Millau EFCSAS2240
iSCSI & Fibre Channel to SAS Bridge
User Manual
V3.4

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

Manual Revision History

Revision	Date	Firmware	
3.0	July 2011	V3_02	JV
3.1	April 2012	V3_02	AP
3.2	May 2012	V3_03	AP
3.3	August 2012	V3_03	AP
3.4	October 2013	V3_04	AP

Warning

The Bridgeworks Potomac EFCSAS2240 iSCSI-FC to SAS Bridge contains no user-serviceable components. Only an Authorized Service Centre should carry out any servicing or repairs. Unauthorized repairs or modifications will immediately void your warranty.

Before You Start

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

Ethernet Cable

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

Fibre Channel Interface

The Fibre Channel Bridge supports the use of SFP modules to connect to the Fibre Channel. You will require the correct type to connect to your existing infrastructure.

Fibre Channel Cable

In addition to the fibre channel interface, you will require a good quality cable of suitable length to go between your Bridge and your initiator or fibre channel switch.

SAS Cable

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

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

Table of Contents

1.0 Introduction

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

The EFCSAS2240 Bridge has been designed to ensure that in the majority of installations it will require the minimum of set up before use. However, we suggest you read the following, which will guide you through setting up the iSCSI and Fibre Channel Networks as well as the SAS aspects of the EFCSAS2240 Bridge.

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

1.1 Overview

The EFCSAS2240 Bridge creates an interface between both iSCSI and Fibre Channel networks, and peripherals that utilise the SAS protocol. The internal circuitry of the EFCSAS2240 Bridge acts as a two-way interface converting the data packets that are received on either the iSCSI or Fibre Channel network into data transfers and electrical signals that storage devices such as disks, tape drives and optical disks understand on the SAS bus.

The Bridgeworks EFCSAS2240 iSCSI/ Fibre Channel Bridge

1.2 Manual Layout

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

✎	This icon represents a note of interest about a step or section of information.

☞	This icon represents an important piece of information.

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

1.3 Definitions

iSCSI Target Device

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

iSCSI Qualified Name (IQN)

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

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

CHAP

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

1.4 Safety Notices

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

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

⚠	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 EFCSAS2240 Bridge

There are 5 basic steps to installing the EFCSAS2240 Bridge

- Connecting the Fibre Channel cables
- Connecting the iSCSI Ethernet cables
- Connecting the SAS cables
- Connecting the Power Supply

2.1 Fibre Channel Connection

The FC Bridge can be used on the following network configurations

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

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

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

Once the SFP is inserted securely into the Bridge, insert one end of a fibre channel cable into the Bridge and the other end into your initiator or switch.

Front Panel of the Bridge Showing FC Cable Connections

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

2.2 Ethernet Connection

The Bridge can be used on the following network configurations:

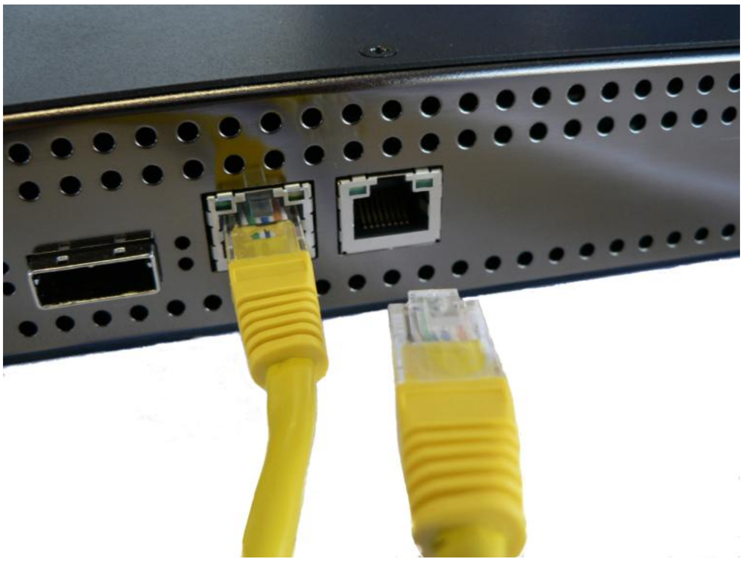
- 10BaseT
- 100BaseT
- 1000BaseT (Gigabit)

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

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

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

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



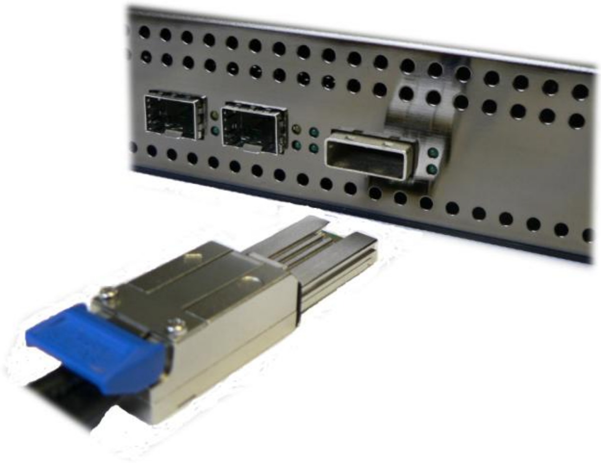
Front Panel of the Bridge Showing Ethernet Cable Connections

2.3 SAS Bus Connections

The SAS bus on the FC Bridge is capable of running at speeds of up to 3Gbits/s. However, devices that operate at slower speeds can still be connected to this SAS bus. In a manner similar to the Ethernet and FC connections, the FC Bridge will automatically negotiate with these devices to obtain their optimal operating speed upon power up. Each SAS port on the FC Bridge port will support up to 4 SAS channels.

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

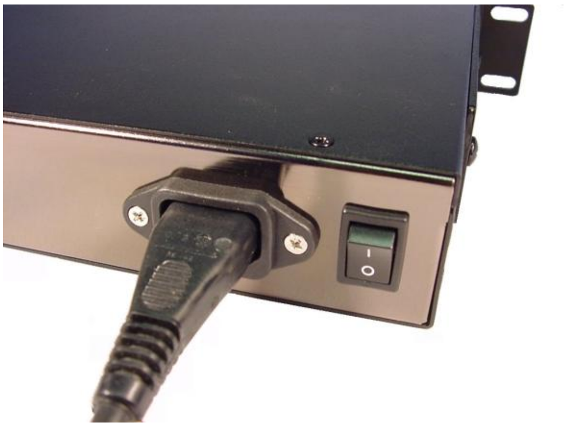
Connecting the SAS Cable to the Bridge SAS Port



2.4 Connecting the Power Supply

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

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



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

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

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

3.0 Configuring the EFCSAS2240 Bridge

Before the EFCSAS2240 Bridge can be used on the network for the first time, it is necessary to configure a number of parameters.

3.1 Using the Web Interface

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

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

3.1.1 Browsers

This Bridge supports the following browsers

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

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

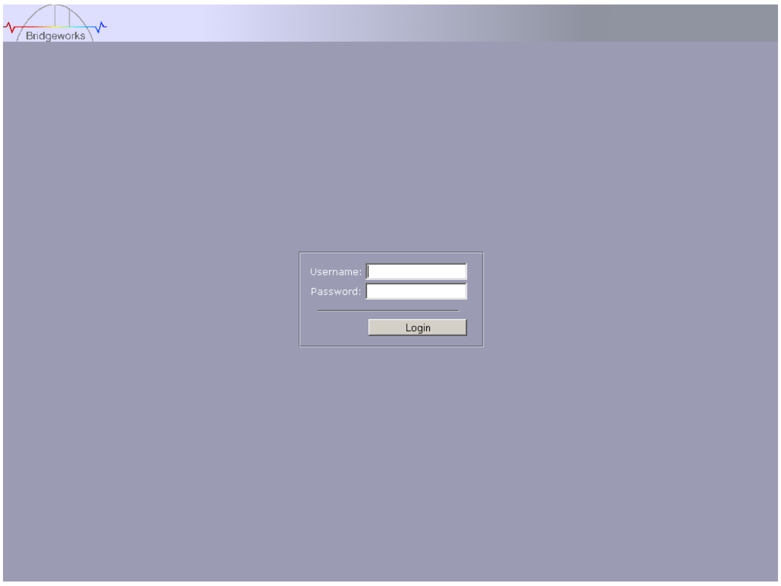
☞ **Important:** If you choose to use a browser that is not on the list of supported browsers Bridgeworks cannot guarantee the behaviour of the Bridge’s functionality.

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.

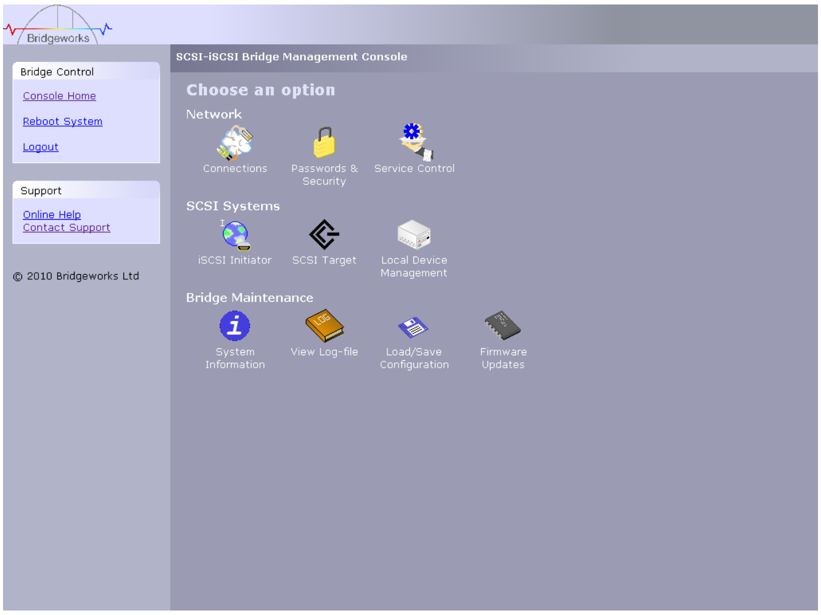


To access the web interface a user name and password must be used, the defaults of which are:

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.

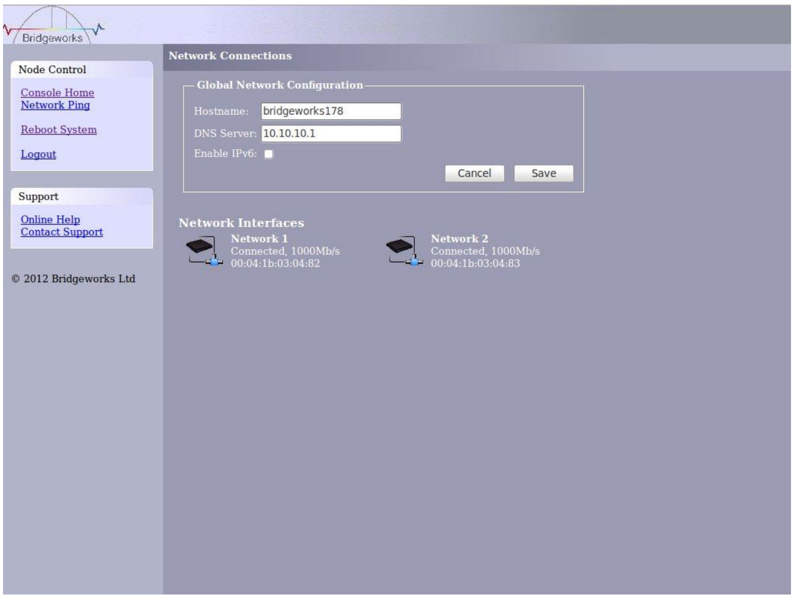


✎	**Note:** For security reasons only one person can access this GUI at any one time. Therefore, to avoid the situation where one person forgets to logout, effectively locking up the GUI, the Bridge incorporates a five minute idle timer, which will automatically logout any user after this period.

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.



Global Network Configuration

Hostname: bridgeworks178

DNS Server: 10.10.10.1

Enable IPv6: □

Network Interfaces

Network 1
Connected, 1000Mb/s
00:04:1b:03:04:82

Network 2
Connected, 1000Mb/s
00:04:1b:03:04:83

© 2012 Bridgeworks Ltd

3.2.1 Setting the Hostname

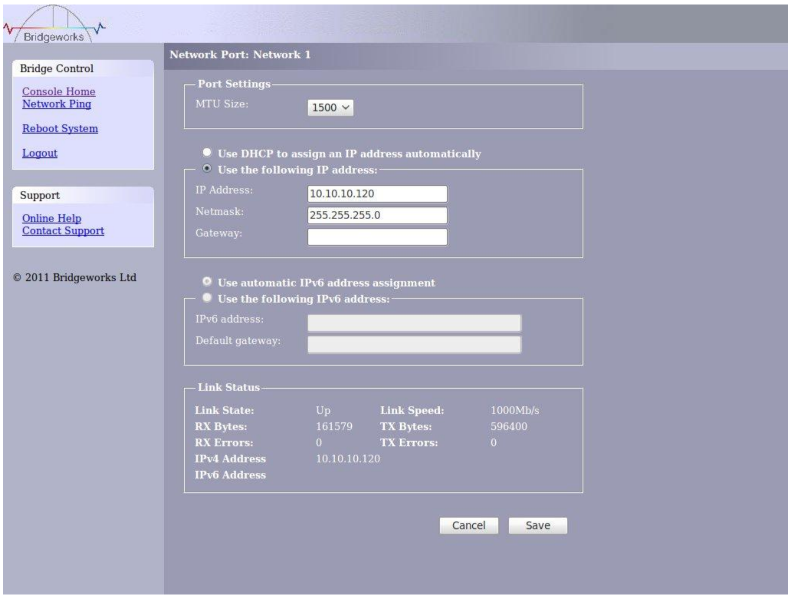
In this box enter the name you wish to use to address this Bridge in the future. We suggest that you use a name that is relevant to its location and/or its purpose.

✎	**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.



Network Port: Network 1

Port Settings

MTU Size: 1500

○ Use DHCP to assign an IP address automatically
● Use the following IP address:

IP Address: 10.10.10.120
Netmask: 255.255.255.0
Gateway:

○ Use automatic IPv6 address assignment
○ Use the following IPv6 address:

IPv6 address:
Default gateway:

Link Status

```
Link State:     Up          Link Speed:   1000Mb/s
RX Bytes:       161579      TX Bytes:     596400
RX Errors:      0           TX Errors:    0
IPv4 Address    10.10.10.120
IPv6 Address
```

3.2.3 Setting the MTU

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

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

3.2.4 Setting the IP Address

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

DHCP - the Bridge will seek out the DHCP server on your network and obtain an IP address from the server each time it powers up.
Static IP - the IP address set in this page will be the IP address the unit will use each time it powers up.

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

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

3.2.5 Setting the Subnet Mask

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

3.2.6 Setting the Gateway Address

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

3.2.7 Setting an IPv6 IP Address

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

3.2.8 Committing the changes

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

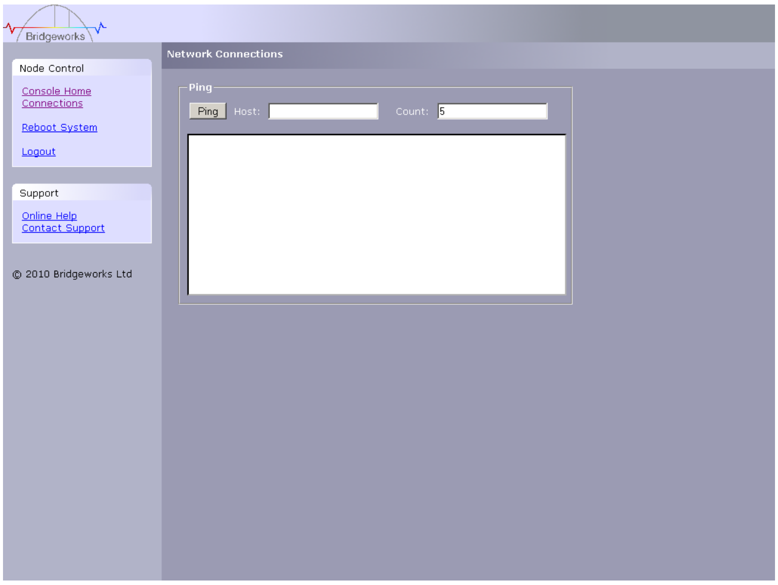
Click the save button to save these parameters and then click the reboot button in the left hand pane.

3.2.9 Reconnect to the Bridge

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

3.2.10 Network Ping

You can test your network connection by using the 'Network Ping' tool. To access the Network Ping, click on the link in the left hand panel.



Network Ping

Enter the IP Address that you want to ping in the Host box and the number of times that you want to ping in the count box. The results of the ping will be displayed in the box below.

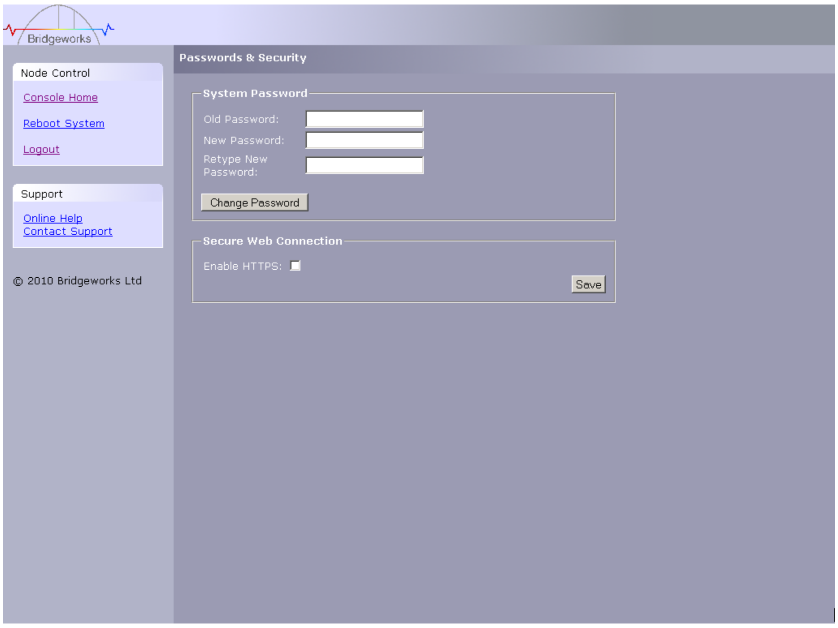
Note: If you enter 0 into the count box the ping will carry on until you leave the page or enter a value greater than 0 in to the count box and hit ping again.

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



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

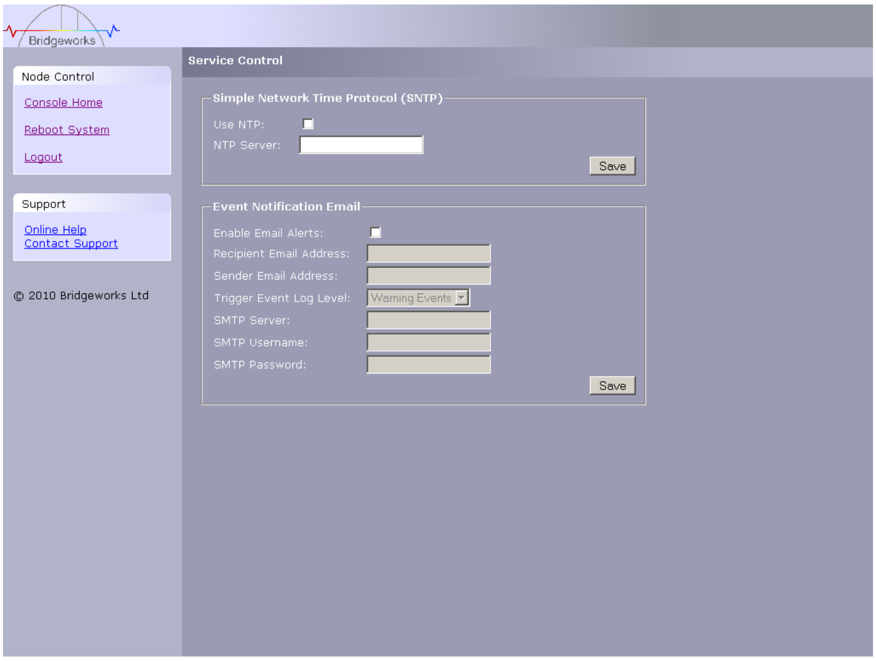
3.4.1 NTP

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



Simple Network Time Protocol (SNTP)

Use NTP: □

NTP Server:

Event Notification Email

Enable Email Alerts: □

Recipient Email Address:

Sender Email Address:

Trigger Event Log Level: Warning Events

SMTP Server:

SMTP Username:

SMTP Password:

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

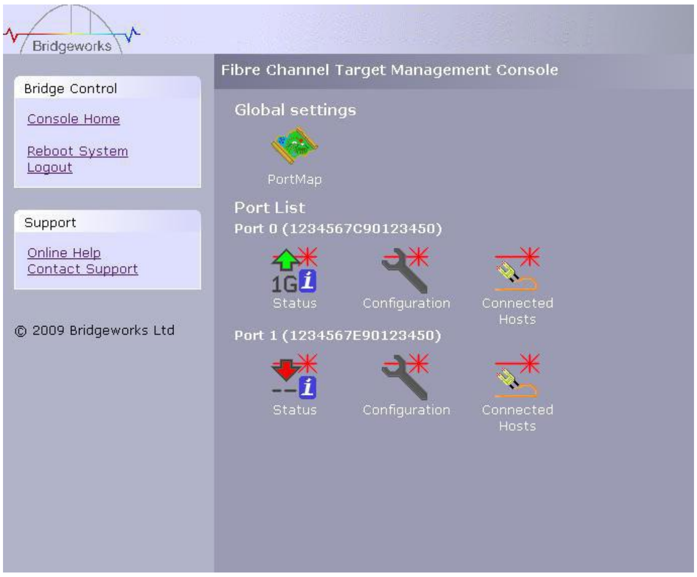
Internet Storage Name Service allows automated discovery, management and configuration of each iSCSI resource from a central point. If this option is enabled the Bridge will register its resources with a central iSNS server. To enable iSNS on the Bridge, click the tick box and enter the IP address for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

3.5 FC Target Interface

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

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

The GUI will now display the following window



Fibre Channel Target Management Console

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

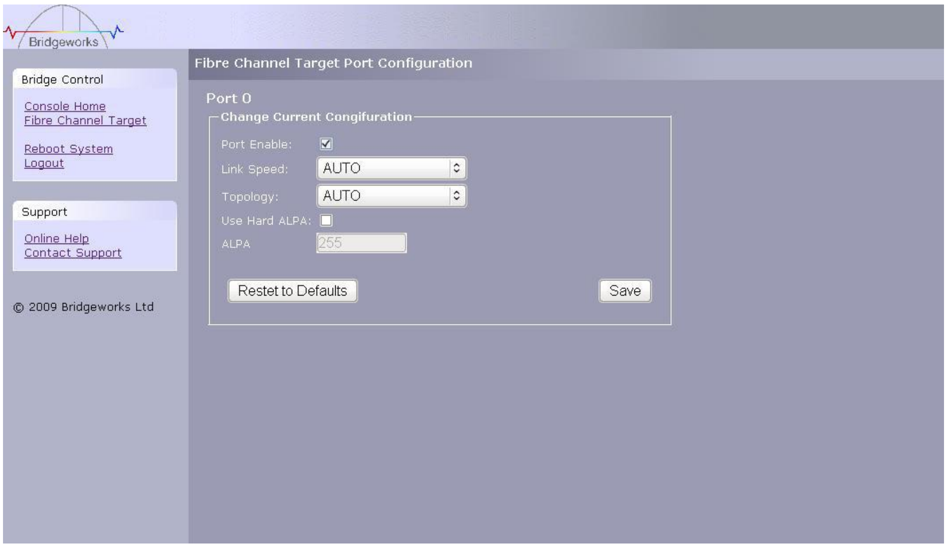
The green / red arrow display whether the port is up or down whilst the number displays the negotiated Fibre Channel speed

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

Port Configuration

Now select the first of the ports configuration icon

The Screen will now display the following



Fibre Channel Target Port Configuration

Port 0

Change Current Congifuration

Port Enable: ☑

Link Speed: AUTO

Topology: AUTO

Use Hard ALPA: □

ALPA 255

The first parameter is the link enable check box

Check this to enable the link on to the FC SAN

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

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

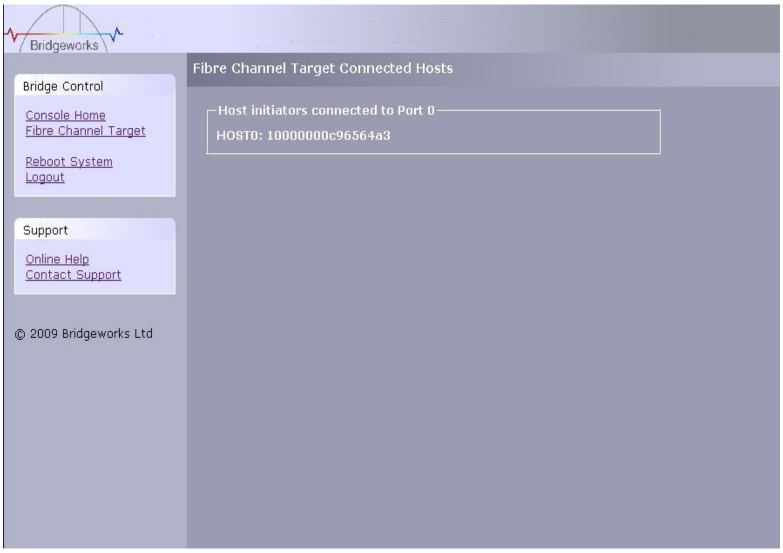
Note: We suggest you leave this unchecked unless you are conversant with the lower levels of the Fibre Channel protocol as certain ALPA addresses are reserved.

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

Repeat this process for the other Network Port as required.

Connected Hosts

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



Fibre Channel Target Connected Hosts

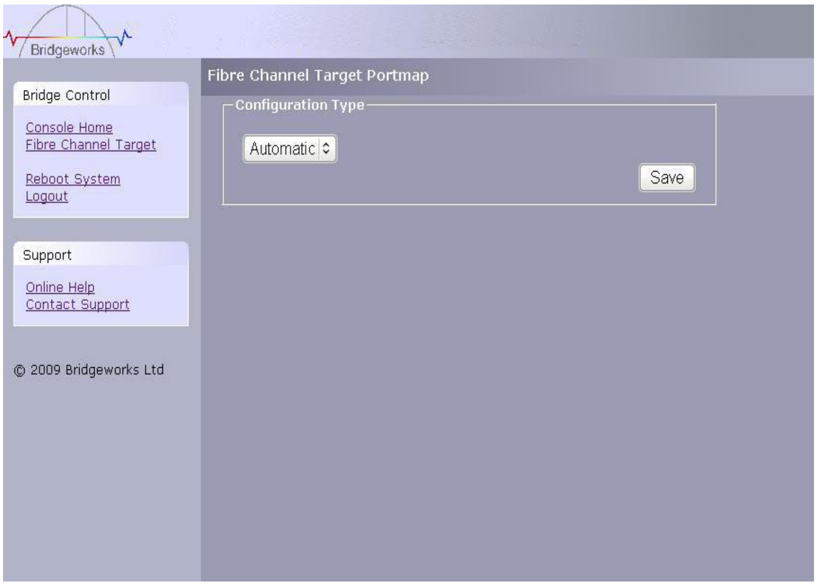
Host initiators connected to Port 0

HOST0: 10000000c96564a3

Port Map

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

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



Fibre Channel Target Portmap

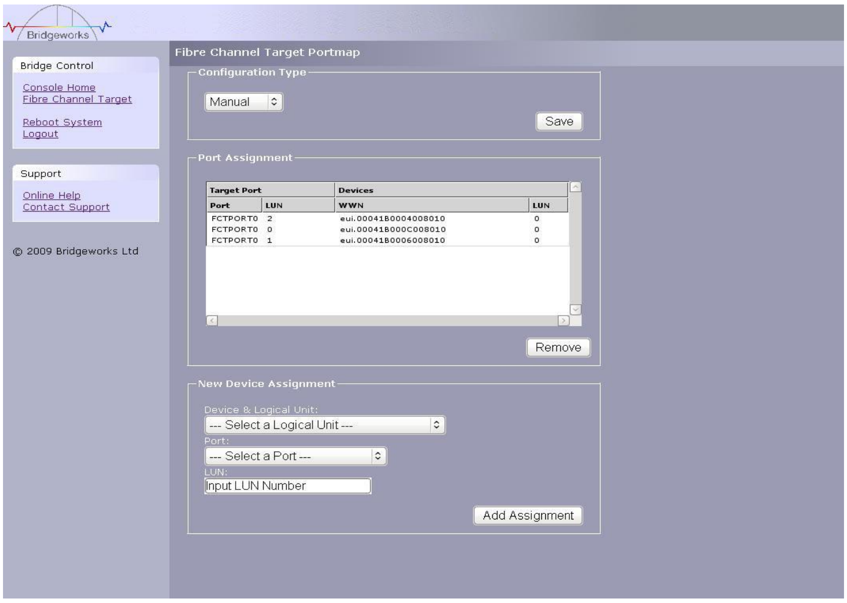
Configuration Type: Automatic

© 2009 Bridgeworks Ltd

There are two choices from the drop down list

- Automatic this will assign to both Fibre Channel ports all the target SAS devices so that any host connected to ether of the Fibre Channel ports will see the same devices.
- Manual this will allow the user to manually assign which SAS target device appears on which Fibre Channel.

Selecting Manual will bring up the following screen



Fibre Channel Target Portmap

Configuration Type: Manual

Port Assignment

Target Port		Devices	
Port	LUN	WWN	LUN
FCTPORT0	2	eui.00041B0004008010	0
FCTPORT0	0	eui.00041B000C008010	0
FCTPORT0	1	eui.00041B0006008010	0

New Device Assignment

Device & Logical Unit: --- Select a Logical Unit ---

Port: --- Select a Port ---

LUN: Input LUN Number

© 2009 Bridgeworks Ltd

To assign a SAS target device to a Fibre Channel Port

- Select the SAS target device from the list in the Logical Unit drop down menu
- Select which Fibre Channel Port you wish the LUN to appear on
- Select the LUN number you wish the device to have on the Selected Fibre Channel Port

- Click the Add Assignment button at the bottom of the panel

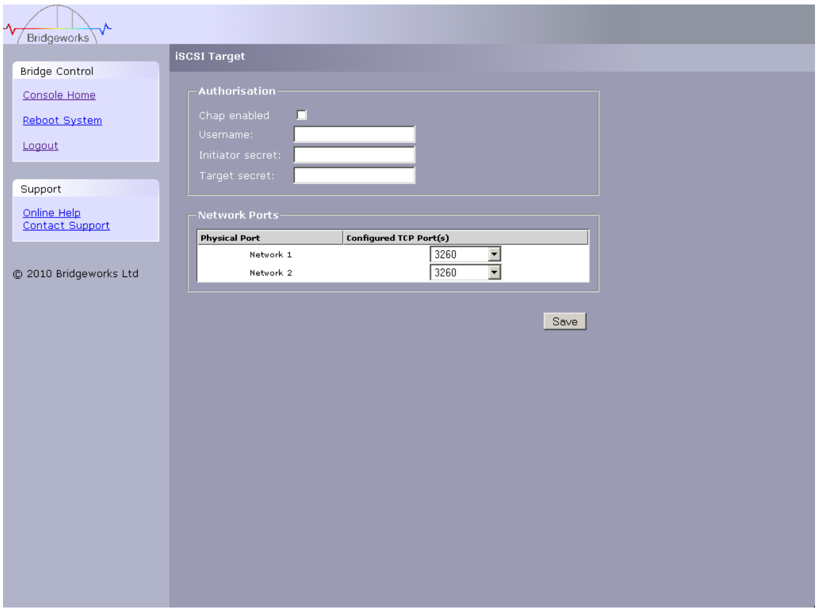
In the example above the Port Assignment shows you 3 devices assigned to Port 0 with the LUN numbers 0, 1 and 2.

3.6 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



Authorisation

Chap enabled □

Username:

Initiator secret:

Target secret:

Network Ports

Physical Port	Configured TCP Port(s)
Network 1	3260
Network 2	3260

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.

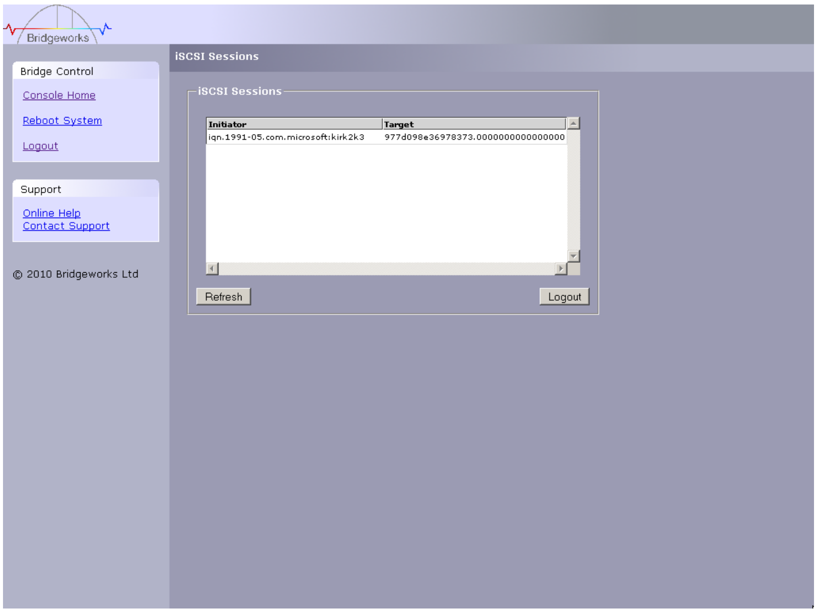
iSCSI uses to two main network ports, 3260 and 860. Within the Multipath configuration the user can specify which ports will be made available to the initiator, 860, 3260 or both.

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.

3.7 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.



Initiator	Target
iqn.1991-05.com.microsoft:kirk2k3	977d098e36978373.0000000000000000

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.

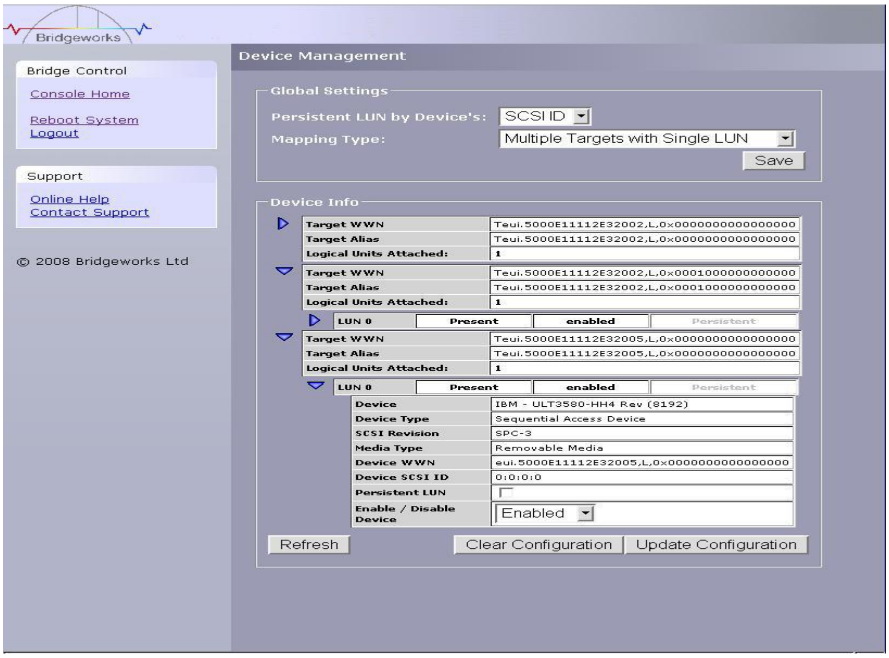
Note: Many initiators are configured to automatically reconnect after completing the logout request. If this is the case then the connections window may not show any change.

3.8 Device Manager

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

From within the main menu select the Device Management section.

The GUI will now display the following window



Device Management

Global Settings

Persistent LUN by Device's: SCSI ID

Mapping Type: Multiple Targets with Single LUN

Device Info

Target WWN	Teui.5000E11112E32002,L,0x0000000000000000
Target Alias	Teui.5000E11112E32002,L,0x0000000000000000
Logical Units Attached:	1

Target WWN	Teui.5000E11112E32002,L,0x0001000000000000
Target Alias	Teui.5000E11112E32002,L,0x0001000000000000
Logical Units Attached:	1

LUN 0	Present	enabled	Persistent

Target WWN	Teui.5000E11112E32005,L,0x0000000000000000
Target Alias	Teui.5000E11112E32005,L,0x0000000000000000
Logical Units Attached:	1

LUN 0	Present	enabled	Persistent

Device	IBM - ULT3580-HH4 Rev (8192)
Device Type	Sequential Access Device
SCSI Revision	SPC-3
Media Type	Removable Media
Device WWN	eui.5000E11112E32005,L,0x0000000000000000
Device SCSI ID	0:0:0:0
Persistent LUN	□
Enable / Disable Device	Enabled

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

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

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

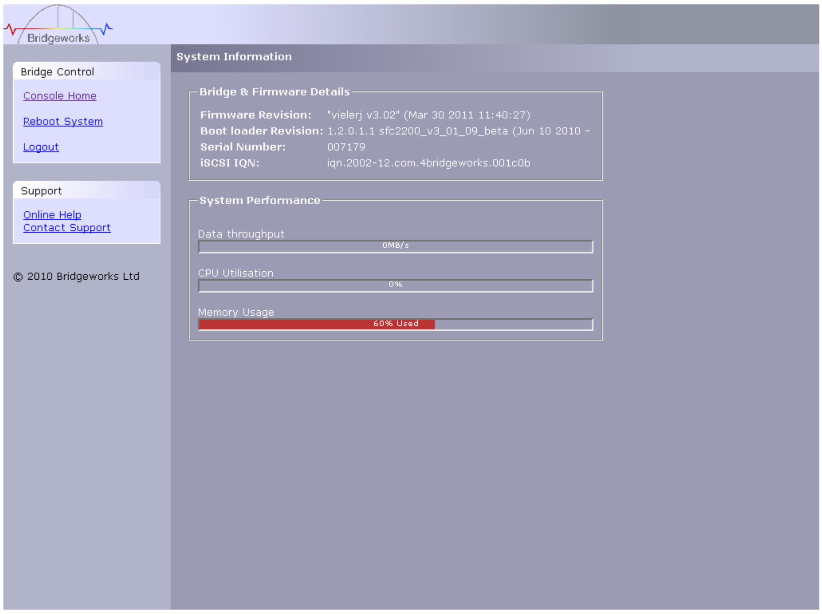
The expanded information also gives you a device control option
Enable / Disable Device – This pull down menu option allows you to disable a SAS device from appearing on the SCSI interface.

4.0 Information

4.1 System Information

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

The GUI will now display the following window



System Information

Bridge & Firmware Details

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 -
Serial Number: 007179
iSCSI IQN: iqn.2002-12.com.4bridgeworks.001c0b

System Performance

Data throughput 0MB/s
CPU Utilisation 0%
Memory Usage 60% Used

Within the top window the following information is displayed

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

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

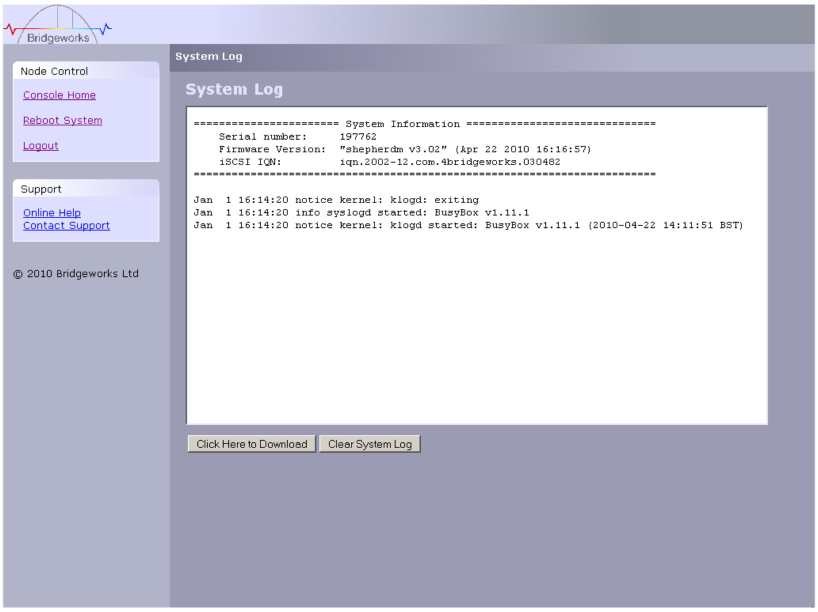
- Data Throughput - This indicates the current performance in MB/s.
- CPU - This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces
- Memory Usage - This indicates the percentage of memory used by all processes

4.2 System Log

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

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

The GUI will now display the following window



```
======================= System Information ==============================
    Serial number:      197762
    Firmware Version:   "shepherdm v3.02" (Apr 22 2010 16:16:57)
    iSCSI IQN:          iqn.2002-12.com.4bridgeworks.030482
=========================================================================

Jan  1 16:14:20 notice kernel: klogd: exiting
Jan  1 16:14:20 info syslogd started: BusyBox v1.11.1
Jan  1 16:14:20 notice kernel: klogd started: BusyBox v1.11.1 (2010-04-22 14:11:51 BST)
```

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.

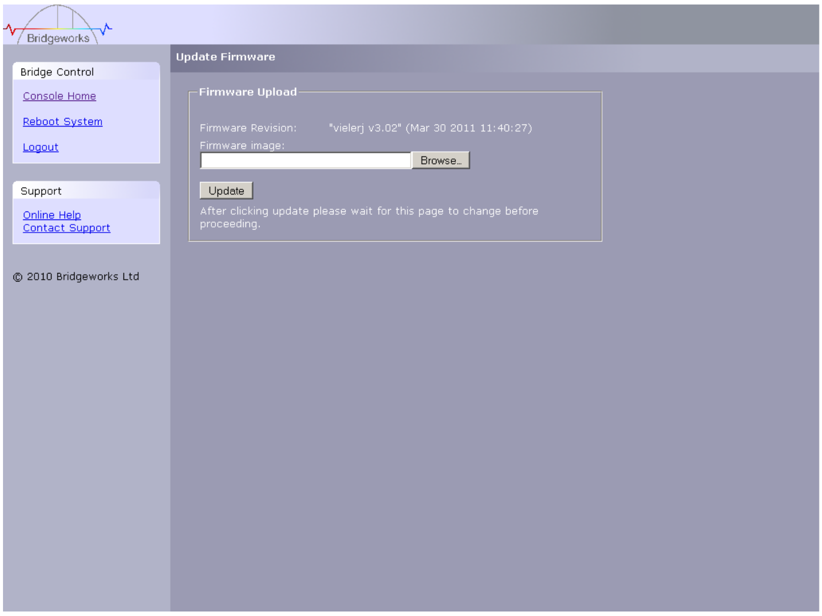
5.0 Maintenance

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.



Firmware Revision: "vielerj v3.02" (Mar 30 2011 11:40:27)

Firmware image:

After clicking update please wait for this page to change before proceeding.

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.

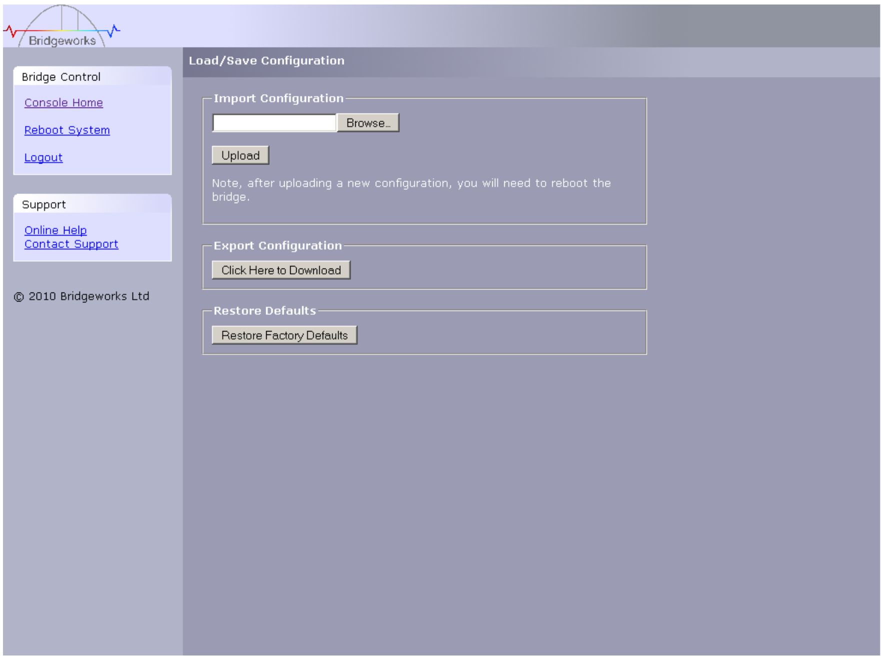
Updating the firmware will take a few minutes after which it will be necessary to reboot the system to bring the new code into memory.

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



Note, after uploading a new configuration, you will need to reboot the bridge.

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

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

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

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

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

5.3 Restoring a Saved Configuration

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

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

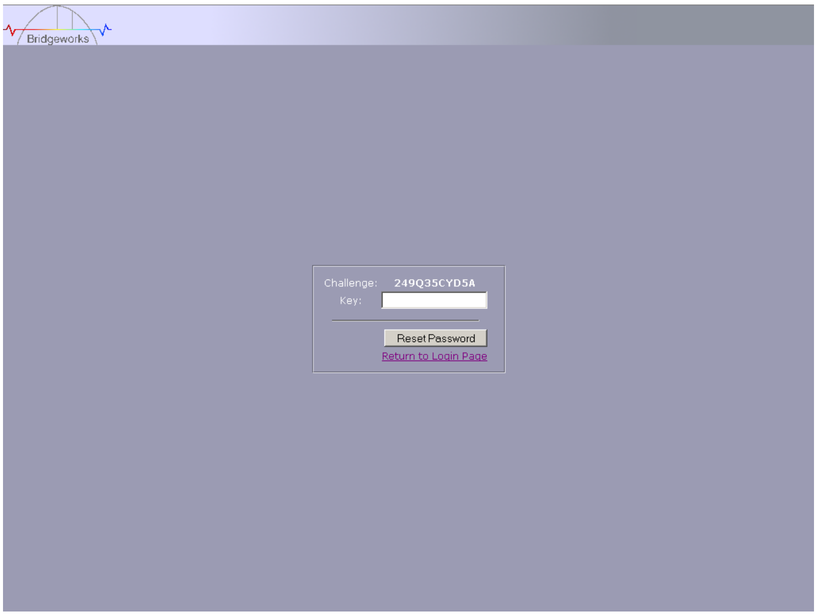
5.4 Restoring Factory Defaults

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

6.0 Trouble shooting

6.1 Lost Password

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



Challenge: 249Q35CYD5A

Key:

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 Issues

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 Isssues

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.

- Ensure any Fibre channel cables do not have any kinks or a bend which exceeds your cable manufacturers maximum bend radius. Also confirm that then connector ends of the cable are fully "clicked in" inside the SFP's on both your initiator and Bridge.

- Some Manufacturers SFP's do not report their speed correctly to the Bridge. To confirm that the speed is correct, first confirm the speed of your SFP by contacting your supplier.

- Once your speed is confirmed navigate to the fibre channel target page and click on the configuration next to the port you are using. Change the link speed form auto to the speed of your SFP. If you are in any doubt it is recommended to use A 4GB SFP as this will prevent any speed compatibility problems.

- Ensure there is no damage to the SFP, confirm the SFP is fully pushed into the FC enclosure and that the clip to secure the cable in place is functioning correctly. When a cable is connected to the initiator correctly the Green LED on the front of the unit will flash.

- If using a fibre channel switch, ensure that the zones are correctly configured for the new device.

- Force a rediscovery from the initiator.

- Reboot the devices and Bridge.

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

6.4 Poor Performance

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

- Ensure your initiator and Bridge are communicating at the fastest possible network speed. Within the GUI is the Network Connections window, select this and check the Link Speed entry in each of the Link Status Boxes. This should be 1000Mb/s - if this is 10 or 100Mb/s, this will limit the performance dramatically.

- Packet loss can be a cause of poor performance. Within the Link Status Box check the number of TX and RX errors for both network Interfaces that are displayed in the Network Connections window. This should be zero or a very small number. If these are showing large numbers of errors, check the connections between the Bridge and the initiator. Also check that the entire network cabling between the Initiator and the Bridge is Cat5e certified.

- By enabling Jumbo packets (increasing the MTU size to 9000 from within the GUI Network Connections window (section 3.2.2)) you can improve the throughput performance of the Bridge. This will only work if ALL of the components in the infrastructure between the Initiator and the Bridge are enabled for Jumbo packets. That includes the HBA, all switches and routers and the Bridge itself. If any of the components are not enabled or not capable of handling Jumbo packets then unexplained packet loss or corruption can happen.

- Data Digests are an extra level of checksum error checking on top of the standard TCP/IP checksum error checking (configured on the initiator). However, the calculation of these extra checksums can greatly affect overall performance. Therefore, Header and Data Digests should only be enabled where the integrity of the Network connection is in doubt.

- Poor GUI performance. If the Bridge is transferring large amounts of data then the response from the GUI may seem a little slow as the process that controls the GUI has the lowest priority for Network and CPU resources.

- It is possible to configure the Bridge so that the data from the initiator is balanced across both the Network Connections. Ensure that you have connected and configured these in accordance with Appendix C and not by enabling the Multipath connection option in the Windows initiator login screen. You should also check the routing tables in your switches, routers and initiator to ensure both IP addresses are not routed down one Network link at any stage.

6.5 Lost IP Address

Introduction

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

Downloading LAN Scan

The utility can be downloaded from:

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

How to use LAN Scan

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

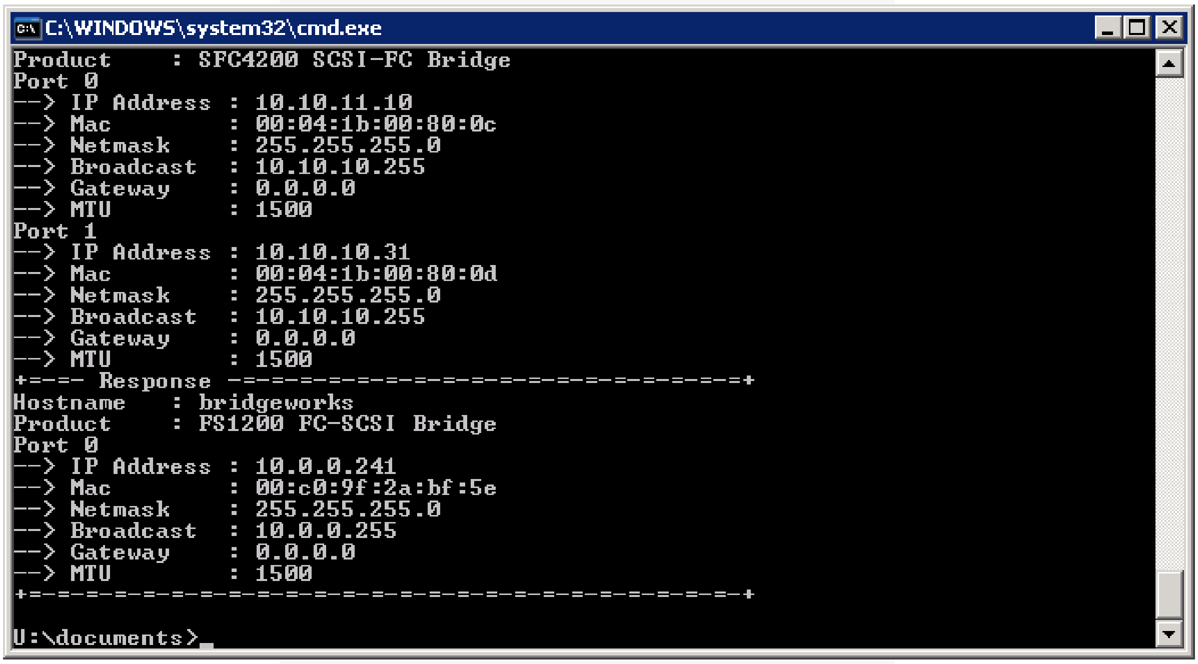
The downloaded file is in .zip format and contains the files lanscan, lanscan.exe and lanscan.bat.

For the GNU/Linux operating system the lanscan executable is needed.
For the Windows operating system the lanscan.exe and lanscan.bat files are required

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

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

Typical output



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

U:\documents>_
```

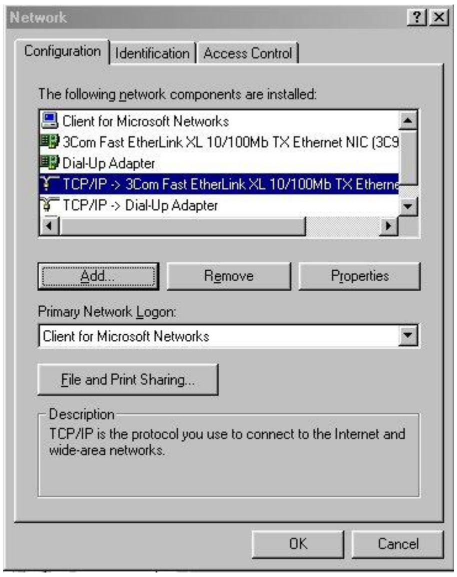
Appendix A Setting up your Computer for Initial Setup

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

The following network components are installed:

- Client for Microsoft Networks
- 3Com Fast EtherLink XL 10/100Mb TX Ethernet NIC (3C9
- Dial-Up Adapter
- TCP/IP -> 3Com Fast EtherLink XL 10/100Mb TX Etherne
- TCP/IP -> Dial-Up Adapter

Primary Network Logon: Client for Microsoft Networks

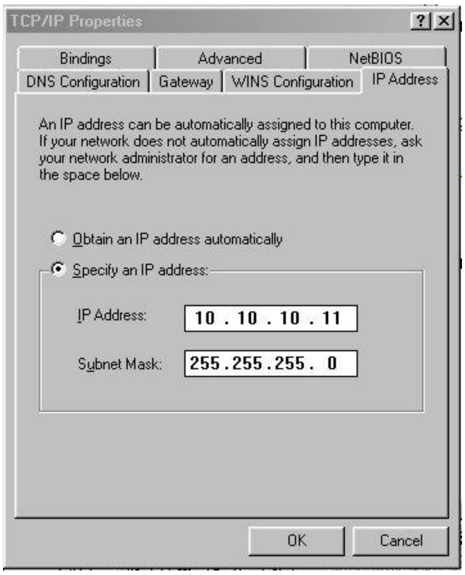
Description

TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

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

Select the **TCP/IP** entry

Then the **Properties** Button



TCP/IP Properties

An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically

● Specify an IP address:

IP Address: 10 . 10 . 10 . 11

Subnet Mask: 255 . 255 . 255 . 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

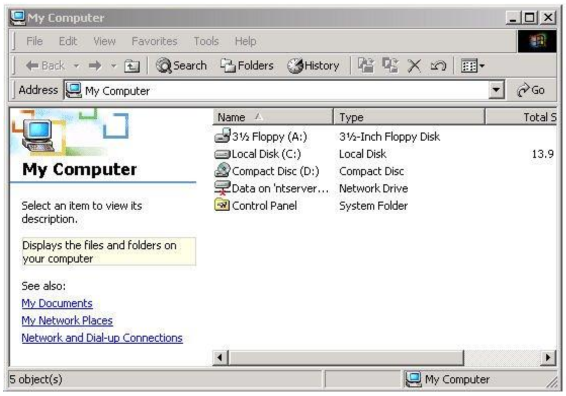
Finally click the OK button and reboot your computer.

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**



Address: My Computer

My Computer

Select an item to view its description.

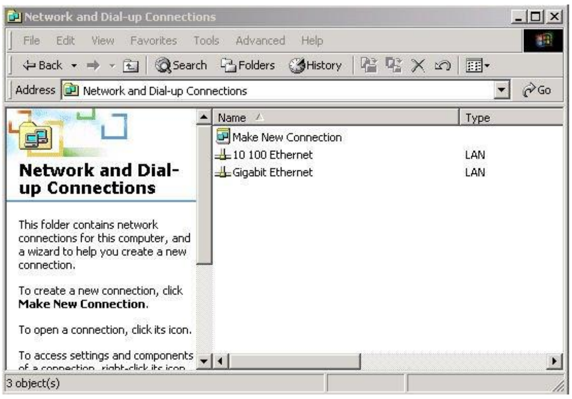
Displays the files and folders on your computer

See also:
My Documents
My Network Places
Network and Dial-up Connections

Name	Type	Total S
3½ Floppy (A:)	3½-Inch Floppy Disk	
Local Disk (C:)	Local Disk	13.9
Compact Disc (D:)	Compact Disc	
Data on 'ntserver…	Network Drive	
Control Panel	System Folder	

5 object(s) My Computer

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



Address: Network and Dial-up Connections

Network and Dial-up Connections

This folder contains network connections for this computer, and a wizard to help you create a new connection.

To create a new connection, click **Make New Connection.**

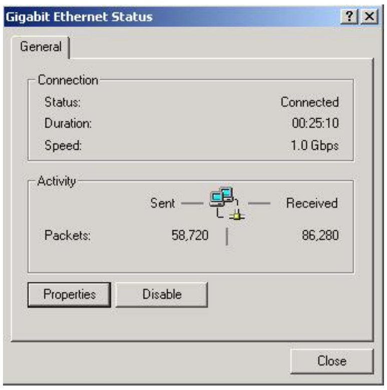
To open a connection, click its icon.

To access settings and components of a connection, right-click its icon

Name	Type
Make New Connection	
10 100 Ethernet	LAN
Gigabit Ethernet	LAN

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.



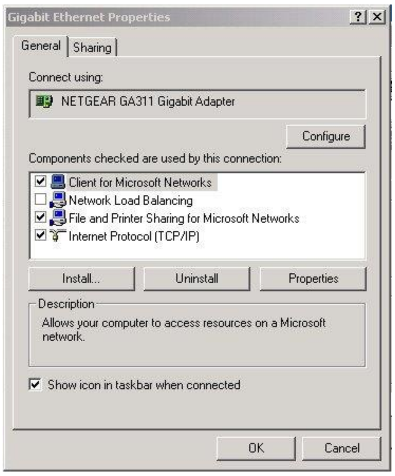
Connection

Status:	Connected
Duration:	00:25:10
Speed:	1.0 Gbps

Activity

	Sent	Received
Packets:	58,720	86,280

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



Connect using:
NETGEAR GA311 Gigabit Adapter

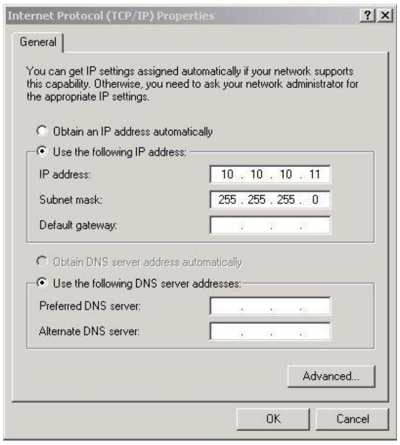
Components checked are used by this connection:

- ☑ Client for Microsoft Networks
- ☐ Network Load Balancing
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

Description
Allows your computer to access resources on a Microsoft network.

☑ Show icon in taskbar when connected

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



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:
IP address: 10 . 10 . 10 . 11
Subnet mask: 255 . 255 . 255 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:
Preferred DNS server: . . .
Alternate DNS server: . . .

Make a Note of your current set up then:

Click **Use the following IP Address**

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

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

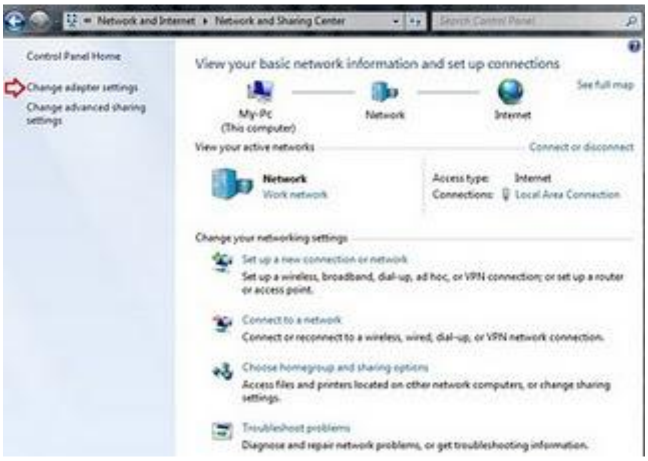
Finally click the OK button.

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

A3 Windows Vista / Server 2008 or Vista or 7

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

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



Network and Internet ▸ Network and Sharing Center

Search Control Panel

Control Panel Home

Change adapter settings

Change advanced sharing settings

View your basic network information and set up connections

My-Pc (This computer) — Network — Internet

See full map

View your active networks

Connect or disconnect

Network
Work network

Access type: Internet
Connections: Local Area Connection

Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

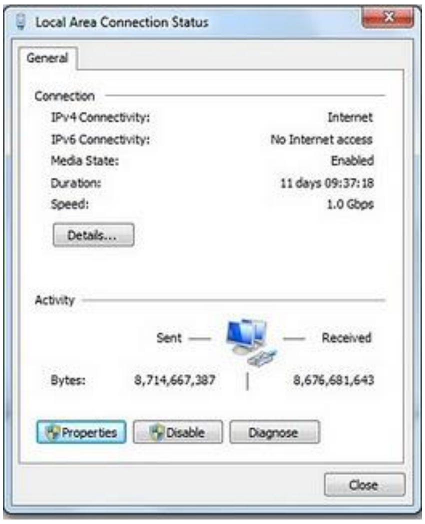
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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.



Local Area Connection Status

General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	11 days 09:37:18
Speed:	1.0 Gbps

Details...

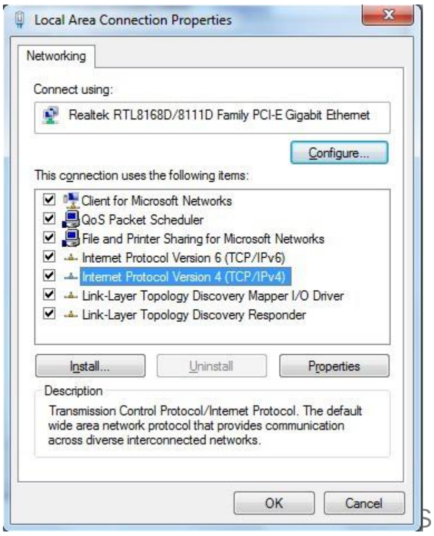
Activity

	Sent	Received
Bytes:	8,714,667,387	8,676,681,643

Properties   Disable   Diagnose

Close

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



Local Area Connection Properties

Networking

Connect using:

Realtek RTL8168D/8111D Family PCI-E Gigabit Ethernet

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

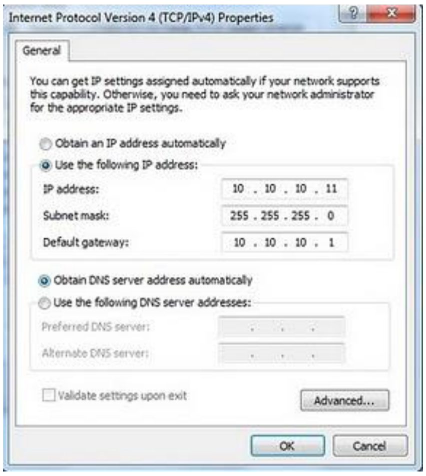
Install...   Uninstall   Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK   Cancel

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


Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 10 . 10 . 10 . 11
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 1

● Obtain DNS server address automatically
○ Use the following DNS server addresses:

Preferred DNS server: . . .
Alternate DNS server: . . .

□ Validate settings upon exit

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.

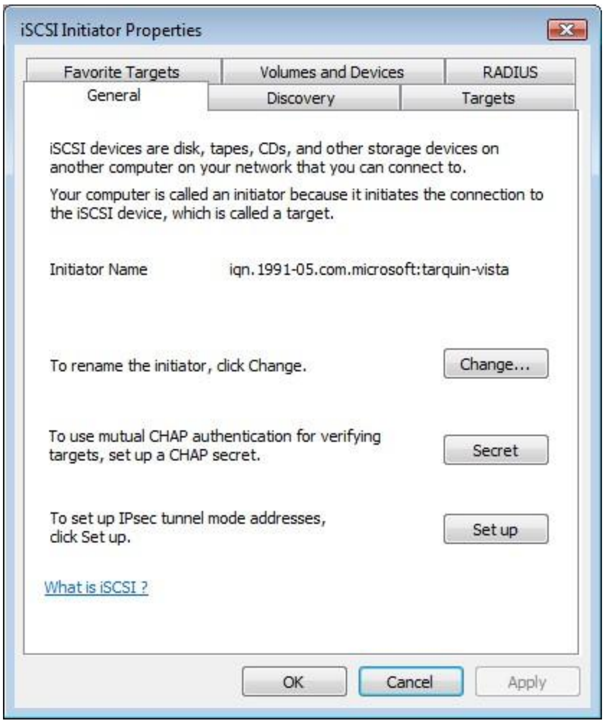
Note: Once you have completed the initial set up of the Bridge, return your computer to the original settings and reconnect to the Bridge.

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.



iSCSI Initiator Properties

iSCSI devices are disk, tapes, CDs, and other storage devices on another computer on your network that you can connect to.

Your computer is called an initiator because it initiates the connection to the iSCSI device, which is called a target.

Initiator Name   iqn.1991-05.com.microsoft:tarquin-vista

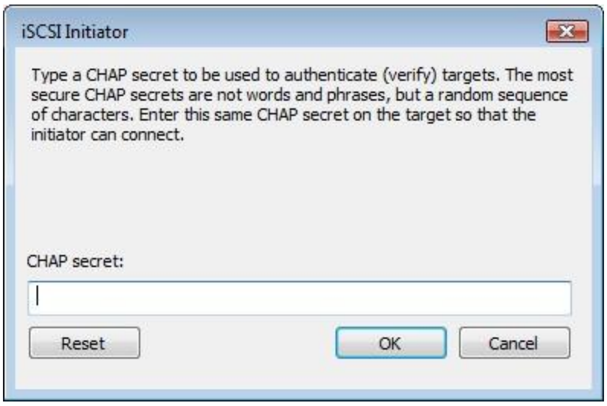
To rename the initiator, click Change.

To use mutual CHAP authentication for verifying targets, set up a CHAP secret.

To set up IPsec tunnel mode addresses, click Set up.

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

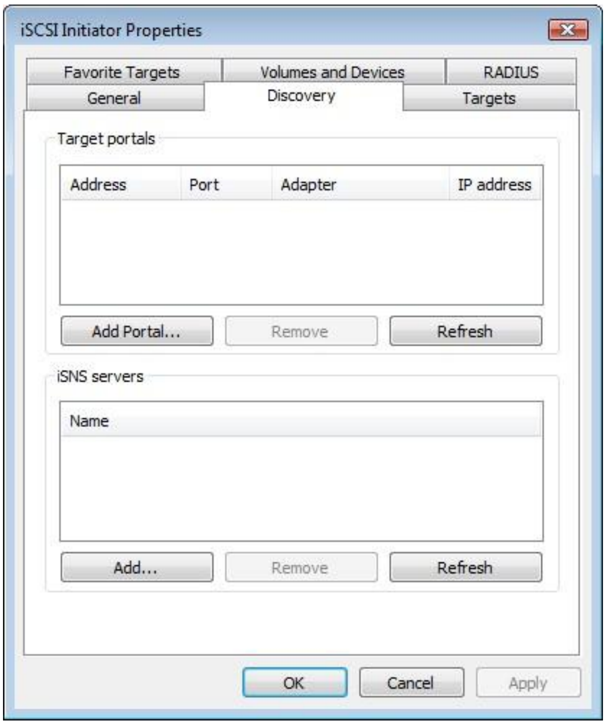
If you intend to use Mutual CHAP authentication you must enter the Initiator secret on this page.
Click on the secret button and a window should be displayed



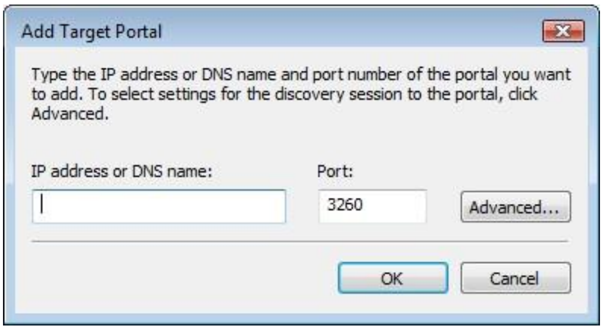
Type a CHAP secret to be used to authenticate (verify) targets. The most secure CHAP secrets are not words and phrases, but a random sequence of characters. Enter this same CHAP secret on the target so that the initiator can connect.

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



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



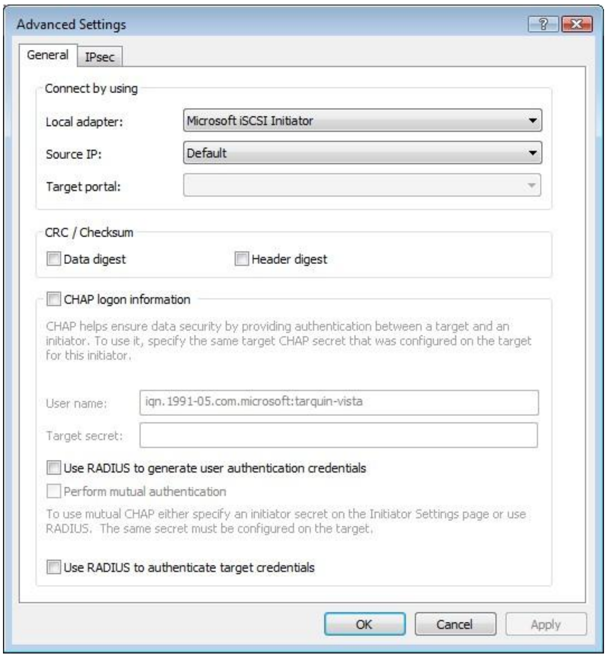
Add Target Portal

Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.

IP address or DNS name:

Port: 3260

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.



Advanced Settings

Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: Default

Target portal:

CRC / Checksum

□ Data digest □ Header digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: iqn.1991-05.com.microsoft:tarquin-vista

Target secret:

□ Use RADIUS to generate user authentication credentials

□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS 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.

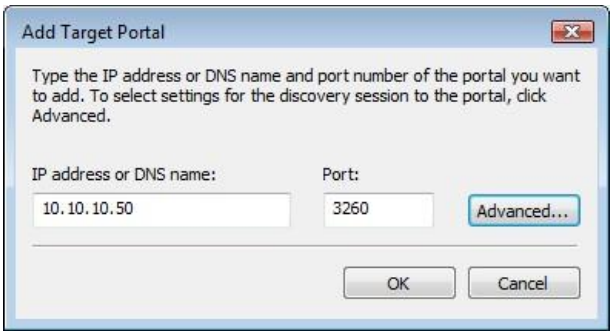
The Source IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the Server and the user wishes to select a particular interface, select the IP-address of that network interface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



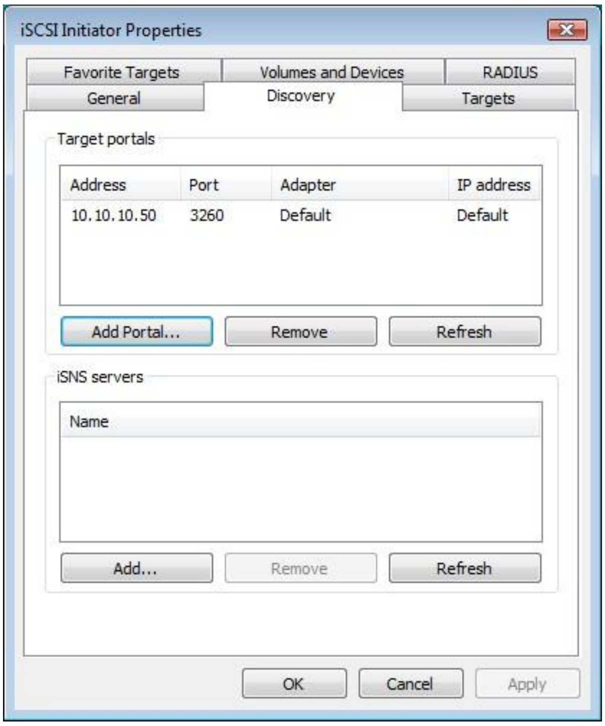
Add Target Portal

Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.

IP address or DNS name: 10.10.10.50

Port: 3260

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.
.

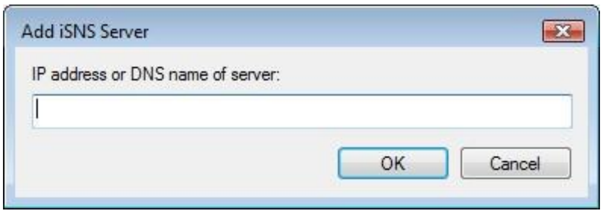


iSCSI Initiator Properties

Target portals

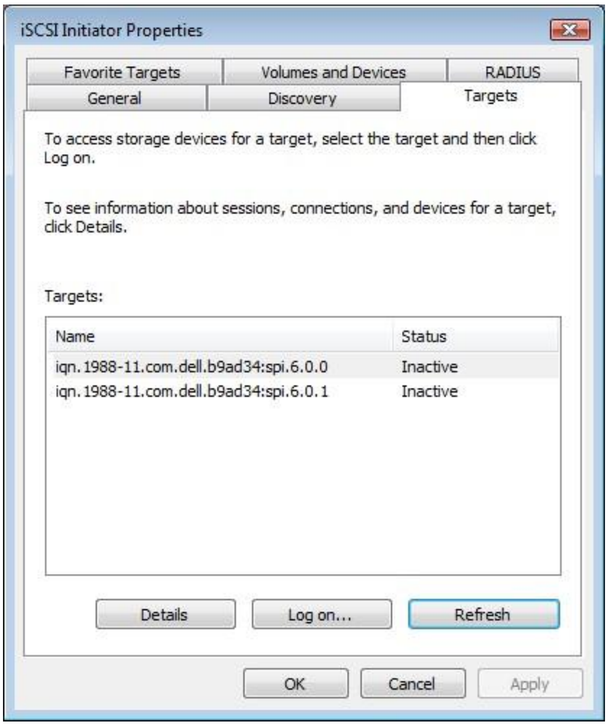
Address	Port	Adapter	IP address
10.10.10.50	3260	Default	Default

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



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



To access storage devices for a target, select the target and then click Log on.

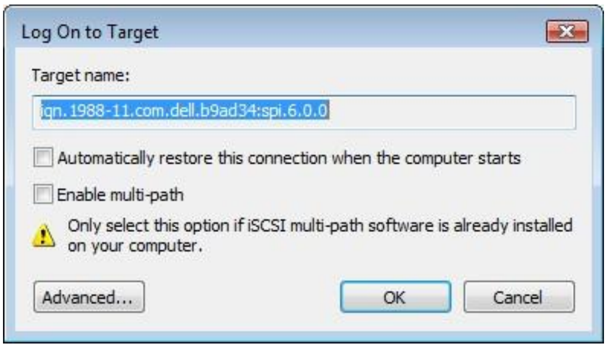
To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status
iqn.1988-11.com.dell.b9ad34:spi.6.0.0	Inactive
iqn.1988-11.com.dell.b9ad34:spi.6.0.1	Inactive

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.



Log On to Target

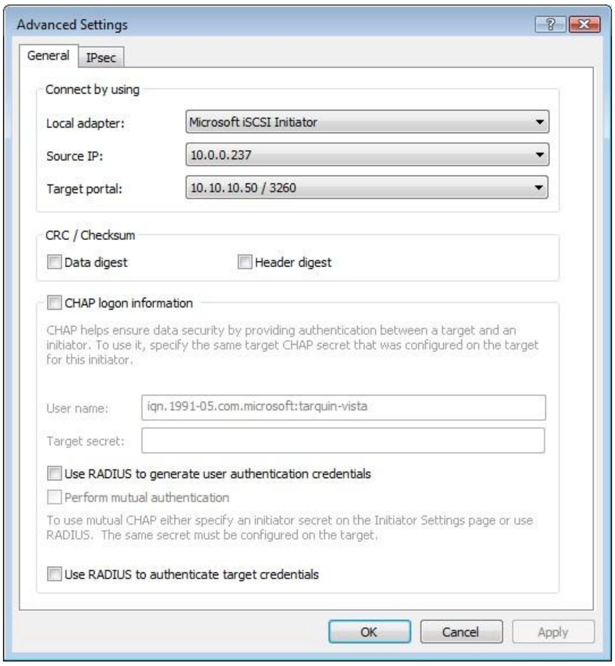
Target name: iqn.1988-11.com.dell.b9ad34:spi.6.0.0

□ Automatically restore this connection when the computer starts

□ Enable multi-path

Only select this option if iSCSI multi-path software is already installed on your computer.

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.



Advanced Settings

Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: 10.0.0.237

Target portal: 10.10.10.50 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: iqn.1991-05.com.microsoft:tarquin-vista

Target secret:

□ Use RADIUS to generate user authentication credentials

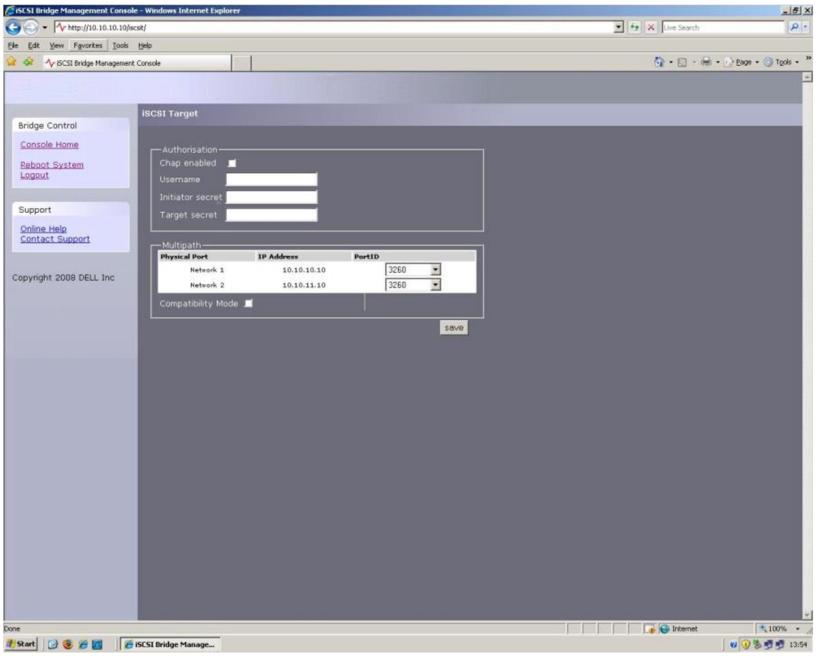
□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS to authenticate target credentials

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

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



iSCSI Bridge Management Console - Windows Internet Explorer
http://10.10.10.10/iscsit/
File Edit View Favorites Tools Help
iSCSI Bridge Management Console
Bridge Control
Console Home
Reboot System
Logout
Support
Online Help
Contact Support
Copyright 2008 DELL Inc
save

iSCSI Target

Authorisation

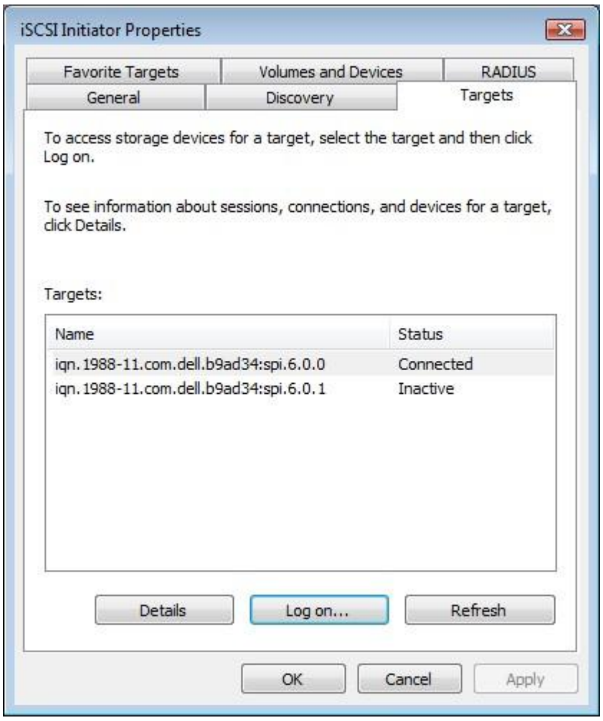
- Chap enabled □
- Username
- Initiator secret
- Target secret

Multipath

Physical Port	IP Address	PortID
Network 1	10.10.10.10	3260
Network 2	10.10.11.10	3260

Compatibility Mode □

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.



To access storage devices for a target, select the target and then click Log on.

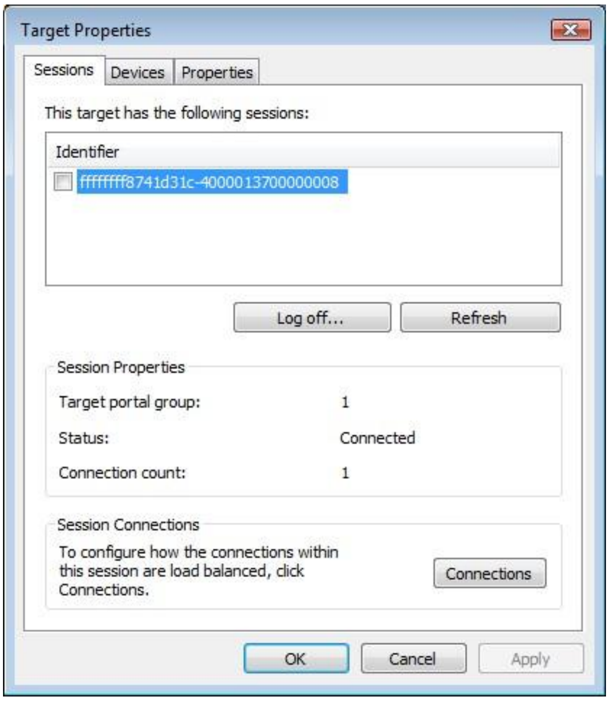
To see information about sessions, connections, and devices for a target, click Details.

Targets:

Name	Status
iqn.1988-11.com.dell.b9ad34:spi.6.0.0	Connected
iqn.1988-11.com.dell.b9ad34:spi.6.0.1	Inactive

Step 4 – Viewing iSCSI Session Details

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



This target has the following sessions:

Identifier
□ ffffffff8741d31c-4000013700000008

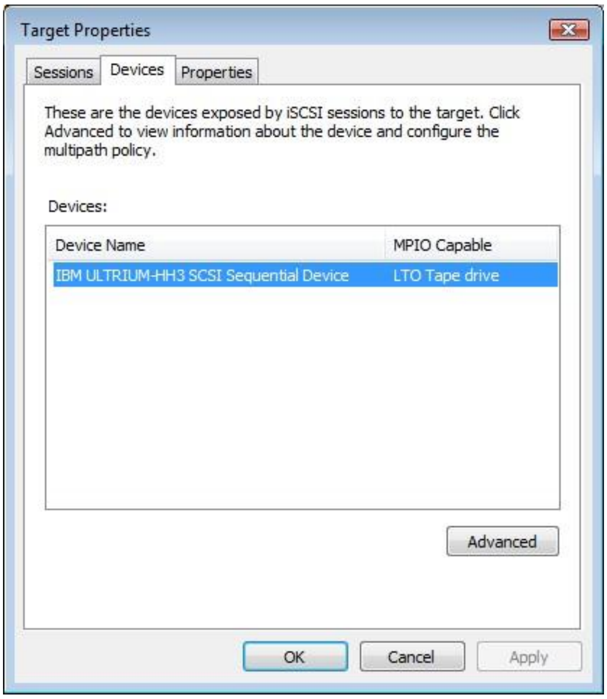
Session Properties

Target portal group:	1
Status:	Connected
Connection count:	1

Session Connections

To configure how the connections within this session are load balanced, click 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.

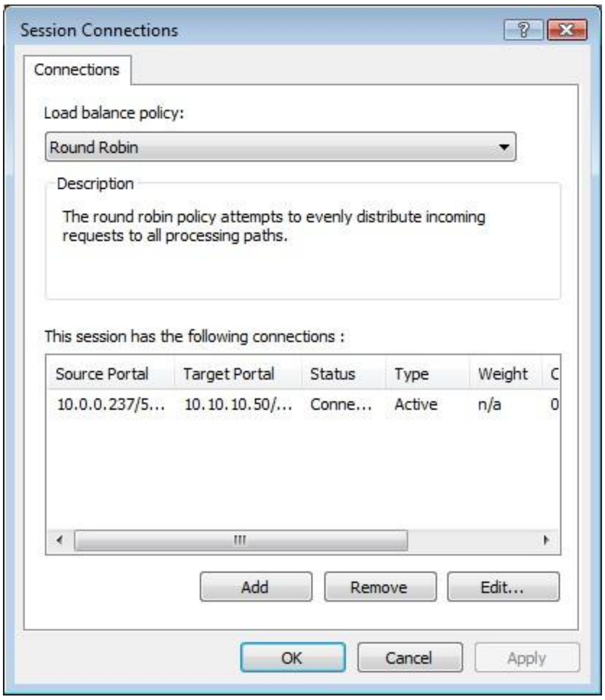


These are the devices exposed by iSCSI sessions to the target. Click Advanced to view information about the device and configure the multipath policy.

Devices:

Device Name	MPIO Capable
IBM ULTRIUM-HH3 SCSI Sequential Device	LTO Tape drive

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.



Load balance policy: Round Robin

Description

The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections :

Source Portal	Target Portal	Status	Type	Weight	C
10.0.0.237/5...	10.10.10.50/...	Conne...	Active	n/a	0

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'.

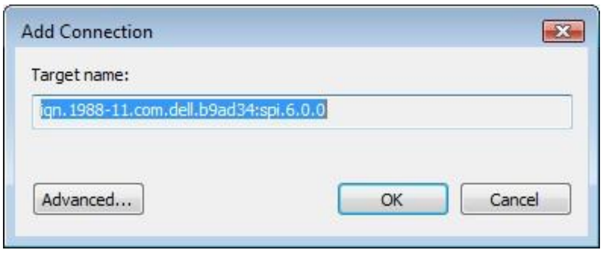
Round Robin will utilize all connections for data and evenly distribute the data.

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.

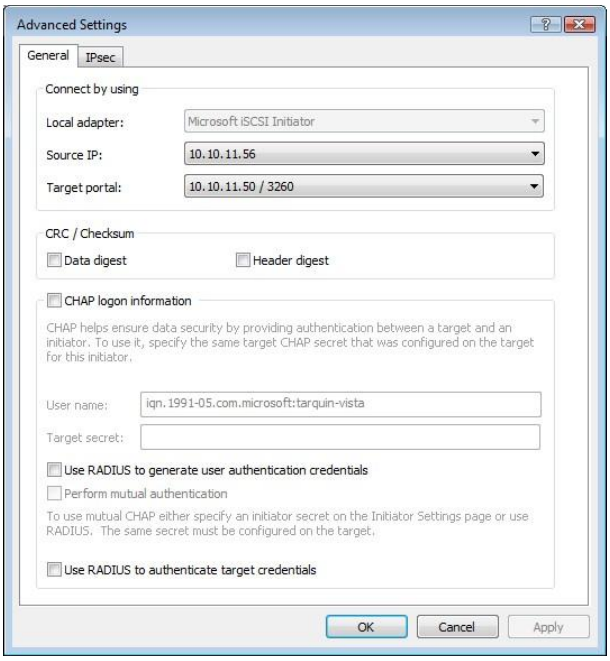
If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

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



Target name: iqn.1988-11.com.dell.b9ad34:spi.6.0.0

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



Connect by using

Local adapter: Microsoft iSCSI Initiator

Source IP: 10.10.11.56

Target portal: 10.10.11.50 / 3260

CRC / Checksum

□ Data digest □ Header digest

□ CHAP logon information

CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.

User name: iqn.1991-05.com.microsoft:tarquin-vista

Target secret:

□ Use RADIUS to generate user authentication credentials

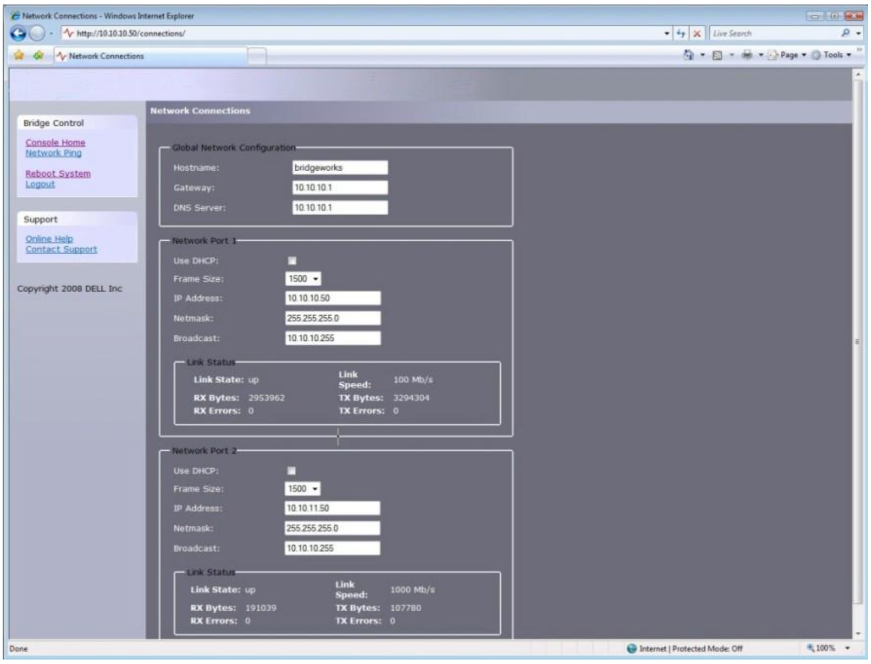
□ Perform mutual authentication

To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.

□ Use RADIUS to authenticate target credentials

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

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



Copyright 2008 DELL Inc

Network Connections

Global Network Configuration

Hostname: bridgeworks

Gateway: 10.10.10.1

DNS Server: 10.10.10.1

Network Port 1

Use DHCP: □

Frame Size: 1500

IP Address: 10.10.10.50

Netmask: 255.255.255.0

Broadcast: 10.10.10.255

Link Status

Link State: up **Link Speed:** 100 Mb/s

RX Bytes: 2953962 **TX Bytes:** 3294304

RX Errors: 0 **TX Errors:** 0

Network Port 2

Use DHCP: □

Frame Size: 1500

IP Address: 10.10.11.50

Netmask: 255.255.255.0

Broadcast: 10.10.10.255

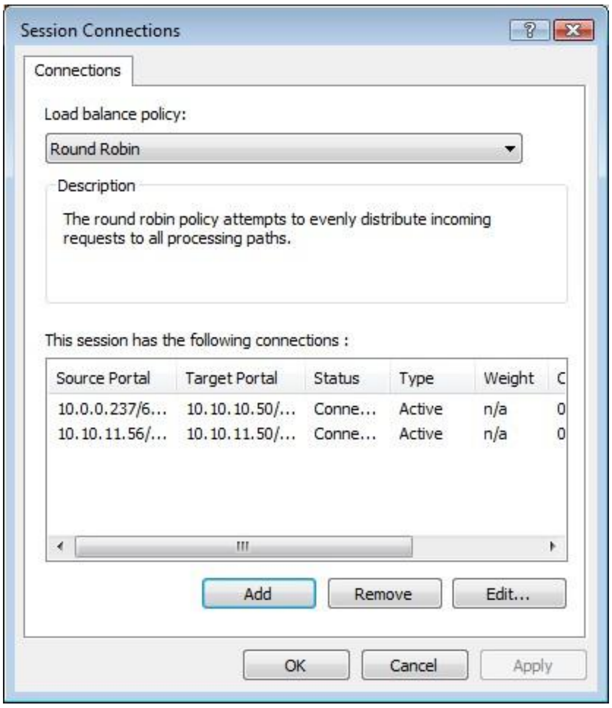
Link Status

Link State: up **Link Speed:** 1000 Mb/s

RX Bytes: 191039 **TX Bytes:** 107780

RX Errors: 0 **TX Errors:** 0

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



Load balance policy: Round Robin

Description

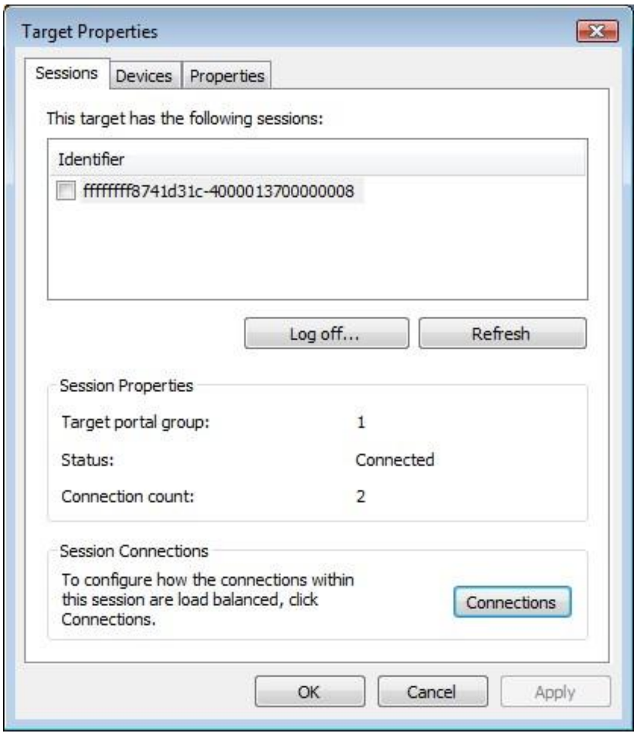
The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections :

Source Portal	Target Portal	Status	Type	Weight	C
10.0.0.237/6...	10.10.10.50/...	Conne...	Active	n/a	0
10.10.11.56/...	10.10.11.50/...	Conne...	Active	n/a	0

.

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.



This target has the following sessions:

Identifier
□ ffffffff8741d31c-4000013700000008

Session Properties

Target portal group: 1

Status: Connected

Connection count: 2

Session Connections

To configure how the connections within this session are load balanced, click Connections.

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

Step 6 – Logging off an iSCSI Session

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

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

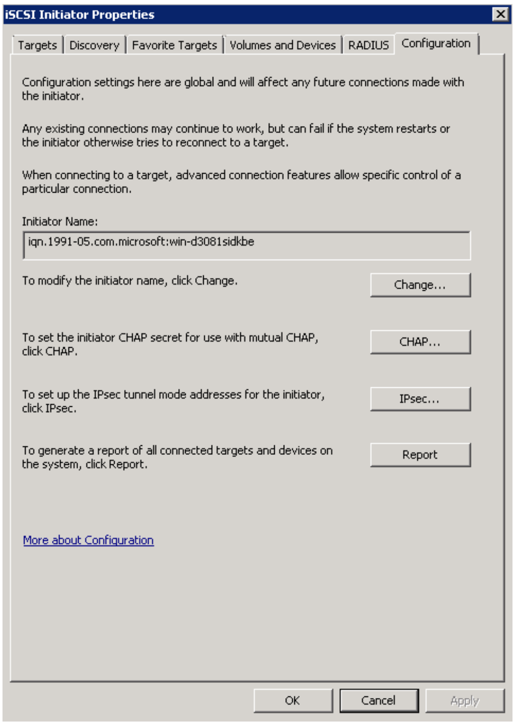
The session identifier should now be removed from the identifier list. Click ok to return to the main iSCSI Initiator window. The iSCSI device should now show as inactive.

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

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

Step 1 – General Set up

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



Configuration settings here are global and will affect any future connections made with the initiator.

Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.

When connecting to a target, advanced connection features allow specific control of a particular connection.

Initiator Name:
iqn.1991-05.com.microsoft:win-d3081sidkbe

To modify the initiator name, click Change.

To set the initiator CHAP secret for use with mutual CHAP, click CHAP.

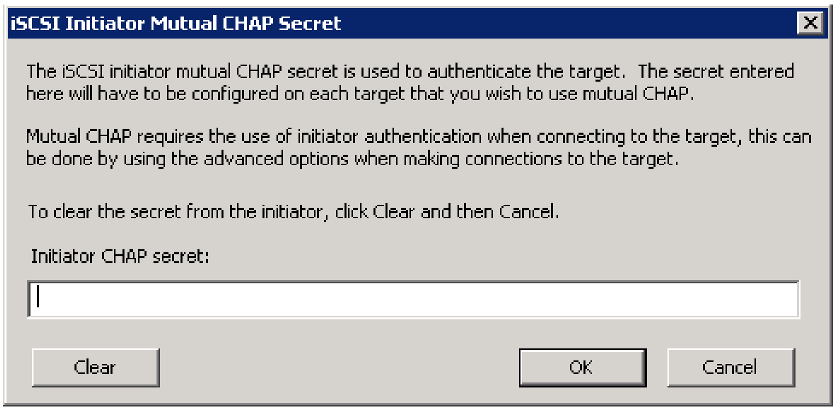
To set up the IPsec tunnel mode addresses for the initiator, click IPsec.

To generate a report of all connected targets and devices on the system, click Report.

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



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.

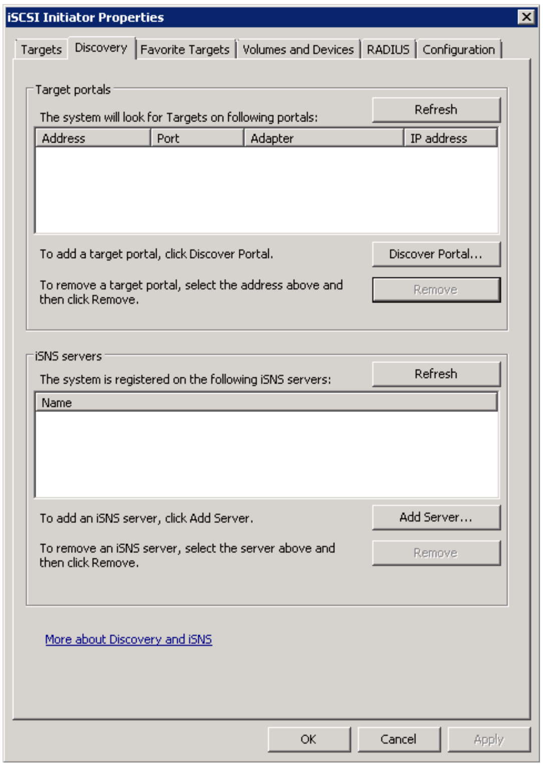
Mutual CHAP requires the use of initiator authentication when connecting to the target, this can be done by using the advanced options when making connections to the target.

To clear the secret from the initiator, click Clear and then Cancel.

Initiator CHAP secret:

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 look for Targets on following portals:

To add a target portal, click Discover Portal.

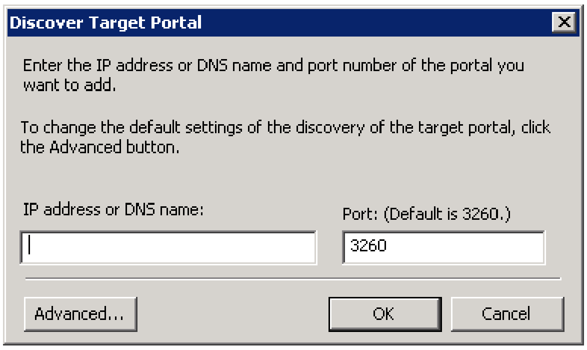
To remove a target portal, select the address above and then click Remove.

The system is registered on the following iSNS servers:

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click 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 port number of the portal you want to add.

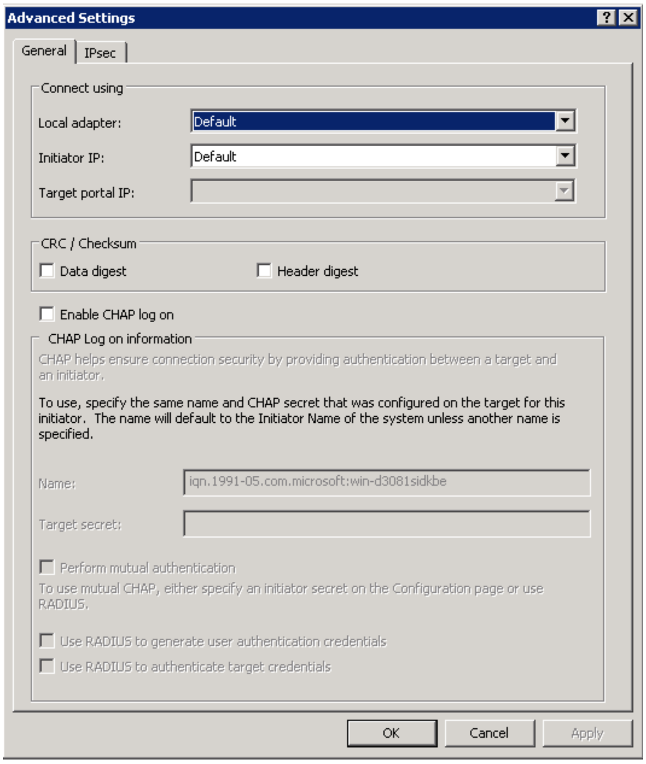
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name:

Port: (Default is 3260.) 3260

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.



Advanced Settings

Connect using

Local adapter: Default

Initiator IP: Default

Target portal IP:

CRC / Checksum

□ Data digest □ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

Target secret:

□ Perform mutual authentication

To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate 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.

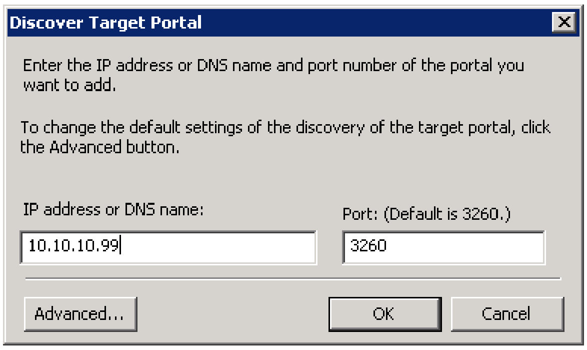
CRC/Checksum settings allow the user to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

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.



Enter the IP address or DNS name and port number of the portal you want to add.

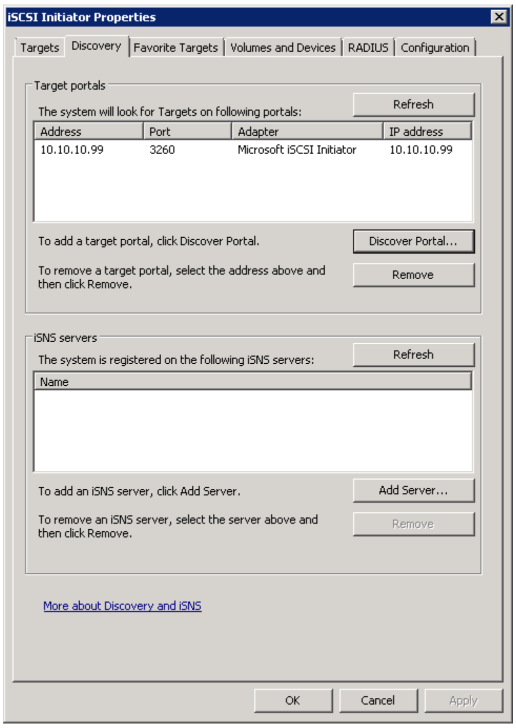
To change the default settings of the discovery of the target portal, click the Advanced button.

IP address or DNS name: 10.10.10.99

Port: (Default is 3260.) 3260

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.



The system will look for Targets on following portals:

Address	Port	Adapter	IP address
10.10.10.99	3260	Microsoft iSCSI Initiator	10.10.10.99

To add a target portal, click Discover Portal.

To remove a target portal, select the address above and then click Remove.

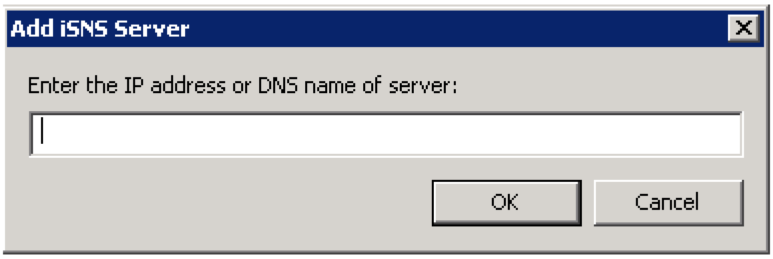
The system is registered on the following iSNS servers:

Name

To add an iSNS server, click Add Server.

To remove an iSNS server, select the server above and then click Remove.

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

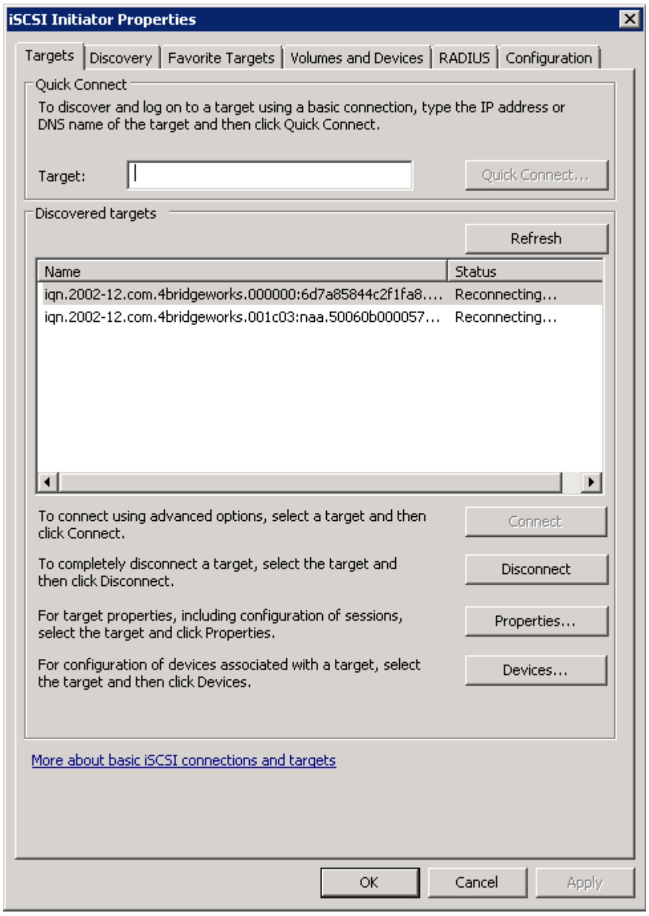


Add iSNS Server

Enter the IP address or DNS name of server:

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



iSCSI Initiator Properties

Quick Connect

To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Target:

Discovered targets

Name	Status
iqn.2002-12.com.4bridgeworks.000000:6d7a85844c2f1fa8....	Reconnecting...
iqn.2002-12.com.4bridgeworks.001c03:naa.50060b000057...	Reconnecting...

To connect using advanced options, select a target and then click Connect.

To completely disconnect a target, select the target and then click Disconnect.

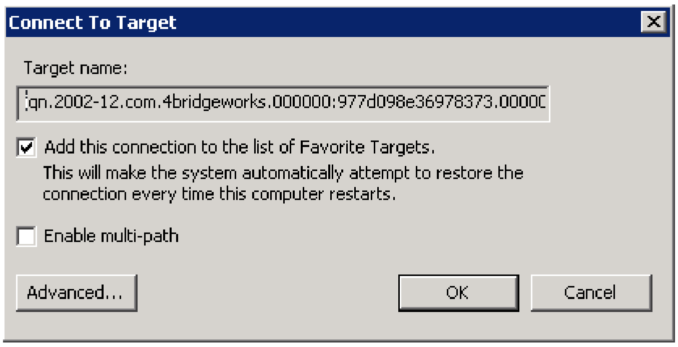
For target properties, including configuration of sessions, select the target and click Properties.

For configuration of devices associated with a target, select the target and then click Devices.

More about basic iSCSI connections and targets

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.

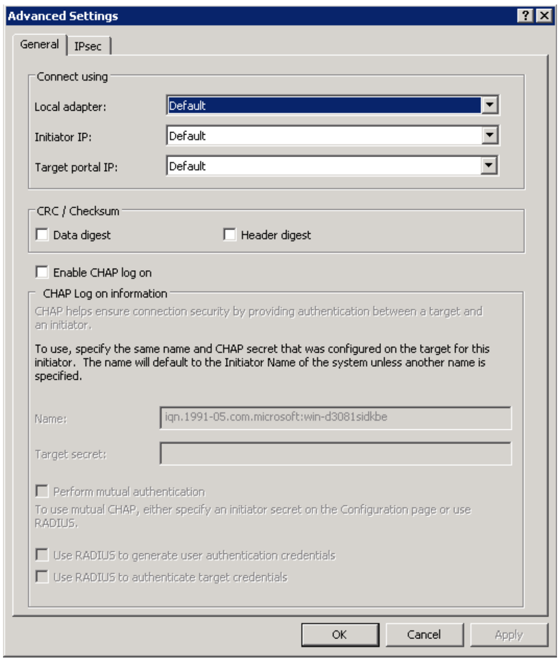


Target name:
iqn.2002-12.com.4bridgeworks.000000:977d098e36978373.0000C

☑ Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.

□ Enable multi-path

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.



Connect using
Local adapter: Default
Initiator IP: Default
Target portal IP: Default

CRC / Checksum
□ Data digest □ Header digest

□ Enable CHAP log on
CHAP Log on information
CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

Target secret:

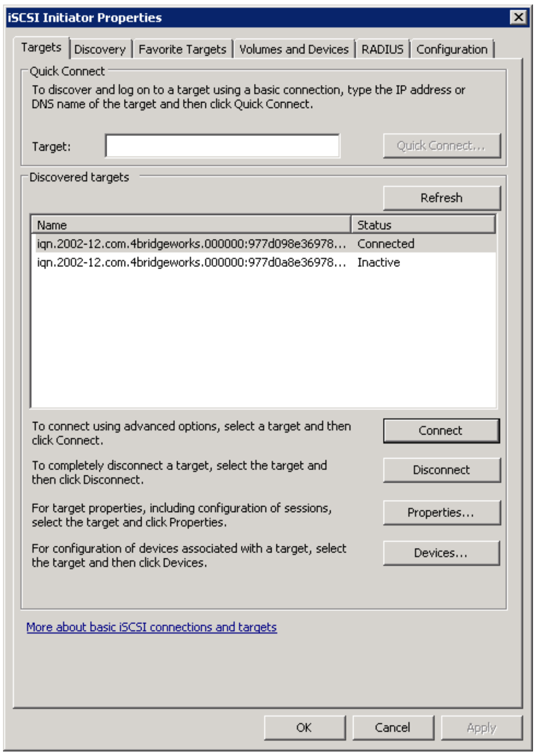
□ Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials
□ Use RADIUS to authenticate 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.



To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

Name	Status
iqn.2002-12.com.4bridgeworks.000000:977d098e36978...	Connected
iqn.2002-12.com.4bridgeworks.000000:977d0a8e36978...	Inactive

To connect using advanced options, select a target and then click Connect.

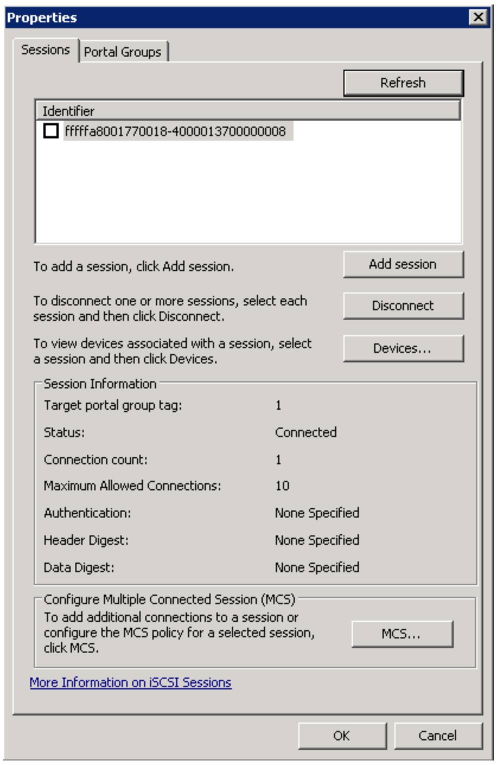
To completely disconnect a target, select the target and then click Disconnect.

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.

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.



Identifier

☐ ffffa8001770018-4000013700000008

To add a session, click Add session.

To disconnect one or more sessions, select each session and then click Disconnect.

To view devices associated with a session, select a session and then click Devices.

Session Information

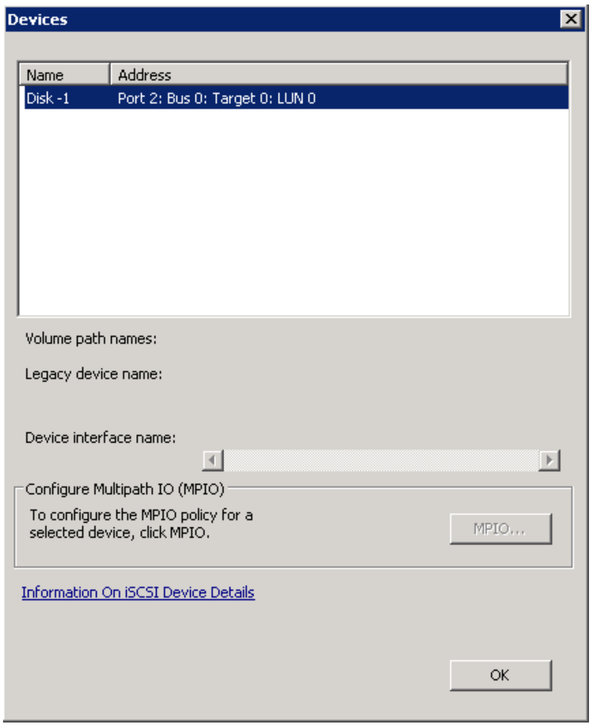
Target portal group tag:	1
Status:	Connected
Connection count:	1
Maximum Allowed Connections:	10
Authentication:	None Specified
Header Digest:	None Specified
Data Digest:	None Specified

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

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.



Name	Address
Disk -1	Port 2: Bus 0: Target 0: LUN 0

Volume path names:

Legacy device name:

Device interface name:

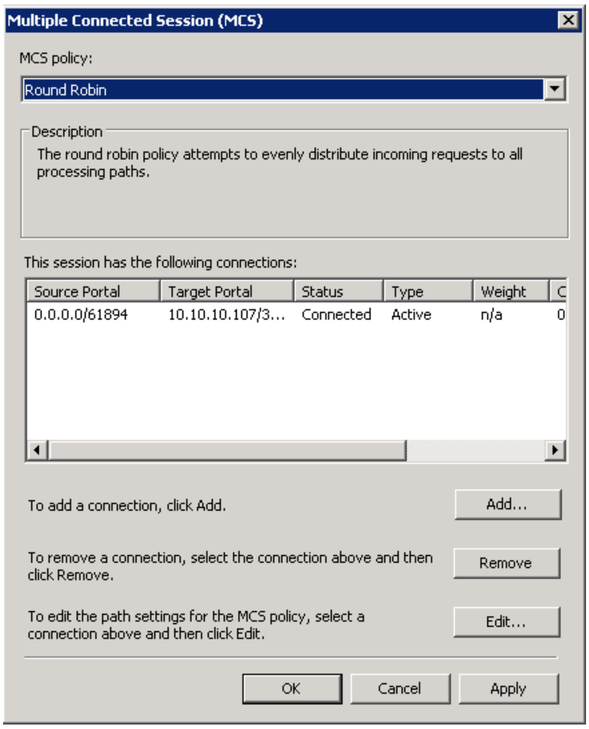
Configure Multipath IO (MPIO)

To configure the MPIO policy for a selected device, click MPIO.

Information On iSCSI Device Details

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.



MCS policy: Round Robin

Description
The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections:

Source Portal	Target Portal	Status	Type	Weight	C
0.0.0.0/61894	10.10.10.107/3...	Connected	Active	n/a	0

To add a connection, click Add.

To remove a connection, select the connection above and then click Remove.

To edit the path settings for the MCS policy, select a connection above and then click Edit.

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'.

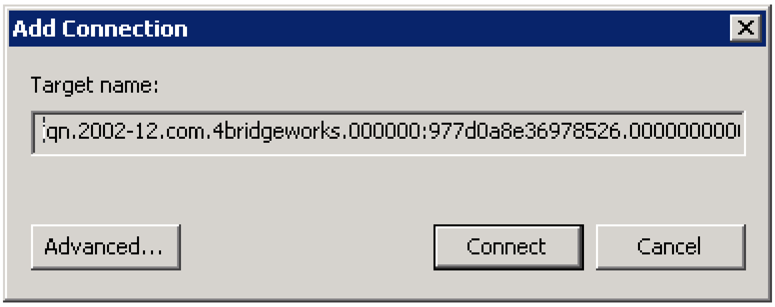
Round Robin will utilize all connections for data and evenly distribute the data.

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.

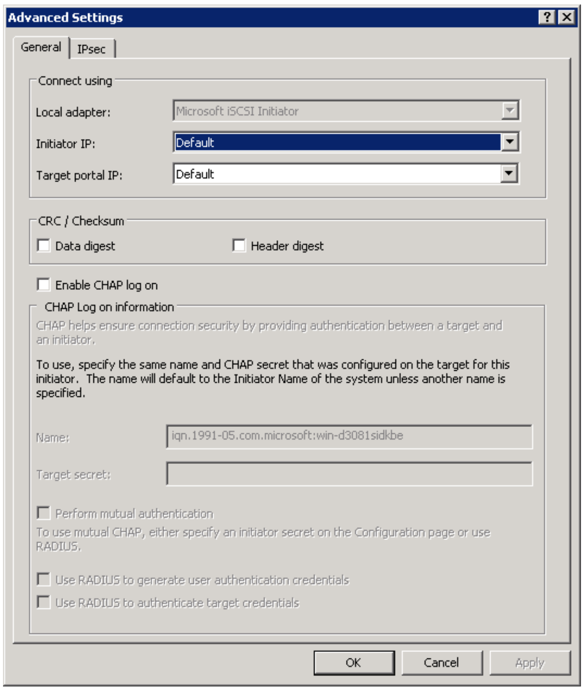


Add Connection

Target name:

iqn.2002-12.com.4bridgeworks.000000:977d0a8e36978526.000000000

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



Advanced Settings

Connect using

Local adapter: Microsoft iSCSI Initiator

Initiator IP: Default

Target portal IP: Default

CRC / Checksum

□ Data digest

□ Header digest

□ Enable CHAP log on

CHAP Log on information

CHAP helps ensure connection security by providing authentication between a target and an initiator.

To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.

Name: iqn.1991-05.com.microsoft:win-d3081sidkbe

Target secret:

□ Perform mutual authentication

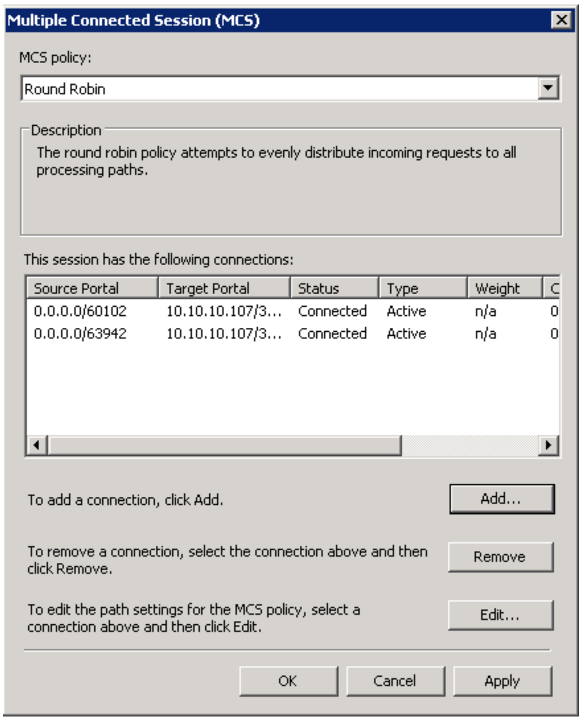
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.

□ Use RADIUS to generate user authentication credentials

□ Use RADIUS to authenticate target credentials

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.



Multiple Connected Session (MCS)

MCS policy: Round Robin

Description

The round robin policy attempts to evenly distribute incoming requests to all processing paths.

This session has the following connections:

Source Portal	Target Portal	Status	Type	Weight	C
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

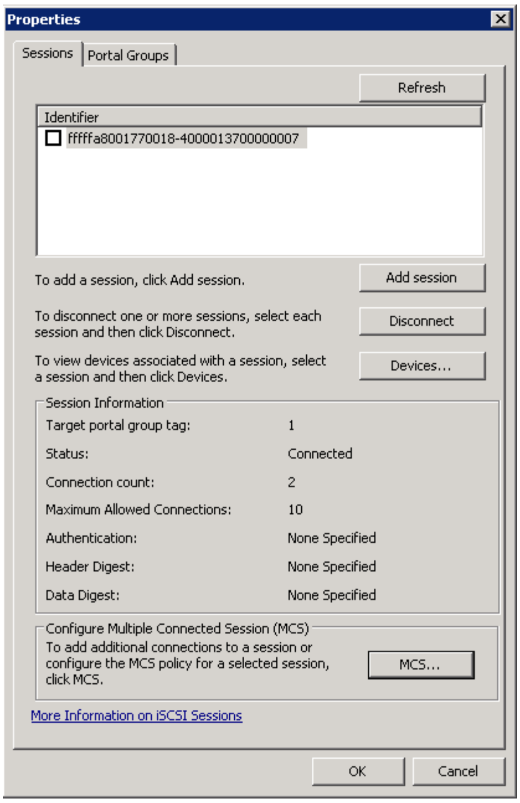
To add a connection, click Add.

To remove a connection, select the connection above and then click Remove.

To edit the path settings for the MCS policy, select a connection above and then click Edit.

The user can add up to 10 different connections.

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



Properties

Identifier

□ ffffa8001770018-4000013700000007

To add a session, click Add session.

To disconnect one or more sessions, select each session and then click Disconnect.

To view devices associated with a session, select a session and then click Devices.

Session Information

Target portal group tag:	1
Status:	Connected
Connection count:	2
Maximum Allowed Connections:	10
Authentication:	None Specified
Header Digest:	None Specified
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

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

Step 6 – Logging off an iSCSI Session

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

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

The iSCSI device should now show as inactive.

Appendix C Removable Storage Service

The following only applies to Windows Server 2003.

You can use the Removable Storage service to temporarily disable an overflow of TUR requests. To do this, enable the service. Then, start and stop the service. This method stops the TUR requests until the computer is restarted or until the driver is changed.

Note: By default, the Removable Storage service is disabled.

To temporarily stop TUR requests, follow these steps:

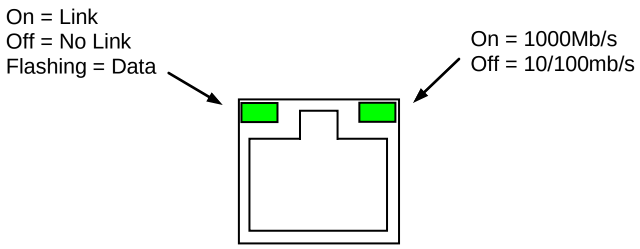
1. Click **Start**, type services.msc, and then click **OK**.
2. In the right pane, double-click **Removable Storage**.
3. In the **Startup type** list, click **Manual**, and then click **Apply**.
4. Click **Start**, and then click **Stop**.
5. In the **Startup type** list, click **Disabled**, and then click **OK**.

Further Information on this topic can be obtained from the Microsoft Website

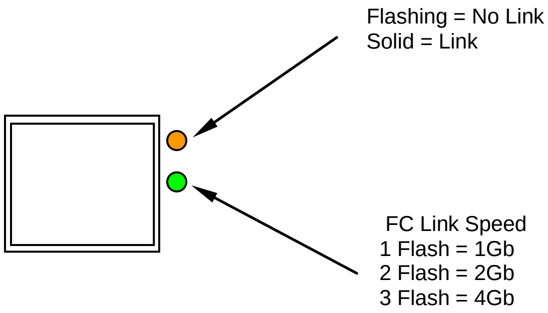
http://support.microsoft.com/kb/842411

Appendix D Visual Indicators

Ethernet



Fibre Channel

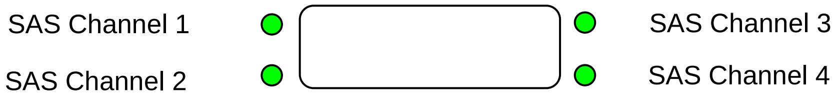


SAS

○ Solid Off – No link detected

● Solid On - Link detected, no activity

◐ Flashing - activity



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

Appendix E Technical Specifications

Physical	
Form Factor	19” 1U Rack mount
Depth	170mm (10.6 in)
Height	44mm (1.7 in)
Width	437mm (17.2 in)
Weight	5.1Kg
Recommended minimum clearance for cooling	100mm (4.in) on front and rear faces
Electrical	
Input voltage	110 - 240V
Frequency	50 - 60Hz
Input current	1 Amp Maximum
Maximum Power Consumption	60 Watts Maximum
Environmental	
Operating	0 to 40C (32F to 104F)
Non Operating	-20C to 60C (-4F to 140F)
Operating Humidity	5% to 90% Non-condensing
Storage Humidity	5% to 90% Non-condensing
Operating Altitude	3,000m (9,842ft)
Non Operating Altitude	8,000m (26,250ft)
Fibre Channel Interface	
Physical Interface	2 SFP connectors
Speed	4Gb, 2Gb, 1Gb Auto or manual selected
Protocol	FC-AL, FC-PLDA, FC-PH, FC-FLA, FCP-SCSI, FC-FS, FC-TAPE
Topology	NL-Port, FL_Port, F_Port, N_Port
Visual Indicators	Link connection, Link Speed
iSCSI Interface	
Physical	***RJ 45***
Speed	10, 100, 1000 Mb/s
Protocol	IPv4, IPv6, CHAP, DHCP, NTP, iSNS
iSCSI Protocol	iSCSI RFC3270, 3721, ERL0, ERL1 ERL2
Visual Indicators	Link, Activity
SAS Interface	
Physical	2x SFF – 8088 External mini-SAS

Speed	1.5Gb/s and 3Gb/s
Protocol	SAS 2.0
Visual Indicators	Link, Activity