

Potomac ESAS102800 iSCSI to SAS Bridge 3006.2800 User Manual V3.5

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	
3.2	July 2011	V3_02	
3.3	May 2012	V3_02	AP
3.4	August 2013	V3_04	AP
3.5	October 2013	V3_04	AP
ι			

Warning

iSCSI to SAS Page 2 The Bridgeworks Potomac ESAS102800 iSCSI to SAS 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.

10Gb Ethernet Cable

Depending on the configuration you have purchased you will require at least one cable from either

- Multimode Multi Mode 50/125 OM3 Patch Cable, up to 300 meters.
- Multimode Multi Mode 50/125 OM4 Patch Cable, up to 550 meters.

Or

• A SFP+ Direct Attached Twin-Ax Copper interface cable, up to 5 meters.

SAS Cable

The Bridge uses a "Mini SAS" style connector, also known as an iPASS connector, with 4 SAS connections per port. You will require a SAS cable that supports this connector at the Bridge end and the type of connect your peripheral device supports at the other.

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

Table of Contents

1.0 Introduction	6
1.1 Overview	6
1.2 Manual Layout	
1.3 Definitions	
1.4 Safety Notices	
2.0 Installing the ESAS102800 Bridge	9
2.1 Connecting the Ethernet Interface	9
2.2 Connecting the 10Gb Ethernet Cables	
2.3 SAS BUS Connection	
2.4 Connecting the Power Supply	13
3.0 Configuring the ESAS102800 Bridge	14
3.1 Using the Web Interface	14
3.1.1 Browsers	14
3.1.2 Connecting to the Web Interface	14
3.2 Configuring the Network Parameters	17
3.2.1 Setting the Hostname	17
3.2.2 Enabling IPv6	17
3.2.3 Setting the MTU	18
3.2.4 Setting the IP Address	18
3.2.5 Setting the Subnet Mask	
3.2.6 Setting the Gateway Address	
3.2.7 Setting an IPv6 IP Address	19
3.2.8 Committing the changes	
3.2.9 Reconnect to the Bridge	
3.2.8 Reconnect to the Bridge	
3.3 Passwords and Security.	
3.4 Network Services	21
3.4.1 NTP	21
3.4.2 Email Alerts	
3.4.3 iSNS	22
3.5 iSCSI Target Connections	23
3.6 iSCSI Sessions	24
3.7 Device Manager	
4.0 Information	26
4.1 System Information	26
4.2 System Log	
5.0 Maintenance	
5.1 Firmware Updates	28
5.2 Saving the Configuration to Disk	29
5.3 Restoring A Saved Configuration	
5.4 Restoring Factory Defaults	
6.0 Trouble shooting	
6.1 Lost Password	31
6.2 Network problems	32
6.3 Device related problems	
6.4 Poor Performance	
6.5 Lost IP Address	
Appendix A Setting up your Computer for Initial Setup	
A1 Windows 95, 98 or NT	
A2 Windows 2000, 2003, XP	37
A3 Windows Vista / Server 2008 or Vista or 7	
Appendix B Microsoft iSCSI Initiator	
B1 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows	
Vista Server 2008 R1 or Server 2003	

B2 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator	in Windows
Server 2008 R2	53
Appendix C Visual Indicators	65
Appendix D Technical Specifications	

1.0 Introduction

Thank you for purchasing the Bridgeworks iSCSI to SAS 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 section that will guide you through setting up both the network and SAS aspects of the iSCSI Bridge

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

1.1 Overview

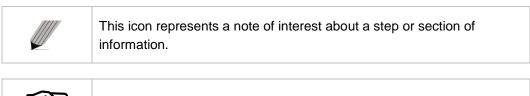
The iSCSI Bridge creates an interface between a network, which utilises the Ethernet protocol, and peripherals that utilise the SAS bus. The internal circuitry of the Bridge acts as a two-way interface converting the data packets that are received on the network into data transfers and electrical signals that storage devices such as disks, tape drives and optical disks understand on the SAS bus.

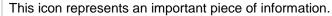


The Bridgeworks Enterprise iSCSI Bridge

1.2 Manual Layout

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







This icon represents a warning, care must be taken and the warning should be read thoroughly.

1.3 Definitions

In order to understand the process of identifying and configuring devices on the SCSI bus for the Server to communicate with it is necessary to understand some of the terms used by the menus.

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

SCSI Target Device

A SCSI device is a device that is connected to the SCSI bus that can be accessed by the Server. Each device on the SCSI bus has a Unique ID number in the range 0-15.

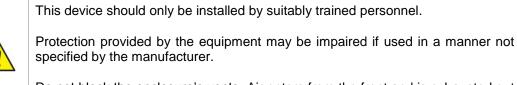


Note: By convention, ID 7 on the SCSI Bus is reserved by the Server's Host Bus Adaptor.

Logical Unit Numbers (LUN)

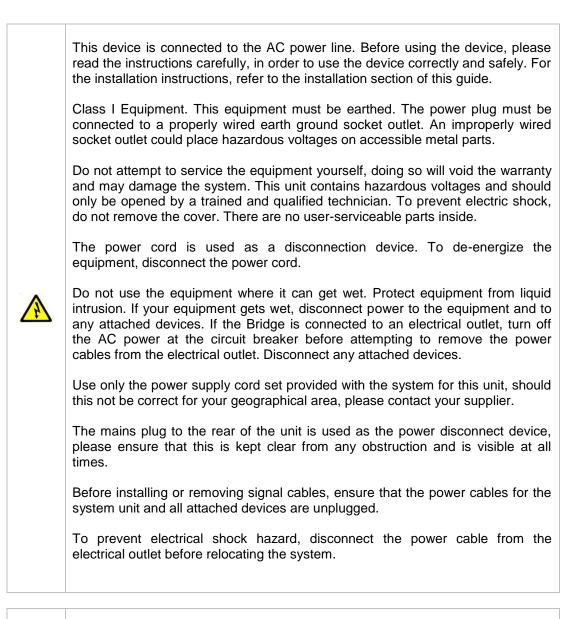
Each SCSI device on the SCSI bus can support sub-devices. These are called LUNs. Within the iSCSI Connect Bridge each SCSI ID on the SCSI bus can support 7 LUNs.

1.4 Safety Notices



This device should only be installed by suitably trained personnel.

Do not block the enclosure's vents. Air enters from the front and is exhausted out the back of the device.





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.

2.0 Installing the ESAS102800 Bridge

There are 3 basic steps to installing the iSCSI Bridge

- Connecting the Ethernet cables
- Connecting the 10Gb Ethernet cables
- Connecting the SAS cables
- Connecting the Power Supply

2.1 Connecting the Ethernet Interface

The iSCSI 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 the iSCSI Bridge when powered up it will automatically select the correct network speed.

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

To connect the iSCSI Bridge to the Ethernet network, inset 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 (Management A) as this is set to 10.10.10.10 for the initial configuration of the Bridge.



Rear Panel of the Bridge Showing Ethernet Cable Connections

2.2 Connecting the 10Gb Ethernet Cables

Depending on the configuration you have purchased one of two cables will be required for your product.

Small Form-factor Pluggable (SFP)

If you have purchased the card with the SFP's already connected the following cables can be used

- Multimode Multi Mode 50/125 OM3 Patch Cables up to 300 meters
- Multimode Multi Mode 50/125 OM4 Patch Cables up to 550 meters

To connect the iSCSI Bridge the Ethernet network or directly to a device, insert one or two SFPS into the unit.



Insert the multimode cables into the SFP you just inserted on the unit as shown below. When the plug is in the correct position a "click" should be heard.



Using a copper solution

If you are using a copper based solution, a SFP+ Direct Attached Twin-Ax Copper interface cable must be used. The maximum supported length of which is 5 meters.

To connect the iSCSI directly to a device, inset one or two SFP+ cables into the connector on the unit as shown below. When the plug is in the correct position a "click" should be heard.





Note: The 10Gb Ethernet ports only support speeds of 10GB/Sec.

2.3 SAS BUS Connection

The SAS bus on the iSCSI Bridge is capable of running at speeds of up to 6Gbits/s. However, devices that operate at slower speeds can still be connected to this SAS bus. In a manner similar to the Ethernet connection, the iSCSI Bridge will automatically negotiate with these devices to obtain their optimal operating speed upon power up. Each SAS port will support up to 4 SAS connections.

Connect the SAS cable(s) to the iSCSI Bridge as shown below, ensuring that connector is the correct way up.



Note: Each SAS port supports 4 independent SAS channels. You can use either port as the initial port.



Connecting the SAS Cable to the Bridge SAS Port

2.4 Connecting the Power Supply

Before connecting the power cord to the unit, ensure the wall plug is removed or is switched off. Connect the power cord to the rear of the iSCSI Bridge.

/////	
////	

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 on the opposite side to the power connector and push in the button. Whenever the Bridge is powered on the green LED on the back panel will be illuminated.



3.0 Configuring the ESAS102800 Bridge

Before the iSCSI 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 8
- Microsoft Internet Explorer 9
- Microsoft Internet Explorer 10
- Mozilla Firefox 20
- Mozilla Firefox 21
- Mozilla Firefox 22
- Google Chrome Latest



Note: JavaScript must be enabled within the web browser to use the web interface's functionality.



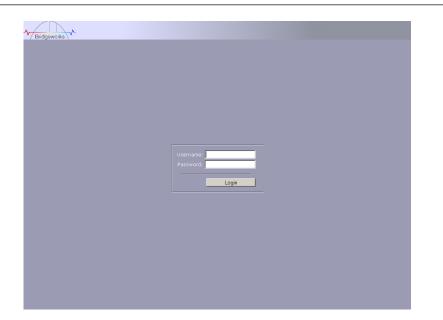
Important: If you choose to use a browser that is not on the list of supported browsers Bridgeworks cannot guarantee the behaviour of the Bridge's functionality.

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.

Bridgeworks	
Bridge Control	Network Connections
Console Home Network Ping Reboot System Logout	Global Network Configuration Hostname: bridge_esas DNS Server: 10.10.10.1 Enable Prot =
Support	Cancel Save
Online Help Contact Support	Network Interfaces Management A Connected, 100Mb/s Connected, 100Mb/s Network Cable Unplugged Network
© 2013 Bridgeworks Ltd	F0:1faf.d1:9c:6f F0:1faf.d1:9c:70 Port 1A Port 1B Network Cable Unplugged Connected, 10Gh/s 00:00cbe:cc:0f:64 00:00:00cbe:cc:0f:60
	<u></u> • • • • • • • • • • • • • • • • • • •

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.

dge Control	Network Port: Networ			
nsole Home				
etwork Ping		1500 ~		
boot System				
gout	Use DHCP to a	assign an IP address automatic		
	🖵 🖲 Use the follow			
port		10.10.10.120		
		255.255.255.0		
ine Help ntact Support		233.233.233.0		
		ring IPv6 address:		
		ing IPvb address:		
		ing IPv6 address:		
		Up Link Speed:	1000Mb/s	
	IPv6 address: Default gateway: Link Status Link State: RX Bytes:	Up Link Speed: 161579 TX Bytes :		
	IPv6 address: Default gateway: Link Status ILink State: RX Bytes: RX Errors:	Up Link Speed: 161579 TX Bytes: 0 TX Errors:		
	IPv6 address: Default gateway: Link Status Link State: RX Bytes: RX Errors: IPv4 Address	Up Link Speed: 161579 TX Bytes :		
	IPv6 address: Default gateway: Link Status ILink State: RX Bytes: RX Errors:	Up Link Speed: 161579 TX Bytes: 0 TX Errors:		

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.

3.2.8 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

Bridgeworks	
	Passwords & Security
Node Control Console Home Reboot System Logout Support Online Help Contact Support	System Password Old Password: New Password: Patype New Password: Change Password Secure Web Connection
© 2010 Bridgeworks Ltd	Enable HTTPS:

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.



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

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

/ Bridgeworks	Service Control	
Bridge Control Console Home		
Reboot System		
Logout	NTP Server:	
		Save
Support		
Online Help Contact Support		
	Recipient Email Address:	
2013 Bridgeworks Ltd	Sender Email Address:	
	Trigger Event Log Level: Error Events 👻	
	SMTP Server:	
	SMTP Username:	
	SMTP Password:	and the second
		Save
	iSNS Server:	
		Save

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.

3.4.3 iSNS

.

Internet Storage Name Service allows automated discovery, management and configuration of each iSCSI resource from a central point. If this option is enabled the Bridge will register its resources with a central iSNS server. To enable iSNS on the Bridge, click the tick box and enter the IP address for the iSNS Server and click the save button.

3.5 iSCSI Target Connections

This configuration page will allow the administrator to configure the password and username for the CHAP authorisation on the Bridge

From within the main menu select the iSCSI Target icon from the SCSI System group

The GUI will now display the following window

A Bridgeworks	
	iSCSI Target
Bridge Control <u>Console Home</u> <u>Reboot System</u>	Authorisation Chap enabled I
Logout	Initiator secret:
Support	Target secret:
<u>Online Help</u> <u>Contact Support</u>	Network Parts Physical Part Configured TCP Part(6)
	Network 1 3260
© 2010 Bridgeworks Ltd	Network 2 3260
	Save

CHAP

To enable CHAP click the tick box and enter the following details

- Username this is the same name as specified in the iSCSI host
- Initiator Secret this is the password defined in the iSCSI host
- Target Secret this is the password that the Bridge will send to the iSCSI host.

Multipath Settings

Multipath is a method of sending data to an iSCSI target over multiple network connections. These network connections can be on the same physical network cable or separate network cables. By using Multipath it is possible to increase the network bandwidth to send data over. A user may have a single iSCSI Session for an iSCSI Target, but within that session may have multiple connections.

iSCSI uses to two main network ports, 3260 and 860. Within the Multipath configuration the user can specify which ports will be made available to the initiator, 860, 3260 or both.

By default, the Bridge will allow up to 10 iSCSI connections per iSCSI Session. However, some initiators will only allow 1 iSCSI Connection per iSCSI Session and will reject any login to an iSCSI Target that tries to negotiate more iSCSI Connections.



Note: See Appendix B for how to set up multipath on a Microsoft based Server.

3.6 iSCSI Sessions

Each initiator will open a session with each target device; to review these connections select the iSCSI secessions page from the SCSI group.

Bridgeworks	
	iSCSI Sessions
Bridge Control	
Console Home	
Reboot System	Initiator Target
Logout	ign.1991-05.com.microsoft:kirk2k3 977d098e36978373.00000000000000000
Support	
Online Help	
Contact Support	
© 2010 Bridgeworks Ltd	
	Refresh Logout

This page lists the current connections i.e. logged on, from iSCSI hosts. It displays which initiator is connected to which Target device.



Note: It is possible that more than one host to be connected to any target device or one host to multiple target devices.

Should it be required, it is possible to send a logout request to a host by highlighting the host connection and pressing the logout button.



Note: Many initiators are configured to automatically reconnect after completing the logout request. If this is the case then the connections window may not show any change.

3.7 Device Manager

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

Bridgeworks								
	evice Management							
Console Home								
Reboot System	Target WWN eui:00041b0000108000 Target Alias 01:00							
Logout	Logical Units Attached: 1 Refresh Clear Configuration Update Configuration							
Support								
Online Help Contact Support								
© 2010 Bridgeworks Ltd								

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

~	Bridgeworks														
		Device	Manac	ement											
ľ	Bridge Control														
	Console Home														
	Reboot System	$\overline{}$	Target WWN Target Alias Logical Units Attached:		eui.00041b0000108000										
	<u>Robot oystem</u>					01:00	0			-					
	Logout		_												
			v [LUN	Prese	nt		oled		Persistent	7				
ľ	Support			Device			0 HR - Lili	rium 2-S	CSLE	Rev (T61D)					
				Device	Туре					vice Device					
	Online Help			SCSI Re			SPC-3								
	Contact Support			Media T			Removable Media naa.500608000057E758								
				Device WWN Device SCSI ID Enable / Disable Device		naa.50060B000			UUUUS/E/58						
	© 2010 Bridgeworks Ltd					ce	Enabled -								
Ľ	© 2010 Bridgeworks Ltu						1				J				
		R	efresh		Clear Cont	iguratio	n	U	odate	e Configuration					

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

Bridgeworks	
	System Information
Bridge Control	
Console Home	
Reboot System	Firmware Revision: "vielerj v3.02" (Mar 30 2011 11:40:27) Boot loader Revision: 1.2.0.1.1 sfc2200_v3_01_09_beta (Jun 10 2010 -
Logout	Serial Number: 007179 iSCSI IQN: ign.2002-12.com.4bridgeworks.001c0b
Support	
Online Help	
Contact Support	Data throughput OMB/s
© 2010 Bridgeworks Ltd	CPU Utilisation
	Memory Usage 60% Urad

Within the top window the following information is displayed

- Current Firmware & Boot Loader Revision Level
- SAS Firmware 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:

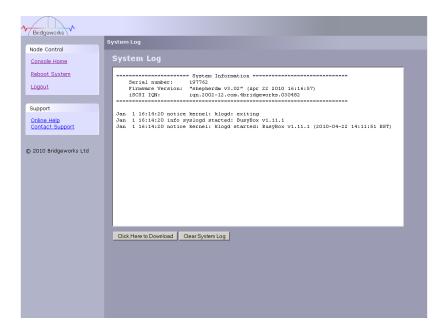
- Data Throughput This indicates the current performance in MB/s.
- CPU This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces
- Memory Usage This indicates the percentage of memory used by all processes

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.

Bridgeworks	
/ Dildgeworks \	Update Firmware
Bridge Control	
Console Home	
Reboot System	
Logout	Firmware image: Browse.
Support	
Online Help Contact Support	After clicking update please wait for this page to change before proceeding.
© 2010 Bridgeworks Ltd	

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

A Bridgeworks	
	Load/Save Configuration
Bridge Control	
Console Home	Import Configuration
Reboot System	Browse.
Logout	Upload
Support	
Online Help Contact Support	
	Click Here to Download
© 2010 Bridgeworks Ltd	Restore Defaults
	Restore Factory Defaults

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.

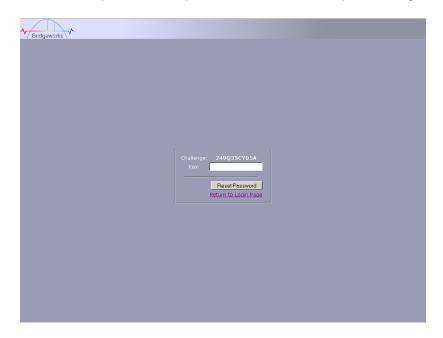
5.4 Restoring Factory Defaults

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 rediscoveries will be attempted without CHAP and no devices will be returned.
- 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.

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\sys	tem32\cmd.exe	_ 🗆 🗡
Product : SF	C4200 SCSI-FC Bridge	
Port Ø		
> IP Address		
> Mac	: 00:04:1b:00:80:0c	
> Netmask	: 255.255.255.0	
> Broadcast	: 10.10.10.255	
> Gateway	: 0.0.0	
> MTU	: 1500	
Port 1	- 44 44 - 24	
> Mac > Netmask	: 00:04:1b:00:80:0d : 255.255.255.0	
> Netmask > Broadcast	· 255.255.255.0 · 10.10.10.255	
> Gateway	· 10.10.10.235	
> MTU	: 1500	
+=-=- Response	• 1399	
	ridgeworks	
	1200 FC-SCSI Bridge	
Port Ø		
> 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	
+=-=-=-=-=-	-=-=-=+	
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

Network	? ×
Configuration Identification Access Control	
The following network components are installed:	
Client for Microsoft Networks Scom Fast EtherLink XL 10/100Mb TX Ethernet NI Dial-Up Adapter	
TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX B	therne
TCP/IP -> Dial-Up Adapter	
Add Remove Prop	erties
Client for Microsoft Networks	•
File and Print Sharing	
Description TCP/IP is the protocol you use to connect to the Inter wide-area networks.	net and
ОК	Cancel

In the Network window's Configuration tab,

Select the TCP/IP entry

Then the Properties Button

Bindings	Adv	Advanced		NetBIOS	
DNS Configuration	Gateway	WINS Co	nfiguration	IP Address	
An IP address can If your network doo your network admit the space below.	es not autor	natically ass	ign IP addi	resses, ask	
С <u>О</u> btain an IP	address aut	omatically			
	address:				
JP Address:	10	. 10 . 1	0.11		
S <u>u</u> bnet Mas	k: 255	. 255 . 29	55.0		

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.

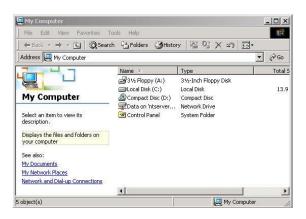


Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

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

🔃 Network and Dial-up Connectio	ns	_ 🗆 ×
File Edit View Favorites To	ols Advanced Help	
↔ Back + → + 🔂 🔞 Search	n 🔁 Folders 🎯 History 🛛 🖓 😤 🗙 ᡢ	
Address 📴 Network and Dial-up Cor	nections	▼ 🖓 Go
Network and Dial- up Connections	Name / Make New Connection 10 100 Ethernet Gigabit Ethernet	LAN LAN
This folder contains network connections for this computer, and a wizard to help you create a new connection.		
To create a new connection, click Make New Connection.		
To open a connection, click its icon.		
To access settings and components	•	•
3 object(s)		1

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.

neral		
Connection		
Status:		Connected
Duration:		00:25:10
Speed:		1.0 Gbps
Activity	Sent — 🗐	Received
Packets:	58,720	86,280
Properties	Disable	
		Clos

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

	311 Gigabit Adapter	
	are used by this conne	Configure
Z 🔜 File and Printe Z 🏹 Internet Proto	rr Sharing for Microsoft col (TCP/IP)	Networks
Install	Uninstall	Properties
Description	er to access resources	on a Microsoft
cachpaon	er to access resources	on a Microsoft

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

	automatically if your network supports d to ask your network administrator for
C Obtain an IP address automa	atically
Use the following IP address	
IP address:	10 . 10 . 10 . 11
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	
C Obtain DNS server address a	automatically
Use the following DNS serve	r addresses:
Preferred DNS server:	
Alternate DNS server:	(() ()

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.

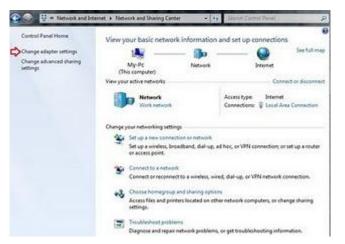


Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

A3 Windows Vista / Server 2008 or Vista or 7

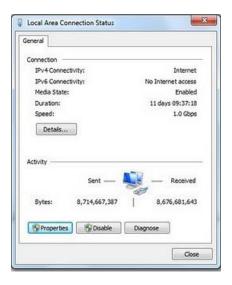
If your computer is running Windows, Vista or 7 follow the instructions below .For users with Windows 95, 98 or NT instructions are detailed in Appendix A1 and for Windows 2000, 2003 or XP, instructions are detailed in Appendix A2.

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**

onnect using:		
Realtek RTL8	168D/8111D Family PC	I-E Gigabit Ethernet
		Configure
his connection uses	the following items:	
🗹 🏪 Client for Mi	crosoft Networks	
🗹 📙 QoS Packet	Scheduler	
🗹 🚚 File and Prin	ter Sharing for Microsoft	Networks
	ocol Version 6 (TCP/IP	
🗹 🔺 Internet Prot		v6)
 Internet Prot Internet Prot Internet Prot Internet Prot Internet Prot 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map	v6) v4) per I/O Driver
A Internet Prot A Internet Prot A Internet Prot A Link-Layer T	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP	v6) v4) per I/O Driver
A Internet Prot A Internet Prot A Internet Prot A Link-Layer T	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map	v6) v4) per I/O Driver
 ✓ ▲ Internet Prot ✓ ▲ Internet Prot ✓ ▲ Link-Layer 1 ✓ ▲ Link-Layer 1 ✓ ▲ Link-Layer 1 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) (v4) per I/O Driver ponder
 ✓ Internet Prot ✓ Internet Prot ✓ Link-Layer T ✓ Link-Layer T ✓ Install Description 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) v4) per I/O Driver ponder P <u>r</u> operties
 ✓ Internet Prot ✓ Internet Prot ✓ Link-Layer 1 ✓ Link-Layer 1 ✓ Link-Layer 1 ✓ Install Description Transmission Cont wide area network 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	v6) v4) per I/O Driver ponder Properties tocol. The default

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

neral	
	ed automatically if your network supports a need to ask your network administrator b.
Obtain an IP address aut	tomatically
Use the following IP addr	ess:
IP address:	10 . 10 . 10 . 11
Subnet mask:	255.255.255.0
Default gateway:	10 . 10 . 10 . 1
Obtain DNS server addres	ss automatically
O Use the following DNS ser	ver addresses:
Preferred DNS server:	4 4 4
Alternate DNS server:	
Validate settings upon ex	Advanced

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 Microsoft iSCSI Initiator

B1 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Vista Server 2008 R1 or Server 2003

There are many iSCSI Initiators available. However, for the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI that is available with Microsoft Vista. However, the following procedure should be identical for all versions of Microsoft iSCSI Initiator.

Step 1 – General Set up

Open the iSCSI initiator and then click on the General Tab. You should see a window as shown below.

Favorite Targets	Volumes and Devices	RADIUS
General	Discovery	Targets
	tapes, CDs, and other storage our network that you can conne	
'our computer is called he iSCSI device, which	an initiator because it initiates t is called a target.	the connection to
nitiator Name	iqn.1991-05.com.microsoft:t	arquin-vista
o rename the initiator,	dick Change.	Change
o use mutual CHAP au argets, set up a CHAP	thentication for verifying secret.	Secret
"o set up IPsec tunnel r lick Set up.	node addresses,	Set up
/hat is iSCSI ?		

In this window the user is able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default. The iSCSI Bridge not support this

If you intend to use Mutual CHAP authentication you must enter the Initiator secret on this page.

Click on the secret button and a window should be displayed

SCSI Initiator	
Type a CHAP secret to be used to aut secure CHAP secrets are not words an of characters. Enter this same CHAP s initiator can connect.	nd phrases, but a random sequence
CHAP secret:	
CHAP secret:	

Enter in the Initiator Secret and click OK. The secret should be between 12 and 16 characters.

Make a note of this secret as you will need to enter this as part of configuring CHAP on the iSCSI Bridge

Step 2 - Discovery of Devices

Before the user can connect to an iSCSI Target, the iSCSI targets must be discovered. Click on the Discovery tab and you should see the window below

Favorite Targe	ts	Volumes and Devices	RADIU
General		Discovery	Targets
arget portals			
Address	Port	Adapter	IP address
Add Portal.		Remove	Refresh
Name			
Add		Remove	Refresh
		1.0	

To add an iSCSI Target portal, click on 'Add Portal'. The user should now be presented with a window.

Type the IP address or DNS nam to add. To select settings for the Advanced.		
IP address or DNS name:	Port:	
[]	3260	Advanced
-		Havancea.

Enter an IP-address for the iSCSI Target. In this example we shall use the IP-address of 10.10.10.50.

Leave the port 3260 unless you have configured your iSCSI Bridge only to respond on port 860, in which case change it to 860. Click on the advanced button to see the advanced options.

	IPsec	
Conne	ect by usin	g
Local	adapter:	Microsoft iSCSI Initiator
Sourc	e IP:	Default 👻
Targe	et portal:	
CRC /	Checksun	1
Da	ata digest	Header digest
initiat	or. To use	ure data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
initiat for th	or. To use iis initiator	it, specify the same target CHAP secret that was configured on the target
initiat for th User	or. To use lis initiator name:	it, specify the same target CHAP secret that was configured on the target
initiat for th User	or. To use iis initiator	it, specify the same target CHAP secret that was configured on the target
initiat for th User Targe	or. To use lis initiator. name: et secret: se RADIUS	it, specify the same target CHAP secret that was configured on the target iqn. 1991-05.com.microsoft:tarquin-vista to generate user authentication credentials
initiat for th User Targe	or. To use his initiator. hame: et secret: se RADIUS erform mut	it, specify the same target CHAP secret that was configured on the target iqn. 1991-05.com.microsoft:tarquin-vista to generate user authentication credentials ual authentication
initiat for th User Targe Use De To us	or. To use his initiator name: et secret: se RADIUS erform mut se mutual C	it, specify the same target CHAP secret that was configured on the target iqn. 1991-05.com.microsoft:tarquin-vista to generate user authentication credentials
initiat for th User Targe User De Radi	or. To use iis initiator name: et secret: se RADIUS erform mut use mutual C US. The s	it, specify the same target CHAP secret that was configured on the target ign.1991-05.com.microsoft:tarquin-vista to generate user authentication credentials ual authentication HAP either specify an initiator secret on the Initiator Settings page or use

The 'Connect by using' box allows the user to specify which iSCSI Adaptor to use and the Source IP. The Local adaptor will only differ from Microsoft iSCSI Initiator setting if an iSCSI Offload card has been installed. For the purpose of this guide we shall only use the Microsoft iSCSI Initiator. Leaving this setting as Default will also use the Microsoft iSCSI Initiator.

The Source IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the Server and the user wishes to select a particular interface, select the IP-address of that network interface from the pull down list.

CRC/Checksum settings allow the user to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended then Header and Data Digests are left disabled, as performance will be affected.

If the iSCSI Bridge has had CHAP enabled, or the user wishes to authenticate the iSCSI Bridge, click on the checkbox 'CHAP login information' to enable CHAP. Now enter the username and target secret that was configured on the iSCSI Bridge. If the user wishes to authenticate the iSCSI Bridge, select 'Perform mutual authentication'.

Note: For mutual CHAP to be performed, the Initiator Secret must be set on the general tab, and be the same as the one configured on the iSCSI Bridge.

The use of RADUS is beyond the scope of this guide. Once the user is satisfied that all advanced options are correct click OK. The user should now see a window as below.

Type the IP address or DNS nan to add. To select settings for th Advanced.		
IP address or DNS name:	Port:	
10.10.10.50	3260	Advanced

Now click OK and the Microsoft iSCSI Initiator shall perform the discovery. This usually performs quickly but can take up to a minute with multiple network ports. Once the discovery is complete, the user should see the target listed in the Target Portals list.

	s	Volumes and Devices	RADIUS	
General		Discovery	Targets	
arget portals				
Address	Port	Adapter	IP address	
10.10.10.50	3260	Default	Default	
Add Portal.		Remove	Refresh	
Name				
Add		Remove	Refresh	

If the user has an iSNS-server then the address can be added in the iSNS-servers list by clicking Add. A window should appear

dd iSNS Server		E
IP address or DNS name of server:		
	ОК	Cancel

Enter the address of the iSNS-Server then click OK. The Microsoft iSCSI-Initiator will now query the iSNS-Server and discover any iSCSI-Targets that are registered.

Step 3 – Targets

Click on the Targets tab.

The devices discovered should now be listed and shown as below

Favorite Targets	Volumes and Devices	RADIUS	
General Discovery		Targets	
og on.	s for a target, select the ta	-	
argets: Name ign. 1988-11.com.dell.b		Status	
iqn. 1988-11.com.dell.b		Inactive	
Details	Log on	Refresh	

In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check the settings used to do the discovery, especially the CHAP settings then return to Targets tab and click Refresh. If still no devices are displayed, check network cables and that the iSCSI Bridge is operational.

To connect to one of the iSCSI Targets, click on one of the target names and then click the 'Log on' button. In this example we have chosen the first target. A window should appear.

Target name:	
ign. 1988-11.com.dell.b9ad3	4:spi.6.0.0
Automatically restore this	connection when the computer starts
Enable multi-path	
Only select this option if i on your computer.	iSCSI multi-path software is already instal

If the user wishes to connect to the target automatically when the computer is booted, click the check box 'Automatically restore this connection when the computer starts'. Even if the user wishes to connect to the iSCSI Target using Multipath, they should not check

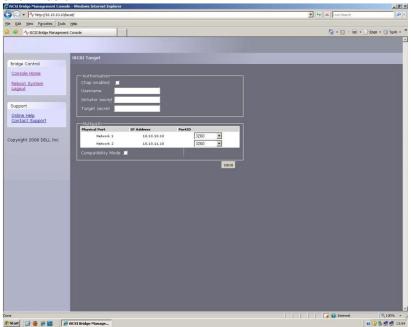
'Enable Multi-path' Check box. This will be covered in a following section. Now click on the advanced button to see the advanced settings. A window should appear as

Now click on the advanced button to see the advanced settings. A window should appear as below.

neral	IPsec	
Connec	ct by usin	
Local a	adapter:	Microsoft iSCSI Initiator 🗸
Source	e IP:	10.0.0.237
Target portal:		10.10.10.50 / 3260 🗸
CRC /	Checksum	
100		
CHAP I	helps ensi	Formation re data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
CHAP I initiato for this	AP logon i helps ensu r. To use s initiator.	nformation re data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
CHAP I initiato for this	AP logon i helps ensi ir. To use s initiator. ame:	nformation re data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
CHAP I initiato for this User n Target Use Per	AP logon i helps ensu r. To use s initiator. ame: : secret: c RADIUS form mutu	nformation re data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target iqn. 1991-05.com.microsoft:tarquin-vista to generate user authentication credentials ual authentication
CHAP I initiato for this User n Target Use Per To use	AP logon i helps ensu r. To use s initiator. ame: : secret: c RADIUS form mutu mutual C	nformation re data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target [iqn. 1991-05.com.microsoft:tarquin-vista to generate user authentication credentials

This advanced settings page is the same as that of the discovery with one addition. On the 'Connect by using' section the user can select the Target Port that he wishes to connect too. This is particularly useful if the user is going to create multiple connections. In this example we have chosen to connect to the IP-address 10.10.10.50 on port 3260.

To see how this relates to the iSCSI Bridge configuration note the IP-addresses in the window shown below.



Set up the Digest and CHAP settings as described in stage 2 during the discovery phase and click OK.

This will now take you back to the window that was shown in figure 10. Click OK once more. The user should now see the iSCSI Target connected.

Favorite Targets	Volumes and Devices	RADIUS	
General	Discovery	Targets	
og on.	s for a target, select the ta		
argets: Name ign. 1988-11.com.dell.b		Status	
ign. 1988-11.com.dell.b	2/1	Connected	
Details	Log on	Refresh	

Step 4 – Viewing iSCSI Session Details

Now that the user has connected to an iSCSI Target, to check that the device is connected click on the Details button. A window should appear.

S	
sessions:	
1370000008	
Log off	Refresh
1	
Connect	ed
1	
	Connections
	Connect

In this window the user can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group. If the user clicks on the Device tab, he should see details of the target device. Here we can see that the device is an IBM LTO Tape drive.

Sessions	Devices	Properties	
Advance multipat	ed to view h policy.	ices exposed by iSC information about t	SI sessions to the target. Click ne device and configure the
Devices			MPIO Capable
IBM UL	TRIUM-H	13 SCSI Sequential [evice LTO Tape drive
			Advanced

Step 5 – Creating multiple connections (Optional)

If the user wishes to create multiple connections to an iSCSI Session, return to the Session tab in the Target Properties window.

Click on the Connections button and a window should appear. This is shown below.

oad balance policy				
Round Robin	y.			•
	policy attempts to rocessing paths.	evenly dist	ribute incor	ning
This session has th Source Portal	e following connec Target Portal	tions : Status	Туре	Weight
10.0.0.237/5	10.10.10.50/	Conne	Active	n/a
٠ [

The Session Connections window shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions there will be at least one 'leading connection'.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

The Load balance policy specifies how the data is distributed over multiple connections. The main policies that should be used are 'Round Robin' and 'Fail Over Only'.

Round Robin will utilize all connections for data and evenly distribute the data.

Fail Over Only will use the Leading connection for data transfer. If a connection should go down then the data transfer shall switch on one of the other connections.

For most purposes Round Robin will provide the greatest performance increase.

If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

To add a new connection to a session, click on the Add button and a new window should appear.

arget name:		
ign.1988-11.com.dell.b9ad3	4:spi.6.0.0	
Advanced		Cancel

Now click on the Advanced button to see the Advanced Settings.

neral IPsec	
Connect by us	ing
Local adapter:	Microsoft iSCSI Initiator 👻
Source IP:	10.10.11.56
Target portal:	10.10.11.50 / 3260
CRC / Checksu	m
Data diges	t Header digest
CHAP helps er	information issure data security by providing authentication between a target and an e it, specify the same target CHAP secret that was configured on the target
CHAP helps en initiator. To us for this initiato	information issure data security by providing authentication between a target and an e it, specify the same target CHAP secret that was configured on the target
CHAP helps er initiator. To us for this initiato User name:	information issue data security by providing authentication between a target and an et, specify the same target CHAP secret that was configured on the target r, ign.1991-05.com.microsoft:tarquin-vista
CHAP helps er initiator. To us for this initiato User name: Target secret:	information issue data security by providing authentication between a target and an et, specify the same target CHAP secret that was configured on the target r, ign.1991-05.com.microsoft:tarquin-vista
CHAP helps er initiator. To us for this initiato User name: Target secret: Use RADIU	n information isure data security by providing authentication between a target and an e.k., specify the same target CHAP secret that was configured on the target r. iqn. 1991-05.com.microsoft:tarquin-vista
CHAP helps er initiator. To us for this initiato User name: Target secret: Use RADIU Perform mu To use mutual	information issue data security by providing authentication between a target and an et, specify the same target CHAP secret that was configured on the target r, iqn.1991-05.com.microsoft:tarquin-vista Sto generate user authentication credentials

Select the Source IP-address and the Target Portal that you wish to connect too via the pull down menus in the "Connect by using" section. When setting up multiple connections you ideally want to connect to different ports and different network interfaces. In this example we have connected to 10.10.10.50/3260 as the leading connection and the second connection will be 10.10.11.50/3260.

The corresponding network configuration on the iSCSI Bridge for the example above is shown below.

letwork Connections - Windows Internet Explorer	
Ar http://10.10.30/connections/ Ar http://10.30.30/connections/ Ar http://10.30.30/connections/ Ar http://10.30.30/connections/ Ar http://10.30.30/connections/ Ar http://10.30/connections/ Ar http://10.30/connec	 I 4y ≤ Live Search
A Network Connections	🖓 * 🖾 * 🖶 Page * 🕥 Tools
andge Control	
Concelle Home	
Network Ping	
Reboot System Hostname: bridgeworks	
Gateway: 10.10.10.1	
DNS Server: 10.10.10.1	
upport	
Ining Help Network Port 1	
Use DHCP:	
Vright 2008 DELL Inc	
IP Address: 10.10.10.50	
Netmask: 255.255.255.0	
Broadcast: 10.10.10.255	
Link Status	
Link State: up Link 100 N Speed:	
RX Bytes: 2953962 TX Bytes: 32943	
RX Errors: 0 TX Errors: 0	
Network Port 2	
Use DHCP:	
Frame Size: 1500 -	
IP Address: 10.10.11.50	
Netmask: 255,255,255,0	
Broadcast: 10.10.255	
- Link Status	
Link	tb/s
RX Bytes: 191039 TX Bytes: 10778	
RX Errors: 0 TX Errors: 0	
	Internet Protected Mode: Off 100%

Set up CHAP and Digest then click OK. The user will now be brought back to the window below. Click OK and now the user should see the Session Connections page with two connections.

Load balance polic	y:				
Round Robin				•	
	policy attempts to rocessing paths.	evenly dist	ribute incor	ning	
This session has th Source Portal	e following connec Target Portal	tions : Status	Type	Weight	1
	10.10.10.50/ 10.10.11.50/		Active	n/a n/a	(
•	III				۶

The user can add up to 8 different connections.

Once the user has completed setting up the connections, click OK to return to the iSCSI session page. You should now see the number of connections increased. In this example we have 2 connections.

Sessions	Devices	Properties		
This targ	et has the	e following ses	sions:	
Identif	ier	C-10		
Ffff	ffff8741d	31c-40000137	80000008	
		[Log off	Refresh
			LOG OIT	Keiresh
Sessio	n Properti	es		
Targe	t portal gro	oup:	1	
Status			Connec	ted
Conne	ction cour	ıt:	2	
Sessio	n Connect	ions		
To cor		w the connecti load balanced,		Connections
this se				

Now click on OK to return to the Microsoft iSCSI Initiator main window.

Step 6 – Logging off an iSCSI Session

To log off an iSCSI Session, follow the following procedure.

- Open the Microsoft iSCSI Initiator and click on the Targets tab.
- Click on the iSCSI session that the user wishes to log off and then click Details.
- In the Target Properties window, select the Sessions Tab and select the identifier that is to be logged off.
- Click the Log off button. This will log off all connections associated with the iSCSI Session.

The session identifier should now be removed from the identifier list. Click ok to return to the main iSCSI Initiator window. The iSCSI device should now show as inactive.

B2 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Server 2008 R2

There are many iSCSI initiators available. For the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI that is available with Microsoft Server 2008 R2.

Step 1 – General Set up

Open the iSCSI initiator and then click on the Configuration Tab. You should see a window as shown below.

rgets Discovery Favorite 1	argets Volumes and Devices	RADIUS Configuration
onfiguration settings here are ne initiator.	global and will affect any future	connections made with
ny existing connections may c ne initiator otherwise tries to re	ontinue to work, but can fail if th econnect to a target.	ne system restarts or
/hen connecting to a target, a articular connection.	dvanced connection features all	ow specific control of a
nitiator Name:		
iqn.1991-05.com.microsoft:wi	n-d3081sidkbe	
o modify the initiator name, cli	ck Change.	Change
o set the initiator CHAP secret lick CHAP.	for use with mutual CHAP,	CHAP
o set up the IPsec tunnel mod ick IPsec.	e addresses for the initiator,	IPsec
o generate a report of all conr ne system, click Report.	nected targets and devices on	Report
lore about Configuration		

In this window the user is able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default.

If you intend to use Mutual CHAP authentication you must enter the initiator secret on this page.

Click on the secret button and a window should be displayed

iSCSI Initiator Mutual CHAP Secret 🛛 🔀
The iSCSI initiator mutual CHAP secret is used to authenticate the target. The secret entered here will have to be configured on each target that you wish to use mutual CHAP.
Mutual CHAP requires the use of initiator authentication when connecting to the target, this can be done by using the advanced options when making connections to the target.
To clear the secret from the initiator, click Clear and then Cancel.
Initiator CHAP secret:
Clear OK Cancel

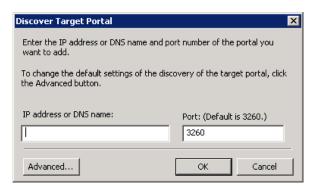
Enter in the initiator secret and click OK. The secret should be between 12 and 16 characters. Make a note of this secret, as you will need to enter this as part of configuring CHAP on the iSCSI Bridge.

Step 2 - Discovery of Devices

Before the user can connect to an iSCSI Target, the targets must be discovered. Click on the Discovery tab and you should see the window below

		on following portals:		Refresh
Address	Port	Adapter		IP address
To add a targel	: portal, click Disc	over Portal.		Discover Portal
To remove a ta then click Remo		t the address above a	and	Remove
NS servers				
	anistavad on the	following iSNS servers		Refresh
The system is i	egistered on the	rollowing ibrab servers	·	
	egistered off the	TOROWING ISING SERVERS	:	
	egistered on the			
Name			:	
Name	server, click Add			Add Server
Name To add an iSNS	server, click Add			Add Server Remove
Name Fo add an iSNS Fo remove an i:	server, click Add	Server.		

To add an iSCSI Target portal, click on 'Discover Portal'. The user should now be presented with a window.



Enter an IP-address for the iSCSI Target. In this example we shall use the IP-address of 10.10.10.99.

Leave the port 3260 unless you have configured your iSCSI Bridge only to respond on port 860, in which case change it to 860. Click on the advanced button to see the advanced options.

neral IPsec	
Connect using	
ocal adapter:	Default
nitiator IP:	Default
Farget portal IP:	_
CRC / Checksum	
Data digest	Header digest
an initiator,	onnection security by providing authentication between a target and
HAP helps ensure of an initiator. To use, specify the s hitiator. The name w	
CHAP helps ensure of an initiator. To use, specify the s	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this
HAP helps ensure of an initiator. Fo use, specify the s nitiator. The name v specified.	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is
HAP helps ensure or in initiator. 'o use, specify the s iliator. The name v pecified. Jame: arget secret: Perform mutual a o use mutual CHAP,	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is ign.1991-05.com.microsoft:win-d3081sidkbe
EHAP helps ensure of in initiator. To use, specify the s visitator. The name v pecified. Name: Target secret: Perform mutual a To use mutual CHAP, ADTUS.	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is iqn.1991-05.com.microsoft:win-d3081sidkbe
EHAP helps ensure of an initiator. To use, specify the s nitiator. The name v specified. Name: Target secret: Perform mutual a To use mutual CHAP, KADIUS.	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is iqn.1991-05.com.microsoft:win-d3081sidkbe uthentication , either specify an initiator secret on the Configuration page or use

The 'Connect using' box allows the user to specify which iSCSI Adaptor to use and the Source IP. The Local adaptor will only differ from Microsoft iSCSI Initiator setting if an iSCSI Offload card has been installed. For the purpose of this guide we shall only use the Microsoft iSCSI Initiator. Leaving this setting as default will also use the Microsoft iSCSI Initiator.

The Initiator IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the server and the user wishes to select a particular interface, select the IP-address of that network interface from the pull down list.

CRC/Checksum settings allow the user to specify whether the discovery is done using Data

and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

If the ISCSI Bridge has had CHAP enabled, or the user wishes to authenticate the ISCSI Bridge, click on the checkbox 'Enable CHAP log on' to enable CHAP. Now enter the username and target secret that was configured on the ISCSI Bridge. If the user wishes to authenticate the ISCSI Bridge, select 'Perform mutual authentication'.



Note: For mutual CHAP to be performed, the Initiator Secret must be set on the general tab, and be the same as the one configured on the iSCSI Bridge.

The use of RADUS is beyond the scope of this guide.

Once the user is satisfied that all advanced options are correct click OK. The user should now see a window as below.

Discover Target Portal	×
Enter the IP address or DNS name and want to add.	port number of the portal you
To change the default settings of the di the Advanced button.	scovery of the target portal, click
IP address or DNS name:	Port: (Default is 3260.)
10.10.10.99	3260
Advanced	OK Cancel

Now click OK and the Microsoft iSCSI Initiator shall perform the discovery. This usually performs quickly but can take up to a minute with multiple network ports.

Once the discovery is complete, the user should see the target listed in the Target Portals list.

	-	on following portals:	Refresh
Address	Port	Adapter Microsoft iSCSI Initial	IP address
10.10.10.99	3260	MICrosoft 15C51 Initia	tor 10.10.10.99
'o add a target p	ortal, click Disco	over Portal.	Discover Portal
fo remove a targe then click Remove		the address above and	Remove
fo add an iSNS se	rver, click Add	Server.	Add Server
	5 server, select	the server above and	Remove

iSCSI to SAS Page 56

If the user has an iSNS-server then the address can be added in the iSNS-servers list by clicking 'Add Server'. A window should appear

Add iSNS Server	×
Enter the IP address or DNS name of server:	
1	
ОК	Cancel

Enter the address of the iSNS-Server then click OK. The Microsoft iSCSI-Initiator will now query the iSNS-Server and discover any iSCSI-Targets that are registered.

Step 3 – Targets

Click on the Targets tab. The devices discovered should now be listed and shown as below

rgets Discovery Favorite Targets Volumes and Devices I	RADIUS Configuration
Duick Connect	
To discover and log on to a target using a basic connection, typ DNS name of the target and then click Quick Connect.	e the IP address or
Target:	Quick Connect
Discovered targets	
	Refresh
Name	Status
iqn.2002-12.com.4bridgeworks.000000:6d7a85844c2f1fa8	Reconnecting
iqn.2002-12.com.4bridgeworks.001c03:naa.50060b000057	Reconnecting
To connect using advanced options, select a target and then click Connect.	Connect
click Connect. To completely disconnect a target, select the target and	Connect Disconnect
click Connect. To completely disconnect a target, select the target and then click Disconnect. For target properties, including configuration of sessions,	Disconnect
click Connect. To completely disconnect a target, select the target and then click Disconnect. For target properties, including configuration of sessions, select the target and click Properties. For configuration of devices associated with a target, select	Disconnect Properties

In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check the settings used to do the discovery, especially the CHAP settings then return to Targets tab and click Refresh. If still no devices are displayed, check network cables and that the iSCSI Bridge is operational.

To connect to one of the iSCSI Targets, click on one of the target names and then click the 'Log on' button. A window should appear.

Connect To Target	×
Target name:	
qn.2002-12.com.4bridgeworks.000000:977d098e36978373.00000	
Add this connection to the list of Favorite Targets. This will make the system automatically attempt to restore the connection every time this computer restarts.	
🔲 Enable multi-path	
Advanced OK Cancel	

Even if the user wishes to connect to the iSCSI Target using Multipath, they should not check 'Enable Multi-path' Check box. This will be covered in a following section.

Now click on the advanced button to see the advanced settings. A window should appear as below.

neral IPsec	
1 1 200 1	
Connect using	
.ocal adapter:	Default
Initiator IP:	Default
Farget portal IP:	Default
CRC / Checksum	
Data digest	Header digest
an initiator.	onnection security by providing authentication between a target and
SHAP helps ensure of an initiator. To use, specify the s	
CHAP helps ensure of an initiator. Fo use, specify the s nitiator. The name v specified.	annection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this ill default to the Initiator Name of the system unless another name is
CHAP helps ensure of an initiator. Fo use, specify the s nitiator. The name v specified. Vame: Farget secret:	annection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this ill default to the Initiator Name of the system unless another name is Ign.1991-05.com.microsoft:win-d3081sidibe
EHAP, helps ensure of an initiator. Fo use, specify the s initiator. The name w specified. Vame: Farget secret: Perform mutual an To use mutual CHAP, (ADIUS,	annection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this all default to the Initiator Name of the system unless another name is ign.1991-05.com.microsoft:win-d3081sidibe
EHAP helps ensure of in initiator. To use, specify the s initiator. The name v specified. Name: l'arget secret: Perform mutual a fouse mutual CHAP, tADTUS.	annection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this ill default to the Initiator Name of the system unless another name is Ign.1991-05.com.microsoft:win-d3081sidibe Understand

This advanced settings page is the same as that of the discovery with one addition. On the 'Connect using' section the user can select the Target Port that he wishes to connect to. This is particularly useful if the user is going to create multiple connections. In this example we have chosen to connect to the IP-address 10.10.10.99 on port 3260.

Set up the Digest and CHAP settings as described in stage 2 during the discovery phase and click OK.

This will now take you back to the Connect to Target window. Click OK once more. The user should now see the iSCSI Target connected.

pets Discovery Favorite Targets Volumes and Devices RADIUS Configuration aick Connect discover and log on to a target using a basic connection, type the IP address or VS name of the target and then click Quick Connect. Quick Connect. arget: Quick Connect. Quick Connect. scovered targets Refresh Jame Status 3 p.2002-12.com.4bridgeworks.000000:977d098e36978 Connected p.2002-12.com.4bridgeworks.000000:977d098e36978 Inactive	
ick Connect discover and log on to a target using a basic connection, type the IP address or VS name of the target and then click Quick Connect. arget: Quick Connect. Quick Connect. Refresh lame Status gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
b discover and log on to a target using a basic connection, type the IP address or VS name of the target and then click Quick Connect. arget: Quick Connect. guick Connect. Refresh Iame Status gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
VS name of the target and then click Quick Connect.	
iscovered targets Refresh Iame Status gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
iscovered targets Refresh Iame Status gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
iscovered targets Refresh Iame Status gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
Refresh Jame Status gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	1
Jame Status pn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
gn.2002-12.com.4bridgeworks.000000:977d098e36978 Connected	
	Т
qn.2002-12.com.4bridgeworks.000000:977d0a8e36978 Inactive	_
connect using advanced options, select a target and then	
connect using advanced options, select a target and then Connect	
o completely disconnect a target, select the target and Disconnect	
	_
or target properties, including configuration of sessions, Properties	
lect the target and click Properties.	_
or configuration of devices associated with a target, select Devices	1
e target and then click Devices.	
re about basic iSCSI connections and targets	
re about basic ISCSI connections and targets	
re about basic ISCSI connections and targets	
re about basic iSCSI connections and targets	
re about basic iSCSI connections and targets	
re about basic iSCSI connections and targets OK Cancel Ap	

Step 4 – Viewing iSCSI Session Details

Now that the user has connected to an iSCSI Target, to check that the device is connected click on the 'Properties' button. A window should appear.

Properties	×	
Sessions Portal Groups		
	Refresh	
Identifier		
fffffa8001770018-400001370000	0008	
To add a session, click Add session.	Add session	
To disconnect one or more sessions, se session and then click Disconnect.	lect each Disconnect	
To view devices associated with a sessi a session and then click Devices.	on, select Devices	
Session Information		
Target portal group tag:	1	
Status:	Connected	
Connection count:	1	
Maximum Allowed Connections:	10	
Authentication:	None Specified	
Header Digest:	None Specified	
Data Digest: None Specified		
Configure Multiple Connected Session To add additional connections to a se configure the MCS policy for a selecte click MCS. More Information on ISCSI Sessions	ssion or	
	OK Cancel	

In this window the user can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group. If the user clicks on the 'Devices...' tab, he should see details of the target device.

Devices				×
Name	Address			
Disk -1	Port 2: Bus 0: Targ	get 0: LUN 0		
Volume path	names:			
Legacy devic	e name'			
Logac, come	o namor			
Device interf				
Device interra	ace name:		E	
– Coofigure Mi	النا = (MPIO) =			
-	the MPIO policy for	ra		
	rice, click MPIO.		MPIO	
Information C	n iSCSI Device Deta	ails		
			ОК	

Step 5 – Creating multiple connections (Optional)

If the user wishes to create multiple connections to an iSCSI Session, return to the Session tab in the Target Properties window.

Click on the 'MCS...' button and a window should appear. This is shown below.

tound Robin					
Description	olicy attempts to even	ly distribute ir	coming reque	sts to all	
his session has the	following connections	:			
1	Target Portal	Status	Tunn	Weight	Т
Source Portal			Туре		
	10.10.10.107/3	Connected	Active	n/a	
				n/a	<u>}</u>
Source Portal 0.0.0.0/61894	10.10.10.107/3				
0.0.0.0/61894	10.10.107/3	Connected	Active	n/a	
0.0.0.0/61894	10.10.10.107/3	Connected	Active	n/a	

The Multiple Connected Session window shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions there will be at least one 'leading connection'.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

The MCS policy specifies how the data is distributed over multiple connections. The main policies that should be used are 'Round Robin' and 'Fail Over Only'.

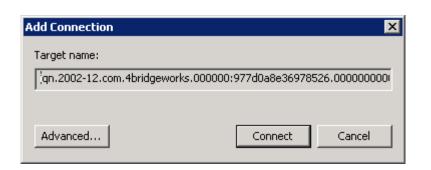
Round Robin will utilize all connections for data and evenly distribute the data.

Fail Over Only will use the Leading connection for data transfer. If a connection should go down then the data transfer shall switch on one of the other connections.

For most purposes Round Robin will provide the greatest performance increase.

If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

To add a new connection to a session, click on the Add button and a new window should appear.



Now click on the Advanced button to see the Advanced Settings.

Connect using	
.ocal adapter:	Microsoft iSCSI Initiator
Initiator IP:	Default
Target portal IP:	Default
CRC / Checksum	
Data digest	Header digest
CHAP Log on inform CHAP helps ensure of an initiator. To use, specify the s nitiator. The name w	
CHAP Log on inform CHAP helps ensure of an initiator. To use, specify the s nitiator. The name v specified.	Nation
CHAP helps ensure o an initiator. To use, specify the s	Nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is
CHAP Log on inform CHAP helps ensure of an initiator. To use, specify the s nitiator. The name v specified. Name: Target secret: Perform mutual a	Nation Onnection security by providing authentication between a target and arme name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is
CHAP Log on inform CHAP helps ensure of an initiator. In losses, specify the s- nitiator. The name w pecified. Vame: larget secret: Perform mutual and to use mutual CHAP, VADIUS.	Nation Onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is

Select the Initiator IP-address and the Target Portal that you wish to connect too via the pull down menus in the "Connect by using" section. When setting up multiple connections you ideally want to connect to different ports and different network interfaces

Set up CHAP then click OK. The user will now be brought back to the window below. Click OK and now the user should see the Session Connections page with two connections.

ultiple Connected	Session (MCS)				2
ACS policy:					
Round Robin					•
Description The round robin po processing paths.	licy attempts to ever	ıly distribute in	coming reque	sts to all	
This session has the l	following connections	:			
Source Portal	Target Portal	Status	Туре	Weight	
0.0.0.0/60102	10.10.10.107/3	Connected	Active	n/a	0
0.0.0.0/63942	10.10.10.107/3	Connected	Active	n/a	0
•					Þ
To add a connection	, click Add.			Add	
To remove a connec click Remove,	tion, select the conne	ection above a	nd then	Remove	
To edit the path sett connection above ar	tings for the MCS poli ad then click Edit.	cy, select a		Edit	
	0	к 🔤	Tancel	Apply	

The user can add up to 10 different connections.

Once the user has completed setting up the connections, click OK to return to the iSCSI session page. You should now see the number of connections increased. In this example we have 2 connections.

Properties			×
Sessions Portal Groups			
		Ref	resh
Identifier			
ffffa8001770018-400001370000	0007		
To add a session, click Add session.		Add s	ession
To disconnect one or more sessions, se session and then click Disconnect.	To disconnect one or more sessions, select each session and then click Disconnect.		
To view devices associated with a sessi a session and then click Devices.	To view devices associated with a session, select a session and then click Devices.		
Session Information			
Target portal group tag:	1		
Status:	Connected		
Connection count:	2		
Maximum Allowed Connections:	10		
Authentication:	None Specif	ied	
Header Digest: None Specified			
Data Digest: None Specified			
Configure Multiple Connected Session To add additional connections to a se configure the MCS policy for a selecte click MCS. More Information on ISCSI Sessions	ssion or	MC	5
	0	ĸ	Cancel

Now click on OK to return to the Microsoft iSCSI Initiator main window.

Step 6 – Logging off an iSCSI Session

To log off an iSCSI Session, follow the following procedure.

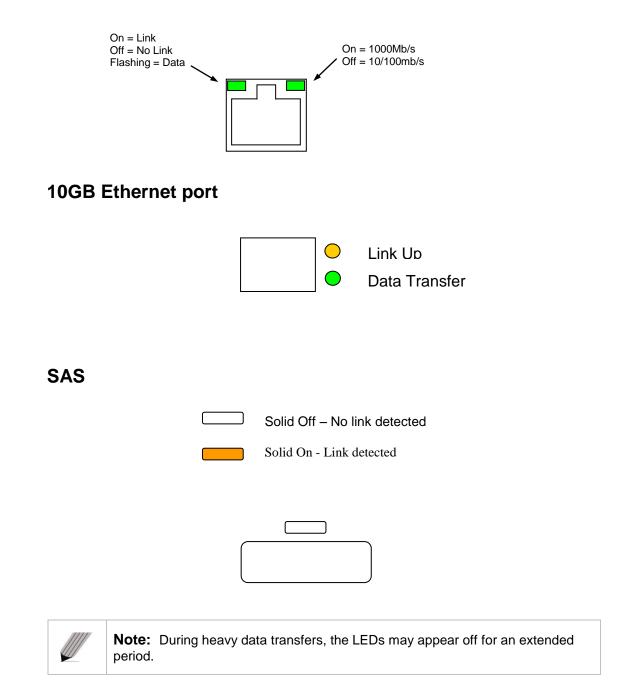
- Open the Microsoft iSCSI Initiator and click on the Targets tab.
- Click on the iSCSI session that the user wishes to log off.
- Click the 'Disconnect' button. This will log off all connections associated with the iSCSI Session.

•

The iSCSI device should now show as inactive.

Appendix C Visual Indicators

Ethernet



Appendix D Technical Specifications

Physical	
Form Factor	19" 1U Rack mount
Depth	612mm (24.12 in)
Height	42.9mm (1.7 in)
Width	434mm (17.09 in)
Weight	12Kg
Recommended minimum clearance for cooling	100mm (4.in) on front and rear faces
Electrical	
Input voltage	100 - 240V
Frequency	50 - 60Hz
Input current	4 Amp Maximum
Maximum Power Consumption	350 Watts Maximum
Environmental	
Operating	10°C to 35°C (50°F to 95°F)
Non Operating	-40°C to 65°C (-40°F to 149°F)
Operating Humidity	8% to 85% Non-condensing
Storage Humidity	5% to 95% Non-condensing
Operating Altitude	-16 to 3,048m (-50 to 10,000ft)
Non Operating Altitude	-16 to 10,600m (-50 to 35,000ft)
iSCSI Interface	
Physical	SFP+ Twin-Ax, 10GBase-SR Laser LC
Speed	10000Mb/s
Protocol	IPv4, IPv6, CHAP, DHCP, NTP, iSNS
ISCSI Protocol	ISCSI RFC3270, 3721, ERL0, ERL1 ERL2
Visual Indicators	Link and Link activity
SAS Interface	
Physical	2x SFF – 8088 External mini-SAS
Speed	1.5Gb/s, 3Gb/s and 6Gb/s
Protocol	SAS 2.0
Visual Indicators	Link, Activity
Ethernet Interface	
Physical	RJ45
Speed	10, 100, 1000Mb/s

Protocol	IPv4, IPv6,
Visual Indicators	Link, Activity