

# Potomac ES1100DT Desktop iSCSI to SCSI Bridge User Manual V3.5

**Bridgeworks** 

135 Somerford Road, Christchurch, Dorset BH23 3PY Tel: +44 (0) 1202 588 588 Fax: +44 (0) 1202 588 589 Email: support@4bridgeworks.com

## **Manual Revision History**

Revision	Date	Firmware	
3.2	August 2011	V3_02	MS
3.3	April 2012	V3_02	AP
3.4	May 2013	V3_04	AP
3.5	October 2013	V3_04	AP

# Warning

The Bridgeworks Potomac ES1100DT iSCSI to SCSI Bridge contains no user-serviceable components. An Authorized Service Centre should only 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.

#### SCSI Cable

The greatest source of SCSI related faults is poor quality SCSI cabling. This is especially true when running at the higher speeds possible with this Bridge. We therefore recommend that you purchase a good quality SCSI 3 compatible cable with High Density 68 way D type connector for your installation.

You will also need to complete your SCSI bus installation with a SCSI Terminator. This is connected to the last peripheral on the SCSI bus. Again we recommend you use a good quality LVD / SE Terminator.

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

# **Table of Contents**

1.0 Introduction	6
1.1 Overview	6
1.2 Manual Layout	7
1.3 Definitions	7
1.4 Safety Notices	8
2.0 Installing the ES1100DT Bridge	9
2.1 Ethernet Connection	9
2.2 SCSI Bus Connections	10
2.3 Connecting the Power Supply	11
3.0 Configuring the ES1100DT Bridge	12
3.1 Using the Web Interface	12
3.1.1 Browsers	12
3.1.2 Connecting to the Web Interface	12
3.2 Configuring the Network Parameters	15
3.2.1 Setting the Hostname	15
3.2.2 Enabling IPv6	15
3.2.3 Setting the MTU	16
3.2.4 Setting the IP Address	16
3.2.5 Setting the Subnet Mask	16
3.2.6 Setting the Gateway Address	16
3.2.7 Setting an IPv6 IP Address	17
3.2.8 Committing the changes	17
3.2.0 Reconnect to the Bridge	17
3.3 Passwords and Security	18
3.4 Network Services	10
3.4 NELWOIK DELVICES	10
3.4.1 INTE	10
2.4.2 EIIIdii Aleris	20
2.5 iSCSI Target Interface	20
	21
3.0 ISUSI SESSIONS	22
3.7 SUSI Initiator	23
3.8 Device Manager	20
4.0 Information	20
4.1 System Information	20
4.2 System Log	27
5.0 Maintenance	28
5.1 Firmware Updates	28
5.2 Saving the Configuration to Disk	29
5.3 Restoring a Saved Configuration	30
5.4 Restoring Factory Defaults	30
6.0 I roubleshooting	31
6.1 Lost Password	31
6.2 Network problems	32
6.3 Device related problems	33
6.4 Poor Performance	34
6.5 Lost IP Address	35
Appendix A Setting up your Computer for Initial Setup	36
A1 Windows 95, 98 or NT	36
A2 Windows 2000, 2003, XP	37
A3 Windows Vista / Server 2008 or Vista or 7	39
Appendix B Microsoft iSCSI Initiator	41
B1 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows	3
Vista Server 2008 R1 or Server 2003	41
B2 Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows	3

Server 2008 R2	. 53
Appendix C Visual Indicators	. 65
Appendix D Technical Specifications	. 66

# **1.0 Introduction**

Thank you for purchasing the Bridgeworks iSCSI to SCSI 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 that will guide you through setting up both the Network and SCSI 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 SCSI 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 CDs understand on the SCSI bus.



The Bridgeworks Desktop iSCSI Bridge

## 1.2 Manual Layout

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

This icon represents an important piece of information.



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

## 1.3 Definitions

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 ES1100DT Bridge

There are 3 basic steps to installing the iSCSI Bridge

- Connecting the Ethernet cable
- Connecting the SCSI cables
- Connecting the Power Supply

## 2.1 Ethernet Connection

The Bridge can be used on the following network configurations:

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

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

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

To connect the Bridge to the Ethernet network, insert a Cat 5E cable directly into the connector on the unit as shown below. When the plug is in the correct position a "click" should be heard.



## 2.2 SCSI Bus Connections

The SCSI bus on the Bridge is capable of running at speeds of up to 160 Mbytes/s. However, devices that operate at slower speeds can still be connected to this SCSI 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.

When adding your SCSI Servers to the SCSI bus it is important to remember that every device on the SCSI bus must have a unique SCSI ID and it is normal for SCSI ID 7 to be reserved for the Server.

The Bridge can support both single-ended and LVD Servers. However, it should be noted that the two bus types have different data transfer speeds and cable length limitations:

- Single-ended termination and/or devices 2 metres length (40 MB/s maximum)
- LVD termination and/or devices 6 metres length variable speeds up to a maximum of 160 MB/s.

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

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



Connecting the SCSI Cable to the Bridge SCSI Port



**Note:** The two securing screws on either side of the connector should ONLY BE FINGER TIGHT.

## 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.

Whenever the Bridge is powered on the green power 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 ES1100DT Bridge

Before the Bridge can be used 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 20
- Mozilla Firefox 21



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



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

## 3.1.2 Connecting to the Web Interface

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

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

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



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

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



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

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





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

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

## 3.2 Configuring the Network Parameters

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

1 Alexandre			
Bridge Control	Network Connections		
Console Home Network Ping Reboot System Logout	Global Network Configuration Hostname: bridgeworks120 DNS Server: 10.10.10.1 Enable IPv6:	Cancel Save	
Support			
Online Help Contact Support	Network Interfaces Network I Connected, 1000Mb/s 0:04:1b:00:1f.c0		

## 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.

	1500 ~			
	1500 ~			
	And the second s			
Use DHCP to J	assign an IP a	ddress automatica	illy	
<ul> <li>Use the follow</li> </ul>	ring IP addres			
IP Address:	10 10 10 12	10		
	255 255 257			
	200.200.200	5.0		
RX Bytes:		TX Bytes:		
RX Errors:		TX Errors:		
IPv6 Address				
IPv6 Address				
	Use DHCP to     See DHCP to     Use DHCP to     See DHCP to     Point and the set of the follow     IPv6 address:     Default gateway:     Link Status     Link State:     RX Bytes:     DX Ferrors	Use DHCP to assign an IP at Use the following IP address IP Address: 10.10.102 Netmask: 255.255.255 Gateway:	Use DHCP to assign an IP address automatice     Use the following IP address:     IP Address:     IP Address:     S25,255,255,0 Gateway:     Gateway:     Use automatic IPv6 address assignment     Use the following IPv6 address:     IPv6 address:     IPv6 address:     Int Status     Link Status     Link State:     Up Link Speed:     RX Bytes:     101577 TX Bytes:     0 TX Errors	Use DHCP to assign an IP address automatically     So the following IP address:     IP Address:     IP Address:     Z55.255.0 Gateway:     Gateway:     Gateway:     Int Status Link Status Link State:     Up Link Speed: 1000Mb/s SX Bytes: 596400 DX Errors: 0 D

## 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 \ '	Dacewords & Poswith
Node Control	Passwurus & security
Console Home	System Possword
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: Seve

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

	- The		_
1	Bridgeworks		
		Service Control	
	Node Control		
	Console Home		
	Reboot System	Use NTP:	
	Logout	NTP Server:	
		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 Interface

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

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

#### CHAP

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

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

#### **Multipath Settings**

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

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

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



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

## 3.6 iSCSI Sessions

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

/ Bridgeworks \ *	
Bridge Control	
<u>Console Home</u>	
Reboot System Initiator Target	
Logout	
Support	
Online Help	
Contact support	
© 2010 Bridgeworks Ltd	

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 SCSI Initiator

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

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

The GUI will now display the following window

Bridgeworks	
	SCSI Initiator
Bridge Control	
Console Home	
Reboot System	The following configuration options will be applied to every port configured in initiating mode.
Logout	
Support	modification to any parameters should be needed, they are provided for the configuration of legacy devices.
Online Help Contact Support	Host ID: 7 Settle Delay: 3
© 2010 Bridgeworks Ltd	Commands 64 per LUN: Disable Wide Transfers: Disable Synchronous Transfers: Save

The settings in the SCSI Initiator page are advanced settings provided for configuration of legacy devices. Typically, no modification to any of these parameters should be required.

#### Host ID

This defines the ID of the Bridge on the SCSI bus and should not require modification unless using the unit with a shared SCSI bus.

#### Settle Delay

When devices are first turned or, when a SCSI bus reset is issued most devices will perform a set of tasks to reinitialise settings and reconfigure certain parameters which can take a little time to perform before the device will respond to commands on the SCSI bus. The settling time is the length of time given to allow devices to reset before issuing commands. Some older devices may take longer than the default 3 seconds which may cause them to be missed when the Bridge rescans the SCSI bus. Increase this parameter in small steps only.

#### **Advanced Options**

The following settings should only be changed if instructed by your support channel:

- Maximum Commands per LUN This is the maximum of commands that the Bridge will allow any one device to accept at any one time Default 64
- Disable Wide Transfers This forces the SCSI bus to work in Narrow Mode (8 bit) only. Default off.
- Disable Synchronous Transfers, This forces the SCSI bus to transfer in Asynchronous Mode only. Default off.

Selecting either of the last two options will have a detrimental affect on the performance of the Bridge.

## 3.8 Device Manager

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

N N		
/ Bridgeworks \	nuico Managomont	
Bridge Control	evice Management	
Console Home		
Reboot System	Target WWN         eui.00041b0000108000           Target Alias         01:00	
Logout	Logical Units Attached: 1	
	Refresh Clear Configuration Update Configuration	
Support		
Online Help		
© 0010 Drideswards Ltd		
© 2010 Bridgeworks Ltd		

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

Bridgeworks											
	Device M	anagem	nent								
Bridge Control	_										
Console Home		vice Info									
Reboot System	T 🗸	Target WWN		/N eui.0004		04160000108000					
<u>noboot oystom</u>	Т	arget Alia	et Alias		01:00		_				
Logout		Logical Units Attached:						-			
			) Pres	ent	enable	d	Persistent	-			
Support		De	vice		HP - Ultriu	m 2-SCS	I Rev (T61D)	-			
Support		De	evice Type		Sequentia	l-access o	device Device				
Online Help		sc	SI Revision		SPC-3						
Contact Support		Me	edia Type		Removabl	e Media	5350	-			
		De	vice SCSI ID		0:1:0:0	56000037	2/30	-			
© 2010 Bridgeworks Ltd		En	able / Disable De	vice	Enabled	-		-			
© coro briagonomo cia						_		-			
	Ref	resh	Clear Co	nfiguratio	n	Upda	ate Configuration				

The expanded information also gives you a device control option

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

# 4.0 Information

## 4.1 System Information

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

The GUI will now display the following window

Pridacuarko	
/ bildgeworks \	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: iqn.2002-12.com.4bridgeworks.001c0b
Support	System Performance
Online Help Contact Support	Data throughput
	0MB/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
- 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.

A Bridgeworks	
/ bildgeworks \	Update Firmware
Bridge Control	
Console Home	
Reboot System	
Logout	Firmware image:
	Browse.
Support	Update
Online Help Contact Support	
© 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

/ DUGGROWIEN 1	
Load/Save Configuration	
Bridge Control   Console Home   Beboot System   Logout     Support   Online Help   Contact Support   Contact Support   Online Help   Contact Support   Contact Support   Citck Here to Download   Restore Defaults   Restore 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 Troubleshooting

## 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.
- SCSI cables can be prone to having bent pins, particularly when using HD68 connectors. Check both ends to make sure no pins are bent. If you are in any doubt, replace the cable with a new one.
- Make sure all SCSI devices are either LVD or single-ended in order to be compatible with this Bridge. For optimal speed do not mix LVD and single-ended devices on the same bus.
- Ensure both ends of each SCSI bus are terminated. Bridgeworks have included an internal terminator within the Bridge.
- 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\syst	tem32\cmd.exe	_ 🗆 🗡
Product : SF	C4200 SCSI-FC Bridge	
Port Ø		
> IP Address		
> Mac	: 00:04:15:00:80:0c	
> Netmask	= 255.255.255.0	
> Broadcast	= 10,10,10,255	
> Gateway	- 4500.0	
> MIU Dant 1	= 1500	
FOPT I	- 10 10 10 21	
> Ir Huuress	- 10.10.10.31	
> Netmask	- 255 255 255 G	
> Broadcast	10.10.10.255	
> Gateway	. 0.0.0.0	
> MTU	: 1500	
+=-=- Response	-=-=-=-=+=-=-=-=-=-=-=-=-=+ <b>+</b>	
Hostname 🕺 : br	idgeworks	
Product : FS	1200 FC-SCSI Bridge	
Port 0		
> IP Address	= <u>10.0.0.241</u>	
> Mac	: 00:c0:9f:2a:bf:5e	
> Netmask	: 255.255.255.0	
> Broadcast	: 10-0-255	
> Gateway	- 4500.0	
> MIU	- 1500	
<b>T</b>		
U:\documents>_		-

# Appendix A Setting up your Computer for Initial Setup

## A1 Windows 95, 98 or NT

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

From the Start menu, choose Settings then Control Panel.

#### Then click the Network icon

Network	?>
Configuration   Identification   Access Control	
The following network components are installed:	
Client for Microsoft Networks     B3Com Fast EtherLink XL 10/100Mb TX Ethernet NIC     Dial-Up Adapter     Tot/P > 3Com Fast EtherLink XL 10/100Mb TX EtherNet Nick 2000 Not Not Network	(3C9 heme
TCP/IP -> Dial-Up Adapter	•
Add Remove Proper	rties
Client for Microsoft Networks	•
<u>File</u> and Print Sharing	
Description TCP/IP is the protocol you use to connect to the Intern wide-area networks.	et and
OK	Cancel

In the Network window's Configuration tab,

Select the TCP/IP entry

Then the Properties Button

Bindings	Adv	anced	N	etBIOS
ONS Configuration	Gateway	WINS Co	nfiguration	IP Address
An IP address can If your network doa your network admi the space below.	be automal es not autor nistrator for	ically assign natically ass an address,	ned to this c ign IP addro and then ty	omputer. esses, ask vpe it in
C <u>O</u> btain an IP	address au	omatically		
_	address:-			
IP Address:	10	. 10 . 1	0.11	
S <u>u</u> bnet Mas	k: 255	. 255 . 25	5.0	

Click on the IP Address tab

Make a Note of your current set up then:

Click on the Specify an IP address button

Enter 10.10.10.11 into the IP Address field

Enter 255.255.255.0 into the Subnet Mask field

Finally click the OK button and reboot your computer.



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

## A2 Windows 2000, 2003, XP

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

From the Desktop or Start menu, select My Computer



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

🛍 Network and Dial-up Connectio	ns	_ 🗆 ×
] File Edit View Favorites To	ols Advanced Help	
] ⇔Back + ⇒ - 🔂   @ Search	- 🔁 Folders 🎯 History 🛛 🚰 😤 🗙 🔊	-
Address 📴 Network and Dial-up Con	nections	<b>▼</b> 🖓 60
Network and Dial- up Connections	Name / Im Make New Connection ↓ 10 100 Ethernet Gigabit Ethernet	LAN LAN LAN
This folder contains network connections for this computer, and a wizard to help you create a new connection.		
Make New Connection. To open a connection, click its icon. To access settings and components of a connection, violat-click its icon	-[4]]	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.

Connection Status: Connecte Duration: 00.251 Speed: 1.0 Gbp Activity Sent P1 Receive
Status: Connecte Duration: 00:25:1 Speed: 1.0 Gbp Activity Sent P1 Receive
Duration: 00.25:1 Speed: 1.0 Gbp Activity Sent P1 Receive
Speed: 1.0 Gbp Activity Sent — 🗐 — Receive
Activity
Packets: 58,720   86,28
Properties Disable

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

	т слуарка Асарка	
'emperante checked a	ra usad bu this comm	Configure
	11	Disperities (
Install	Uninstall	Flopenies
Install	Uninstall	Flopenes
Install Description Allows your computer network.	to access resources	on a Microsoft

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

fou can get IP settings assigned automatically if your network supports in capability. Otherwise, you need to ask your network administrator for ne appropriate IP settings. O Dbtain an IP address automatically			
IP address:	10 . 10 . 10 . 11		
Subnet mask:	255 . 255 . 255 . 0		
Default gateway:			
C Obtain DNS server address	s automaticallu		
Use the following DNS service	ver addresses:		
Preferred DNS server:	<u> </u>		
Alternate DNS server:			

Make a Note of your current set up then:

Click Use the following IP Address

Enter 10.10.10.11 into the IP Address field

Enter 255.255.255.0 into the Subnet Mask field

Finally click the OK button.



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

## A3 Windows Vista / Server 2008 or Vista or 7

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

From the Start menu, select Control Panel



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

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



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

Connect using:		
Realtek RTL81	168D/8111D Family PCI	-E Gigabit Ethernet
		Configure
This connection uses	the following items:	
Client for Mic	crosoft Networks	
🗹 📕 QoS Packet	Scheduler	
File and Print	tor Sharing for Microsoft	Natworke
	ter shaning for Microsoft	Trocivoina
Internet Prot	ocol Version 6 (TCP/IP)	v6)
<ul> <li>Internet Prot</li> <li>Internet Prot</li> </ul>	cocol Version 6 (TCP/IP) cocol Version 4 (TCP/IP)	76) 74)
Internet Prot     Internet Prot     Internet Prot     Link-Layer T	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map	v6) v4) per I/O Driver
<ul> <li>✓ Internet Prot</li> <li>✓ Internet Prot</li> <li>✓ Link-Layer T</li> <li>✓ Link-Layer T</li> </ul>	ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map opology Discovery Resp	v6) v4) per I/O Driver ponder
<ul> <li>✓ Internet Prot</li> <li>✓ Internet Prot</li> <li>✓ △ Internet Prot</li> <li>✓ △ Link-Layer T</li> <li>✓ △ Link-Layer T</li> </ul>	icocol Version 6 (TCP/IPv ocol Version 4 (TCP/IPv ocol Version 4 (TCP/IPv fopology Discovery Map fopology Discovery Resp	r6) (4) per I/O Driver ponder
✓     Internet Prote       ✓     Internet Prote	ocol Version 6 (TCP/IP) ocol Version 6 (TCP/IP) ocol Version 4 (TCP/IP) opology Discovery Map opology Discovery Resp Uninstall	r6) (4) per I/O Driver ponder Properties
A Internet Prot     A Internet Prot     A Internet Prot     A Internet Prot     A Int-Layer T     A Ink-Layer T     A Ink-Layer T     A Ink-Layer T     A Ink-Layer T	Cool Version 6 (TCP/IP) cool Version 6 (TCP/IP) cool Version 4 (TCP/IP) coology Discovery Map copology Discovery Resp Uninstall	r6) (4) per I/O Driver ponder Properties
✓ ▲ Internet Prot     ✓ ▲ Internet Prot     ✓ ▲ Internet Prot     ✓ ▲ Link-Layer T     ✓ ▲ Link-Layer T     ✓ ▲ Link-Layer T     ✓ ■ Link-Layer T     ✓ ■ Link-Layer T	col Version 6 (TCP/IP) cocl Version 6 (TCP/IP) cocl Version 4 (TCP/IP) copology Discovery Map copology Discovery Resp Uninstall	AG (A)
✓ ▲ Internet Prot     ✓ ▲ Internet Prot     ✓ ▲ Internet Prot     ✓ ▲ Link-Layer T     ✓ ▲ Link-Layer T     ✓ ▲ Link-Layer T     ✓ ■ Link-Layer T     ✓ ■ Link-Layer T     ✓ ■ Link-Layer T	Cool Version 6 (TCP/IP) cool Version 4 (TCP/IP) cool gy Discovery Map copology Discovery Res Uninstall rol Protocol/Internet Prot protocol that provides c	All of the second secon
✓ ▲ Internet Prot     ✓ ▲ Internet Prot     ✓ ▲ Internet Prot     ✓ ↓ Link-Layer T     ✓ ↓ Link-Layer T	Cool Version 1 (TCP/IP) cool Version 4 (TCP/IP) cool version 4 (TCP/IP) coology Discovery Map coology Discovery Resp Uninstall rol Protocol/Internet Proj protocol that provides c reconnected networks.	Alpha A

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

eneral			
You can get IP settings assignt this capability. Otherwise, you for the appropriate IP settings	ed automatically if your network supports need to ask your network administrator		
💮 Obtain an IP address aut	omatically		
() Use the following IP addr	ess:		
IP address:	10 . 10 . 10 . 11		
Subnet mask:	255.255.255.0		
Default gateway:	10 . 10 . 10 . 1		
Obtain DNS server addres	is automatically		
O Use the following DNS ser	ver addresses:		
Preferred DNS server:	41.74		
Alternate DNS server:	1. (1.) A		
Validate settings upon ex	Advanced		

Make a Note of your current set up then: Click Use the following IP Address Enter 10.10.10.11 into the IP Address field Enter 255.255.255.0 into the Subnet Mask field Finally click the OK button.

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

# Appendix B Microsoft iSCSI Initiator

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

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

#### Step 1 – General Set up

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

	Volumes and Devices	RADIUS
General	Discovery	Targets
SCSI devices are disk, t nother computer on yc	apes, CDs, and other storage ( our network that you can conne	devices on ect to.
'our computer is called he iSCSI device, which	an initiator because it initiates t is called a target.	he connection to
nitiator Name	iqn.1991-05.com.microsoft:t	arquin-vista
o rename the initiator,	dick Change.	Change
o use mutual CHAP aut argets, set up a CHAP	hentication 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

Type a CHAP secret to be used to aut secure CHAP secrets are not words ar of characters. Enter this same CHAP s initiator can connect.	thenticate (verify) targets. The most nd phrases, but a random sequence secret on the target so that the
HAP secret:	
HAP 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 Targ	ets	Volumes and Device	s RADIU
General		Discovery	Targets
arget portals			
Address	Port	Adapter	IP address
Add Porta	al	Remove	Refresh
NS servers			
Add		Remove	Refresh
9		102	

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	ne and port number of e discovery session t	of the portal you wan o the portal, click
Advanced.		
IP address or DNS name:	Port:	
1	2260	

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
LUCAI	auapter.	
Sourc	e IP:	Default
Targe	et portal:	
CRC	/ Checksum	
Da	ata digest	Header digest
Ch	HAP logon	information
CHAP initiat for th	helps ens or, To use iis 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
CHAP initiat for th	helps ens or. To use iis initiator, name:	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	) helps ens or. To use iis initiator. name: at secret:	ire 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	<sup>o</sup> helps ens or. To use iis initiator, name: et secret: se RADIUS	ire 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	Phelps ens or. To use is initiator. name: et secret: se RADIUS erform mut	In the security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target iqn. 1991-05.com.microsoft:tarquin-vista to generate user authentication credentials ual authentication
CHAP initiat for th User Targe User Targe De Radi	P helps ens or. To use is initiator, name: et secret: se RADIUS erform mut se mutual C US. The si	In the specify an initiator secret on the Initiator Settings page or use are secret must be configured on the target.
CHAP initiat for th User Targe Use To us RADI	Phelps ens or, To use is initiator, name: et secret: se RADIUS erform mut e mutual C US, The s se RADIUS	Indiadan 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 ame secret must be configured on the target. to authenticate target credentials

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 nam to add. To select settings for the Advanced.	e and port number o discovery session t	of the portal you wan to the portal, click
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.

ravonice rarger	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
Name			
		Remove	Refresh
Add			

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		Đ
IP address or DNS name of ser	ver:	
[		
	ОК	Cancel

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

## Step 3 – Targets

Click on the Targets tab.

The devices discovered should now be listed and shown as below

Favorite Targets	Volumes and Devices	RADIUS
General	Discovery	Targets
o access storage device og on. o see information about lick Details.	s for a target, select the t sessions, connections, an	arget and then click d devices for a targe
argets: Name ign, 1988-11.com.dell.b	9ad34:spi.6.0.0	Status Inactive
iqn. 1988-11.com.dell.b	9ad34:spi.6.0.1	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 connection when the computer starts         Enable multi-path         Only select this option if iSCSI multi-path software is already instal         Only select this option if iscond the software is already instal	Target name:	
Automatically restore this connection when the computer starts     Enable multi-path     Only select this option if iSCSI multi-path software is already instal     on processory computer	ign.1988-11.com.dell.b9ad34:	spi.6.0.0
Enable multi-path  Only select this option if iSCSI multi-path software is already instal  on your computer.	Automatically restore this co	onnection when the computer starts
Only select this option if iSCSI multi-path software is already instal	Enable multi-path	
on you compate.	Only select this option if iS on your computer.	CSI multi-path software is already installe

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.

neral	IPsec	
Conn	ect by usin	g
Local	adapter:	Microsoft iSCSI Initiator
Source	te IP:	10.0.0.237 👻
Target portal: 10.1		10.10.10.50 / 3260
CRC	/ Checksun	
CHAP	HAP logon helps ens	Header digest 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
CHAF initiat for th	HAP logon helps ens or. To use nis initiator	Header digest 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
CHAF initial for th User Targe	ATA digest HAP logon P helps ens cor. To use his initiator name: et secret:	Header digest 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
CHAF initiat for th User Targe	HAP logon HAP logon P helps ens ror. To use nis initiator name: et secret: se RADIUS	Header digest  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
Di Di CHAFA CHAFA for th User Targe User Targe De RADI	HAP logon P helps ens cor. To use is initiator name: et secret: se RADIUS erform mut se mutual C US. The s	Header digest      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      iqn. 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 ame secret must be configured on the target.

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 Device	RADIUS
General	Discovery	Targets
To access storage device og on. To see information about lick Details.	s for a target, select the sessions, connections, ar	target and then click nd devices for a targe
argets: Name	Dad 24 rati 6 0 0	Status
ign. 1988-11. com. dell. b	Pad 34:spi. 6.0.1	Inactive
Details	Log on	Refresh

#### Step 4 – Viewing iSCSI Session Details

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

essions Devices Properti	es	
This target has the following	sessions:	
Identifier	a	
fffffff8741d31c-4000	1370000008	
ſ	1	D-Eh
	LOG OTT	Kerresh
Session Properties		
Target portal group:	1	
Status:	Connected	í.
Connection count:	1	
Session Connections		
To configure how the con this session are load balar	nections within need, <mark>d</mark> ick	Connections
Connections		

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

Sessions	Devices	Properties	
These a Advance multipat	re the dev ed to view h policy.	ices exposed by iSCSI se information about the de	essions to the target. Click evice and configure the
Devices	: Name		MPIO Capable
IBM UL	TRIUM-H	13 SCSI Sequential Devic	e LTO Tape drive
			Advanced

#### Step 5 – Creating multiple connections (Optional)

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

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

oad balance polic	y:				
Round Robin				•	
Description The round robin requests to all p	policy attempts to processing paths.	evenly dist	ribute incor	ming	
This session has th Source Portal	ne following connec	ctions : Status	Type	Weight	(
10.0.0.237/5	10.10.10.50/	Conne	Active	n/a	C
					Þ.
٠ [					

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

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

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

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

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

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

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

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

arget name:		
ign. 1988-11. com. dell. b9ad34	:spi.6.0.0	

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

eneral IPsec	
Connect by usin	9
Local adapter:	Microsoft iSCSI Initiator 👻
Source IP:	10.10.11.56
Target portal:	10.10.11.50 / 3260 👻
CPC / Checksum	
cree / cricersun	1201208 00 12
CHAP logon i CHAP helps ensu initiator. To use for this initiator.	Header digest  formation  ure data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target
Data digest CHAP logon i CHAP helps ensi initiator. To use for this initiator. User name:	Header digest  formation  are 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
Data digest CHAP logon i CHAP helps ensi initiator. To use for this initiator. User name: Target secret:	Header digest  nformation 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
Data digest CHAP logon i CHAP logon i CHAP helps ens initiator. To use for this initiator. User name: Target secret: Use RADIUS	Header digest  nformation  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
Data digest Data digest CHAP logon i CHAP logon i CHAP logon i CHAP index of the logon i CHAP l	Header digest  nformation  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 ual authentication
Data digest Data digest CHAP logon i CHAP holps ensinitiator. To use for this initiator. User name: Target secret: User RADIUS Perform mutual CRADIUS. The se	Header digest  nformation  are data security by providing authentication between a target and an it, specify the same target CHAP secret that was configured on the target  iqn. 1991-05.com.microsoft:tarquin-vista  to generate user authentication credentials ual authentication HAP either specify an initiator secret on the Initiator Settings page or use ame secret must be configured on the target.

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.

Jetwork Connections - Windows Internet Explorer	0.0
. + http://10.10.10.50/connections/	<ul> <li>↓ 49 X</li> <li>Live Search</li> </ul>
🚱 🔨 Network Connections	🖓 🔹 🔝 🔹 📾 🔹 🕜 Page 🔹 🌀 Tools
ridge Control	
Console Home	
Global Network Configuration	
teboot.System Hostname: bridgeworks	
Gateway: 10.10.10.1	
DNS Server: 10.10.10.1	
pport	
Interview Port 1	
Use DHCP:	
yright 2008 DELL Inc	
IP Address: 10.10.10.50	
Netmask: 255 255 25 0	
Broadcast: 10.10.10.255	
- Link Statue	
Link State: up Link 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 State: up Link 1000 Mb/s	
RX Bytes: 191039 TX Bytes: 107780	
RX Errors: 0 TX Errors: 0	
	G Internet   Protected Mode: Off

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					
Load balance polic	y.				
Round Robin				•	
Description					
The round robin	policy attempts to	evenly dist	ribute incor	ming	
requests to all p	processing paths.				
This service has the					
This session has u	le following connec	uons ;	line with	Ponte and	
Source Portal	Target Portal	Status	Туре	Weight	1
10.0.0.237/6	10.10.10.50/	Conne	Active	n/a	1
10 10 11 001	10.10.11.50/	Conne	Active	n/a	1
10.10.11.56/					
10.10.11.56/					
10.10.11.56/					
10.10.11.56/					
	III				•
•				- 11	•

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	get has the	e following sessio	ns:	
Identif	ier			
🔲 ffff	ffff8741d	31c-4000013700	000008	
		187 J		
		L	og off	Refresh
		1		
Sessio	n Properti	25		
Targe	t portal gro	oup:	1	
Status	:		Connecte	ed
Conne	ection cour	it:	2	
Sessio	n Connect	ions		
To cor	nfigure hov ession are ections.	v the connection load balanced, cl	s within lick	Connections
this se				

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

Potomac ES1100DT Page 51

#### 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 Tar	gets	Volumes	and Device	s   RAE	DIUS	Configuration
Configu the initia	ration settin ator.	gs here are glo	obal ar	nd will aff	ect any futi	ure con	nectio	ins made with
Any exi the initia	sting connec ator otherwi	tions may con se tries to reco	inue t Innect	o work, b to a tarç	ut can fail i jet.	f the sy	stem	restarts or
When o particula	onnecting to ar connectio	a target, adv n.	anced	connecti	on features	allow s	pecifi	c control of a
Initiator	Name:							
iqn.19	91-05.com.r	nicrosoft:win-d	3081s	idkbe				
ſo modi	fy the initiat	or name, click	Chang	e.				Change
To set t click CH	he initiator ( AP,	HAP secret fo	r use v	with mutu	al CHAP,			CHAP
To set u click IPs	ip the IPsec ec.	tunnel mode a	ddress	ses for th	e initiator,			IPsec
To gene the syst	erate a repo tem, click Re	t of all connec port.	ted ta	rgets and	l devices or	1		Report
More at	oout 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

The system will le	ook for Targets o	n following portals:	Refresh
Address	Port	Adapter	IP address
To add a target (	portal, click Disco	ver Portal.	Discover Portal
To remove a tare then click Remov	get portal, select 'e.	the address above and	Remove
The system is re Name	gistered on the fo	llowing iSNS servers:	Refresh
To add an iSNS s	erver, click Add S	ierver.	Add Server
To add an iSNS s To remove an iSI :hen click Remov	erver, click Add S VS server, select e.	erver. the server above and	Add Server Remove

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

Discover Target Portal	×
Enter the IP address or DNS name and p want to add.	ort 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.) 3260
Advanced	OK Cancel

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.

eral IPsec	
Connect using	
connect daing	
Local adapter:	
Initiator IP:	Default
Target portal IP:	<b>_</b>
CRC / Checksum — —	
Data digest	Header digest
Enable CHAP log	iou
CHAP Log on infor	) on mation
Enable CHAP log CHAP Log on infor CHAP helps ensure an initiator. To use, specify the	) on mation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this
Enable CHAP log     CHAP Log on infor     CHAP helps ensure: an initiator.     To use, specify the initiator. The name specified. Name:	i on mation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is iqn.1991-05.com.microsoft:win-d3081sidkbe
Enable CHAP log     CHAP Log on infor     CHAP helps ensure:     an initiator.     To use, specify the     nitiator. The name     specified.     Vame:     Target secret:	Ton mation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is [ Iqn.1991-05.com.microsoft:win-d3081sidkbe ]
Enable CHAP log     CHAP Log on infor     CHAP helps ensure:     an initiator.     To use, specify the     initiator. The name     specified.     Vame:     Target secret:     Perform mutual	Ton mation connection security by providing authentication between a target and same 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
Enable CHAP log     CHAP Log on infor     CHAP helps ensure:     an initiator.     To use, specify the     nitiator.     The name     specified.     Vame:     farget secret:         Perform mutual     To use mutual CHAF     XADIUS.	I on mation connection security by providing authentication between a target and same name and CHAP secret that was configured on the target for this will default to the Initiator Name of the system unless another name is [Iqn.1991-05.com.microsoft:win-d3081sidkbe
Enable CHAP log     CHAP Log on infor     CHAP helps ensure:     an initiator.     To use, specify the     mitiator. The name     specified.     Name:     Target secret:     Perform mutual     Perform mutual     CHAP     RADIUS.     Use RADIUS to:	on     mation     connection security by providing authentication between a target and     same name and CHAP secret that was configured on the target for this     will default to the Initiator Name of the system unless another name is     [Iqn.1991-05.com.microsoft:win-d3081sidkbe     [Iqn.1991-05.co
Enable CHAP log CHAP Log on infor CHAP helps ensure an initiator. To use, specify the initiator. Name: Target secret: Perform mutual To use mutual CHAP RADIUS. Use RADIUS to ( Use RADIUS to (	on     mation     connection security by providing authentication between a target and     same name and CHAP secret that was configured on the target for this     will default to the Initiator Name of the system unless another name is         Iqn.1991-05.com.microsoft:win-d3081sidkbe         Iqn.1991-05.com.microsoft:win-d3081sidkbe         generate user authentication recreit on the Configuration page or use     generate user authentication credentials     athenticate target credentials

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

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

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

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

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



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

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

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

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

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

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

	1	n following portals:	
4ddress	Port	Adapter	IP address
fo add a target p	ortal, click Disco	ver Portal.	Discover Portal
fo remove a targe hen click Remove	et portal, select	the address above and	Remove
fo add an iSNS se	rver. click Add S	ēerver.	Add Server
fo remove an iSN: hen click Remove	5 server, select	the server above and	Remove

iSCSI to SCSI Page 56

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

Add iSNS Server	×
Enter the IP address or DNS name of server:	
·	
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

gets Discovery Eavorite Targets Volumes and Devices	RADIUS Configuration
uick Connect	
o discover and log on to a target using a basic connection, typ NS name of the target and then click Quick Connect.	e the IP address or
Farget:	Quick Connect
iscovered targets	Refresh
Name	Status
ign 2002-12 com 4bridgeworks 000000/6d7a85844c2f1fa8	Reconnecting
iqn.2002-12.com.4bridgeworks.001c03:naa.50060b000057	Reconnecting
connect using advanced options, select a target and then	
to controls ability and allocal options, solver a taliger and then	
click Connect.	Connect
click Connect. To completely disconnect a target, select the target and then click Disconnect.	Disconnect
click Connect. To completely disconnect a target, select the target and then click Disconnect. For target properties, including configuration of sessions, select the target and click Properties.	Disconnect Properties
click Connect. To completely disconnect a target, select the target and then click Disconnect. For target properties, including configuration of sessions, select the target and click Properties. For configuration of devices associated with a target, select the target and then click Devices.	Disconnect Properties Devices

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

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

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

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

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

ieral IPsec   Connect using	
Connect using	
.ocal adapter:	Default
nitiator IP:	Default
Farget portal IP:	Default
CRC / Checksum	
🗌 Data digest	Header digest
Enable CHAP log or	-
CHAP Log on informa	tion
an initiator. To use, specify the sar	menutor security by providing adure rutation between a target and me name and CHAP secret that was configured on the target for this I default to the Teilitator Name of the custom unless another name is
specified.	raeladir to the Initiator Name of the system diless another hame is
Vame:	iqn.1991-05.com.microsoft:win-d3081sidkbe
Target secret:	
Perform mutual aut	ihentication
Fo use mutual CHAP, e RADIUS.	ather specify an initiator secret on the Configuration page or use
Use RADIUS to ger	nerate user authentication credentials
Use RADIUS to aut	henticate target credentials

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.

SI Iniciacor P	roperties				
argets Disco	very Favorite Targets Volu	mes and Devices	RADIL	JS Configuration	
Quick Connect					
To discover a DNS name of	nd log on to a target using a b the target and then click Quick	asic connection, t Connect.	ype the	IP address or	
Target:				Quick Connect	
Discovered ta	gets			Refresh	1
Name			Status		1
ian.2002-12.	com.4bridaeworks.000000:97	7d098e36978	Connec	ted	
, To connect us click Connect.	ing advanced options, select a	a target and then		Connect	
To completely then click Disc	disconnect a target, select th onnect.	e target and		Disconnect	1
For target pro select the tar	perties, including configuratio get and click Properties.	n of sessions,		Properties	
For configural the target an	ion of devices associated with d then click Devices.	a target, select		Devices	
More about ba	sic ISCSI connections and targ	<u>ets</u>			

#### Step 4 – Viewing iSCSI Session Details

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

Properties	×
Sessions Portal Groups	
	Refresh
Identifier	
fffffa8001770018-400001370000	00008
To add a session, click Add session.	Add session
To disconnect one or more sessions, se session and then click Disconnect.	lect each Disconnect
To view devices associated with a sessi a session and then click Devices.	ion, select Devices
Session Information	
Target portal group tag:	1
Status:	Connected
Connection count:	1
Maximum Allowed Connections:	10
Authentication:	None Specified
Header Digest:	None Specified
Data Digest:	None Specified
Configure Multiple Connected Session To add additional connections to a se configure the MCS policy for a selecte click MCS. More Information on ISC5I Sessions	n (MCS) ssion or ad session, MCS
	OK Cancel

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

Devices			×
Name	Address		
Disk -1	Port 2: Bus 0: Target 0:	LUN 0	
I			
Volume path	names:		
Legacy devic	e name:		
2.			
Device interf	ace name:		
Configure Mu	Iltipath IO (MPIO)		
selected dev	the MPIO policy for a rice, click MPIO,		MPIO
	,		
T-Course None C	- SCOT Device Debails		
Information C	In IDCDI Device Decails		
			OK

iSCSI to SCSI Page 60

#### 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 po processing paths.	olicy attempts to even	ly distribute ir	coming reque	sts to all	
his session has the	following connections	:			
Source Portal	Target Portal	Status	Туре	Weight	
0.0.0.0/61894	10.10.10.107/3	Connected	Active	n/a	
0.0.0.0/61894	10.10.10.107/3	Connected	Active	n/a	
0.0.0.0/61894	10.10.10.107/3	Connected	Active	n/a	•
0.0.0.0/61894	10.10.10.107/3	Connected	Active	n/a Add	•
<ul> <li>0.0.0.0/61894</li> <li>I add a connection</li> <li>To remove a connection</li> <li>Co remove.</li> </ul>	10.10.10.107/3 n, click Add. ction, select the conne	Connected	Active	n/a Add Remove	•

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

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

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

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

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

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

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

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



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

Connect using	
.ocal adapter:	Microsoft iSCSI Initiator
Initiator IP:	Default
Target portal IP:	Default
CRC / Checksum	
🗌 Data digest	Header digest
Enable CHAP log CHAP Log on inform CHAP helps ensure c an initiator. o use, specify the s nitiator. The name v inectified.	on 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
Enable CHAP log CHAP Log on inform CHAP helps ensure of an initiator. To use, specify the s nitiator. The name w specified.	on 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-d3081sidibe
Enable CHAP log CHAP Log on inform CHAP helps ensure of an initiator. To use, specify the s nitiator. The name w specified. Vame: Farget secret:	on hation hation hation connection 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
Enable CHAP log     CHAP Log on inform     CHAP Log on inform     CHAP Lebs ensure o     initiator.     To use, specify the s     initiator. The name v     peofied.     Vame:     Target secret:     Perform mutual a     To use mutual CHAP,     ADULS.	on hation
Enable CHAP log     CHAP Log on inform     CHAP Log on inform     CHAP Log on inform     CHAP Logs ensure o     initiator.     To use, specify the s     initiator.     To use, specified.     Iarget secret:         Perform mutual a         Perform mutual a         Co use mutual CHAP,         (ADIUS.         Use RADIUS to g	on hation nnection 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 ign.1991-05.com.microso

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

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

ultiple Connected Session (MCS)						
ACS policy:						
Round Robin					•	
Description The round robin policy attempts to evenly distribute incoming requests to all processing paths.						
This session has the l	following connections	:				
Source Portal	Target Portal	Status	Туре	Weight		
0.0.0.0/60102	10.10.10.107/3	Connected	Active	n/a	0	
0.0.0.0/63942	10.10.10.107/3	Connected	Active	n/a	0	
۲ <b>.</b>					Þ	
To add a connection, click Add.						
To remove a connection, select the connection above and then						
To edit the path settings for the MCS policy, select a Edit						
	0	к	Tancel	Apply		

The user can add up to 10 different connections.

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

Properties		×			
Sessions Portal Groups					
1		Refresh			
Identifier	0007				
To add a session, click Add session.	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 Specified					
Header Digest: None Speci		fied			
Data Digest:	Data Digest: None Specified				
Configure Multiple Connected Session (MCS) To add additional connections to a session or configure the MCS policy for a selected session, click MCS. More Information on ISCSI Sessions					
		DK 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.





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

# 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		
SCSI Interface			
Physical	VHDLC 68way LVD/SE		
Speed	Auto negotiation up to Ultra160 (Ultra 320)		
Width	Auto negotiation for narrow and wide		
Visual Indicators	SCSI Bus busy		