

Potomac ESAS2800 iSCSI to SAS Bridge 3006.2800 User Manual V3.3

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
3.3	October 2013	V3_04	AP

Warning

The Bridgeworks Potomac ESAS2800 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.

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	
1.1 Overview	6
1.2 Manual Layout	7
1.3 Definitions	7
1.4 Safety Notices	8
2.0 Installing the ESAS2800 Bridge	9
2.1 Connecting the Ethernet Interface	
2.2 SAS BUS Connection	
2.3 Connecting the Power Supply	
3.0 Configuring the ESAS2800 Bridge	
3.1 Using the Web Interface	12
3.1.1 Browsers	
3.1.2 Connecting to the Web Interface	
3.2 Configuring the Network Parameters	
3.2.1 Setting the Hostname	
3.2.2 Enabling IPv6	
- · · · · · · · · · · · · · · · · · · ·	
5	
3.2.4 Setting the IP Address	
3.2.5 Setting the Subnet Mask	
3.2.6 Setting the Gateway Address	
3.2.7 Setting an IPv6 IP Address	
3.2.8 Committing the changes	
3.2.9 Reconnect to the Bridge	
3.3 Passwords and Security	
3.4 Network Services	19
3.4.1 NTP	19
3.4.2 Email Alerts	19
3.4.3 iSNS	20
3.5 iSCSI Target Connections	
3.6 iSCSI Sessions	
3.7 Device Manager	
4.0 Information	
4.1 System Information	
4.2 System Log	
5.0 Maintenance	
	26
5.2 Saving the Configuration to Disk	20
5 5	
· · · · · · · · · · · · · · · · · · ·	
6.0 Trouble shooting	
6.1 Lost Password	
6.2 Network problems	
6.3 Device related problems	
6.4 Poor Performance	
6.5 Lost IP Address	
Appendix A Setting up your Computer for Initial Setup	34
A1 Windows 95, 98 or NT	34
A2 Windows 2000, 2003, XP	35
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	

Appendix C Visual Indicators	64
Appendix D Technical Specifications	65

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

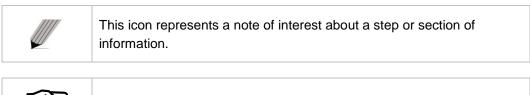
The iSCSI Bridge creates an interface between a network, which utilises the Ethernet protocol, and peripherals that utilise the SAS bus. The internal circuitry of the Bridge acts as a two-way interface converting the data packets that are received on the network into data transfers and electrical signals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

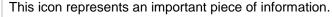


The Bridgeworks Small Enterprise iSCSI Bridge

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.

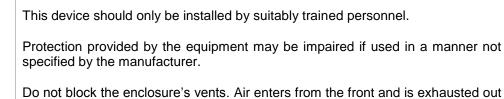


Note: By convention, ID 7 on the SCSI Bus is reserved by the Server's Host Bus Adaptor.

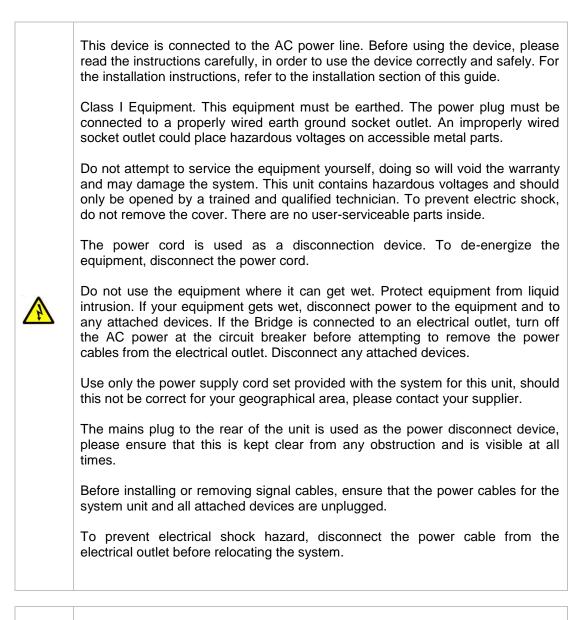
Logical Unit Numbers (LUN)

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



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 ESAS2800 Bridge

There are 3 basic steps to installing the iSCSI Bridge

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

2.1 Connecting the Ethernet Interface

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

2.2 SAS BUS Connection

The SAS bus on the Bridge is capable of running at speeds of up to 3Gbits/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 Bridge will automatically negotiate with these devices to obtain their optimal operating speed upon power up. Each SAS port on the Bridge port will support up to 4 SAS channels.

Connect the SAS cable to the front of the Bridge as shown below, ensuring that connector is the correct way up.

Connecting the SAS Cable to the Bridge SAS Port



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 ESAS2800 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 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.



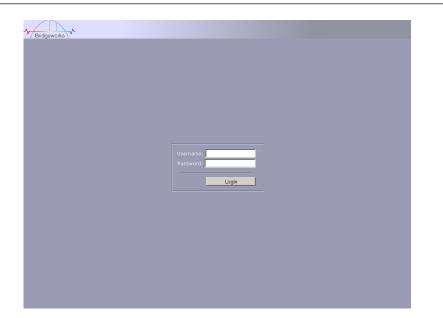
Important: If you choose to use a browser that is not on the list of supported browsers Bridgeworks cannot guarantee the behaviour of the Nodes functionality.

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.

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.

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

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
Node Control	
Console Home	
Reboot System	Use NTP:
Logout	NTP Server:
angens	Save
Support	
Online Help	Enable Email Alerts:
Contact Support	Recipient Email Address:
	Sender Email Address:
© 2010 Bridgeworks Ltd	Trigger Event Log Level: Warning Events 🔽
	SMTP Server:
	SMTP Username:
	SMTP Password:
	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

Bridgeworks	
	iSCSI Target
Bridge Control	
Console Home	
Reboot System	Chap enabled I
Logout	Initiator secret:
	Target secret:
Support	
Online Help Contact Support	Network Ports
	Physical Port Configured TCP Port(s)
	Network 1 3260
© 2010 Bridgeworks Ltd	Network 2 3260
	Seve

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	
Bridge Control	iSCSI Sessions
Console Home	-iSCSI Sessions
Reboot System	
	Initiator Target ign.1991-05.com.microsoft:kirk2k3 977d098e36978373.0000000000000000000000000000000000
Logout	
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

This configuration page will allow the administrator to configure a number of parameters that control the behavior of the SAS bus.

From within the main menu select the Device Management section.

The GUI will now display the following window

Eridge Control Console Home Reboot System Legout Support Online Help Contact Support © 2008 Bridgeworks Ltd					-	ple Targets wi	ith Single LUN 💽
Online Help Contact Support	1000						
© 2008 Bridgeworks Ltd		Targe	twwn		Teui.50	00E11112E32002	.,L,0×00000000000000000
© 2008 Bridgeworks Ltd		Target Alias Logical Units Attached: 7 Target WWN Target Alias Logical Units Attached:		ched:	Teui.5000E11112E32002,L,0×0000000000000000000000000000000		
	~			Teui.5000E11112E32002,L,0×000100000000000 Teui.5000E11112E32002,L,0×0001000000000000 1			
				Prese		enabled	Persistent
		Targe	t WWN t Alias al Units Atta	ched:			;,L,0×0000000000000000000000000000000000
		State of the local state of the	LUN O	Prese	nt [enabled	Persistent
			Device Device Ty SCSI Rev Media Typ	ision	Sequen SPC-3	ILT3580-HH4 Rev Itial Access Device able Media	
			Device W Device St Persisten	CSI ID	eui.500 0:0:0:0		L,0×00000000000000000
			Enable / Device	Disable	Enab	oled 🗾	
	Re	fresh	_	Cle	ar Cor	nfiguration L	Jpdate Configuration

In the first Box at the top of the screen are a number of options for configuring how the Bridge will present the SAS devices on the SCSI interface.

• Single Target with Multiple LUNs – Choose this option if you require all the devices on the SAS ports to appear as a single WWN with devices as LUN underneath this.

By clicking on the blue triangle in the Device info box you can display further information about each SAS device.

The expanded information also gives you a device control option

Enable / Disable Device – This pull down menu option allows you to disable a SAS device from appearing on the SCSI 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	
	isosriqit. iqn.2002 iz.com.tonugeworks.co.rcob	
Support		
Online Help Contact Support		
	OMB/s	
© 2010 Bridgeworks Ltd	CPU Utilisation	
	Memory Usage	
	60% Used	

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:

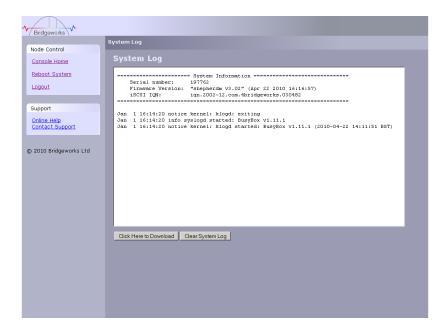
- Data Throughput This indicates the current performance in MB/s.
- CPU This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces
- Memory Usage This indicates the percentage of memory used by all processes

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	
/ blidgeworks \	Update Firmware
Bridge Control	
Console Home	
Reboot System	
Logout	Firmware image: Browse.
Support	Update
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

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

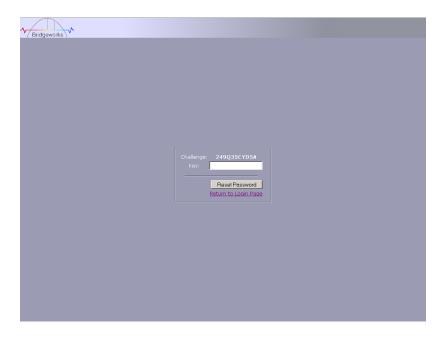
5.4 Restoring Factory Defaults

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	<u>? ×</u>
Configuration Identification Access Control	Ι
The following network components are instal	lled:
Client for Microsoft Networks Client for Microsoft Networks Client Fast EtherLink XL 10/100Mb TX E Dial-Up Adapter	
Y TCP/IP → 3Com Fast EtherLink XL 10/1 TCP/IP → Dial-Up Adapter	00Mb TX Ethems
Add Remove	Properties
Client for Microsoft Networks	•
<u>F</u> ile and Print Sharing	
Description TCP/IP is the protocol you use to connect wide-area networks.	to the Internet and
	IK Cancel

In the Network window's Configuration tab,

Select the TCP/IP entry

Then the Properties Button

Adv	anced	N	letBIOS
Gateway	WINS Con	figuration	IP Address
s not autor	natically assig	gn IP addi	resses, ask
iddress aut	omatically		
address: —			
10	. 10 . 10	. 11	
255	. 255 . 25!	5.0]
	Gateway be automat s not autor strator for ddress aut address: 10	be automatically assign s not automatically assign strator for an address, a ddress automatically address: 10, 10, 10, 10	Gateway WINS Configuration be automatically assigned to this s not automatically assign IP add strator for an address, and then the ddress automatically address: 10, 10, 10, 11, 11

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.

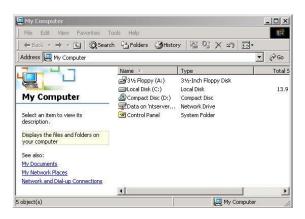


Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

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	ools Advanced Help	1
] 😓 Back 🔹 ⇒ → 🔂 @ Search	n 🖫 Folders 🎯 History 📴 😤 🗙 ᡢ	
Address 📴 Network and Dial-up Cor	nections	▼ 🖓 Go
Network and Dial- up Connections	Name / Name / Nake New Connection Lo 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	-	Þ
3 object(s)		

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**

	1 Gigabit Adapter	
omponents checked a		Configure
10	Uninstall	Properties
Install	Uninstall	
Install Description Allows your computer network.		

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

	d automatically if your network supports sed to ask your network administrator for
C Obtain an IP address autor	matically
Use the following IP address	\$\$;
IP address:	10 . 10 . 10 . 11
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	3 3 2
C Obtain DNS server address	s automatically
Use the following DNS service	ver addresses:
Preferred DNS server:	
Alternate DNS server:	(((((((((((((((((((
	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.

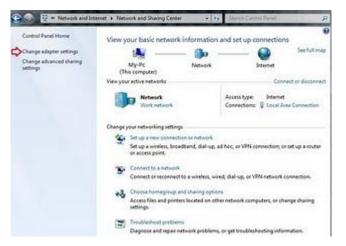


Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

A3 Windows Vista / Server 2008 or Vista or 7

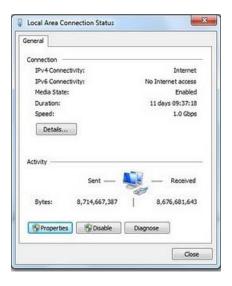
If your computer is running Windows, Vista or 7 follow the instructions below .For users with Windows 95, 98 or NT instructions are detailed in Appendix A1 and for Windows 2000, 2003 or XP, instructions are detailed in Appendix A2.

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**

Connect using:		
Realtek RTL8	168D/8111D Family PC	-E Gigabit Ethernet
		Configure
This connection uses	the following items:	
Client for Mic		
QoS Packet		
E File and Prin	ter Sharing for Microsoft	Networks
A Internet Dest		
	ocol Version 6 (TCP/IP	/6)
🗹 📥 Internet Prot	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP	/6) /4)
 Internet Prot Link-Layer T 	ocol Version 6 (TCP/IP	v6) v4) per I/O Driver
 ✓ Internet Prot ✓ Link-Layer 1 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map	v6) v4) per I/O Driver
 ✓ Internet Prot ✓ Link-Layer 1 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map	v6) v4) per I/O Driver
 ✓ Internet Prot ✓ Link-Layer 1 ✓ Link-Layer 1 	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res	r6) r4) per I/O Driver ponder
Internet Prot ink-Layer 1	ocol Version 6 (TCP/IP ocol Version 4 (TCP/IP opology Discovery Map opology Discovery Res Uninstall	r6) /4) per I/O Driver ponder Properties tocol. The default
✓ Internet Prot ✓ Internet Prot ✓ Link-Layer T ✓ Link-Layer T ✓ Link-Layer T ✓	ocol Version 6 (TCP/IP- ocol Version 4 (TCP/IP- opology Discovery Map opology Discovery Res	r6) /4) per I/O Driver ponder <u>Properties</u> tocol. The default

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

ieneral	
	ed automatically if your network supports need to ask your network administrator
💮 Obtain an IP address auto	omatically
() Use the following IP addre	ess:
IP address:	10 , 10 , 10 , 11
Subnet mask:	255.255.255.0
Default gateway:	10 . 10 . 10 . 1
Obtain DNS server addres	is automatically
O Use the following DNS ser	ver addresses:
Preferred DNS server:	41-141-14
Alternate DNS server:	the second
Validate settings upon ex	dt 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 Target	s	Volumes and Devices	RADIU
General		Discovery	Targets
arget portals			
Address	Port	Adapter	IP address
Add Portal		Remove	Refresh
Name			
Add		Remove	Refresh

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

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 👻
Target 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 name to add. To select settings for the o 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.

Favorite Target	s	Volumes and Devices	RADIU
General		Discovery	Targets
arget portals			
Address	Port	Adapter	IP address
10.10.10.50	3260	Default	Default
Add Portal.		Remove	Refresh
SNS servers Name			
Add		Remove	Refresh
Auum			

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		
P address or DNS name of server:		
	· · · · · · · · · · · · · · · · · · ·	100
	OK	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'		itatus nactive	
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.

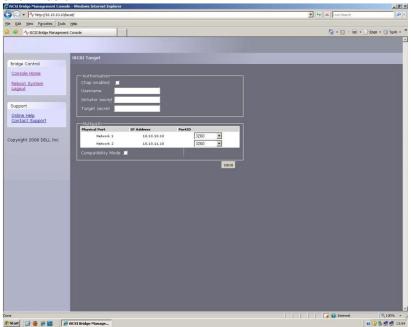
ign. 1988-11.com.dell.b9ad34:spi	.6.0.0
Automatically restore this conn	ection when the computer starts
🔲 Enable multi-path	
Only select this option if iSCSI on your computer.	[multi-path software is already install

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 below.

eneral	IPsec	
Conne	ect by usin	g
Local	adapter:	Microsoft iSCSI Initiator
Source IP:		10.0.0.237
Targe	et portal:	10.10.10.50 / 3260
-	Checksur	84 X0
CRC /	Checksun	
Da	ata digest	Header digest
C	- HAP logon	information
CHAP initiat for th	HAP logon	information ure data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
CHAP initiat for th User	HAP logon helps ens or. To use is initiator.	information ure data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
CHAP Initiat for th User Targe	HAP logon helps ens or. To use is initiator. name: at secret: se RADIUS	information ure 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
CHAP initiat for th User Targe	HAP logon helps ens or. To use is initiator. name: at secret: se RADIUS	information ure data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target ign. 1991-05.com.microsoft:targuin-vista
CHAP initiat for th User Targe Use De To us	HAP logon P helps ens ror. To use is initiator. name: st secret: se RADIUS erform mut e mutual C	information ure 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 Devi	ices RADIUS
General	Discovery	Targets
og on.	es for a target, select th t sessions, connections,	
argets:		Status
iqn. 1988-11.com.dell.b	9ad34:spi.6.0.0	Connected
iqn. 1988-11.com.dell.b	9ad34:spi.6.0.1	Inactive

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.

	Devices	Properties	16		
Sessions	Devices	Properties	8		
Advance	re the dev ed to view h p <mark>o</mark> licy.	ices exposed information a	l by iSCSI sessio about the device	ons to the target. Click a and configure the	
Devices					
Device	Name			MPIO Capable	
IBM UL	TRIUM-H	13 SCSI Sequ	iential Device	LTO Tape drive	
				Advancer	d

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 polic					
Round Robin	,.			•	
	policy attempts to rocessing paths.	evenly dist	ribute incor	ning	
This session has th Source Portal	e following connec Target Portal	ctions : Status	Туре	Weight	(
10.0.0.237/5	10.10.10.50/	Conne	Active	n/a	(
4					Þ
				Edit	- 20

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. b9ad:	4:spi.6.0.0	
Advanced	ОК	Cancel

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

eneral	IPsec	
Conne	ect by usin	g
Local	adapter:	Microsoft iSCSI Initiator 👻
Sourc	e IP:	10.10.11.56
Targe	et portal:	10.10.11.50 / 3260 💌
CRC /	Checksum	1
🕅 Da	ata digest	Header digest
		information ure data security by providing authentication between a target and an
initiat for th	or. To use is initiator.	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	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 User i	or. To use is initiator.	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 User i Targe	or. To use is initiator. name: et secret: se RADIUS	ure data security by providing authentication between a target and an 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
initiat for th User r Targe Us Pe To us	or. To use is initiator. name: et secret: se RADIUS erform mut e mutual C	ure 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
initiat for th User i Targe Us De To us RADII	or. To use is initiator. name: et secret: se RADIUS erform mut e mutual C US. The s	ure data security by providing authentication between a target and an 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

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.

twork Connections - Windows Internet Explorer	• 4 × Live Search
V Network Connections	T N = M + D Page + ○ Tools
ridge Control	
Global Network Configuration	
eboot System Hostname: bridgeworks	
ogout Gateway: 10.10.10.1	
upport DNS Server: 10.10.10.1	
Indine Help	
ontact Support Use DHCP:	
Frame Size: 1500 •	
pyright 2008 DELL Inc. IP Address: 10.10.10.50	
Netmask: 255 255 0	
Broadcast: 10.10.10.255	
- Link Status	
Link State: up Link Speed: 100 Mb/s	
RX Bytes: 2953962 TX Bytes: 3294304 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: 10.10.10.255	
Link Status Link Status Emerget 1000 Mb/s	
Link State: up Speed: 1000 Mb/s RX Bytes: 191039 TX Bytes: 107780	
RX Errors: 0 TX Errors: 0	

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 policy	v:				
Round Robin				•	
	policy attempts to rocessing paths.	evenly dist	ribute incor	ning	
This session has th	e following connec	10002028 10002028	÷	Weight	(
Source Portal	Target Portal	Status	IVDe		
	Target Portal 10.10.10.50/ 10.10.11.50/		Type Active Active	n/a n/a	(
10.0.0.237/6	10.10.10.50/	Conne	Active	n/a	

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.

essions	Devices	Properties		
This targ	et has the	e following sess	iions:	
Identif	ier	S and		
🔲 ffff	ffff8741d	31c-400001370	80000008	
			Log off	Refresh
Sessio	n Properti	2S		
Targe	t portal gro	oup:	1	
Status			Connect	ted
Conne	ction cour	it:	2	
Sessio	n Connect	ions		
022		w the connection 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.

argets	Discovery	Favorite Targets	Volumes and Devices	RADIUS	Configuration
Configur he initia		gs here are global a	nd will affect any futur	e connectio	ons made with
		tions may continue se tries to reconnec	to work, but can fail if t t to a target.	he system	restarts or
	onnecting to ir connection		d connection features a	llow specifi	ic control of a
Initiator	Name:				
ign.199	91-05.com.n	nicrosoft:win-d3081	sidkbe		
Fo modif	y the initiat	or name, click Chan	ge.		Change
Fo set ti :lick CH#		HAP secret for use	with mutual CHAP,		CHAP
Fo set u :lick IPse		tunnel mode addres	sses for the initiator,		IPsec
	rate a repor em, click Re		argets and devices on		Report
More ab	out Configu	ration			

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				

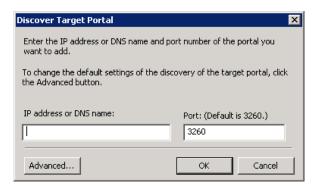
Enter in the initiator secret and click OK. The secret should be between 12 and 16 characters. Make a note of this secret, as you will need to enter this as part of configuring CHAP on the iSCSI Bridge.

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

	look for Targets on f	ollowing portals:	Refresh
Address	Port	Adapter	IP address
o add a target	portal, click Discove	r Portal.	Discover Portal
'o remove a ta hen click Remo		e address above and	Remove
NS servers			
'he system is r Name	egistered on the follo	wing iSNS servers:	Refresh
vame			
			Add Server
'o add an iSNS	server, click Add Ser	ver.	
o remove an is	5NS server, select th		Remove
	5NS server, select th		Remove
o remove an is	5NS server, select th		Remove

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
5	
CHAP Log on inform	nation
CHAP Log on inform	
CHAP Log on inform CHAP helps ensure c an initiator.	nation onnection security by providing authentication between a target and
CHAP Log on inform CHAP helps ensure c 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
CHAP Log on inform HAP helps ensure c an initiator. To use, specify the s nitiator. The name w	nation onnection security by providing authentication between a target and
CHAP Log on inform HAP helps ensure c an initiator. To use, specify the s nitiator. The name w	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this
CHAP Log on inform HAP helps ensure c an initiator. To use, specify the s nitiator. The name v specified.	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this
CHAP helps ensure o an initiator. To use, specify the s	nation
CHAP Log on inform EHAP helps ensure c an initiator. To use, specify the s nitiator. The name v specified.	nation
CHAP Log on inform CHAP helps ensure c an initiator. To use, specify the s nitiator. The name v specified. Vame: Farget secret:	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 ign.1991-05.com.microsoft:win-d3081sidkbe
CHAP Log on inform EHAP helps ensure c 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 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 uthentication
CHAP Log on inform EHAP helps ensure c 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 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
CHAP Log on inform CHAP helps ensure c an initiator. The name v specified. Name: larget secret: Perform mutual a To use mutual CHAP, ADULS.	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 ign.1991-05.com.microsoft:win-d3081sidkbe uthentication
CHAP Log on inform EHAP helps ensure c an initiator. To use, specify the s nitiator. The name v specified. Name: Target secret: Perform mutual ia To use mutual CHAP, ADJUS. Use RADJUS to g	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 ign.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 p want to add.	port number of the portal you
To change the default settings of the dis the Advanced button.	covery of the target portal, click
IP address or DNS name:	Port: (Default is 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.

	erties		
gets Discovery	Favorite Targ	ets Volumes and Devices	RADIUS Configuration
Target portals	. f T	6-11	Refresh
Address	Port	on following portals: Adapter	IP address
10.10.10.99	3260	Microsoft iSCSI Initia	
To add a target p	oortal, click Disc	over Portal.	Discover Portal
To remove a targ then click Remov		t the address above and	Remove
SNS servers			
The such as is used	at a factor of the state of the	Fellowie e iCNC commune	Refresh
	gistered on the I	following iSNS servers:	Refresh
The system is req Name	gistered on the I	following iSNS servers:	Refresh
	gistered on the I	following iSNS servers:	Refresh
	gistered on the I	following ISNS servers:	Refresh
Name	-		Refresh Add Server
Name To add an iSNS s	erver, click Add	Server.	Add Server
Name To add an iSNS s	erver, click Add		
Name To add an iSNS s To remove an iSN	erver, click Add	Server.	Add Server
Name To add an ISNS s To remove an ISN then click Remov	erver, click Add VS server, selec e.	Server.	Add Server
Name To add an iSNS s To remove an iSN	erver, click Add VS server, selec e.	Server.	Add Server
Name To add an ISNS s To remove an ISN then click Remov	erver, click Add VS server, selec e.	Server.	Add Server
Name To add an ISNS s To remove an ISN then click Remov	erver, click Add VS server, selec e.	Server.	Add Server

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 se	rver:	
	OK	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

I Initiator Properties	
rgets Discovery Favorite Targets Volumes and Devices F	ADIUS Configuration
Quick Connect	
To discover and log on to a target using a basic connection, type DNS name of the target and then click Quick Connect.	e the IP address or
arget:	Quick Connect
iscovered targets	
	Refresh
Name	Status
iqn.2002-12.com.4bridgeworks.000000:6d7a85844c2f1fa8	Reconnecting
iqn.2002-12.com.4bridgeworks.001c03:naa.50060b000057	Reconnecting
۹	Þ
	Connect
lick Connect.	Connect Disconnect
fo connect using advanced options, select a target and then lick Connect. fo completely disconnect a target, select the target and hen click Disconnect. for target properties, including configuration of sessions, select the target and click Properties.	
lick Connect. To completely disconnect a target, select the target and hen click Disconnect. For target properties, including configuration of sessions,	Disconnect
lick Connect. To completely disconnect a target, select the target and hen 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
lick Connect. To completely disconnect a target, select the target and hen click Disconnect. For target properties, including configuration of sessions, elect the target and click Properties. For configuration of devices associated with a target, select he target and then click Devices.	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:	
rn.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 Ca	incel

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	
Connect using	
.ocal adapter:	Default 🔽
nitiator IP:	Default
Farget portal IP:	Default
CRC / Checksum	
Data digest	F Header digest
m initiator. To use, specify the si	onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this
SHAP helps ensure co an initiator. To use, specify the si	onnection security by providing authentication between a target and
CHAP helps ensure co an initiator. Fo use, specify the si- nitiator. The name w 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
EHAP helps ensure co an initiator. To use, specify the s- nitiator. The name w specified. Name: Target secret: Perform mutual ar to 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-d3081sidibe
EHAP helps ensure co en initiator. To use, specify the so histor. The name w pecified. Name: (arget secret: Perform mutual and to use mutual CHAP, (ADIUS,	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-d3081sidibe
EHAP helps ensure co in initiator. To use, specify the s- nitiator. The name w pecified. Name: arget secret: Perform mutual and to use mutual CHAP, tADIUS.	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-d3081sidibe uthentication either specify an initiator secret on the Configuration page or use

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.

argets Discovery Favorite Targets Volumes and Devices RADIUS Configuration Quick Connect To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect. Quick Connect. Target: Quick Connect. Quick Connect. Discovered targets Refresh Name Status Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Inactive To connect using advanced options, select a target and then click Connect. Connect To connect using advanced options, select the target and then click Connect. Disconnect For target properties, including configuration of sessions, select the target and click Properties Properties For configuration of devices associated with a target, select Devices the target and then click Devices. Devices etarget and then click Devices. Devices for eabout basic ISCSI connections and targets Devices	5I Initiator Properties		
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect Target: Quick Connect Discovered targets Refresh Name Status Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected Ign.2002-12.com.4bridgeworks.000000:977d088e36978 Inactive To connect using advanced options, select a target and then click Osconnect. Connect For target properties, including configuration of sessions, select the target and click Properties Properties For configuration of devices associated with a target, select Devices the raget and then click Devices. Devices	argets Discovery Favorite Targets Volumes and Devices	RADIUS Configuratio	n į
DNS name of the target and then click Quick Connect. Target: Quick Connect Discovered targets Refresh Name Status Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Tartive To connect using advanced options, select a target and then click Connect. To completely disconnect. For target properties, including configuration of sessions, select the target and click Properties For configuration of devices associated with a target, select the target and then click Devices. there about basic ISCSI connections and targets	Quick Connect	· ·	
Discovered targets Refresh Name Status kgn.2002-12.com.4bridgeworks.000000:977d098636978 Connected ign.2002-12.com.4bridgeworks.000000:977d098636978 Inactive To connect using advanced options, select a target and then cick Connect To completely disconnect. To completely disconnect. For target properties, including configuration of sessions, select the target and cick Properties For configuration of devices associated with a target, select the target and then cick Devices. To reabout basic ISCSI connections and targets	To discover and log on to a target using a basic connection, to DNS name of the target and then click Quick Connect.	type the IP address or	
Name Status Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Inactive To connect using advanced options, select a target and then click Connect Connect To completely disconnect a target, select the target and then click Disconnect Disconnect For target properties, including configuration of sessions, select the target and click Properties Properties For configuration of devices associated with a target, select Devices ther adout basic ISCSI connections and targets Devices	Target:	Quick Connect	,
Name Status Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected ign.2002-12.com.4bridgeworks.000000:977d0a8e36978 Inactive To connect using advanced options, select a target and then click Connect. Connect To completely disconnect. Disconnect For target properties, including configuration of sessions, select the target and then click Properties. Properties For configuration of devices associated with a target, select the target and then click Devices. Devices Hore about basic ISCSI connections and targets Properties	Discovered targets		
Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Connected Ign.2002-12.com.4bridgeworks.000000:977d098e36978 Inactive To connect using advanced options, select a target and then click Connect. Connect To completely disconnect. Disconnect For target properties, including configuration of sessions, select the target and click Properties Properties For configuration of devices associated with a target, select the target and then click Devices. Devices More about basic ISCSI connections and targets Properties		Refresh	
Ign.2002-12.com.4bridgeworks.000000:977d0a8e36978 Inactive To connect using advanced options, select a target and then Connect To completely disconnect. 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 the target and then click Devices. Hore about basic ISCSI connections and targets	Name	Status	
To connect using advanced options, select a target and then Connect click Connect. Connect a target, select the target and Disconnect then click Disconnect. Disconnect For target properties, including configuration of sessions, Select the target and click Properties For configuration of devices associated with a target, select the target and then click Devices. Devices	iqn.2002-12.com.4bridgeworks.000000:977d098e36978	Connected	_
click Connect.	ign.2002-12.com.4bridgeworks.0000001977d0a8e36978	Inactive	
click Connect.			
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 the target and then click Devices. Nore about basic ISCSI connections and targets		Connect	
Select the target and click Properties. For configuration of devices associated with a target, select Devices More about basic ISCSI connections and targets		Disconnect	
the target and then click Devices.		Properties	
		Devices	
OK Cancel Coroliz	tore about basic iSCSI connections and targets		
OK Cancel Inclu			
	ок	Cancel Ap	nlw

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.

operties			
Sessions Portal Groups			
		R	efresh
Identifier			
ffffa8001770018-40000137000	00008		
, To add a session, click Add session.		Add	session
To disconnect one or more sessions, s session and then click Disconnect.	elect each	Dis	connect
To view devices associated with a sess a session and then click Devices.	sion, select	De	vices
Session Information			
Target portal group tag:	1		
Status:	Connecte	ed	
Connection count:	1		
Maximum Allowed Connections:	10		
Authentication:	None Spe	ecified	
Header Digest:	None Spe	ecified	
Data Digest:	None Spe	ecified	
Configure Multiple Connected Sessio To add additional connections to a s configure the MCS policy for a select click MCS. More Information on ISCSI Sessions	ession or	M	ICS
		ок	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			2	×
Name	Address			
Disk -1	Port 2: Bus 0: Targ	get 0: LUN 0		
Volume path	names:			
Legacy devic	e name:			
Device interf				
	4		F	
-	Iltipath IO (MPIO) —		 	1
	the MPIO policy for rice, click MPIO.	ra	MPIO	
Information C	n iSCSI Device Deta	ails		
		_		
			ок	

Potomac ESAS2800 Page 59

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 The round robin p processing paths.	olicy attempts to even	ly distribute in	icoming reque	sts to all	
his session has the	following connections	:			
				LUL-L-L-L-L	
Source Portal 0.0.0.0/61894	Target Portal	Status Connected	Type Active	Weight n/a	
	-				
	-				
	10.10.10.107/3				
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'.

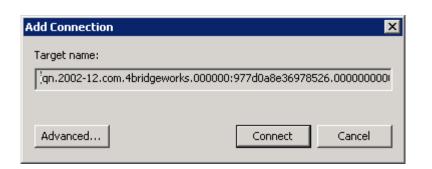
Round Robin will utilize all connections for data and evenly distribute the data.

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
nitiator IP:	Default
larget portal IP:	Default
CRC / Checksum Data digest	Header digest
Data uigest	i neauer uigest
CHAP Log on inform CHAP helps ensure c an initiator.	nation onnection security by providing authentication between a target and ame name and CHAP secret that was configured on the target for this
CHAP helps ensure c an initiator. Fo use, specify the s	nation onnection security by providing authentication between a target and
CHAP Log on inform CHAP helps ensure c an initiator. To use, specify the s nitiator. The name w specified.	nation
CHAP Log on inform CHAP helps ensure c 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 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-d3081sidibe
CHAP Log on inform CHAP helps ensure c an initiator. The new system nitiator. The name w peofied. Vame: larget secret: Perform mutual al to use mutual CHAP, XADIUS.	hation 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 Uthentication

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.

CS policy:					
lound Robin					•
Description The round robin p processing paths.	olicy attempts to ever	Iy distribute in	coming reque	ists to all	
his session has the	following connections	:			
Source Portal	Target Portal	Status	Туре	Weight	
0.0.0.0/60102	10.10.10.107/3	Connected	Active	n/a	1
0.0.0.0/63942	10.10.10.107/3	Connected	Active	n/a	
•					▶
To add a connectio	n, click Add.			Add	
To remove a connection, select the connection above and then					
	ction, select the conne	ection above a	ina then	Remove	
lick Remove.	ttings for the MCS poli			Edit	

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			
1		Refresh	
Identifier	0007		
	0007		
To add a session, click Add session.	To add a session, click Add session.		
To disconnect one or more sessions, sel session and then click Disconnect.	Disconnect		
To view devices associated with a sessi a session and then click Devices.	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 Specif	ied	
Configure Multiple Connected Session	(MCS)		
To add additional connections to a ses configure the MCS policy for a selecte click MCS.		MCS	
More Information on iSCSI Sessions			
	0	K 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.

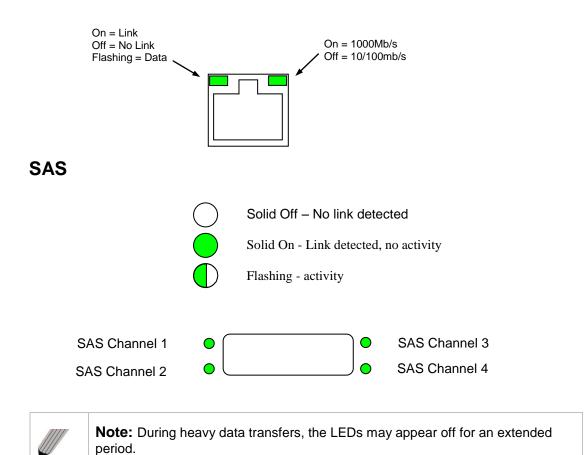
- Open the Microsoft iSCSI Initiator and click on the Targets tab.
- Click on the iSCSI session that the user wishes to log off.
- Click the 'Disconnect' button. This will log off all connections associated with the iSCSI Session.

•

The iSCSI device should now show as inactive.

Appendix C Visual Indicators

Ethernet



iSCSI to SAS

Appendix D 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)		
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		
SAS Interface			
Physical	2x SFF – 8088 External mini-SAS		
Speed	1.5Gb/s and 3Gb/s		
Protocol	SAS 2.0		
Visual Indicators	Link, Activity		