rear panel LEDs

Using mini-SAS (SFF-8088) external connectors, the 693x2 model support 6-Gbps.

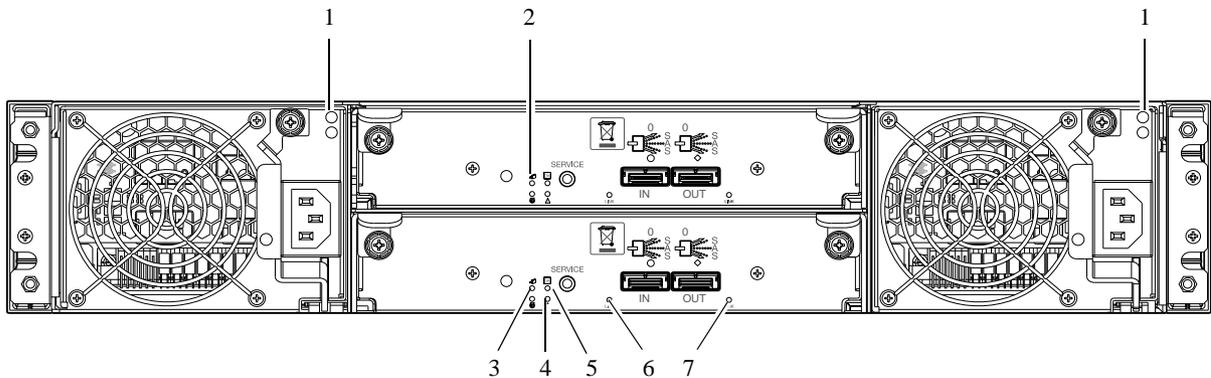


Table 36 LEDs — 693x2 rear panel

LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 72.
2 — Unit Locator	White	Off Blink	Normal operation. Physically identifies the expansion module.
3 — OK to Remove	Blue	Off	Not implemented.
4 — Fault/Service Required	Yellow	On Blink	A fault is detected or a service action is required. Hardware-controlled power-up.

Table 36 LEDs — 693x2 rear panel

LED No./Description	Color	State	Definition
5 — FRU OK	Green	On Off Blink	Expansion module is operating normally. Expansion module is not OK. System is booting.
6 — SAS In Port Status	Green	On Off	Port is connected and the link is up. Port is empty or link is down.
7 — SAS Out Port Status	Green	On Off	Port is connected and the link is up. Port is empty or link is down.

695x2/697x2 12-drive enclosure rear panel LEDs

The rear panel layouts of the 695x2 and 697x2 drive enclosures are basically identical. Using SAS (8470) external connectors, both models support 3-Gbps data rate for backend SAS expansion. Although power switches are shown on AC power supplies in the in the diagram below. See [Powering on/powering off](#) on page 27 for more information.

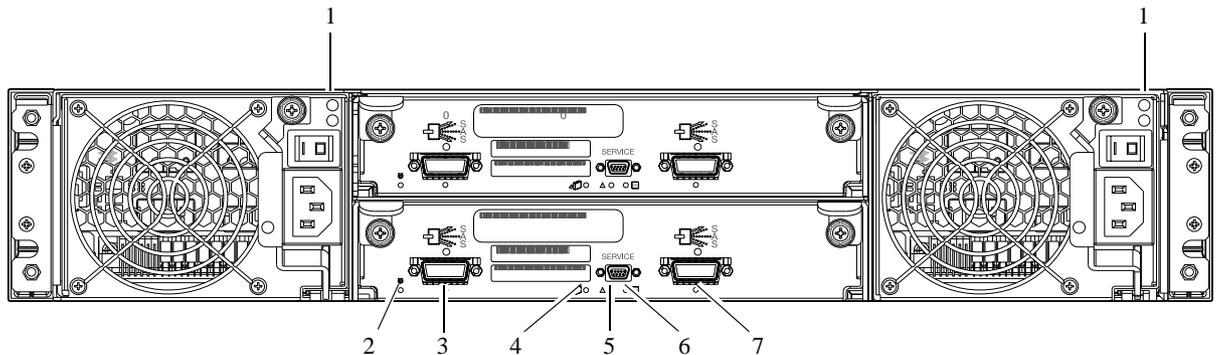
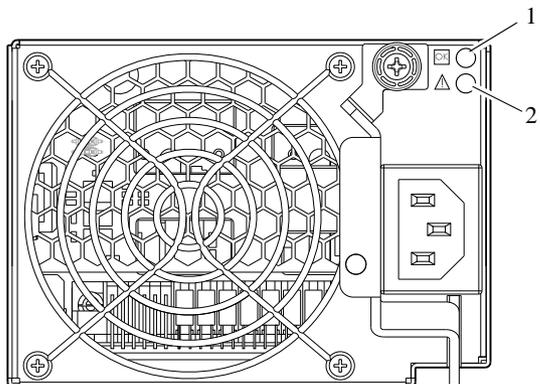


Table 37 LEDs — 695x2/697x2 rear panel

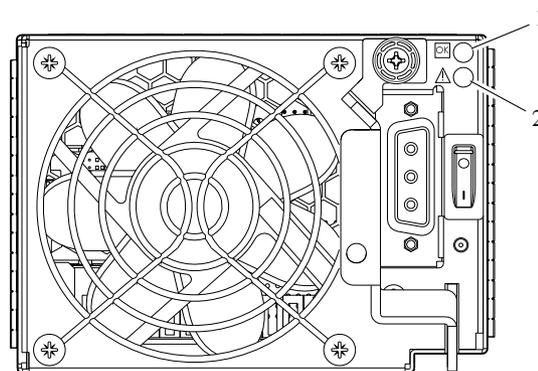
LED No./Description	Color	State	Definition
1 — Power Supply	—	—	See Power supply LEDs on page 72.
2 — Unit Locator	White	Off Blink	Normal operation. Physically identifies the expansion module.
3 — SAS In Port Status	Green	On Off	Port is connected and link is up. Port is empty or link is down.
4 — OK to Remove	Blue	Off	Not implemented.
5 — Fault/Service Required	Yellow	On Blink	A fault is detected or a service action is required. Hardware-controlled power-up.
6 — FRU OK	Green	On Off Blink	Expansion module is operating normally. Expansion module is not OK. System is booting.
7 — SAS Out Port Status	Green	On Off	Port is connected and link is up. Port is empty or link is down.

Power supply LEDs

Power redundancy is achieved through two independent load-sharing power supplies. In the event of a power supply failure, or the failure of the power source, the storage system can operate continuously on a single power supply. Greater redundancy can be achieved by connecting the power supplies to separate circuits. DC power supplies are equipped with a power switch. AC power supplies may or may not have a power switch (the newer model shown below has no power switch). Whether a power supply has a power switch is significant to powering on/off.



AC model



DC model

Table 38 LEDs — power supply units — rear panel

LED No./Description	Color	State	Definition
1 — Input Source Power Good	Green	On	Power is on and input voltage is normal.
		Off	Power is off, or input voltage is below the minimum threshold.
2 — Voltage/Fan Fault/Service Required	Yellow	On	Output voltage is out of range, or a fan is operating below the minimum required RPM.
		Off	Output voltage is normal.

 **NOTE:** See [Powering on/powering off](#) on page 27 for information on power-cycling enclosures.

B Environmental requirements and specifications

Safety requirements

Install the system in accordance with the local safety codes and regulations at the facility site. Follow all cautions and instructions marked on the equipment.

Site requirements and guidelines

The following sections provide requirements and guidelines that you must address when preparing your site for the installation.

When selecting an installation site for the system, choose a location not subject to excessive heat, direct sunlight, dust, or chemical exposure. These conditions greatly reduce the system's longevity and might void your warranty.

Site wiring and AC power requirements

The following are required for all installations using AC power supplies:

Table 39 Power requirements - AC Input

Measurement	Rating
Input power requirements	88-264VAC, 40-440Hz, 4.5-1.9A
Maximum input power	436W maximum continuous
Heat dissipation	1,488 BTUs/hour

- All AC mains and supply conductors to power distribution boxes for the rack-mounted system must be enclosed in a metal conduit or raceway when specified by local, national, or other applicable government codes and regulations.
- Ensure that the voltage and frequency of your power source match the voltage and frequency inscribed on the equipment's electrical rating label.
- To ensure redundancy, provide two separate power sources for the enclosures. These power sources must be independent of each other, and each must be controlled by a separate circuit breaker at the power distribution point.
- The system requires voltages within minimum fluctuation. The customer-supplied facilities' voltage must maintain a voltage with not more than ± 5 percent fluctuation. The customer facilities must also provide suitable surge protection.
- Site wiring must include an earth ground connection to the AC power source. The supply conductors and power distribution boxes (or equivalent metal enclosure) must be grounded at both ends.
- Power circuits and associated circuit breakers must provide sufficient power and overload protection. To prevent possible damage to the AC power distribution boxes and other components in the rack, use an external, independent power source that is isolated from large switching loads (such as air conditioning motors, elevator motors, and factory loads).

Site wiring and DC power requirements

The following are required for all installations using DC power supplies:

Table 40 Power requirements - DC Input

Measurement	Rating
Input power requirements	-34 to -72VDC, -48/-60V nominal

Table 40 Power requirements - DC Input

Measurement	Rating
Maximum input power	436W maximum continuous
Heat dissipation	1,488 BTUs/hour

- All DC mains and supply conductors to power distribution boxes for the rack-mounted system must comply with local, national, or other applicable government codes and regulations.
- Ensure that the voltage of your power source matches the voltage inscribed on the equipment's electrical label.
- To ensure redundancy, provide two separate power sources for the enclosures. These power sources must be independent of each other, and each must be controlled by a separate circuit breaker at the power distribution point.
- The system requires voltages within minimum fluctuation. The customer-supplied facilities' voltage must maintain a voltage within the range specified on the equipment's electrical rating label. The customer facilities must also provide suitable surge protection.
- Site wiring must include an earth ground connection to the DC power source. Grounding must comply with local, national, or other applicable government codes and regulations.
- Power circuits and associated circuit breakers must provide sufficient power and overload protection.

Weight and placement guidelines

Refer to [Physical requirements](#) on page 75 for detailed size and weight specifications.

- The weight of an enclosure depends on the number and type of modules installed.
- Ideally, use two people to lift an enclosure. However, one person can safely lift an enclosure if its weight is reduced by removing the power supply modules and disk drive modules.
- Do not place enclosures in a vertical position. Always install and operate the enclosures in a horizontal orientation.
- When installing enclosures in a rack, make sure that any surfaces over which you might move the rack can support the weight. To prevent accidents when moving equipment, especially on sloped loading docks and up ramps to raised floors, ensure you have a sufficient number of helpers. Remove obstacles such as cables and other objects from the floor.
- To prevent the rack from tipping, and to minimize personnel injury in the event of a seismic occurrence, securely anchor the rack to a wall or other rigid structure that is attached to both the floor and to the ceiling of the room.

Electrical guidelines

- These enclosures work with single-phase power systems having an earth ground connection. To reduce the risk of electric shock, do not plug an enclosure into any other type of power system. Contact your facilities manager or a qualified electrician if you are not sure what type of power is supplied to your building.
- Enclosures are shipped with a grounding-type (three-wire) power cord. To reduce the risk of electric shock, always plug the cord into a grounded power outlet.
- Do not use household extension cords with the enclosures. Not all power cords have the same current ratings. Household extension cords do not have overload protection and are not meant for use with computer systems.

Ventilation requirements

Refer to [Environmental requirements](#) on page 76 for detailed environmental requirements.

- Do not block or cover ventilation openings at the front and rear of an enclosure. Never place an enclosure near a radiator or heating vent. Failure to follow these guidelines can cause overheating and affect the reliability and warranty of your enclosure.

- Leave a minimum of 6 inches (15.2 cm) at the front and back of each enclosure to ensure adequate airflow for cooling. No cooling clearance is required on the sides, top, or bottom of enclosures.
- Leave enough space in front and in back of an enclosure to allow access to enclosure components for servicing. Removing a component requires a clearance of at least 15 inches (38.1 cm) in front of and behind the enclosure.

Cabling requirements

- Keep power and interface cables clear of foot traffic. Route cables in locations that protect the cables from damage.
- Route interface cables away from motors and other sources of magnetic or radio frequency interference.
- Stay within the cable length limitations.

Management host requirements

A local management host with at least one serial port connection is recommended for the initial installation and configuration of a controller enclosure. After you configure one or both of the controller modules with an IP address, you then use a remote management host on an Ethernet network to manage and monitor.

 **NOTE:** Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Physical requirements

The floor space at the installation site must be strong enough to support the combined weight of the rack, controller enclosures, drive enclosures, and any additional equipment. The site also requires sufficient space for installation, operation, and servicing the enclosures, together with sufficient ventilation to allow a free flow of air to all enclosures.

[Table 41](#) and [Table 42](#) on page 76 show enclosure dimensions and weights. Enclosure designators are described below. Enclosure weights assume the following configuration characteristics:

- 3U12 enclosure (LFF)
 - “3U12” denotes the 3.5” 12-drive enclosure (with controller or expansion modules)
 - 3U12 chassis is equipped with a disk in each disk drive slot
- Two controller or expansion modules per enclosure
- Two power supplies per enclosure

Table 41 Rackmount enclosure dimensions

Specifications	Rackmount
3U Height (y-axis):	5.15 inches (13 cm)
Width (x-axis): • Chassis-only	17 inches (43.2 cm)
Depth (z-axis): 12-drive enclosure (3U12): • Rackmount flange to chassis rear panel	20.77 inches (52.8 cm)

Table 42 Rackmount enclosure weights

Specifications	Rackmount
12-drive controller enclosure (2U12) • Chassis with FRUs (no disks) ^{1,2} • Chassis with FRUs (including disks) ^{1,3}	22.0 lb (9.9 kg) [chassis] 47.0 lb (21.3 kg) 68.0 lb (30.8 kg)
693x2 (3.5" 12-drive enclosure) • Chassis with FRUs (no disks) ^{1,2} • Chassis with FRUs (including disks) ^{1,3}	22.0 lb (9.9 kg) [chassis] 47.0 lb (21.3 kg) 68.0 lb (30.8 kg)

¹Weights shown are nominal, and subject to variances.

²Weights may vary due to different power supplies, IOMs, and differing calibrations between scales.

³Weights may vary due to actual number and type of disk drives (SAS, SATA, SSD) installed.

Environmental requirements

Table 43 Operating environmental specifications

Specification	Range
Altitude	10000 feet (standard rotating drive) 40000 feet (solid state drive)
Relative humidity	10% to 90% RH, 104°F (40°C) non-condensing
Temperature	32°F to 158°F (0°C to 70°C)
Shock	60.0 g, 2 ms
Vibration	0.5 g, 10 Hz to 500 Hz

Electrical requirements

Site wiring and power requirements

Each enclosure has two power supply modules for redundancy. If full redundancy is required, use a separate power source for each module. The AC power supply unit in each power supply module is auto-ranging and is automatically configured to an input voltage range from 88–264 VAC with an input frequency of 40–440 Hz. The power supply modules meet standard voltage requirements for both U.S. and international operation. The power supply modules use standard industrial wiring with line-to-neutral or line-to-line power connections.

Power cord requirements

Each enclosure is shipped with two AC power cords that are appropriate for use in a typical outlet in the destination country. Each power cord connects one of the power and cooling modules to an

independent, external power source. To ensure power redundancy, connect the two power cords to two separate circuits; for example, to one commercial circuit and one uninterruptible power source (UPS).

C Electrostatic discharge

Preventing electrostatic discharge

To prevent damaging the system, be aware of the precautions you need to follow when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always be properly grounded when touching a static-sensitive component or assembly.

Grounding methods to prevent electrostatic discharge

Several methods are used for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or computer chassis. Wrist straps are flexible straps with a minimum of 1 megohm \pm 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an authorized reseller install the part. For more information on static electricity or assistance with product installation, contact an authorized reseller.

D USB device connection

Rear panel USB ports

Phoenix RPC12 series controllers contain two different USB (universal serial bus) management interfaces: a *Host* interface and a *Device* interface. Both interfaces pertain to the Management Controller (MC), and each interface is accessed via its port on the controller module face plate. The port labeled Host (USB Type A) is reserved for future use, and its discussion is deferred. This appendix describes the port labeled CLI (USB Type B), which enables direct connection between a management computer and the controller, using the command line interface and appropriate cable (see [Figure 24](#) for USB port locations).

USB CLI port

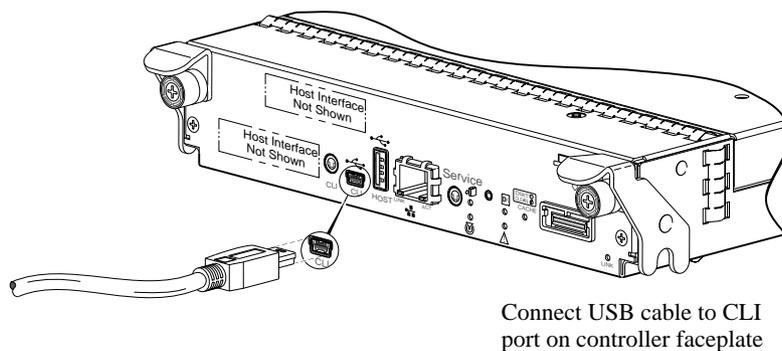


Figure 24 USB device connection — CLI port

Phoenix RPC12 series controllers feature a USB CLI port used to cable directly to the controller and initially set IP addresses, or perform other configuration tasks. The USB CLI port employs a mini-USB Type B form factor, and requires a new cable and additional support, so that a server or other computer running a Linux or Windows operating system can recognize the controller enclosure as a connected device. Without this support, the computer might not recognize that a new device is connected, or might not be able to communicate with it.

For Linux computers, no new driver files are needed, but a Linux configuration file must be created or modified (see [Linux](#) on page 82). For Windows computers a special device driver file, `gserial.inf`, must be downloaded from a CD or web site, and installed on the computer that will be cabled directly to the controller's CLI port (see [Microsoft Windows](#) on page 82).

Emulated serial port

Once attached to the controller module, the management computer should detect a new USB device. Using the Emulated Serial Port interface, the RPC12 series controller presents a single serial port using a *customer vendor ID* and *product ID*. Effective presentation of the emulated serial port assumes the management computer previously had terminal emulator installed (see [Supported host applications](#)). Serial port configuration is unnecessary.

IMPORTANT: Certain operating systems require a device driver or special mode of operation to enable proper functioning of the USB CLI port (see [Device driver/special operation mode](#)).

Supported host applications

RPC12 series controllers support the following applications to facilitate connection.

Table 44 Supported terminal emulator applications

Application	Operating system
HyperTerminal and TeraTerm	Microsoft Windows (all versions)
Minicom	Linux (all versions)
	Solaris
	HP-UX

Command Line Interface

Once the management computer detects connection to the USB-capable device, the Management Controller (MC) awaits input of characters from the host computer via the command line. To see the command line prompt, you must press *Enter*. The MC provides direct access to the CLI.

 **NOTE:** Directly cabling to the CLI port is an out-of-band connection, because it communicates outside of the data paths used to transfer information from a computer or network to the controller enclosure.

Device driver/special operation mode

Certain operating systems require a device driver or special mode of operation. Product and vendor identification information required for such setup is provided below.

Table 45 USB vendor and product identification codes

USB Identification code type	Code
Dot Hill Systems, Inc. vendor ID code	0x210C
Phoenix RPC12 series product ID code	0xa4a7

Microsoft Windows

Microsoft Windows operating systems provide a USB serial port driver. However, the USB driver requires details for connecting to Phoenix RPC12 series controller enclosures. Phoenix provides a device driver for use in the Windows environment. The USB device driver and installation instructions are provided on the ship kit CD. Alternatively, you can download these data.

Linux

Although Linux operating systems do not require installation of a device driver, certain parameters must be provided during driver loading to enable recognition of the Phoenix RPC12 series controller enclosures.

Setting parameters for the device driver

1. Enter the following command:

```
modprobe usbserial vendor=0x210c product=0xa4a7 use_acm=1
```

2. Press Enter to execute the command.

The Linux device driver is loaded with the parameters required to recognize the controllers.

 **NOTE:** Optionally, this information can be incorporated into the `/etc/modules.conf` file.

Index

Numerics

2U12

3.5" 12-drive enclosure 75

2U24

2.5" 24-drive enclosure 75

A

accessing

CLI (command line interface) 44

RAIDar (web-based management GUI) 47

AssuredSnap

licensed replication feature 38

audience 11

C

cables

FCC compliance statement 38, 50, 75

shielded 38, 50, 75

cabling

cable routing requirements 75

connecting controller and drive enclosures 19

connecting storage systems for replication 38

considerations 31

direct attach configurations 32

switch attach configurations 37

cache

post-write 18

read-ahead 18

clearance requirements

service 75

ventilation 75

command-line interface

using to set controller IP addresses 44

CompactFlash

transporting 55

components

12-drive enclosure front panel 13

2122/3120 rear panel 17

2130/3130 rear panel 17

24-drive enclosure front panel 13

3420/3430 rear panel

AC PSU 17

CLI port (RS-232) 17

CLI port (USB) 17

DC power switch 17

DC PSU 17

expansion port 17

host ports 17

network port 17

service port 17

USB Type A (reserved for future use) 17

3520/3530 rear panel

AC PSU 16

CLI port (RS-232) 16

CLI port (USB) 16

DC power switch 16

DC PSU 16

expansion port 16

host ports 16

network port 16

service port 16

USB Type A (reserved for future use) 16

3720/3730 rear panel

AC PSU 16

CLI port (RS-232) 16

CLI port (USB) 16

DC power switch 16

DC PSU 16

E/T button (disabled) 16

expansion port 16

host ports 16

network port 16

service port 16

USB Type A (reserved for future use) 16

3920/3930 rear panel

AC PSU 15

CLI port (RS-232) 15

CLI port (USB) 15

DC power switch 15

DC PSU 15

E/T button (disabled) 15

expansion port 15

host ports 15

iSCSI ports 15

network port 15

service port 15

USB Type A (reserved for future use) 15

controller module face plate

3420/3430 14

3520/3530 14

3720/3730 14

3920/3930 13

connecting

controller enclosures to hosts 31, 34

serial cable to set IP address 44

to remote management hosts 38

connections

test 27

verify 27

console requirement 75

controller enclosures

connecting to hosts 31, 34

connecting to remote management hosts 38

conventions

document 12

D

DHCP

obtaining IP addresses 43

server 43

- direct attach configurations [31](#), [34](#)
- disk drive
 - LEDs [65](#)
 - slot numbering
 - 12-drive enclosure [13](#)
- document
 - conventions [12](#)
 - prerequisite knowledge [11](#)
 - related documentation [11](#)

E

- electrostatic discharge
 - grounding methods [79](#)
 - precautions [79](#)
- enclosure
 - cabling [20](#)
 - dimensions [76](#)
 - IDs, correcting [50](#)
 - initial configuration [19](#)
 - input frequency requirement [76](#)
 - input voltage requirement [76](#)
 - installation checklist [19](#)
 - site requirements [75](#)
 - troubleshooting [50](#)
 - weight [76](#)
- Ethernet cables
 - requirements [33](#), [50](#)

F

- faults
 - isolating
 - a host-side connection [55](#)
 - expansion port connection fault [57](#)
 - methodology [49](#)

H

- host ports
 - FC [32](#)
 - loop topology [32](#)
 - point-to-point topology [32](#)
 - iSCSI (10GbE) [32](#)
 - iSCSI (1Gb) [32](#)
 - SAS [32](#)
- hosts
 - defined [31](#)
 - optional software [31](#)
 - system requirements [31](#)
- humidity operating range [76](#)

I

- IDs, correcting for enclosure [50](#)
- IP addresses
 - setting using DHCP [43](#)
 - setting using the CLI [44](#)

L

- LEDs
 - 2122/3120 face plate

- Fault/Service Required [70](#)
- FRU OK [71](#)
- OK to Remove [70](#)
- SAS In Port Status [71](#)
- SAS Out Port Status [71](#)
- Unit Locator [70](#)
- 2130/3130/5130 face plate
 - Fault/Service Required [71](#)
 - FRU OK [71](#)
 - OK to Remove [71](#)
 - SAS In Port Status [71](#)
 - SAS Out Port Status [71](#)
 - Unit Locator [71](#)
- 2U12 front panel
 - Disk drive [65](#)
 - Fault/Service Required [65](#)
 - FRU OK [65](#)
- 3420/3430 face plate
 - Cache Status [70](#)
 - Expansion Port Status [70](#)
 - Fault/Service Required [69](#)
 - FRU OK [69](#)
 - Link Activity [69](#)
 - Link Status [69](#)
 - Network Port Activity [70](#)
 - Network Port Link Status [70](#)
 - OK to Remove [69](#)
 - Unit Locator [69](#)
- 3520/3530 face plate
 - Cache Status [69](#)
 - Expansion Port Status [69](#)
 - Fault/Service Required [68](#)
 - FRU OK [68](#)
 - Link Activity [68](#)
 - Link Status [68](#)
 - Network Port Activity [69](#)
 - Network Port Link Status [69](#)
 - OK to Remove [68](#)
 - Unit Locator [68](#)
- 3720/3730 face plate
 - Cache Status [68](#)
 - Expansion Port Status [68](#)
 - Fault/Service Required [67](#)
 - FRU OK [67](#)
 - Link Activity [67](#)
 - Link Status [67](#)
 - Network Port Activity [68](#)
 - Network Port Link Status [67](#)
 - OK to Remove [67](#)
 - Unit Locator [67](#)
- 3920/3930 face plate
 - Cache Status [67](#)
 - Expansion Port Status [67](#)
 - Fault/Service Required [66](#)
 - FRU OK [66](#)
 - Link Activity [66](#)
 - Link Status [66](#)
 - Network Port Activity [66](#)
 - Network Port Link Status [66](#)

- OK to Remove [66](#)
- Unit Locator [66](#)
- Disk drives LFF
 - Power/Activity/Fault [65](#)
- Power Supply Unit (PSU)
 - AC [72](#)
 - DC [72](#)
- using to diagnose fault conditions [50](#)
- local management host requirement [75](#)

M

- MIL-STD-Compliance
 - MIL-STD-810F [11](#)
- MPIO DSM
 - Dot Hill MPIO DSM installation [31](#)
 - native Microsoft installation [31](#)
 - see related documentation [31](#)

O

- operating ranges, environmental [76](#)
- optional software [31](#)

P

- physical requirements [75](#)
- power cord requirements [76](#)
- power cycle
 - power off [30](#)
 - power on [28](#), [30](#)
- power supply
 - AC power requirements [73](#)
 - DC power requirements [73](#)
 - site wiring requirements [73](#)
- prerequisite knowledge [11](#)

R

- RAIDar
 - web-based storage management interface [47](#)
- regulatory compliance
 - notices
 - shielded cables [38](#), [50](#), [75](#)
- related documentation [11](#)
- remote management [38](#)
- requirements
 - cabling [75](#)
 - clearance [75](#)
 - Ethernet cables [50](#)
 - host system [31](#)
 - physical [75](#)
 - ventilation [74](#)
- RFI/EMI connector hoods [38](#), [50](#), [75](#)

S

- safety precautions [73](#)
- SCSI Enclosure Services (SES) driver [31](#)
- sensors
 - locating [62](#)
 - power supply [62](#)
 - temperature [62](#)

- voltage [63](#)
- shock operating range [76](#)
- site planning
 - local management host requirement [75](#)
 - physical requirements [75](#)
 - safety precautions [73](#)
- storage system setup
 - configuring [47](#)
 - getting started [47](#)
 - provisioning [47](#)
 - replicating [47](#)
- super-capacitor pack [18](#)
- switch attach configurations [37](#)

T

- temperature operating range [76](#)
- troubleshooting [49](#)
 - controller failure, single controller configuration [54](#)
 - correcting enclosure IDs [50](#)
 - enclosure does not initialize [50](#)
 - expansion port connection fault [57](#)
 - host-side connection fault [55](#)
 - using system LEDs [50](#)

U

- Unified LUN Presentation [31](#)
- USB device connection
 - command line interface (CLI) [82](#)
 - device driver [82](#)
 - emulated serial port [81](#)
 - rear panel USB ports [81](#)
 - supported host applications [82](#)
 - vendor and product ID codes [82](#)

V

- ventilation requirements [74](#)
- vibration operating range [76](#)

W

- warnings
 - temperature [61](#)
 - voltage [61](#)

