



Oresund

FCE2200

Fibre Channel to iSCSI Bridge

User Manual

V3.2

Bridgeworks

135 Somerford Road, Christchurch,
Dorset BH23 3PY

Tel: +44 (0) 1202 588 588

Fax: +44 (0) 1202 588 589

Email: support@4bridgeworks.com

Manual Revision History

Revision	Date	Firmware	
3.0	July 2011		
3.1	April 2012	V3_02	AP
3.2	May 2012	V3_03	AP

Warning

The Bridgeworks Oresund FCE2200 FC to iSCSI Bridge contains no user-serviceable components. Only an Authorized Service Centre should carry out any servicing or repairs. Unauthorized repairs or modifications will immediately void your warranty.

Before You Start

There are a number of additional pieces of equipment you will require for the successful installation of your Bridge:

Ethernet Cable

You will require a good quality cable of suitable length to go between your network access point and the Bridge. This should be marked as certified to Cat 5e and have a RJ45 style connector at the Bridge end.

Fibre Channel Interface

The Fibre Channel Bridge supports the use of SFP modules to connect to the Fibre Channel. You will require the correct type to connect to your existing infrastructure. If you are in doubt about the correct type please consult your reseller.

If you are in any doubt contact your reseller for extra assistance.

Table of Contents

1.0	Introduction.....	5
1.1	Overview.....	5
1.2	Manual Layout	6
1.3	Definitions.....	6
1.4	Safety Notices.....	7
2.0	Installing the FCE2200 Bridge	8
2.1	Connecting the Fibre Channel Interface.....	8
2.2	Ethernet Connection	9
2.3	Connecting the Power Supply.....	10
3.0	Configuring the FCE2200 Bridge	11
3.1	Using the Web Interface.....	11
3.1.1	Browsers.....	11
3.1.2	Connecting to the Web Interface.....	11
3.2	Configuring the Network Parameters	14
3.2.1	Setting the Hostname.....	14
3.2.2	Enabling IPv6.....	14
3.2.3	Setting the MTU	15
3.2.4	Setting the IP Address	15
3.2.5	Setting the Subnet Mask	15
3.2.6	Setting the Gateway Address.....	15
3.2.7	Setting an IPv6 IP Address	16
3.2.8	Committing the changes	16
3.2.9	Reconnect to the Bridge.....	16
3.3	Passwords and Security.....	17
3.4	Network Services.....	18
3.4.1	NTP	18
3.4.2	Email Alerts.....	18
3.5	FC Target Connections.....	20
3.6	Configuring and Connecting iSCSI Devices	24
3.6.1	Discovering iSCSI Targets	24
3.6.2	Logon.....	26
3.7	Device Manager.....	28
4.0	Information.....	29
4.1	System Information	29
4.2	System Log.....	30
5.0	Maintenance	31
5.1	Firmware Updates.....	31
5.2	Saving the Configuration to Disk	32
5.3	Restoring a Saved Configuration	33
5.4	Restoring Factory Defaults.....	33
6.0	Trouble shooting.....	34
6.1	Lost Password	34
6.2	Network problems	35
6.3	Device related problems	36
6.4	Poor Performance.....	37
6.5	Lost IP Address	38
	Appendix A Setting up your Computer for Initial Setup	39
	A1 Windows 95, 98 or NT.....	39
	A2 Windows 2000, 2003, XP	40
	A3 Windows Vista / Server 2008 or Vista or 7	42
	Appendix B Visual Indicators.....	44
	Appendix C Technical Specifications.....	45

1.0 Introduction

Thank you for purchasing the Bridgeworks Fibre Channel to iSCSI Bridge.

The Bridge has been designed to ensure that in the majority of installations it will require the minimum of set up before use. However, we suggest you read the following, which will guide you through setting up both the Fibre Channel Network and iSCSI aspects of the Fibre Channel Bridge

The GUI Management section will guide you through the initial set up required to install the Bridge on to your network

1.1 Overview




The Fibre Channel Bridge creates an interface between a network, which utilises the Fibre Channel protocol, and iSCSI devices that reside upon the Ethernet network. The internal circuitry of the Bridge acts as a two-way interface converting the data packets that are received on the Fibre Channel network to iSCSI data packets ready for transporting these across a network to iSCSI enabled storage devices such as disks, tape drives.



The Bridgeworks FCE2200 Fibre Channel Bridge

1.2 Manual Layout

Throughout the manual symbols will be used to quickly identify different pieces of information.

	This icon represents a note of interest about a step or section of information.
	This icon represents an important piece of information.
	This icon represents a warning, care must be taken and the warning should be read thoroughly.

1.3 Definitions

iSCSI Target Device

iSCSI target devices are devices such as disk drives, tape drives or RAID controllers that are attached to the network. Each device is identified by an IQN – iSCSI Qualified Name.

iSCSI Qualified Name (IQN)


Anything connected to a network, be it a computer, printer or iSCSI device must have a unique identifier, such as an IP address, to enable other devices to communicate with it. With iSCSI devices (both targets and initiators) an extra level of identification in addition to the IP address is employed. This is called the IQN. The IQN includes the iSCSI Target's name and an identifier for the shared iSCSI device.


Example: 2002-12.com.4bridgeworks.sdt600a014d10: 5


CHAP

CHAP is an authentication scheme used by Servers to validate the identity of clients and vice versa. When CHAP is enabled, the initiator must send the correct Username and Target Password to gain access to the iSCSI Bridge. The Initiator Secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the Initiator, the iSCSI Bridge will authenticate itself with the initiator using the initiator secret

1.4 Safety Notices

	<p>This device should only be installed by suitably trained personnel.</p> <p>Protection provided by the equipment may be impaired if used in a manner not specified by the manufacturer.</p> <p>Do not block the enclosure's vents. Air enters from the front and is exhausted out the back of the device.</p>
---	---

	<p>This device is connected to the AC power line. Before using the device, please read the instructions carefully, in order to use the device correctly and safely. For the installation instructions, refer to the installation section of this guide.</p> <p>Class I Equipment. This equipment must be earthed. The power plug must be connected to a properly wired earth ground socket outlet. An improperly wired socket outlet could place hazardous voltages on accessible metal parts.</p> <p>Do not attempt to service the equipment yourself, doing so will void the warranty and may damage the system. This unit contains hazardous voltages and should only be opened by a trained and qualified technician. To prevent electric shock, do not remove the cover. There are no user-serviceable parts inside.</p> <p>The power cord is used as a disconnection device. To de-energize the equipment, disconnect the power cord.</p> <p>Do not use the equipment where it can get wet. Protect equipment from liquid intrusion. If your equipment gets wet, disconnect power to the equipment and to any attached devices. If the Bridge is connected to an electrical outlet, turn off the AC power at the circuit breaker before attempting to remove the power cables from the electrical outlet. Disconnect any attached devices.</p> <p>Use only the power supply cord set provided with the system for this unit, should this not be correct for your geographical area, please contact your supplier.</p> <p>The mains plug to the rear of the unit is used as the power disconnect device, please ensure that this is kept clear from any obstruction and is visible at all times.</p> <p>Before installing or removing signal cables, ensure that the power cables for the system unit and all attached devices are unplugged.</p> <p>To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.</p>
---	---

	<p>Class 1 Laser Product: Certain models will use a Small Form Factor Pluggable GBIC module for connection to an optical network. These devices may use a Class 1 Laser device – it is important that you do not stare into the Laser beam.</p>
---	---

2.0 Installing the FCE2200 Bridge

There are 3 basic steps to installing the FC Bridge

- Connecting the Fibre Channel Interface
- Ethernet Connection
- Connecting the Power Supply

2.1 Connecting the Fibre Channel Interface

The FC Bridge can be used on the following network configurations

- 1Gb FC
- 2Gb FC
- 4Gb FC

It is not necessary to specify which network type you are connected to as the FC Bridge will automatically select the correct network speed when first powered up.

The connection to the FC network is via an industry Small Form-factor Pluggable (SFP) interface Module that is inserted into the SFP receptacle on the front of the unit.

Front Panel of the Bridge Showing FC Cable Connections



Note: Only use an SFP that meets or exceeds the following standards:
EU: IEC/EN 60825-1, North America: FCC, CDRH

2.2 Ethernet Connection


The Bridge can be used on the following network configurations:

- 10BaseT
- 100BaseT
- 1000BaseT (Gigabit)

It is not necessary to specify which network type you are connected to, as when powered up the Bridge will automatically select the correct network speed.

The connection to the Ethernet network is via an industry standard twisted pair, RJ45 copper interface on the front of the unit.

To connect the Bridge to the Ethernet network, insert one or two Cat 5E cables into the connector on the unit as shown below. When the plug is in the correct position a “click” should be heard.

	Note: If you only intend to use a single network connection, use the left-hand network socket as this is set to 10.10.10.10 for the initial configuration of the Bridge
---	--



Front Panel of the Bridge Showing Ethernet Cable Connections

2.3 Connecting the Power Supply

Before connecting the Power Supply to the unit, ensure the wall plug is removed or switched off.

Connect the Power Supply to the rear of the Bridge as shown below.



Note: Before powering up the Bridge, ensure all the peripherals are powered up and you have a connection to the network.

To turn on the Bridge use the switch next to the power connector and push in the button. (The image above shows the button in the off position). Whenever the Bridge is powered on the blue LED on the front panel will be illuminated.

Now that the Bridge is installed, the next stage is to configure it. This is described in the next chapter.

3.0 Configuring the FCE2200 Bridge

Before the FC Bridge can be used on the network for the first time, it is necessary to configure a number of parameters.

3.1 Using the Web Interface

Now that the Bridge is fully connected the primary method for configuring any option is through its web interface. The following section highlights the requirements needed to access these pages and the consistent layout used throughout.



Note: The default IP address of the web interface for the Bridge is **http://10.10.10.10/**

3.1.1 Browsers

This Bridge supports the following browsers

- Microsoft Internet Explorer 7
- Microsoft Internet Explorer 8
- Microsoft Internet Explorer 9
- Mozilla Firefox 9
- Mozilla Firefox 10
- Google Chrome Latest



Note: JavaScript must be enabled within the web browser to use the web interfaces functionality.



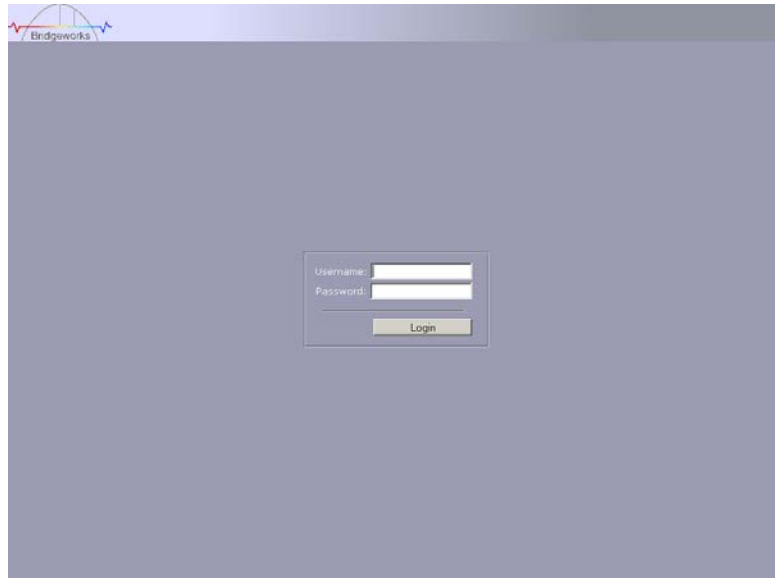
Important: If you choose to use a browser that is not on the list of supported browsers Bridgeworks cannot guarantee the behaviour of the Nodes functionality.

3.1.2 Connecting to the Web Interface

From within your web browser, connect to the Bridge using the address **http://10.10.10.10/** (or, if you have changed this previously, the address of the left-hand network port).

Depending on your current network parameters, it may be necessary to change your network settings on your computer for the initial set up. See Appendix A for further help.

Once you have connected to the web interface on the Bridge you will see the entry page shown below.



To access the web interface a user name and password must be used, the defaults of which are:

Username: **admin**
Password: **admin**



Note: We suggest that you change your password at the next possible opportunity.

The GUI will now display the Console Home menu screen as shown below.

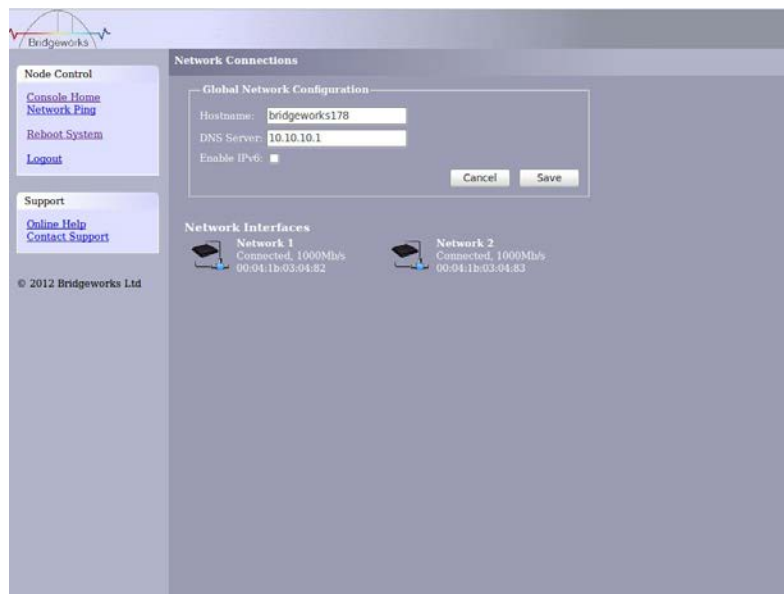


Note: For security reasons only one person can access this GUI at any one time. Therefore, to avoid the situation where one person forgets to logout, effectively locking up the GUI, the Bridge incorporates a five minute idle timer, which will automatically logout any user after this period.

Within the Support section there is a link that will open up your mail service with Bridgeworks' Email address loaded and an Online Help button. The Online help is contextually aware of which GUI page you are currently viewing and will provide you with help relevant to the display and configuration data.

3.2 Configuring the Network Parameters

Click on the Connections icon to enter the network configuration page.



3.2.1 Setting the Hostname

In this box enter the name you wish to use to address this Bridge in the future. We suggest that you use a name that is relevant to its location and/or its purpose.



Note: If you select the DHCP mode, ensure your DHCP server is set to automatically update the DNS server.

3.2.2 Enabling IPv6

Checking this box will enable the Bridge to use IPv6 IP addresses. As with Ipv4, you can either choose to use DHCP or assign a static IPv6 address.

To change the settings of a specific connection, click on the connection. You will be presented with the screen as shown below where you can make changes to the connection.

Bridge Control
[Console Home](#)
[Network Ping](#)
[Reboot System](#)
[Logout](#)

Support
[Online Help](#)
[Contact Support](#)

© 2011 Bridgeworks Ltd

Network Port: Network 1

Port Settings

MTU Size: 1500

☒ Use DHCP to assign an IP address automatically

☐ Use the following IP address:

IP Address: 10.10.10.120
 Netmask: 255.255.255.0
 Gateway:

☒ Use automatic IPv6 address assignment

☐ Use the following IPv6 address:

IPv6 address:
 Default gateway:

Link Status

Link State:	Up	Link Speed:	1000Mbps
RX Bytes:	161579	TX Bytes:	596400
RX Errors:	0	TX Errors:	0
IPv4 Address:	10.10.10.120		
IPv6 Address:			

Cancel Save

3.2.3 Setting the MTU

Enabling larger frames on a jumbo frame capable network can improve the performance of your backup operations. Jumbo frames are Ethernet frames that contain more than 1500 bytes of payload (MTU). Before enabling jumbo frames, ensure that all the devices/hosts located on the network support the jumbo frame size that you intend to use to connect to the Bridge. If you experience network related problems while using jumbo frames, use a smaller jumbo frame size. Consult your networking equipment documentation for additional instructions.

Some networking switches require you to specify the size of the jumbo frame (MTU) when enabling, as opposed to a simple enable command. On these switches it might be required to add the necessary bytes needed for the frame header (i.e., header information + MTU). Typical header size is 28 bytes, so a 9000 byte MTU would translate to 9028 byte setting. Refer to your switch documentation to understand what the maximum frame size settings are for your switch.

3.2.4 Setting the IP Address

There are two possibilities when configuring the IP address for the Bridge:

DHCP - the Bridge will seek out the DHCP server on your network and obtain an IP address from the server each time it powers up.

Static IP - the IP address set in this page will be the IP address the unit will use each time it powers up.

Depending on your configuration, either click the DHCP button or set your Static IP address.



Note: If you select the DHCP mode, ensure your DHCP server is set to automatically update the DNS server.

3.2.5 Setting the Subnet Mask

If the Bridge is configured to use DHCP the net mask will be issued from the DHCP server. If you are using static IP address enter the IP mask in this box.

3.2.6 Setting the Gateway Address

Enter in this box the address of your gateway controller for your network.

3.2.7 Setting an IPv6 IP Address

If IPv6 is enabled on the network connections page, here you can choose to use DHCP to automatically assign an IPv6 address, or you can set a static IPv6 address. If you choose to assign a static IPv6 address, you will also need to assign an IPv6 subnet mask.

3.2.8 Committing the changes



Note: Before you commit these parameters to memory, it is worth checking that all the parameters and spellings are correct and that these have been written down in a safe place for future reference.

Click the save button to save these parameters and then click the reboot button in the left hand pane.

3.2.9 Reconnect to the Bridge

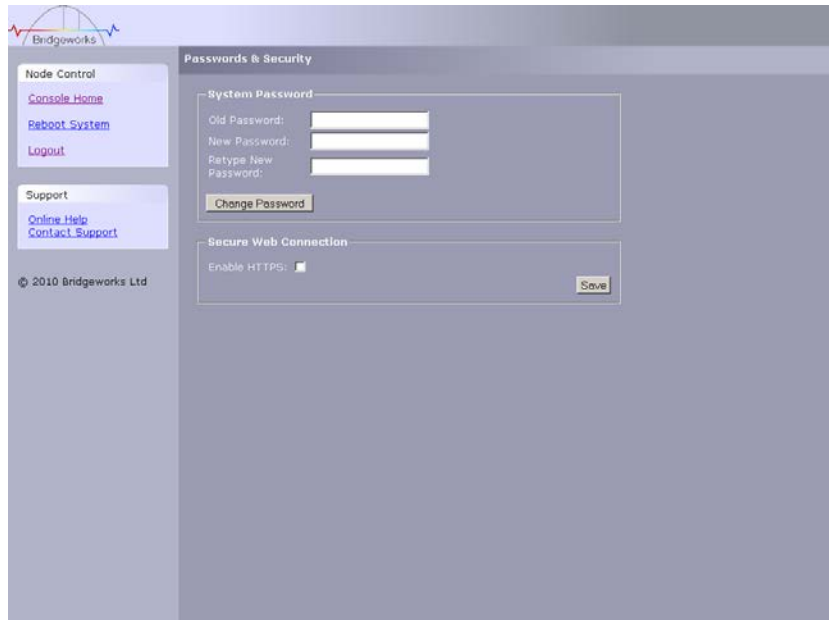
If you made changes to your computer, return them to their previous setting and reconnect to the Bridge using the IP address or hostname, depending on which addressing mode you selected.

3.3 Passwords and Security

This configuration page will allow the administrator to change the access password for the GUI.

From within the main menu select the Password and Security icon under the Network section

The GUI will now display the following window




The screenshot shows the 'Passwords & Security' configuration page in the Bridgeworks GUI. On the left is a sidebar with 'Node Control' (Console Home, Reboot System, Logout) and 'Support' (Online Help, Contact Support) links, along with a copyright notice for 2010 Bridgeworks Ltd. The main content area has a title bar 'Passwords & Security'. It contains two sections: 'System Password' with three input fields for 'Old Password', 'New Password', and 'Retype New Password', followed by a 'Change Password' button; and 'Secure Web Connection' with an 'Enable HTTPS' checkbox and a 'Save' button.

To change your password, type the existing password and the new password into the appropriate boxes and press save.

Secure Connection – by clicking this box it will force all further transactions with the GUI to be done via a secure, encrypted HTTPS connection.

Once you have clicked this option, save the configuration, logout and login again.

	<p>Note: It is not possible to reset the password without logging into the GUI so ensure you remember your password!</p>
---	---

3.4 Network Services

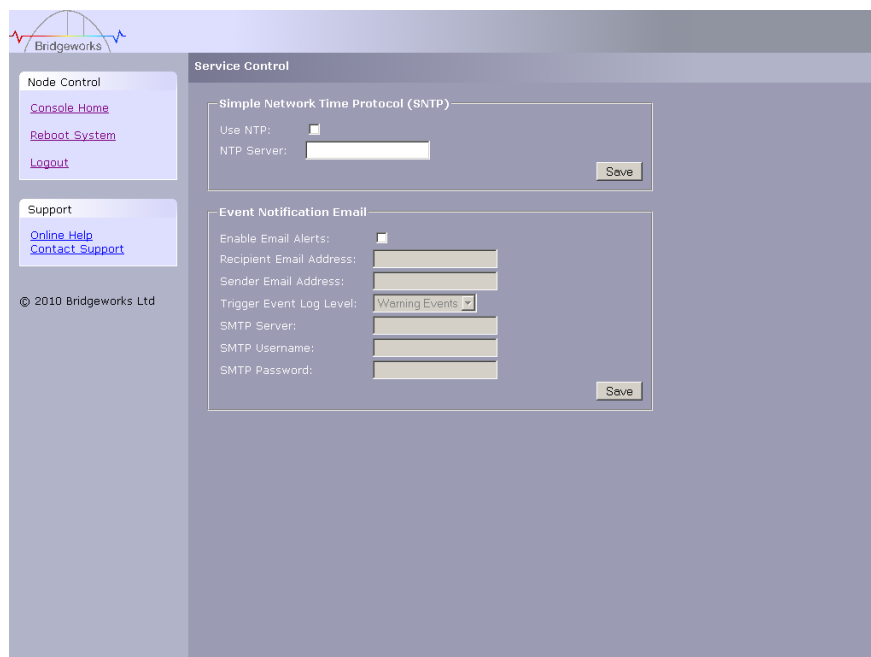
3.4.1 NTP

The Network Time Protocol (NTP) is a protocol for synchronising the clocks of computer systems over the IP network. This is used by the Bridge to synchronise its internal clock with the rest of the network.

This configuration page will allow the administrator to configure the IP addresses for the Network Time Domain server.

From within the main menu select the Service Control icon under the Network section

The GUI will now display the following window



The screenshot shows the Bridgeworks Service Control interface. On the left is a sidebar with 'Node Control' (Console Home, Reboot System, Logout) and 'Support' (Online Help, Contact Support) links, along with a copyright notice for 2010 Bridgeworks Ltd. The main area is titled 'Service Control' and contains two sections. The 'Simple Network Time Protocol (SNTP)' section has a 'Use NTP' checkbox and an 'NTP Server' text field, with a 'Save' button. The 'Event Notification Email' section has an 'Enable Email Alerts' checkbox, and fields for 'Recipient Email Address', 'Sender Email Address', 'Trigger Event Log Level' (a dropdown menu currently showing 'Warning Events'), 'SMTP Server', 'SMTP Username', and 'SMTP Password', with a 'Save' button.

To enable NTP on the Bridge, click the tick box and enter the IP address for the NTP Server and then click the save button.

3.4.2 Email Alerts

The Bridge can notify a systems administrator when certain level log events are observed in the Bridges logs.

To enable email alerts on the Bridge, click the tick box next to “Enable Alerts”, this will allow you to alter the contents of the currently greyed out fields. The following fields need to be completed.

Recipient Email Address - This is the email address to which the emails will be sent.

Senders Email Address - This is the email address that emails will be sent from. This can be any address and does not have to be genuine, which is useful for email filtering. For example entering logs@4bridgeworks.com would allow emails from this address to be filtered to a specified folder in the users email client.

Trigger Event Log Level - This allows the user to specify what severity of event will trigger the log to be emailed with Critical Events being the most severe and Warning Events being the least. For each level picked the higher level logs will also be emailed, for example selecting Error Events will also send all Critical Events.

Below are examples of events that will be sent for each log level

- Critical: The Bridge is running at non recommended temperatures
- Error: The Bridge rejected a login attempt.
- Warning: An Initiator has logged out of the Bridge.

3.5 FC Target Connections

This configuration page will allow the administrator to configure the Fibre Channel Interface of the Bridge

From within the main menu select the FC Target icon from the SCSI System section.

The GUI will now display the following window



The left hand most icons display the current state of each Fibre Channel Port.

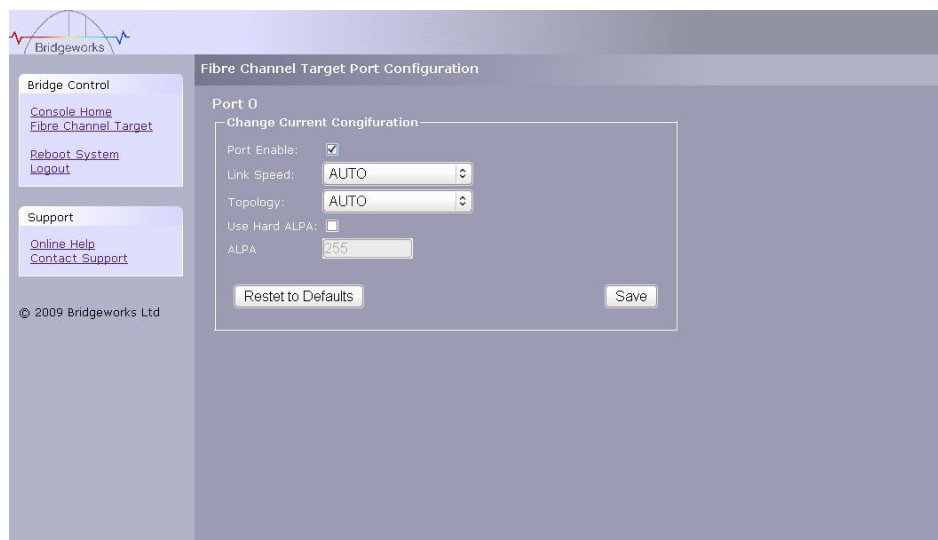
The green / red arrow display whether the port is up or down whilst the number displays the negotiated Fibre Channel speed

Clicking on the icon will take you into a further screen displaying more detailed information.

Port Configuration

Now select the first of the ports configuration icon

The Screen will now display the following




The first parameter is the link enable check box

Check this to enable the link on to the FC SAN

The link speed pull down menu allows you to select the FC network speed. We recommend you select the automatic option from the pull down menu

Topology – this allows you to force the FC topology when the Bridge logs on to the FC network

	Note: We suggest you leave this unchecked unless you are conversant with the lower levels of the Fibre Channel protocol as certain ALPA addresses are reserved.
---	--

Save – This will save the configuration to the local Flash memory for use at the next reboot.

Repeat this process for the other Network Port as required.

Connected Hosts

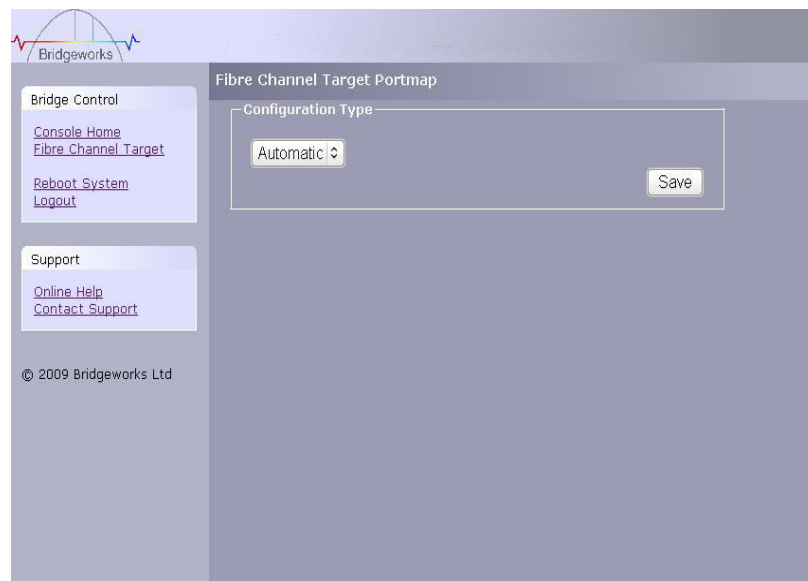
To List which hosts are connected to the Bridge, from the Fibre Channel main page select the connected hosts icon for the port you require



Port Map

Once the Fibre Channel interface has been configured the target devices can now be assigned to the Fibre Channel ports.

From the Fibre Channel Management page select the port map icon.

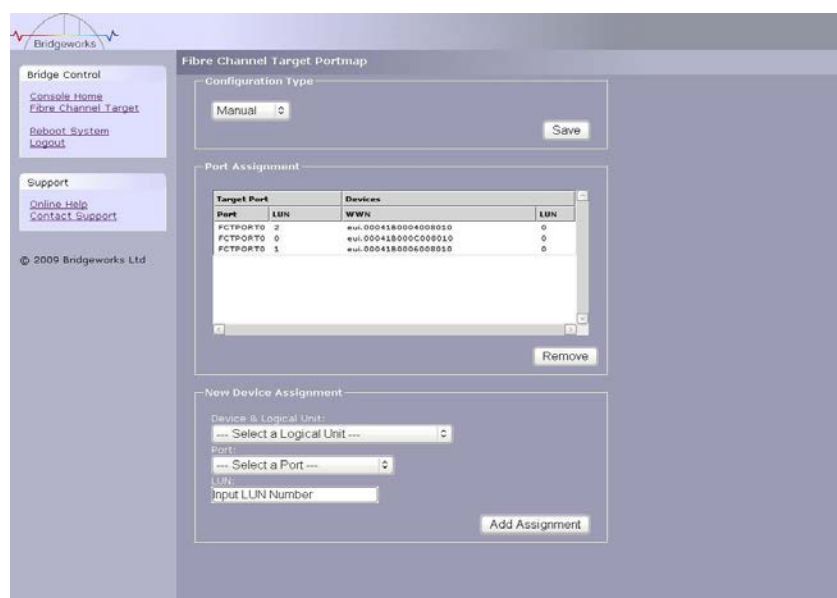


There are two choices from the drop down list

Automatic this will assign to both Fibre Channel ports all the target devices so that any host connected to either of the Fibre Channel ports will see the same devices.

Manual this will allow the user to manually assign which target device appears on which Fibre Channel.

Selecting Manual will bring up the following screen



To assign a target device to a Fibre Channel Port

- Select the target device from the list in the Logical Unit drop down menu
- Select which Fibre Channel Port you wish the LUN to appear on
- Select the LUN number you wish the device to have on the Selected Fibre Channel Port
- Click the Add Assignment button at the bottom of the panel

In the example above the Port Assignment shows you 3 devices assigned to Port 0 with the LUN numbers 0, 1 and 2.

3.6 Configuring and Connecting iSCSI Devices

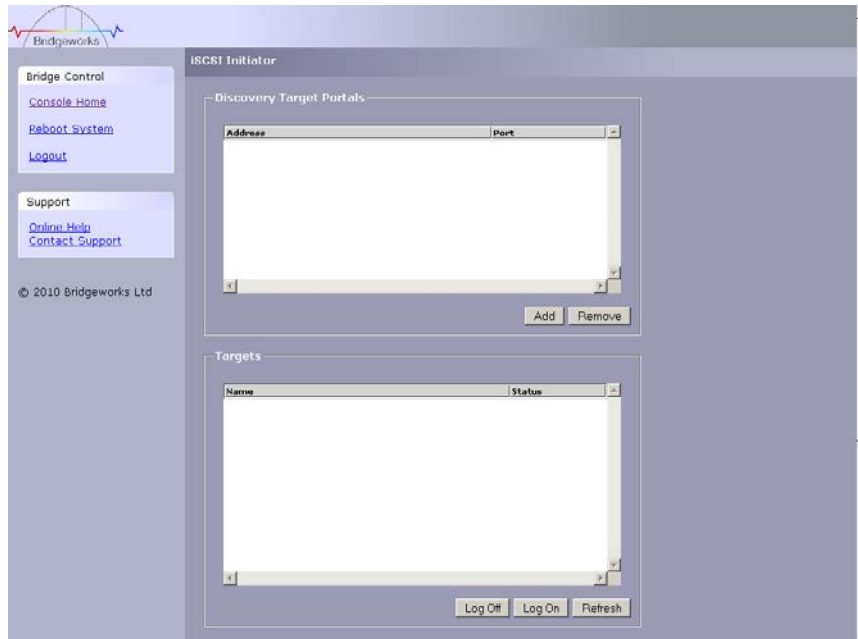
To add a device to the iSCSI Connect Bridge requires 2 basic steps:

- Identify the iSCSI Device(s) you wish to use
- Login to the iSCSI Device(s)

The following sequence is repeated for each device you wish to connect to the iSCSI Bridge.

3.6.1 Discovering iSCSI Targets

From the main menu, click on the iSCSI Initiator logo.



Click on the 'Add' in the 'Discovery Target Portals' window.

Add Discovery Portal

Discovery Portal

IP Address

Port

☐ CHAP Login

User name

Target secret

Ok Cancel

In the “Add Discovery Portal” window insert the IP address of the iSCSI target device you wish to connect to and the source interface.

If the iSCSI device has CHAP enabled for discoveries then you will need to check the ‘CHAP Login’ box and fill in the username and password. When complete click on the ‘OK’ button.

The unit will now go through a process called iSCSI Discovery. This will access the iSCSI Target and request the unit to report on the devices within it. Any devices found will appear in the Targets window below along with its IQN. If the iSCSI Target Device had more than 1 device attached, then all of these devices would be shown.

iSCSI Initiator

Discovery Target Portals

Address	Port
10.0.0.169	3260

Add Remove

Targets

Name	Status
iqn.2006-03.com.kernsafe:kirk.2k3.SCS10	inactive
iqn.2006-03.com.kernsafe:kirk.2k3.SCS11	inactive

Log Off Log On Refresh

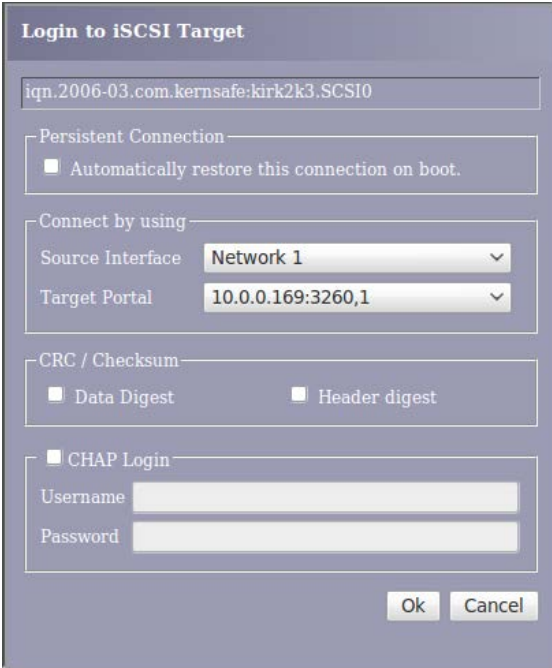
In the example above we can see that IP Address 10.10.10.169 has two devices attached to it. Their status is inactive; this is because at this point we have only made a Discovery request

to the iSCSI Target Device. To enable the device an iSCSI logon function has to be performed.

3.6.2 Logon

To logon to an IQN, highlight the IQN by clicking on its entry in the Targets window and then click the 'Log On' button.

At this point a new window will appear.



The image shows a 'Login to iSCSI Target' dialog box. It has a title bar with the text 'Login to iSCSI Target'. Inside the dialog, there is a text field containing the IQN 'iqn.2006-03.com.kernsafe:kirk2k3.SCSI0'. Below this is a section titled 'Persistent Connection' with a checkbox labeled 'Automatically restore this connection on boot.' which is currently unchecked. The next section is 'Connect by using', which contains two dropdown menus: 'Source Interface' set to 'Network 1' and 'Target Portal' set to '10.0.0.169:3260,1'. Below these is a section titled 'CRC / Checksum' with two checkboxes: 'Data Digest' and 'Header digest', both of which are unchecked. The final section is 'CHAP Login', which has a checkbox that is unchecked, and two text fields for 'Username' and 'Password'. At the bottom right of the dialog are 'Ok' and 'Cancel' buttons.

Persistent Connection

If you wish for the unit to connect to this IQN after a reset or reboot, then this box needs to be checked. It is recommended that this feature be enabled.

Connect by using

Source interface: The source interface is the physical network interface you are using to connect to your target from your board. For example if you are connecting using the left network port you would select network 1 and the right network port would be network 2.

Target Portal: The target portal is the IP address and port that you want to connect to on the target device. The IP address must be an address allocated to a network interface that the Bridge has a network link to. The ports that are supported by the Bridge are either 3260 or 860.

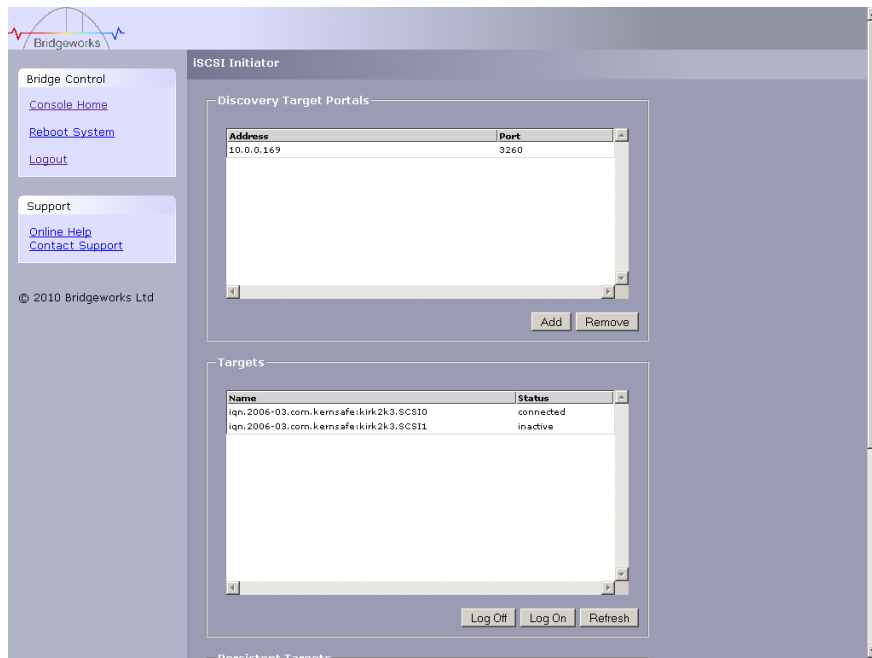
CHAP Login

If the iSCSI Target Device has CHAP enabled, check the tick box and enter the username and password to communicate with this device.

Once you have completed this window, click the OK button.

The Bridge should now display the IQN with a connected status as shown below.

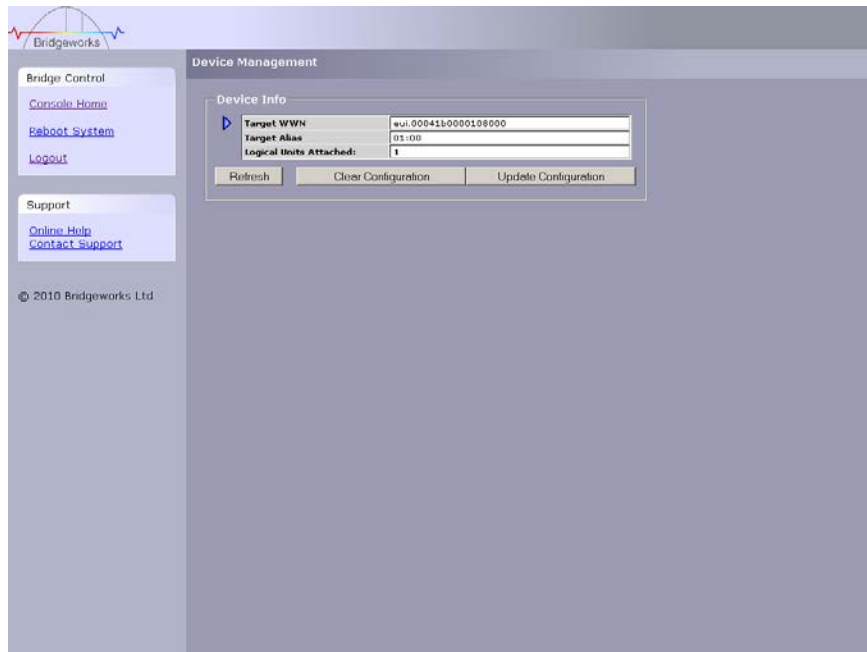
Repeat this process for all the required iSCSI Target Devices



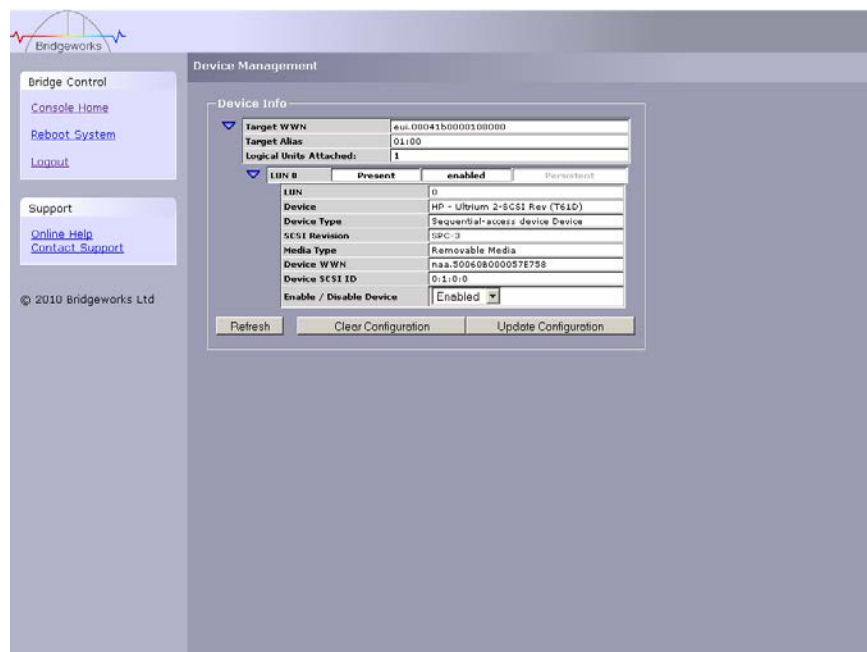
Note: If you enabled Persistent Connection these devices will be also displayed in the Persistent Targets window below the Targets window.

3.7 Device Manager

From within the Console Home menu select the Device Management icon. This will display all the configured devices.



To display further details of the connected devices, click on the blue triangle the left of the target.



The expanded information also gives you a device control option

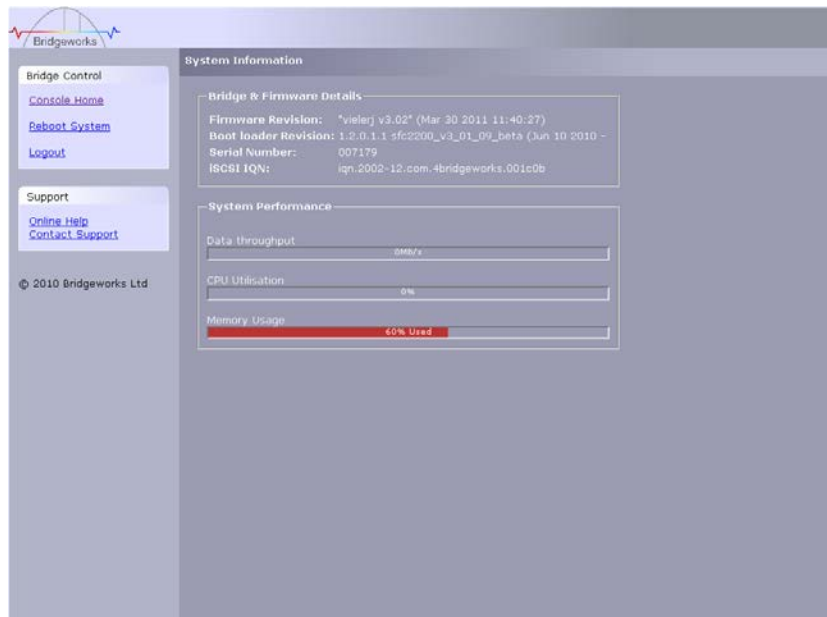
Enable / Disable Device – This pull down menu option allows you to disable a device from appearing on the interface.

4.0 Information

4.1 System Information

This System Information page will allow the administrator to view the Performance of the Bridge. From within the main menu select the System Information icon from the Bridge Maintenance section.

The GUI will now display the following window



Within the top window the following information is displayed

- Current Firmware & Boot Loader Revision Level
- Serial Number of the Bridge
- iSCSI Qualified Name (IQN)

Within the lower window are 3 bar graphs, which provide an approximation of the following performance parameters:

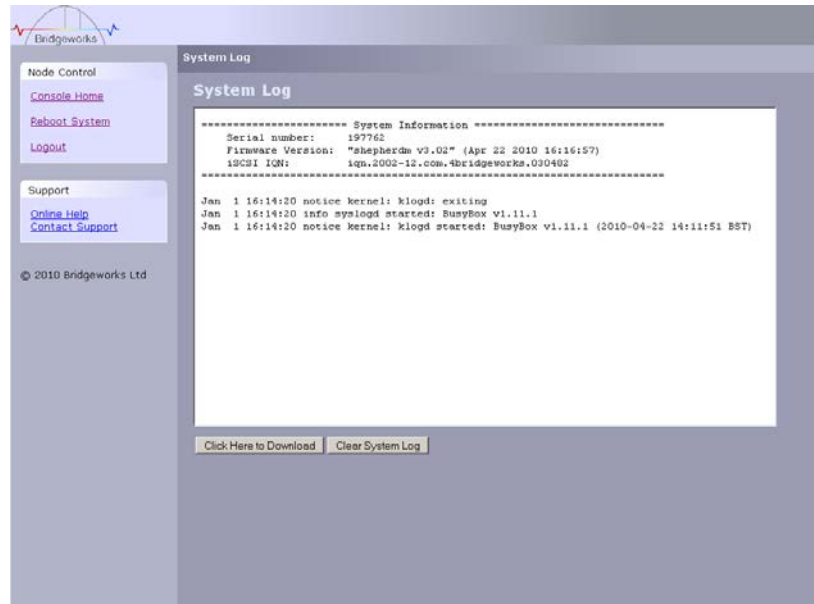
- Data Throughput - This indicates the current performance in MB/s.
- CPU - This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces
- Memory Usage - This indicates the percentage of memory used by all processes

4.2 System Log

This System Log page allows the administrator to view the logged status of the Bridge.

From within the main menu select the View Log-file icon from the Bridge Maintenance section.

The GUI will now display the following window



Below the log display pane are two options:

- Clear System Log – this will delete the current and saved logs within the Bridge
- Download – this will download the log file to your local disk. You may be asked by our support team to email this log file to them to aid them in any problem resolution.

5.0 Maintenance

5.1 Firmware Updates

The Firmware Updates page will allow the administrator to load new firmware into the Bridge.

From within the main menu select the Firmware Updates icon from the Bridge Maintenance section.

The GUI will now display the following window.



From time to time it may be necessary to upgrade the firmware within the Bridge. New versions contain resolutions to known issues as well as new features and improvements to the functionality of the Bridge. It is advisable to check for the latest release on a regular basis.

New versions of the firmware can be downloaded from the Bridgeworks web site at:

http://www.4bridgeworks.com/software_downloads.phtml

Once you have downloaded the new firmware to a local disk drive:

- Click on the browse button to locate the file you have downloaded from the website.
- Click on the update button.

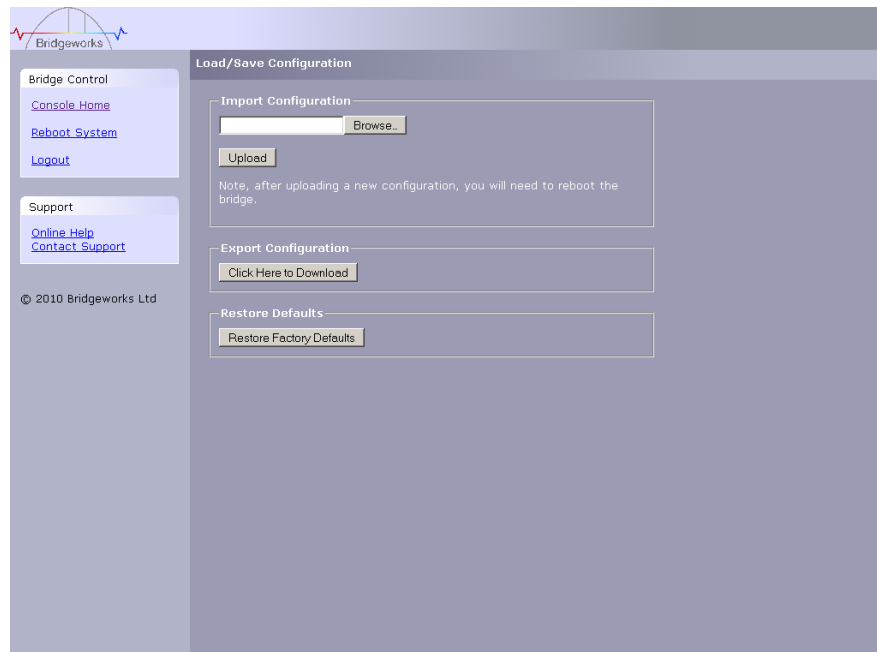
Updating the firmware will take a few minutes after which it will be necessary to reboot the system to bring the new code into memory.

5.2 Saving the Configuration to Disk

The Load/Save Configuration page will allow the administrator to save and load the configuration parameters to a file on a local disk.

From within the main menu select the Load/Save Configuration icon from the Bridge Maintenance section.

The GUI will now display the following window



Once you have finished configuring your Bridge we recommend that you save your configuration data to a local disk. By doing so you could save valuable time if the unit requires replacement, or if you require restoring an old firmware version, as the configuration may change due to upgrades.

It is possible to create a “Boiler Plate” configuration and load this into each new Bridge as it is initialised. This can ease the rollout of multiple Bridges within an enterprise.

To save the configuration data click on the “Click here to Download” link from within the Export Configuration window located in the centre of the page.

Depending on the browser you are using, select the option to save file to disk.

The Bridge will now download an encoded file that contains all the configuration settings for the Bridge.

5.3 Restoring a Saved Configuration

To reload the configuration, click on the Browse button and locate the required configuration to upload into the Bridge. Once located click the upload button and the new configuration data will be uploaded.

Once completed, use the various configuration pages to make any further adjustments required and then reboot the system.

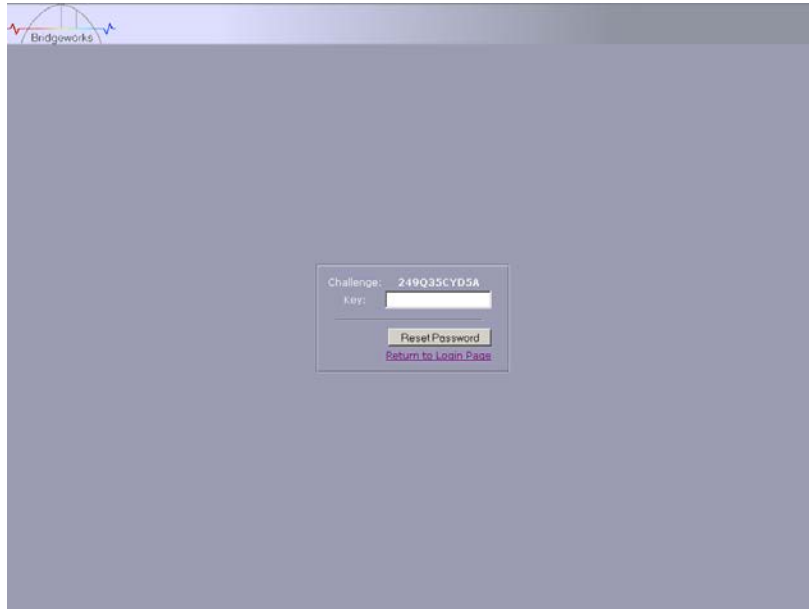
5.4 Restoring Factory Defaults

By clicking on this button all the parameters will be set back to the factory defaults. This includes IP address, hostname and passwords. We recommend that if you return the Bridge for maintenance that you reset to defaults to protect passwords and other sensitive information

6.0 Trouble shooting

6.1 Lost Password

If you have lost the admin password it is possible to reset it with help from Bridgeworks.



First ensure that there is nothing entered into the user field and then type PASSWORDRESET into the password field.

The unit will respond with a challenge key.

Copy this key into an email along with your name, company and contact details – you must include your company's personnel email address for security purposes.

Send this email to support@4bridgeworks.com and a key will be returned for you to enter into the key field.

Press the reset button once you have entered the key – this will reset the admin user password back to admin.

6.2 Network problems

Under normal operation you should be able to “ping” the network address of the Bridge and receive a response. If this fails, run through the following checklist to help you identify the problem.

- Ensure that the Bridge is properly plugged into the library and that the library is powered on. Make sure that the power LED on the Bridge is illuminated.
- Ensure that the Ethernet cable is plugged in at both ends .
- Note the status of the LEDs positioned within the Ethernet connector – make sure that the “Link present” LED is illuminated. If it is not, check with your Network Administrator.
- If you are using a Bridge with two Ethernet ports and only one network cable, try using the other network address and/or the other network port.
- Ensure you are using the correct network address and netmask.
- Scan the network using the LAN Scan utility to find all the Bridges connected to the network in case the network address is different from that expected. See Section Lost IP Address.

If none of the above resolves your problem, then after consulting with your Network Administrator, please contact support.

6.3 Device related problems

Once the Bridge has booted and the target devices have finished initialising, these devices should be available on the host machine. After checking that you have correctly configured the initiator, run through the following checklist to help you identify the problem.

- Ensure that the devices are powered on and are ready – some libraries can take 5 minutes or more before they are ready and appear on the Bridge. (The power up status of libraries are usually displayed on the front panel).
- Ensure that the cables between the Bridge and the devices are connected.
- Connect to the Bridge via the GUI and check that devices are present in the Device management window and are enabled – you will need to drill down each device entry to see this option.
- If you can “ping” the Bridge but the GUI fails to appear check the setting within the Web Browser you are using. If you are directly connected to the Bridge then any proxy setting will require adjustment and may require you to contact your administrator.
- Ensure that the CHAP settings for the initiator and the Bridge are the same.
- A common mistake is when enabling CHAP only for a device after the initial discovery by the initiator. It will be necessary to remove the address from the discoveries tab and recreate it with the appropriate CHAP settings, otherwise any rediscovers will be attempted without CHAP and no devices will be returned.
- Ensure any Fibre channel cables do not have any kinks or a bend which exceeds your cable manufacturers maximum bend radius. Also confirm that then connector ends of the cable are fully “clicked in” inside the SFP’s on both your initiator and Bridge.
- Some Manufacturers SFP’s do not report their speed correctly to the Bridge. To confirm that the speed is correct, first confirm the speed of your SFP by contacting your supplier.
- Once your speed is confirmed navigate to the fibre channel target page and click on the configuration next to the port you are using. Change the link speed form auto to the speed of your SFP. For more detailed instructions on this procedure see section (Error! Reference source not found. 5.1)If you are in any doubt it is recommended to use A 4GB SFP as this will prevent any speed compatibility problems.
- Ensure there is no damage to the SFP, confirm the SFP is fully pushed into the FC enclosure and that the clip to secure the cable in place is functioning correctly. When a cable is connected to the device correctly the Green LED on the front of the unit will flash. For further information see section (Error! Reference source not found.)
- Force a rediscovery from the initiator.
- Reboot the devices and Bridge.

If none of the above resolves your problem, please contact support.

6.4 Poor Performance

Poor performance can be caused by many differing reasons. The following checklist is provided as a guide to where you may find ways to improve performance.

- Ensure your initiator and Bridge are communicating at the fastest possible network speed. Within the GUI is the Network Connections window, select this and check the Link Speed entry in each of the Link Status Boxes. This should be 1000Mb/s - if this is 10 or 100Mb/s, this will limit the performance dramatically.
- Packet loss can be a cause of poor performance. Within the Link Status Box check the number of TX and RX errors for both network Interfaces that are displayed in the Network Connections window. This should be zero or a very small number. If these are showing large numbers of errors, check the connections between the Bridge and the initiator. Also check that the entire network cabling between the Initiator and the Bridge is Cat5e certified.
- By enabling Jumbo packets (increasing the MTU size to 9000 from within the GUI Network Connections window (section 3.2.2)) you can improve the throughput performance of the Bridge. This will only work if ALL of the components in the infrastructure between the Initiator and the Bridge are enabled for Jumbo packets. That includes the HBA, all switches and routers and the Bridge itself. If any of the components are not enabled or not capable of handling Jumbo packets then unexplained packet loss or corruption can happen.
- Data Digests are an extra level of checksum error checking on top of the standard TCP/IP checksum error checking (configured on the initiator). However, the calculation of these extra checksums can greatly affect overall performance. Therefore, Header and Data Digests should only be enabled where the integrity of the Network connection is in doubt.
- Poor GUI performance. If the Bridge is transferring large amounts of data then the response from the GUI may seem a little slow as the process that controls the GUI has the lowest priority for Network and CPU resources.
- It is possible to configure the Bridge so that the data from the initiator is balanced across both the Network Connections. Ensure that you have connected and configured these in accordance with Appendix C and not by enabling the Multipath connection option in the Windows initiator login screen. You should also check the routing tables in your switches, routers and initiator to ensure both IP addresses are not routed down one Network link at any stage.

6.5 Lost IP Address

Introduction

The utility will find any device irrespective of its IP address; this can be helpful in determining the IP address of a Bridgeworks device with an unknown IP address and for checking the number of Bridgeworks devices on a network.

Downloading LAN Scan

The utility can be downloaded from:

<http://www.4bridgeworks.com/support/software.shtml>

How to use LAN Scan

The utility is available under both Windows and Linux, and is a CLI based tool.

The downloaded file is in .zip format and contains the files lanscan, lanscan.exe and lanscan.bat.

For the GNU/Linux operating system the lanscan executable is needed.

For the Windows operating system the lanscan.exe and lanscan.bat files are required

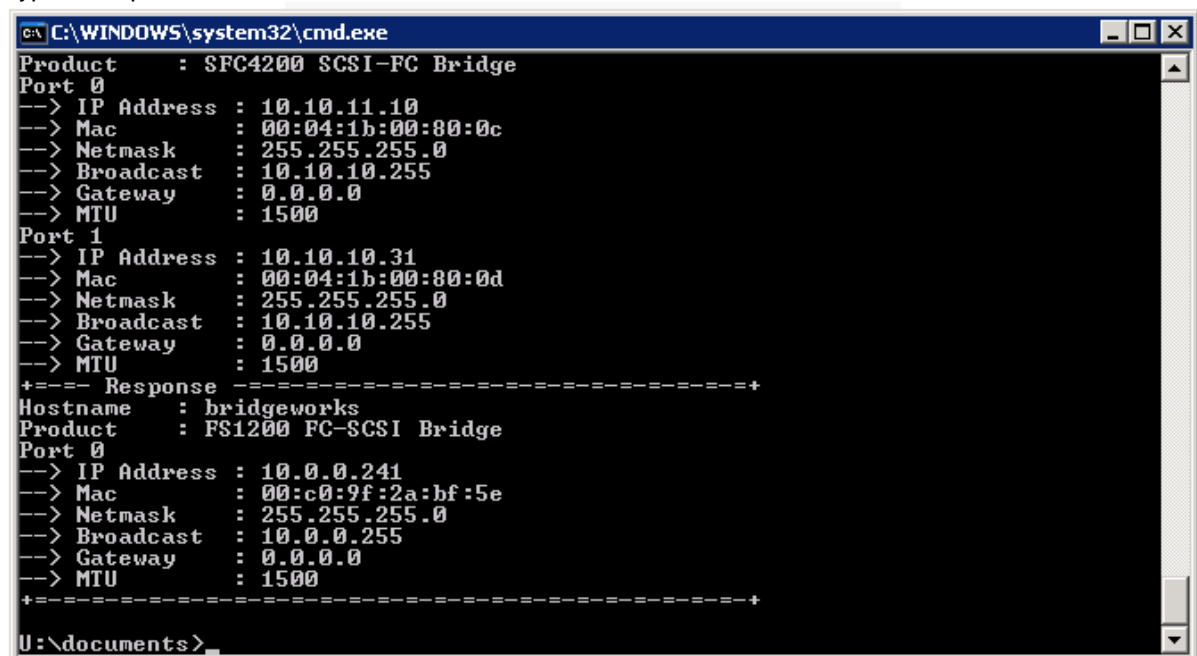
Linux

Execute lanscan within a console and the output is displayed on screen.

Windows

Double click on lanscan.bat. This will create a file named lanscan.txt. Open lanscan.txt within a text editor to view the discovered Bridgeworks devices.

Typical output



```
C:\WINDOWS\system32\cmd.exe
Product      : SFC4200 SCSI-FC Bridge
Port 0
--> IP Address : 10.10.11.10
--> Mac       : 00:04:1b:00:80:0c
--> Netmask   : 255.255.255.0
--> Broadcast : 10.10.10.255
--> Gateway   : 0.0.0.0
--> MTU       : 1500
Port 1
--> IP Address : 10.10.10.31
--> Mac       : 00:04:1b:00:80:0d
--> Netmask   : 255.255.255.0
--> Broadcast : 10.10.10.255
--> Gateway   : 0.0.0.0
--> MTU       : 1500
+==-- Response -==+
Hostname    : bridgeworks
Product     : FS1200 FC-SCSI Bridge
Port 0
--> IP Address : 10.0.0.241
--> Mac       : 00:c0:9f:2a:bf:5e
--> Netmask   : 255.255.255.0
--> Broadcast : 10.0.0.255
--> Gateway   : 0.0.0.0
--> MTU       : 1500
+==-- Response -==+
U:\documents>
```

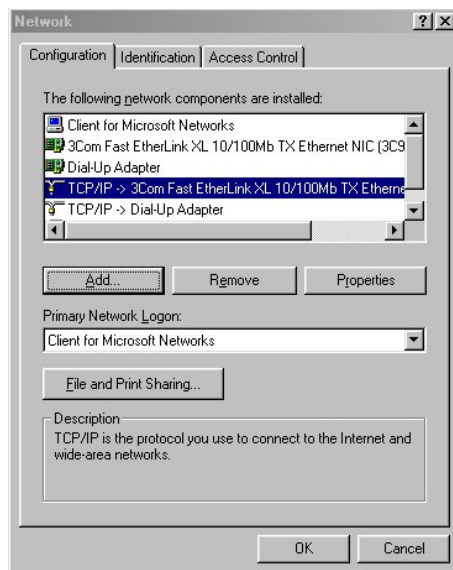
Appendix A Setting up your Computer for Initial Setup

A1 Windows 95, 98 or NT

If your computer is running Windows 95, 98 or NT follow the instructions below. For users with Windows 2000, 2003 or XP, instructions are detailed in Appendix A2 and for Windows Server 2008, 7 or Vista, instructions are detailed in Appendix A3.

From the **Start** menu, choose **Settings** then **Control Panel**.

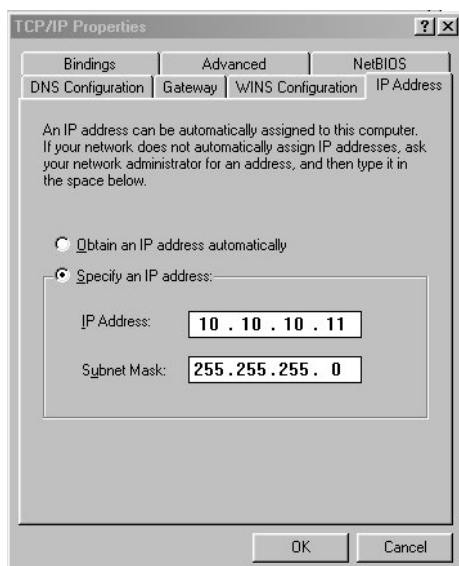
Then click the **Network** icon



In the **Network** window's **Configuration** tab,

Select the **TCP/IP** entry

Then the **Properties** Button



Click on the **IP Address** tab

Make a Note of your current set up then:

Click on the **Specify an IP** address button

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

Finally click the OK button and reboot your computer.



Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

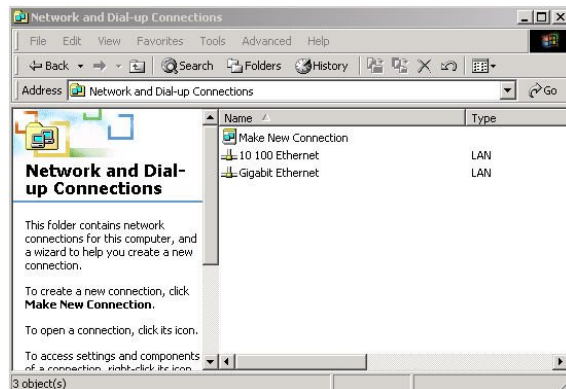
A2 Windows 2000, 2003, XP

If your computer is running Windows, 2000, 2003 or XP follow the instructions below .For users with Windows 95, 98 or NT instructions are detailed in Appendix A1 and for Windows Server 2008, 7 or Vista, instructions are detailed in Appendix A3.

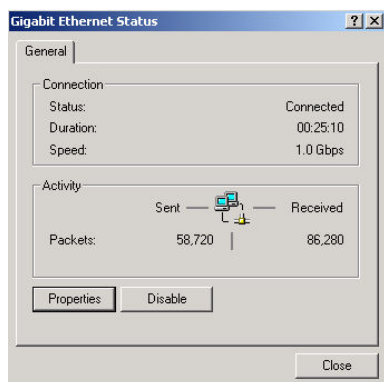
From the **Desktop** or **Start** menu, select **My Computer**



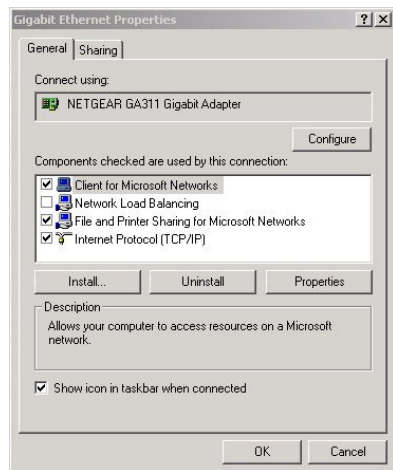
In the My Computer window select **Network and Dial-up Connections** positioned in the bottom left hand corner



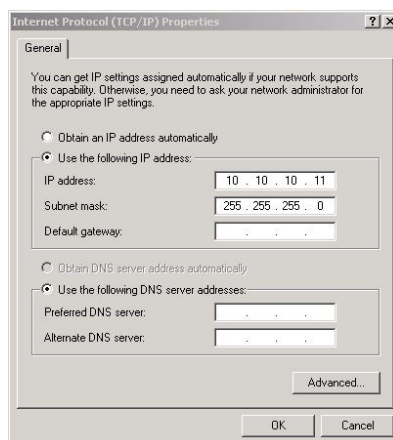
From within the displayed **Network and Dial-up Connections** select the interface connection that will be used to connect to the Bridge – in this example we have selected the Gigabit Ethernet interface.



A general status page will be displayed. From within this page select **Properties**



Select the **Internet Protocol (TCP/IP)** entry and then **Properties**



Make a Note of your current set up then:

Click **Use the following IP Address**

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

Finally click the OK button.

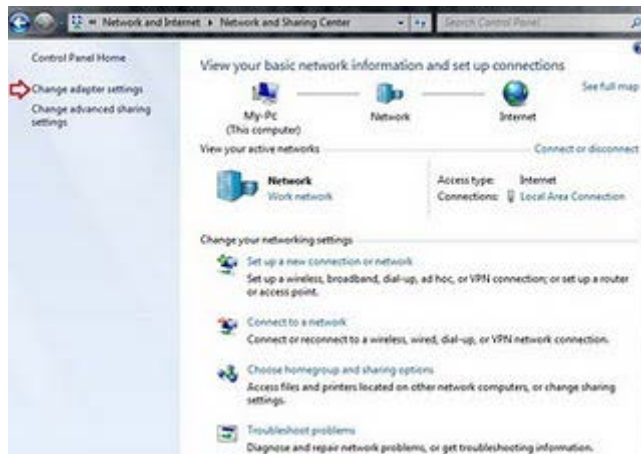


Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

A3 Windows Vista / Server 2008 or Vista or 7

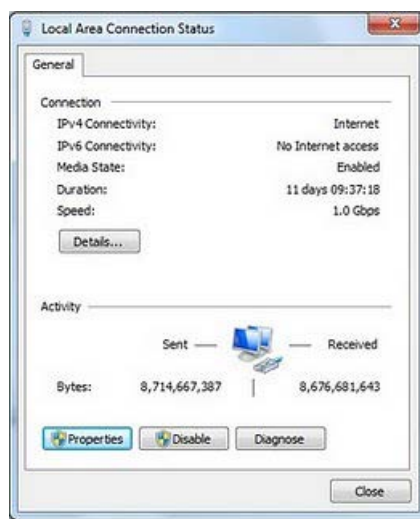
If your computer is running Windows, Vista or 7 follow the instructions below .For users with Windows 95, 98 or NT instructions are detailed in Appendix A1 and for Windows 2000, 2003 or XP, instructions are detailed in Appendix A2.

From the **Start** menu, select **Control Panel**

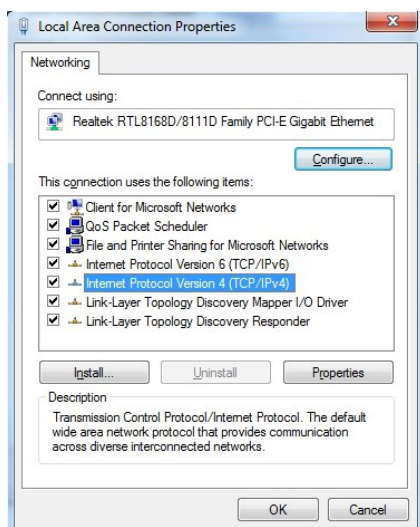


From the control panel select the **Network and Internet** link, followed by the **Network and Sharing Centre** link.

Now you can see the **Local Area connection** dialogue box. Double click Local Area Connections.



A general status page will be displayed. From within this page select **Properties**



Select the **Internet Protocol Version 4 (TCP/IP)** entry and then **Properties**



Make a Note of your current set up then:

Click **Use the following IP Address**

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

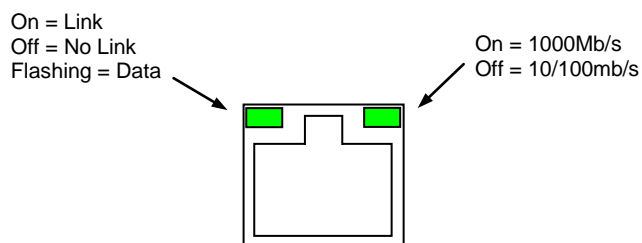
Finally click the OK button.



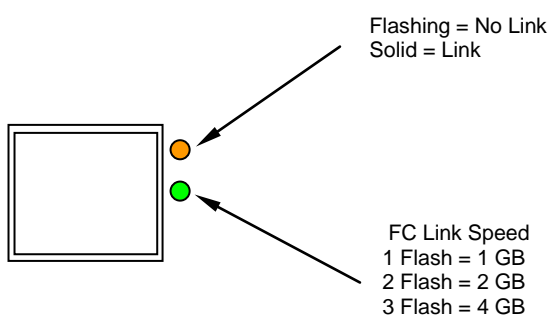
Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

Appendix B Visual Indicators

Ethernet



Fibre Channel



Note: During heavy data transfers, the LEDs may appear off for an extended period.

Appendix C Technical Specifications

Physical	
Form Factor	19" 1U Rack mount
Depth	170mm (10.6 in)
Height	44mm (1.7 in)
Width	437mm (17.2 in)
Weight	5.1Kg
Recommended minimum clearance for cooling	100mm (4.in) on front and rear faces
Electrical	
Input voltage	110 - 240V
Frequency	50 - 60Hz
Input current	1 Amp Maximum
Maximum Power Consumption	60 Watts Maximum
Environmental	
Operating	0 to 40C (32F to 104F)
Non Operating	-20C to 60C (-4F to 140F)
Operating Humidity	5% to 90% Non-condensing
Storage Humidity	5% to 90% Non-condensing
Operating Altitude	3,000m (9,842ft)
Non Operating Altitude	8,000m (26,250ft)
Fibre Channel Interface	
Physical Interface	2 SFP connectors
Speed	4Gb, 2Gb, 1Gb Auto or manual selected
Protocol	FC-AL, FC-PLDA, FC-PH, FC-FLA, FCP-SCSI, FC-FS, FC-TAPE
Topology	NL_Port, FL_Port, F_Port, N_Port
Visual Indicators	Link connection, Link Speed
iSCSI Interface	
Physical	RJ 45
Speed	10, 100, 1000Mb/s
Protocol	IPv4, IPv6, CHAP, DHCP, NTP, iSNS
ISCSI Protocol	ISCSI RFC3270, 3721, ERL0, ERL1 ERL2
Visual Indicators	Link and Link activity