



Jon Tate
Michael Engelbrecht

Implementing the SAN10Q-2

For less complex SAN environments, with fewer servers and storage arrays, a single switch or dual cascaded switches offer redundancy and performance with minimal administration and lower cost than larger directors. One option for these smaller infrastructures is an entry-level switch such as the IBM® TotalStorage® Storage Switch SAN10Q-2, which offers edge switch capability with full 4 Gbps port speed.

Note: The SAN10Q-2 also has a command-line interface (CLI). In this chapter we use the GUI to perform our implementation. For details of the CLI, refer to *System Storage SAN10Q 4 Gbps 10-Port Fibre Channel SwitchType 6918 User's Guide*, 31R1632.

Introducing IBM TotalStorage Switch SAN10Q-2

IBM TotalStorage Storage Switch SAN10Q-2 is an affordable, capable, and extremely easy to use, entry-level IBM System. The SAN10Q-2 is a one-half width, 1U rack height, ten-port 4-Gb switch, as shown in Figure 1. This switch provides the following features:

- ▶ Throughput of 1, 2, or 4 gigabits per second on all ports, short wave, and long wave
- ▶ Single E port support for the inclusion of another IBM System Storage™ SAN10Q-2 for redundancy or extension of SAN to larger fabric
- ▶ Hardware-enforced zoning that helps protect against non-secure, unauthorized, and unauthenticated network and management access and World Wide Name spoofing
- ▶ Hot-pluggable optical transceivers that can be replaced without taking switch offline
- ▶ All firmware included, and no additional license keys required
- ▶ Per-port buffering: ASIC-embedded memory (non-shared) and 8-credit zero wait for each port

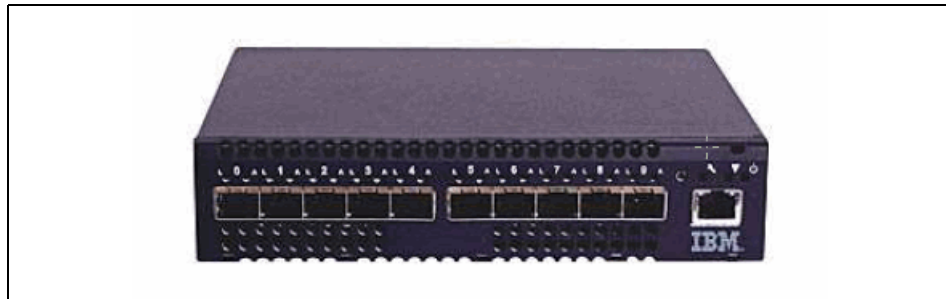


Figure 1 IBM TotalStorage Storage Switch SAN10Q-2

More option and pricing information about the TotalStorage Switch SAN10Q-2 can be found on the IBM storage Web site at:

http://www-03.ibm.com/servers/storage/san/q_type/san10q/

Installation

The items shown in Figure 2 all are supplied with the SAN10Q switch. The Support and Documentation CD contains all documentation and software required to install and set up the switch.

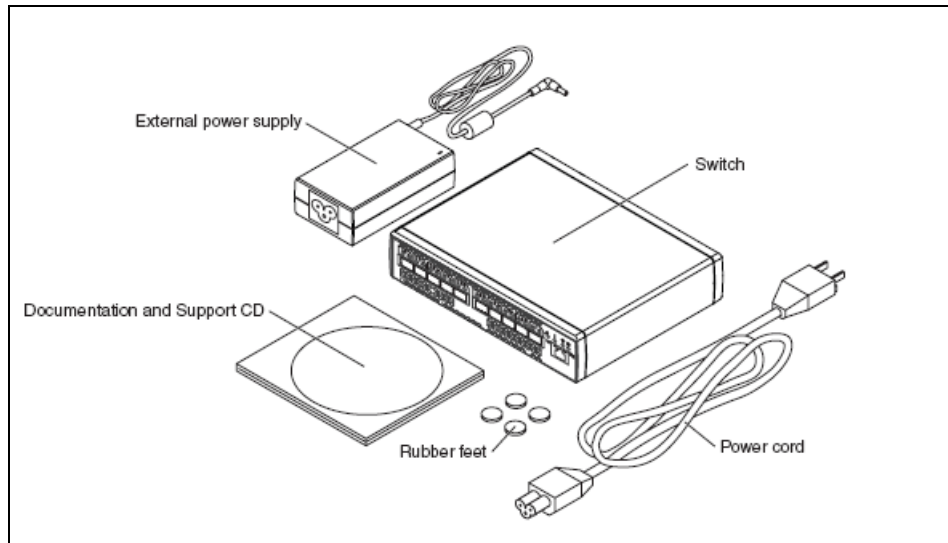


Figure 2 SAN10Q

Documentation

All documentation is on the supplied CD. In the following topics, we explain how to install the CD so that you can read the documentation.

Autostart is enabled by default on your CD drive. Upon insertion of the CD, you should see the display shown in Figure 3. If autostart is disabled on the workstation, click **Start** → **Run**, and at the C> prompt type `H:\win32.bat`, where *H* is the drive letter of the CD drive on this workstation.

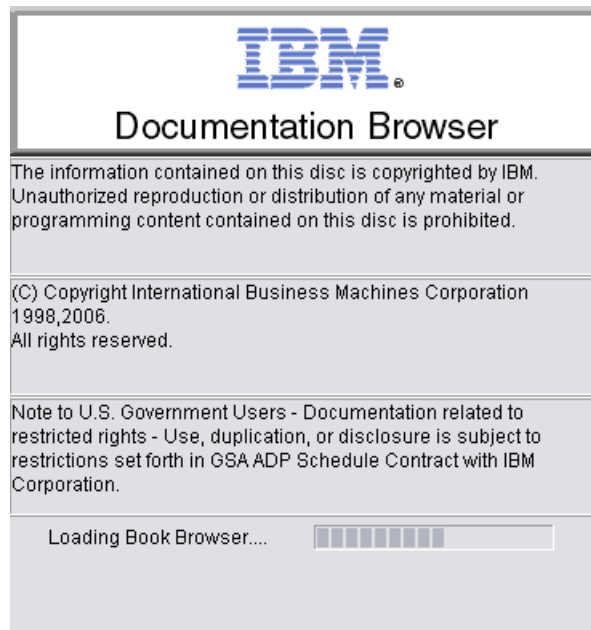


Figure 3 Document browser setup

If you do not have Acrobat® Reader V5, you must install Acrobat Reader now. When you receive the message shown in Figure 4, click the **Install** button.



Figure 4 Acrobat Installation warning

Note: If you have a later version of Acrobat, such as Version 5.1 or later, installed, you are still required to click the **Install** button to continue.

Click the **OK**, button, shown in Figure 5, to continue with the installation.

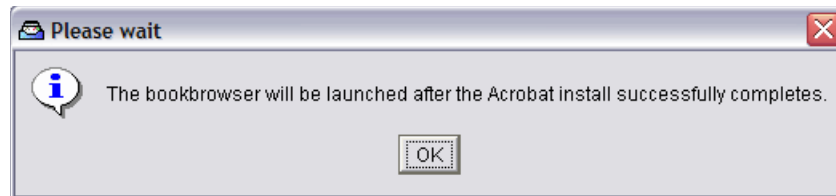


Figure 5 Status display

Next, as shown in Figure 6, you have to make the decision to either cancel the Acrobat install or continue it.



Figure 6 Acrobat installation window.

If you have Acrobat reader V5.1 or later already installed on your workstation, click the **Cancel** button now.

If you do not have Acrobat installed, or if you have a version earlier than V5.0, click the **Next** button and continue to install Acrobat.

When the installation of Acrobat is finished, or if you cancelled the installation of Acrobat, the Document Browser window displays, as shown in Figure 7. All documentation required for installation and operation can be accessed from this window.

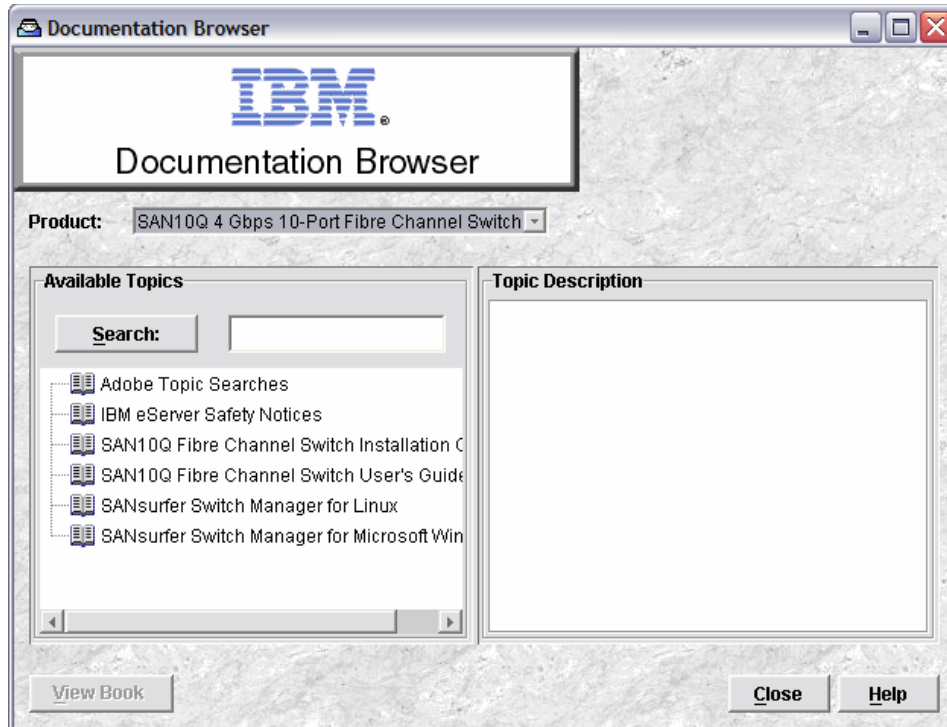


Figure 7 Document browser

Installing SANsurfer Switch Manager

In Table 1 we show the SANsurfer® workstation requirements.

Table 1 SANsurfer workstation requirements

Component	Requirements
Operating system	<ul style="list-style-type: none"> ▶ Microsoft® Windows® 2000, 2003, and Windows XP ▶ Red Hat Enterprise Linux® Version 3 or later ▶ SUSE Linux Enterprise Server 9.0
Memory	256 MB or more
Disk space	150 MB per installation
Processor	500 MHz or faster

Component	Requirements
Hardware	CD drive, RJ-45 Ethernet port
Internet browser	<ul style="list-style-type: none"> ▶ Microsoft Internet Explorer® 5.0 or later ▶ Netscape Navigator 4.72 or later ▶ Mozilla 1.02 or later ▶ Java™ 2 Run Time Environment to support the Web applet

Next we show an example of how to install the SANSurfer switch manager using a Windows XP operating system.

Explore the CD and from the root directory click the **SANSurfer Switch Manager** folder. Read the readme file and the release notes. From the Windows folder, double-click **Windows_5.00.1.05.exe**, as shown in Figure 8.

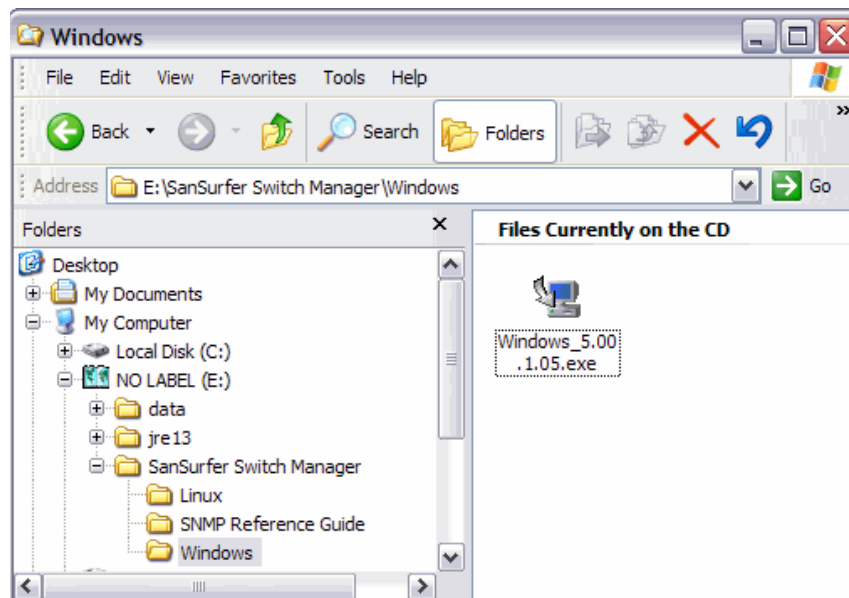


Figure 8 Switch Manager directory on CD

The install program now starts, and you see a progress window, as shown in Figure 9.

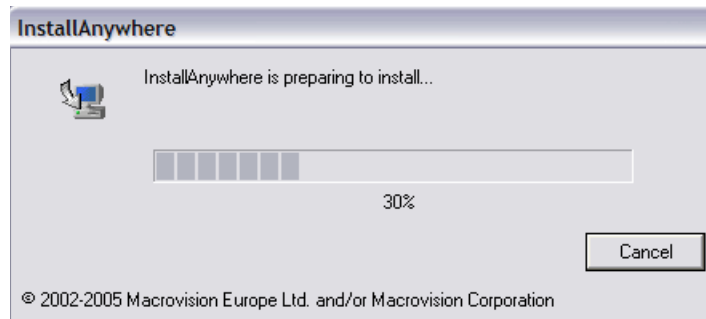


Figure 9 Preparing to install

Read the introduction window, shown in Figure 10, and click the **Next** button on this window.

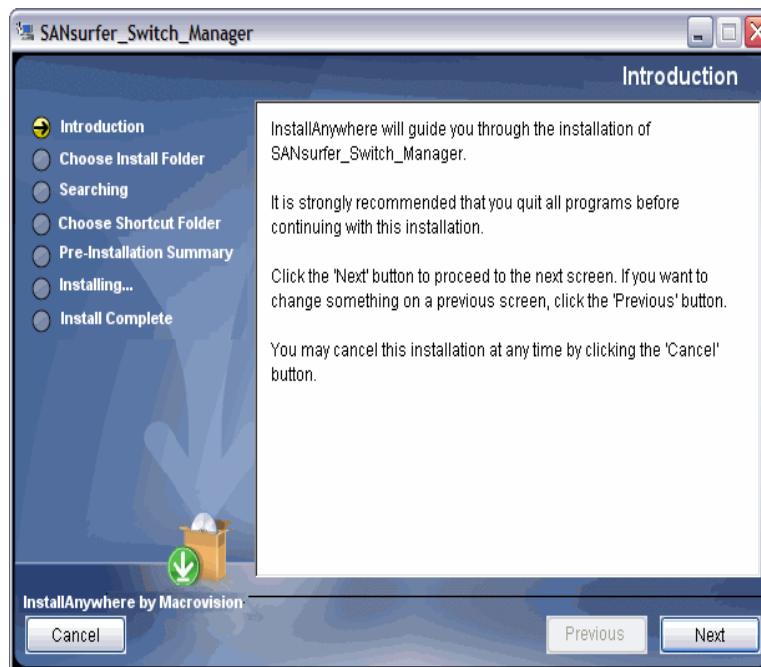


Figure 10 Switch Manager Introduction

Now choose the folder in which you wish to install Switch Manager, or select the default, and click the **Next** button, as shown in Figure 11.

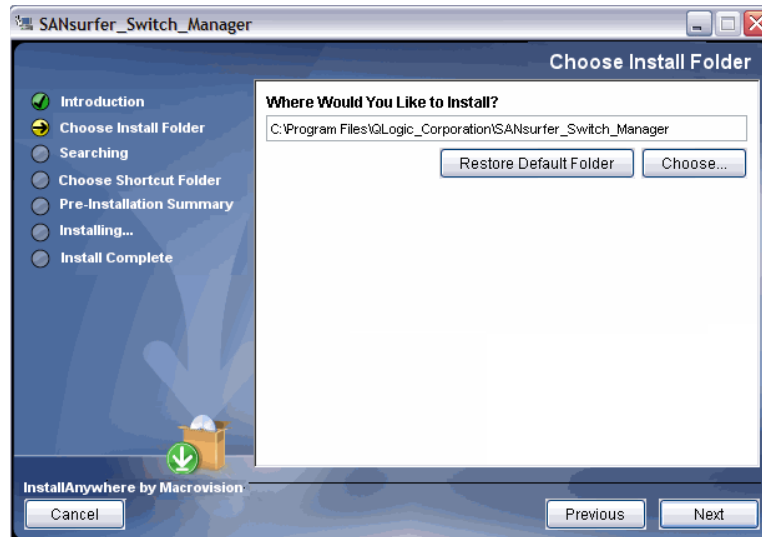


Figure 11 Switch Manager install folder

The install process now checks your installed software for compatibility, as shown in Figure 12.

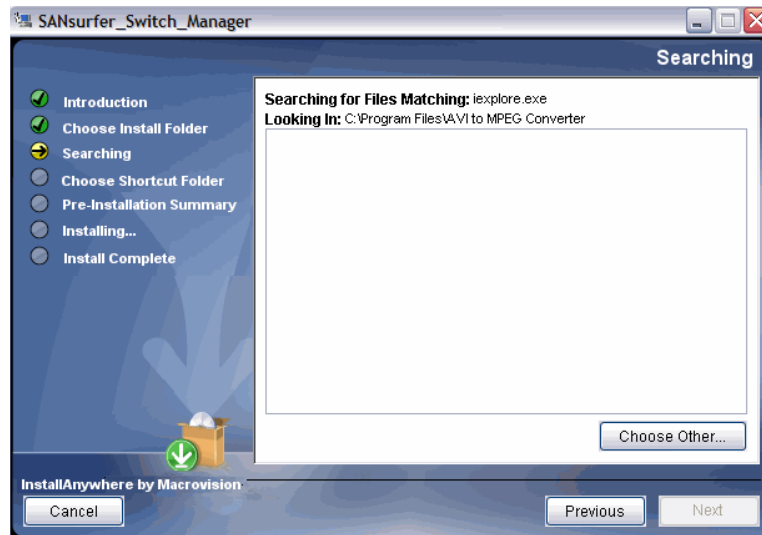


Figure 12 Checking software

You are now given the option of where to create the icon for Switch Manager, as shown in Figure 13. Select your option and click **Next**.

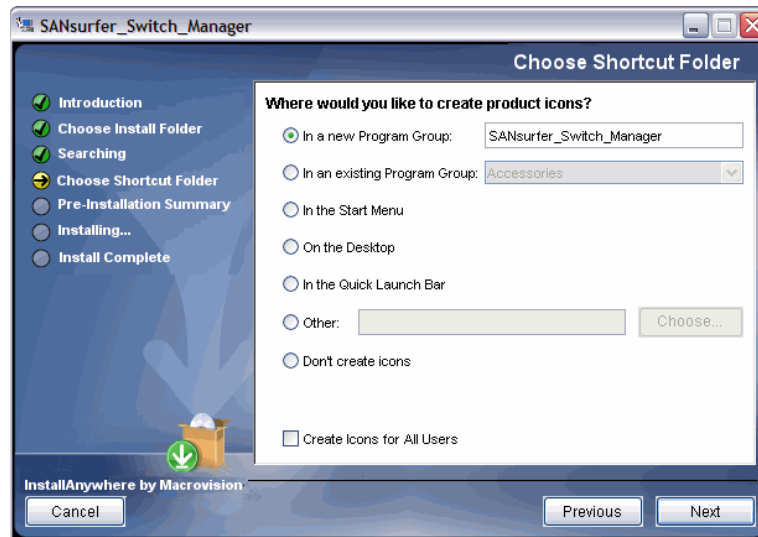


Figure 13 Selecting icon preference

You get to review details regarding the installation, shown in Figure 14. To continue, click **Install**.

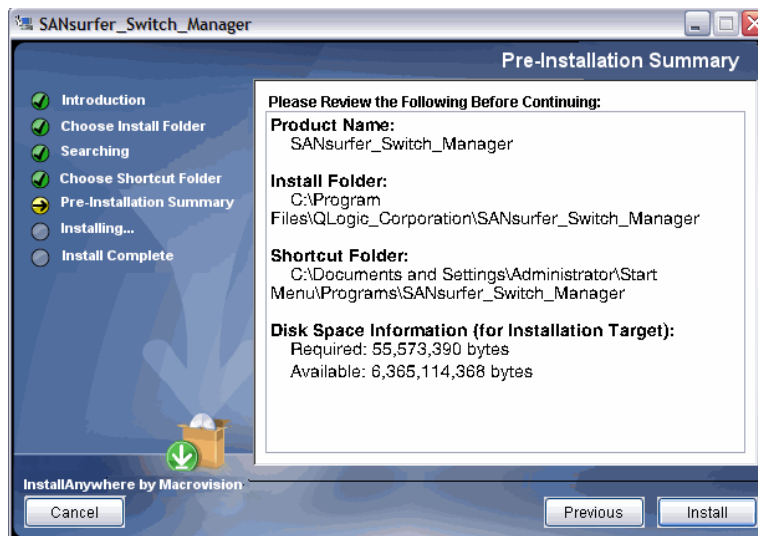


Figure 14 Installation review

SANsurfer Switch Manager is now being installed, as shown in the progress window shown in Figure 15. This takes a few minutes.

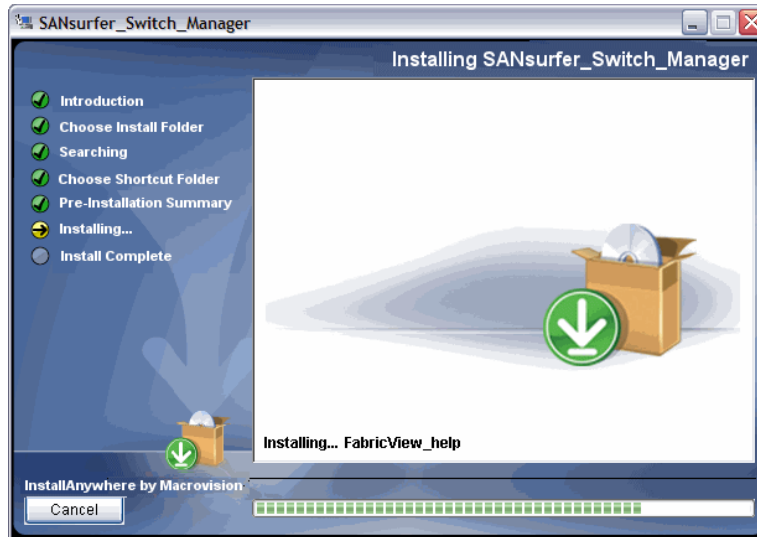


Figure 15 Switch Manager installation

Figure 16 shows that installation is complete.

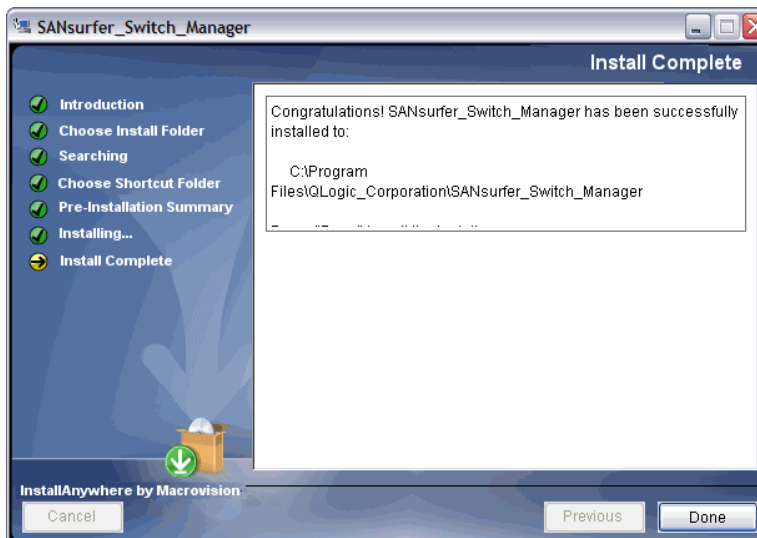


Figure 16 SANsurfer Switch Manager installation complete

This completes the installation of SANsurfer Switch Manager. You can launch this application from your Start Program menu or the icon on your desktop.

Installing the Fibre Channel switch

In this section we describe how to install the switch:

1. Connect the new switch to the external power supply, and plug in the line cord to the power supply.
2. Install either a standard RJ-45 Ethernet cable from the SAN10Q to the management network, or a cross-over RJ-45 Ethernet cable to your workstation where you have installed SANsurfer.
3. Obtain the IP address that you intend to use on the SAN10Q switch.
4. Make sure that your workstation's Ethernet port is set up in the same IP subnet as the required switch address.
5. Start SANsurfer Switch Manager on your workstation.

Start up SANsurfer using the icon on your desktop (Figure 17) or from your program list.

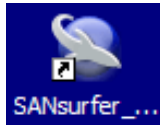


Figure 17 Start SANsurfer

From the Initial Start Dialog window (Figure 18) select the **Open Configuration Wizard** button and select **Proceed**.

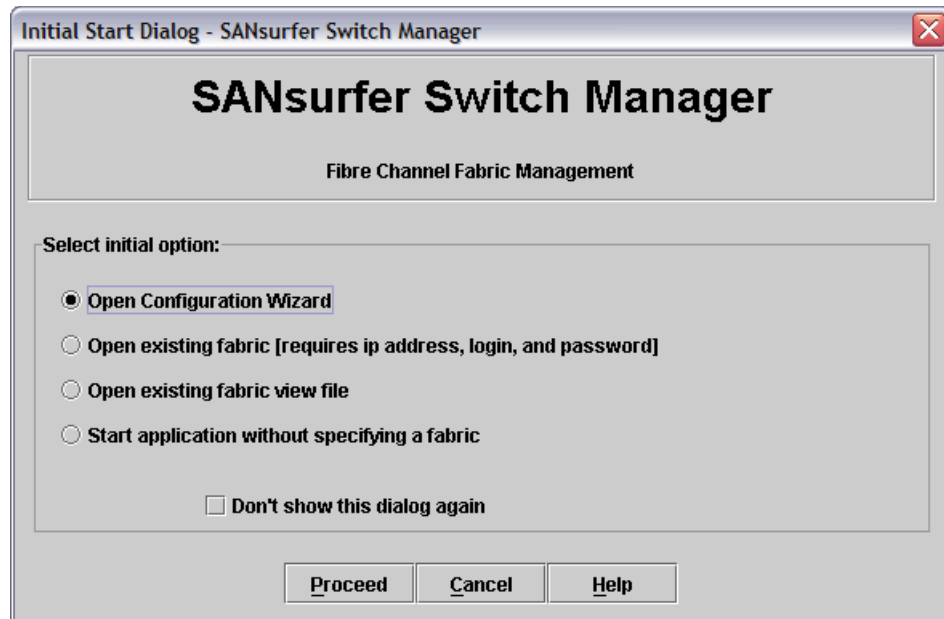


Figure 18 SANsurfer Initial Start Dialog window

Read the overview window (Figure 19) and select **Next**.

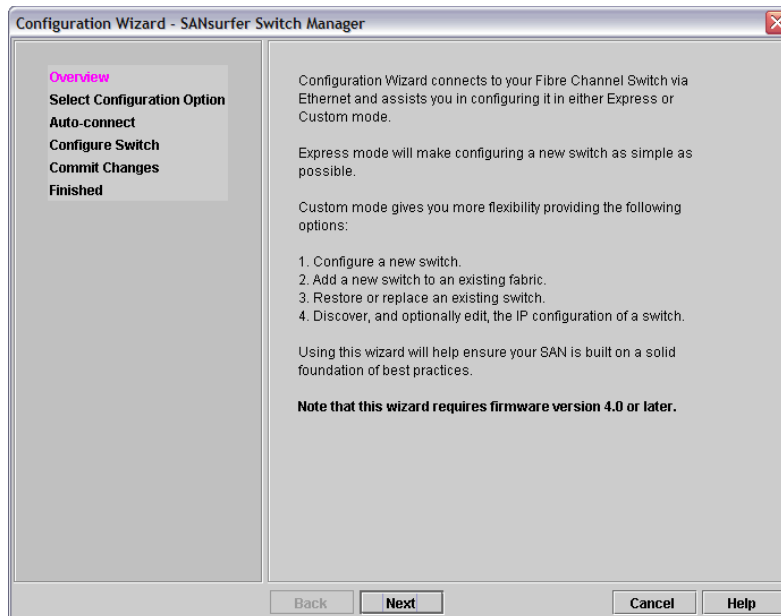


Figure 19 Configuration Wizard overview

Select the **Express** option from the Select Configuration Option window (Figure 20) and then select **Next**.

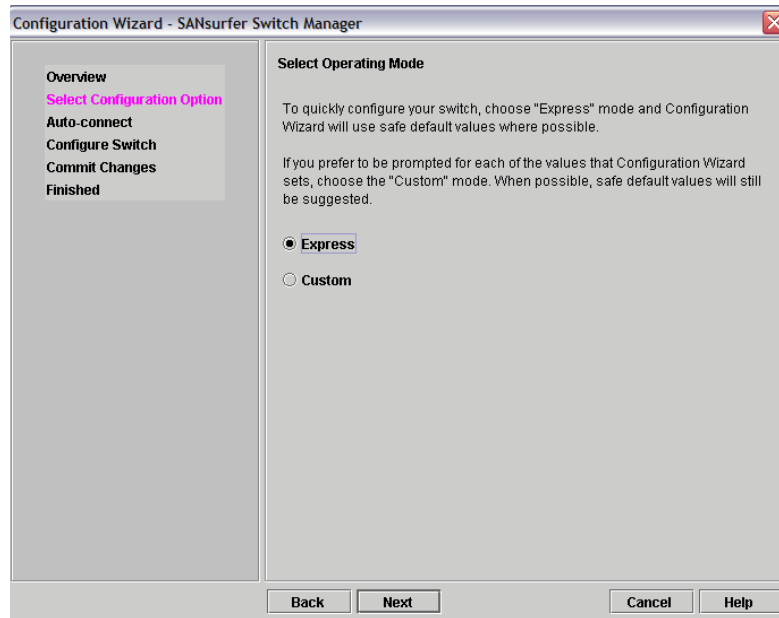


Figure 20 Configuration Wizard selection window

In the Network Configuration window, enter the IP address and subnet mask that you wish to configure on the new switch. The wizard checks to make sure that the subnet that you enter is on the same subnet that is configured on your workstation's local Ethernet interface. If not, you cannot continue, and a warning message is displayed, as shown in Figure 21.

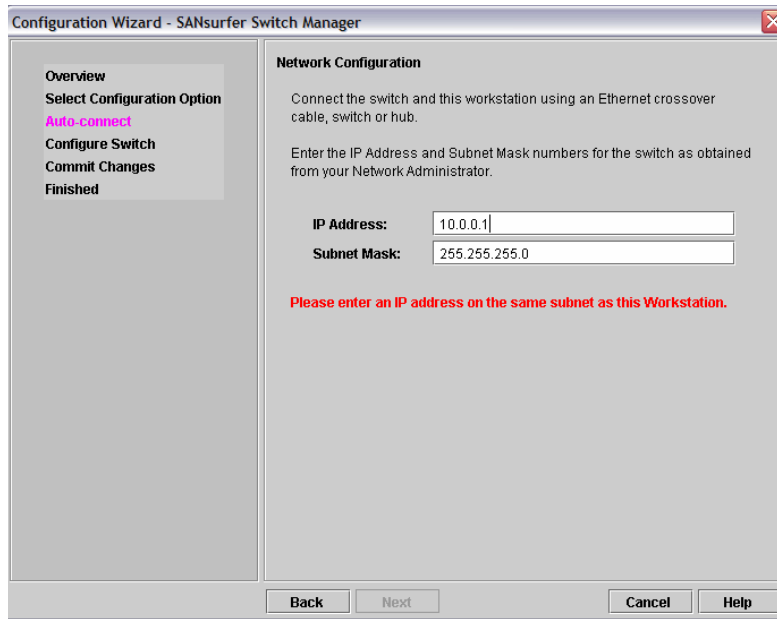
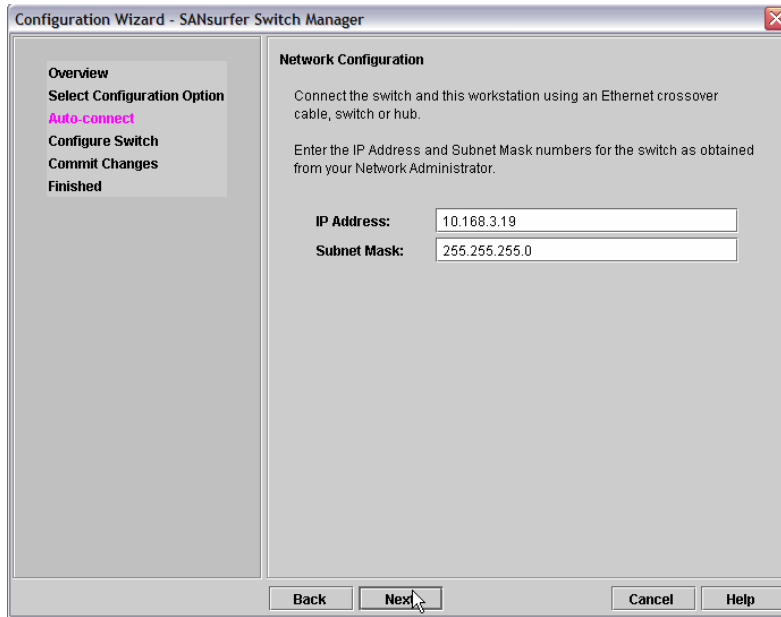


Figure 21 Configuration Wizard Network Configuration warning window

Enter the correct IP address information, as shown in Figure 22, and select **Next**.



The image shows a Windows-style dialog box titled "Configuration Wizard - SANsurfer Switch Manager". On the left is a vertical sidebar with a list of steps: "Overview", "Select Configuration Option", "Auto-connect" (highlighted in pink), "Configure Switch", "Commit Changes", and "Finished". The main area on the right is titled "Network Configuration". It contains the following text: "Connect the switch and this workstation using an Ethernet crossover cable, switch or hub." and "Enter the IP Address and Subnet Mask numbers for the switch as obtained from your Network Administrator." Below this text are two input fields. The first is labeled "IP Address:" and contains the text "10.168.3.19". The second is labeled "Subnet Mask:" and contains the text "255.255.255.0". At the bottom of the window are four buttons: "Back", "Next" (with a mouse cursor pointing to it), "Cancel", and "Help".

Figure 22 Configuration Wizard Network Configuration window

The default password for the *admin* user is *password*. Enter this information in the Auto-connect window (Figure 22 on page 17) and select **Next**.

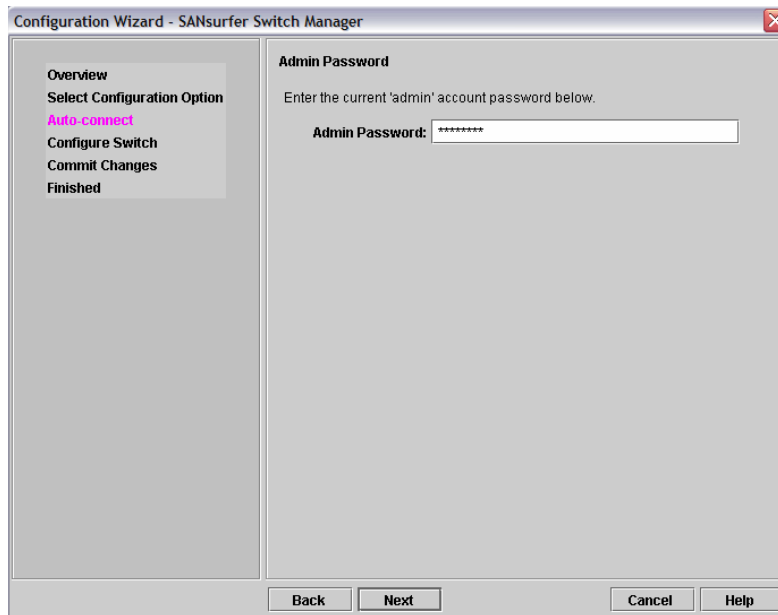


Figure 23 Configuration Wizard Auto-connect window

Follow the instructions, as shown in Figure 24, and select **Next**.

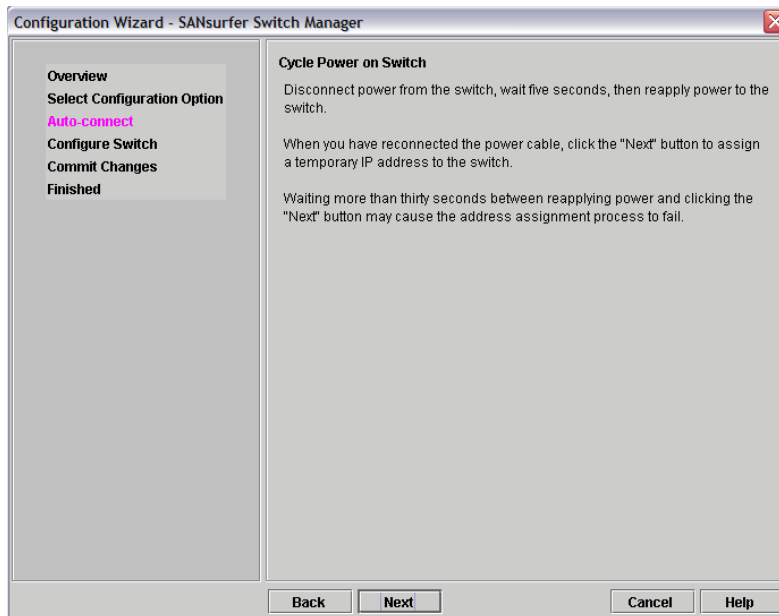


Figure 24 Configuration Wizard Auto connect window

During boot up of the SAN10Q, the window shown in Figure 25 is displayed.

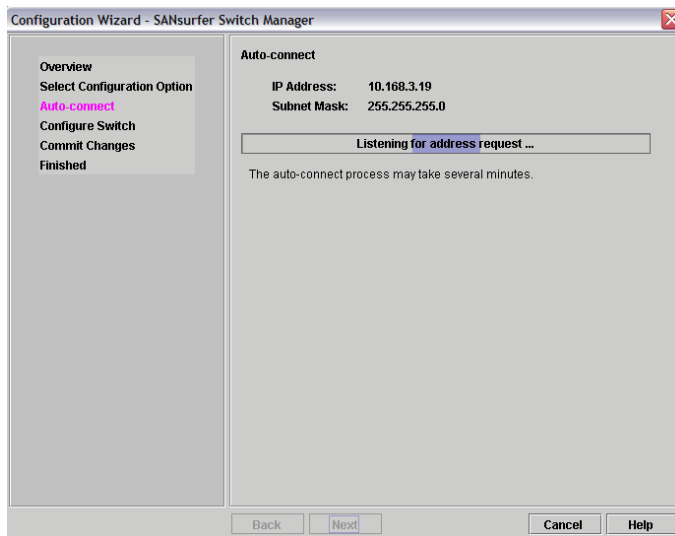


Figure 25 Configuration Wizard status window

When the switch has booted, it sends a request for an IP address to SANsurfer. SANsurfer then assigns the switch the IP address that you configured, as shown in Figure 26.

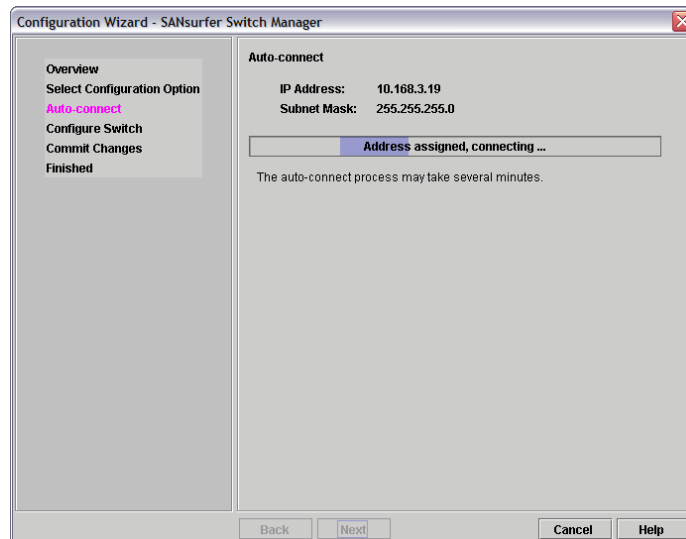


Figure 26 Configuration Wizard IP address setup

You now receive a security warning, due to this being a new installation. Select **OK** to continue (Figure 27).

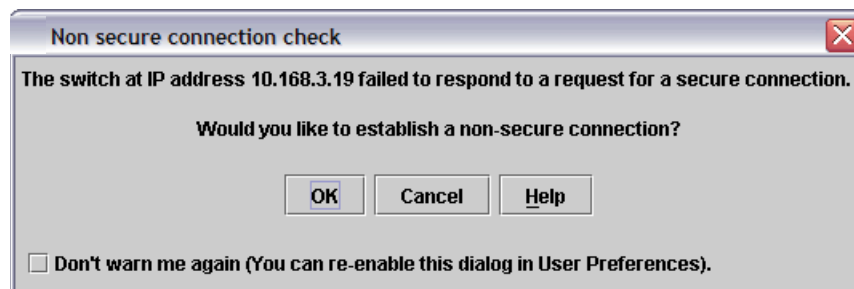


Figure 27 Security warning

The window shown in Figure 28 is displayed when the wizard has successfully configured the IP settings. Select **Next** to continue with switch setup.

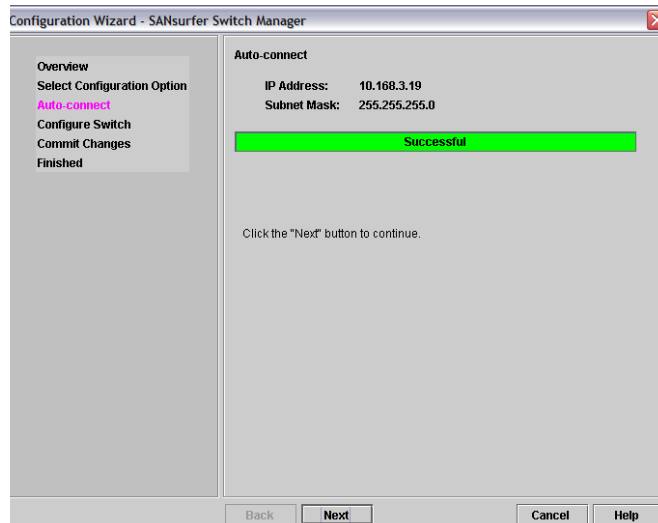


Figure 28 Configuration Wizard auto-connect successful

You now have the option to change your *admin* user password. Read the minimum requirements for this password and key them into this window, as shown in Figure 29. Select **Next** to continue.

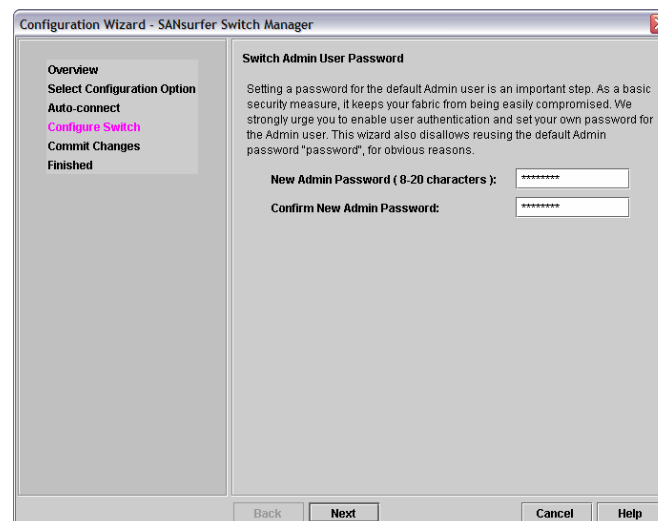


Figure 29 Configuration Wizard change password

You can now monitor the final stage of the setup while SANsurfer applies the changes to your switch, as shown in Figure 30. Wait for the completion message and select **Finish**.

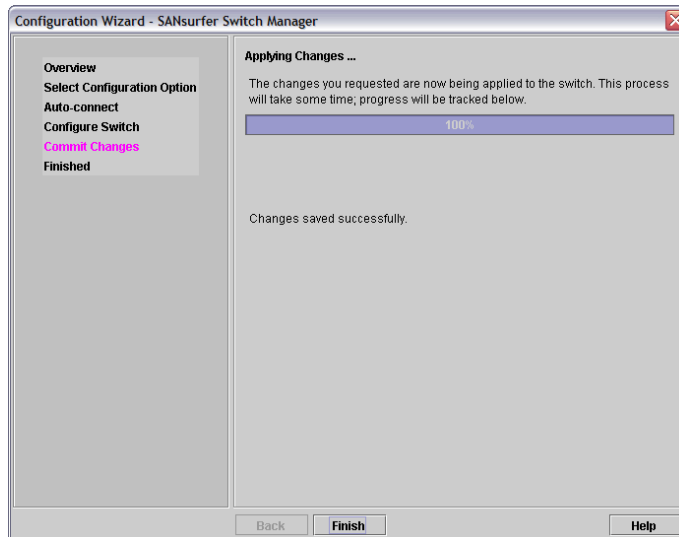


Figure 30 Configuration Wizard applying changes

This completes the initial setup of the switch. Select the **Close** button, as shown in Figure 31.

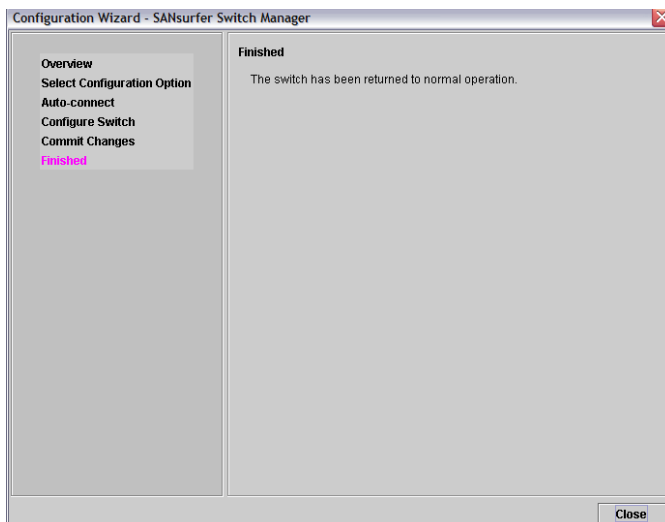


Figure 31 Configuration Wizard completion

You are now taken into the initial SANsurfer Switch Manager window, as shown in Figure 32.

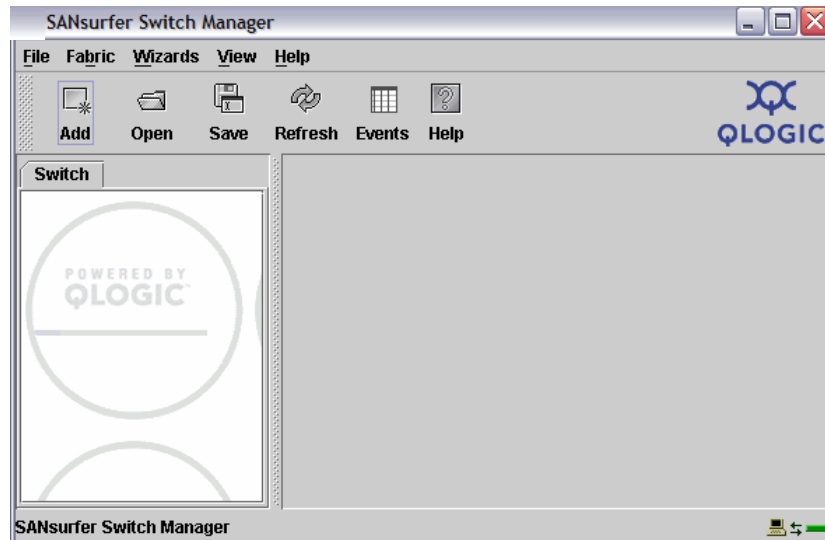


Figure 32 SANsurfer Switch Manager initial display

Now select **Fabric** → **Add Fabric** from the main menu (Figure 33).

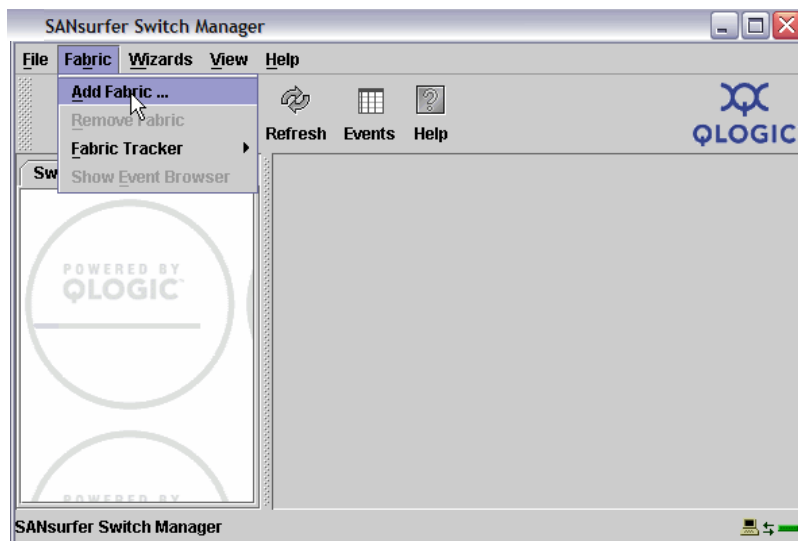
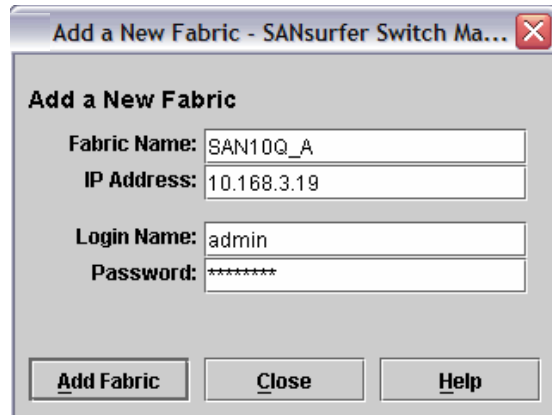


Figure 33 SANsurfer Switch Manager Add Fabric

Give your fabric a name, then key in the IP address as well as the admin user name and password, as shown in Figure 34. The password is the same one that you set in the window shown in Figure 22 on page 17.

A dialog box titled "Add a New Fabric - SANsurfer Switch Ma..." with a close button (X) in the top right corner. The dialog contains four input fields: "Fabric Name:" with the text "SAN10Q_A", "IP Address:" with the text "10.168.3.19", "Login Name:" with the text "admin", and "Password:" with the text "*****". At the bottom, there are three buttons: "Add Fabric", "Close", and "Help".

Add a New Fabric

Fabric Name: SAN10Q_A

IP Address: 10.168.3.19

Login Name: admin

Password: *****

Add Fabric **Close** **Help**

Figure 34 Add New Fabric

Respond **OK** to the non-secure connection check message shown in Figure 35.

A dialog box titled "Non secure connection check" with a close button (X) in the top right corner. The dialog contains a message: "Fabric-SAN10Q_A: The switch at IP address 10.168.3.19 failed to respond to a request for a secure connection." Below the message is the question "Would you like to establish a non-secure connection?". At the bottom, there are three buttons: "OK", "Cancel", and "Help". Below the buttons is a checkbox labeled "Don't warn me again (You can re-enable this dialog in User Preferences).".

Non secure connection check

Fabric-SAN10Q_A: The switch at IP address 10.168.3.19 failed to respond to a request for a secure connection.

Would you like to establish a non-secure connection?

OK **Cancel** **Help**

☐ Don't warn me again (You can re-enable this dialog in User Preferences).

Figure 35 Non secure connection message

You should now get a display similar to Figure 36, which shows the status of your switch.

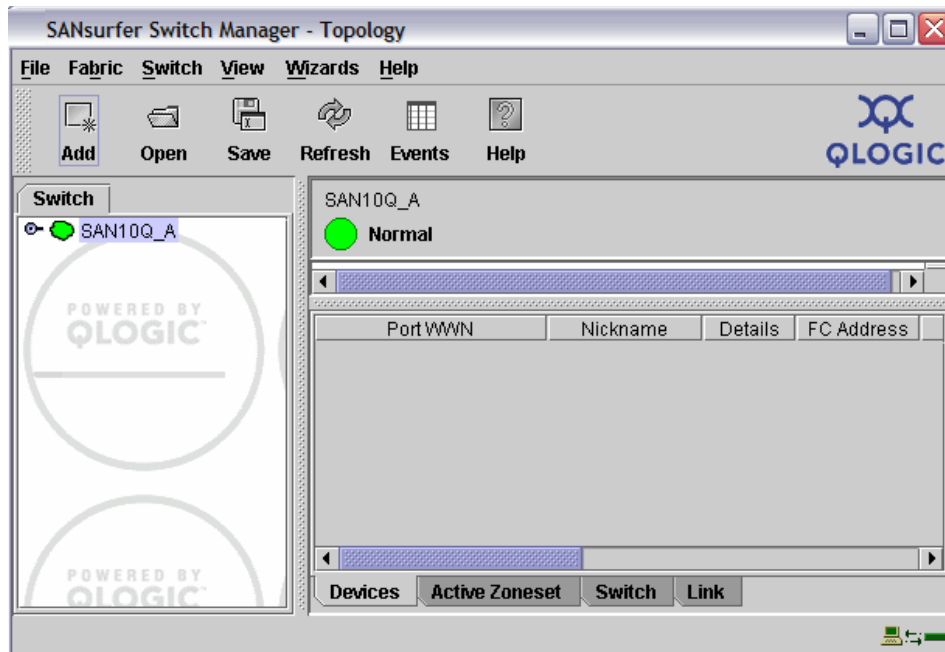


Figure 36 New fabric topology

The next step is to exit SANsurfer. Select **File** → **Exit**, as shown in Figure 37.

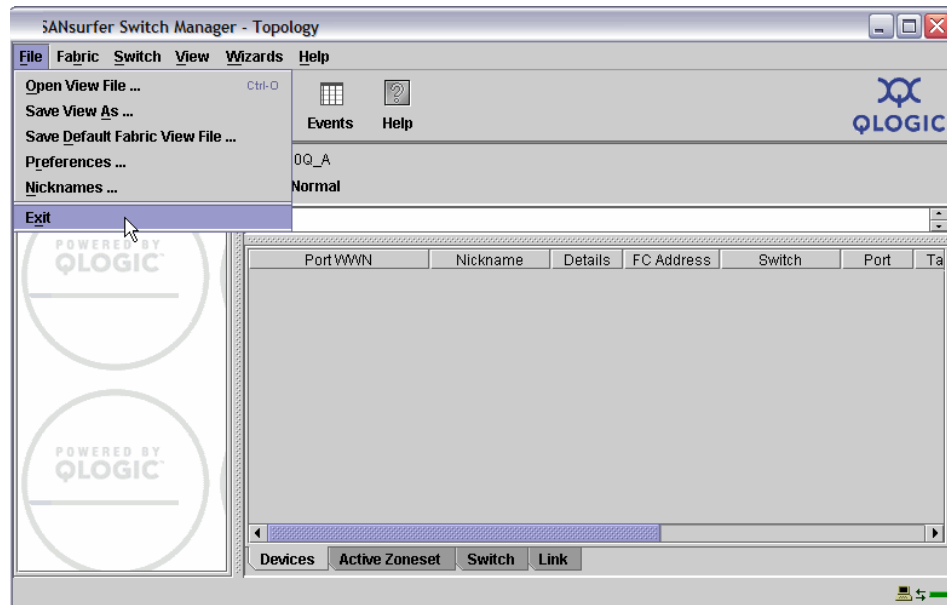


Figure 37 Exit SANsurfer

You now get the window shown in Figure 38 to enter an encryption key. We recommend that you enter an encryption key to secure your SAN fabric. If this is not done, then anyone who installs SANsurfer can access and modify your fabric, with the default blank key. You can use your switch admin password as the key, or use any other key that you can remember.



Figure 38 Encryption key

This completes the hardware installation process. There is also the possibility to configure the switch from the command line. This procedure is documented in the *System Storage SAN10Q 4 Gbps 10-Port Fibre Channel SwitchType 6918 Installation Guide*, which is available on the CD shipped with the switch.

Factory default reset

Select the switch that you want to reset to default, and from the faceplate menu, select **Switch** → **Restore Factory Defaults**, as shown in Figure 39.

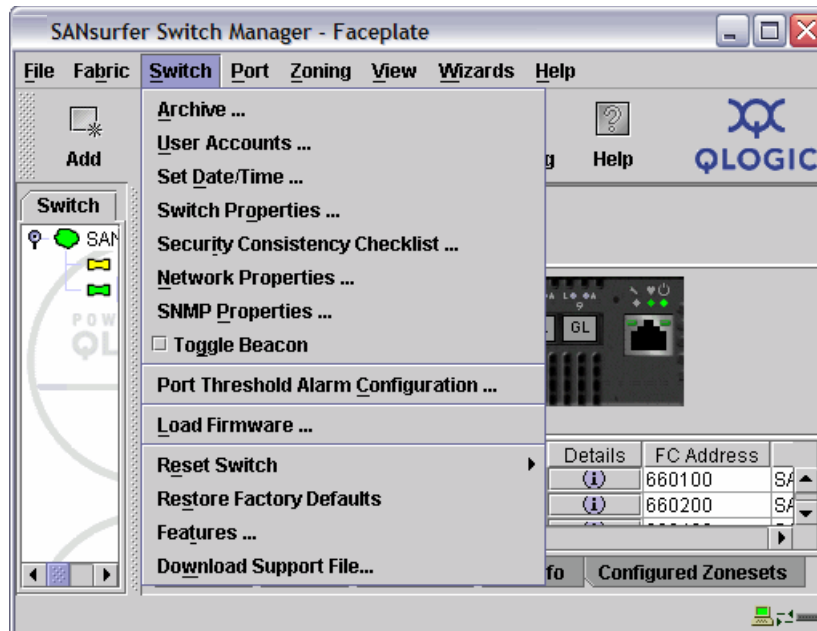


Figure 39 Reset to factory defaults

Take note of the warning message, as shown in Figure 40, and click **OK** to continue. At this time you lose the connection, because all settings are reset to the factory default and you have to start from the beginning to configure the switch.

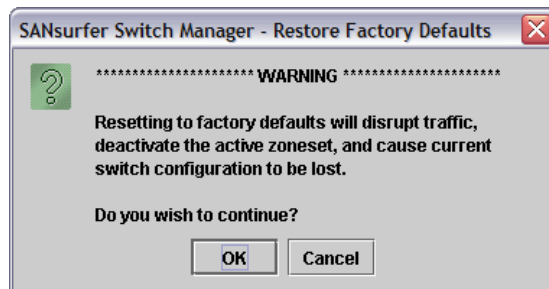


Figure 40 Default warning message

Attention: This does not reset the password information to default. To do that, see “Maintenance mode” on page 68.

Configuring the Fibre Channel switch

Prior to installing your devices and ISL link, you must perform the following procedure.

Start SANsurfer, and enter the key you set during installation, as shown in Figure 41.



Figure 41 Enter encryption key

The first window displayed is the topology display, you can modify the different windows to get a good display, as shown in Figure 42.

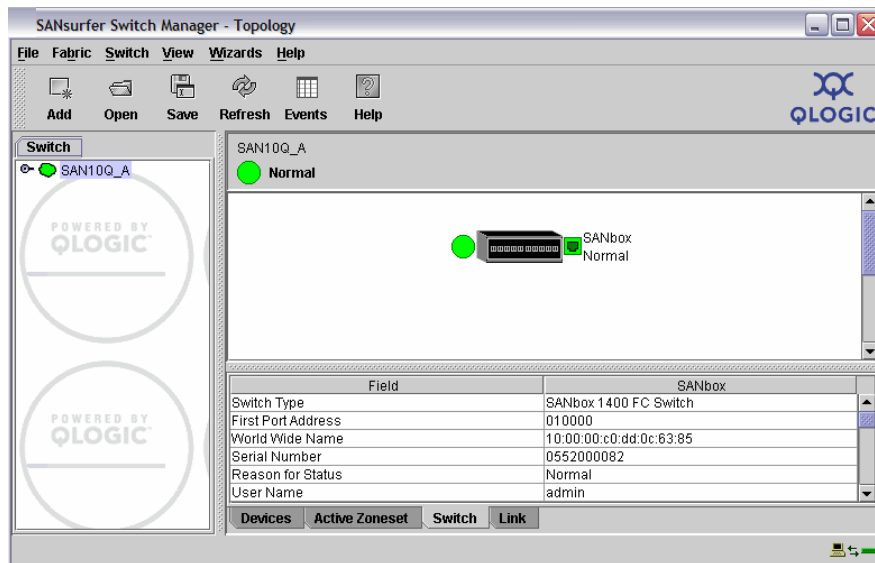


Figure 42 SANsurfer Topology window

Figure 43 shows the different elements within the SANsurfer main window.

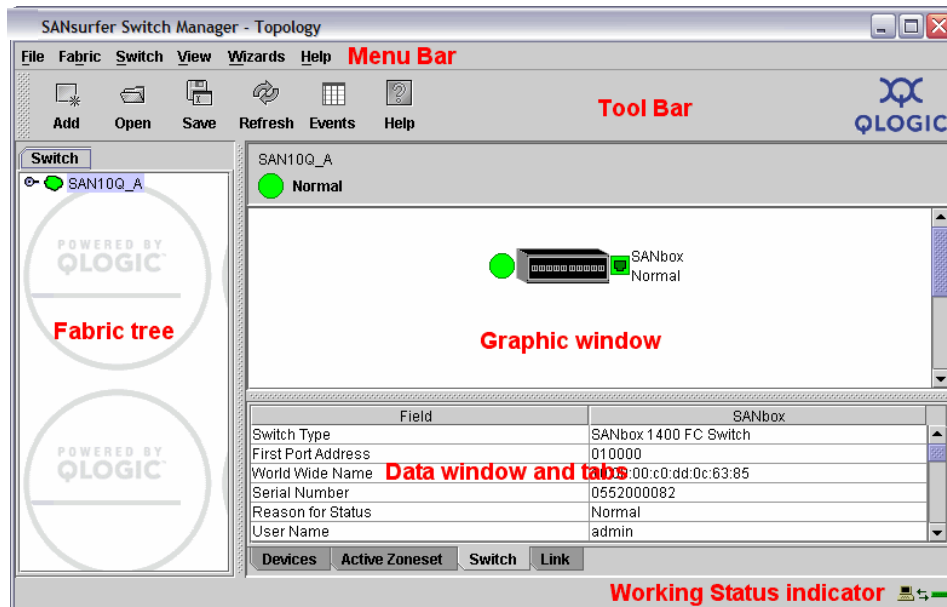


Figure 43 SANsurfer Switch Manager

The different elements are:

- ▶ Menu bar
- ▶ Toolbar
- ▶ Fabric tree
- ▶ Graphic window
- ▶ Data window and tabs
- ▶ Working status indicator

Using the fabric tree on the left side window, or by double-clicking the switch in the graphic window, you can open the Faceplate window, as shown in Figure 44.

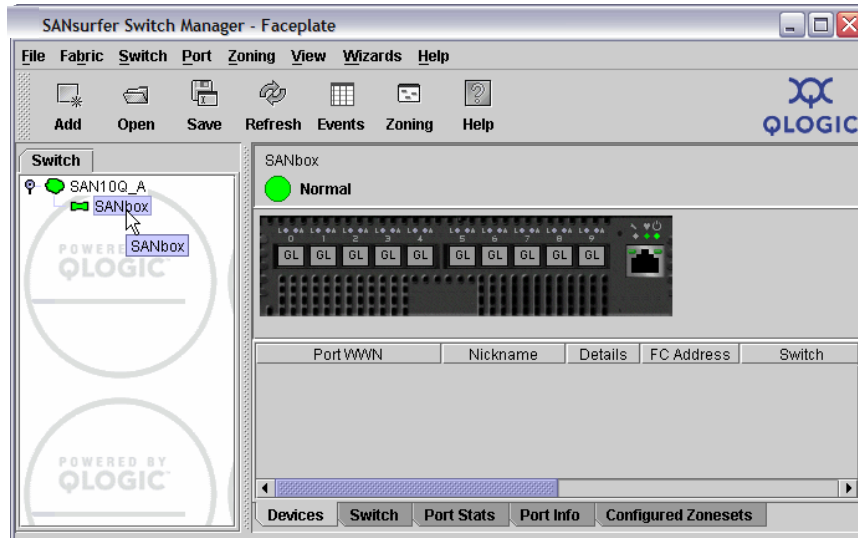


Figure 44 SANsurfer Faceplate window

Selecting the **Switch** tab from the menu bar, you see all the options to use for configuring the switch, as shown in Figure 45.

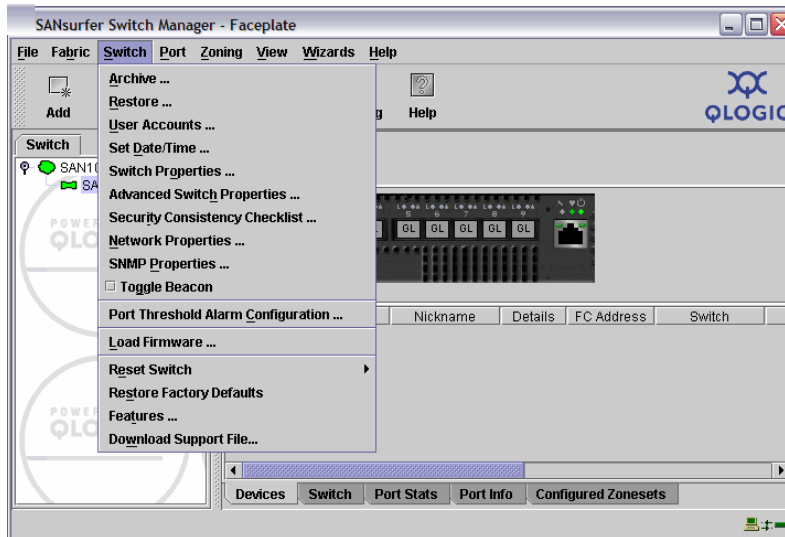


Figure 45 SANsurfer switch configuration menu

User accounts

From the Selecting User Accounts menu, you can add user accounts, as shown in Figure 46. Using the bottom tabs, you can also remove, change, and modify any account. The *admin* and *images* accounts cannot be removed.

The **User Account Administration** window displays a table of existing accounts and a form to add a new account.

Login	Admin Authority	Days to Expiration
images	false	never expires
admin	true	never expires

Add Account

New Account Login:

☒ Admin Authority Enabled

New Password:

Verify Password:

Account Expiration Date

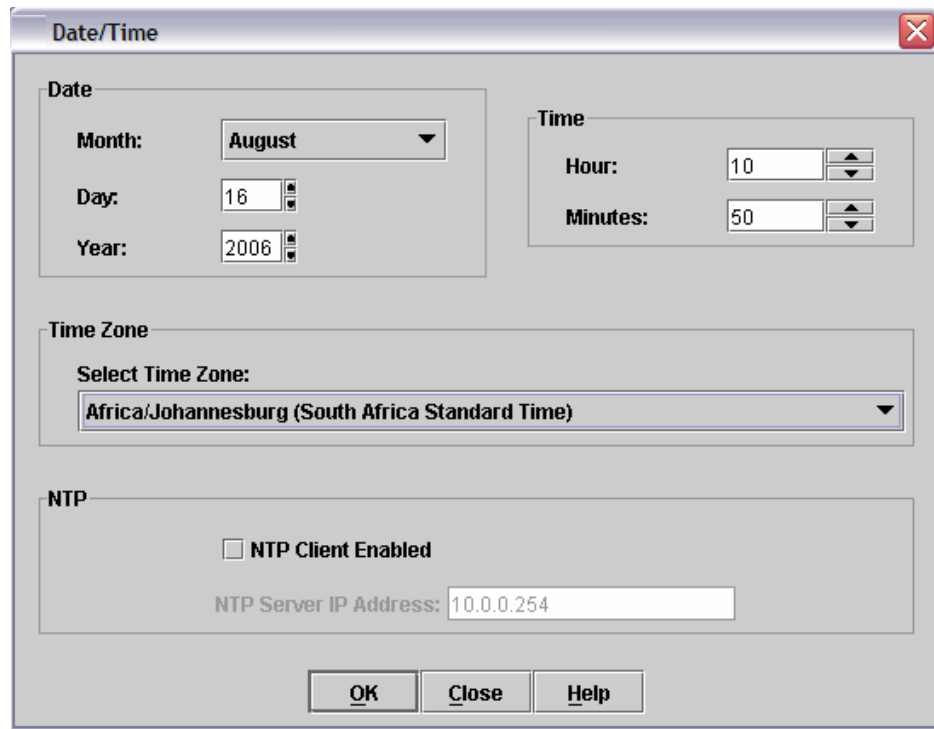
☒ Permanent account (no expiration date)

☐ Account will expire in days (max of 2000 days)

Figure 46 User Accounts Administration

Date and time

Next you can set the date and time of the switch. From this window, shown in Figure 47, you can also select your time zone and set up an NTP server.



The image shows a 'Date/Time' configuration window with a title bar and a close button. It is divided into four main sections: 'Date', 'Time', 'Time Zone', and 'NTP'. The 'Date' section has fields for 'Month' (a dropdown menu showing 'August'), 'Day' (a text box with '16'), and 'Year' (a text box with '2006'). The 'Time' section has fields for 'Hour' (a text box with '10') and 'Minutes' (a text box with '50'). The 'Time Zone' section has a label 'Select Time Zone:' and a dropdown menu showing 'Africa/Johannesburg (South Africa Standard Time)'. The 'NTP' section has a checkbox labeled 'NTP Client Enabled' which is currently unchecked, and a text box for 'NTP Server IP Address' containing '10.0.0.254'. At the bottom of the window are three buttons: 'OK', 'Close', and 'Help'.

Section	Field	Value
Date	Month	August
	Day	16
	Year	2006
Time	Hour	10
	Minutes	50
Time Zone	Select Time Zone	Africa/Johannesburg (South Africa Standard Time)
NTP	NTP Client Enabled	<input type="checkbox"/>
NTP	NTP Server IP Address	10.0.0.254

Figure 47 Date and time setup

Switch properties

From the menu shown in Figure 48, we set all the important switch properties.

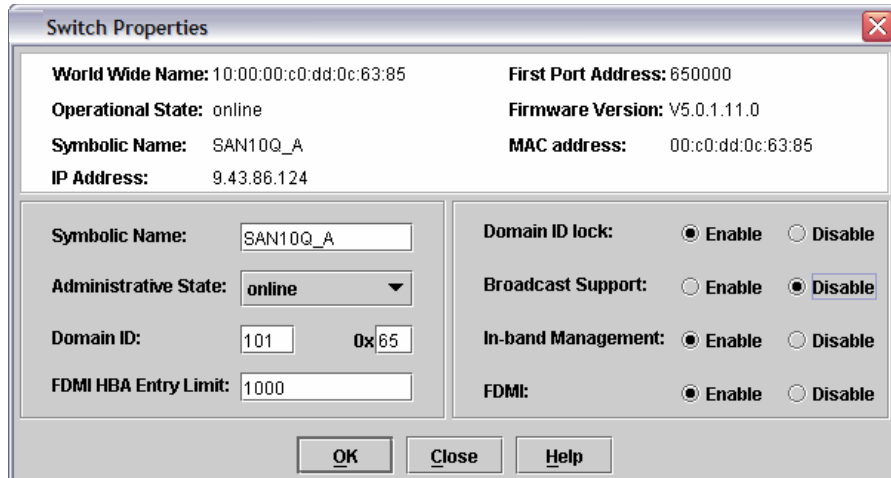
The image shows a 'Switch Properties' dialog box with a title bar and a close button. It contains several fields and controls. On the top left, 'World Wide Name' is 10:00:00:c0:dd:0c:63:85, 'Operational State' is online, 'Symbolic Name' is SAN10Q_A, and 'IP Address' is 9.43.86.124. On the top right, 'First Port Address' is 650000, 'Firmware Version' is V5.0.1.11.0, and 'MAC address' is 00:c0:dd:0c:63:85. Below these, on the left, are fields for 'Symbolic Name' (SAN10Q_A), 'Administrative State' (online), 'Domain ID' (101), 'FDMI HBA Entry Limit' (1000), and a hex field '0x65'. On the right, there are four radio button groups: 'Domain ID lock' (Enable selected), 'Broadcast Support' (Disable selected), 'In-band Management' (Enable selected), and 'FDMI' (Enable selected). At the bottom are 'OK', 'Close', and 'Help' buttons.

Figure 48 Switch Properties

The switch properties are:

- ▶ Symbolic name: This is the user-defined name of the switch, used to easily identify this switch on the management work station, and can be up to 32 characters long.
- ▶ Administrative state: You can set the switch to one of three states:
 - Online
 - Offline
 - Diagnostics
- ▶ Domain ID: You use this to set your domain ID. The domain ID must be unique for each switch in the fabric.

Attention: Make sure that you have done this prior to connecting an ISL to another switch.

- ▶ FDMI HBA entry limit: This sets the limit for the maximum number of HBAs that can be registered with a switch. If the number of HBAs exceeds the maximum number, the Fabric Device Management Interface (FDMI) information for those HBAs cannot be registered.

- ▶ Domain ID lock: The default setting is *disabled*. This means that the principal switch assigns domain IDs to all joining switches. If you wish to have control over the domain IDs in your fabric, ensure that you enable this button.
- ▶ Broadcast support: The default setting is disabled. Broadcast is supported on the switch that allows for TCP/IP support.
- ▶ In-band management: The default setting is enabled. This allows in-band requests to the switch, such as SNMP, Management Server, GUI, and API messaging across Fibre Channel to our switch.
- ▶ FDM: This enables or disables the Fabric Device Management Interface.

Advanced switch properties

You can modify some advanced switch properties from this menu, shown in Figure 49.

The screenshot shows a window titled "Advanced Switch Properties" with a close button in the top right corner. The window is divided into several sections:

- World Wide Name:** 10:00:00:c0:dd:0c:63:85
- First Port Address:** 650000
- Operational State:** online
- Firmware Version:** V5.0.1.11.0
- Symbolic Name:** SAN10Q_A
- MAC address:** 00:c0:dd:0c:63:85
- IP Address:** 9.43.86.124

Below these fields are two main configuration sections:

- Timeout Values:**
 - R_A_TOV:** 10000
 - E_D_TOV:** 2000
- Interop Mode:**
 - Interop Mode:** ☒ Standard ☐ Interop_1
 - Legacy Address Format:** ☐ Enable ☒ Disable

At the bottom of the dialog are three buttons: **OK**, **Close**, and **Help**.

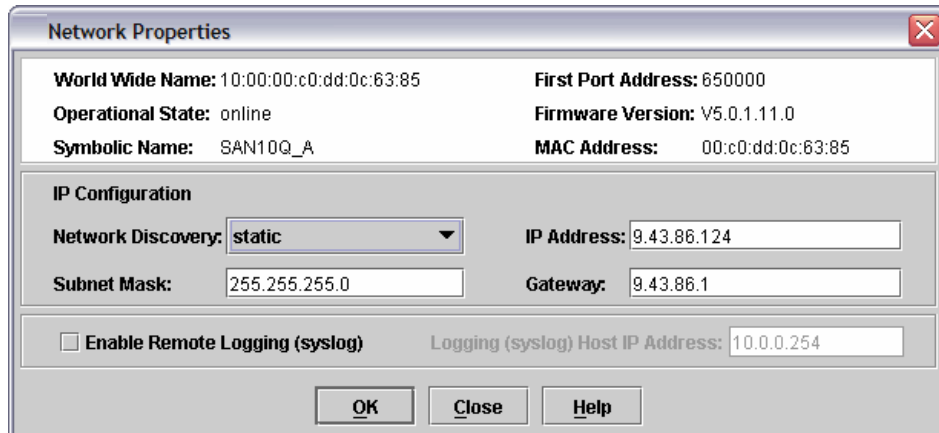
Figure 49 Advanced switch properties

These switch properties are:

- ▶ Time-out values: We do *not* recommend that you change the default time-out values, because these have to be the same across the fabric.
- ▶ Interop mode: Use the *Standard* option for FC-SW-2 compliant switches to propagate only the active zone set to all switches in the fabric. Use the *Interop_1* parameter for non-FC-SW-2 compliant switches to propagate the active zone set and all inactive zone sets to all switches in the fabric.

Network properties

You can modify your management interface setting from this window, shown in Figure 50. You can also set the management interface under the Network Discovery option to obtain its IP setting via BootP server, RARP, and DHCP.



The 'Network Properties' dialog box displays various network configuration parameters. It is organized into several sections: a top section for basic identifiers, an 'IP Configuration' section for network settings, and a bottom section for logging options. The 'World Wide Name' is 10:00:00:c0:dd:0c:63:85, 'First Port Address' is 650000, 'Operational State' is online, 'Firmware Version' is V5.0.1.11.0, 'Symbolic Name' is SAN10Q_A, and 'MAC Address' is 00:c0:dd:0c:63:85. In the 'IP Configuration' section, 'Network Discovery' is set to 'static' (via a dropdown), 'IP Address' is 9.43.86.124, 'Subnet Mask' is 255.255.255.0, and 'Gateway' is 9.43.86.1. The 'Enable Remote Logging (syslog)' checkbox is unchecked, and the 'Logging (syslog) Host IP Address' is 10.0.0.254. At the bottom are 'OK', 'Close', and 'Help' buttons.

World Wide Name: 10:00:00:c0:dd:0c:63:85	First Port Address: 650000
Operational State: online	Firmware Version: V5.0.1.11.0
Symbolic Name: SAN10Q_A	MAC Address: 00:c0:dd:0c:63:85

IP Configuration	
Network Discovery: static	IP Address: 9.43.86.124
Subnet Mask: 255.255.255.0	Gateway: 9.43.86.1

<input type="checkbox"/> Enable Remote Logging (syslog)	Logging (syslog) Host IP Address: 10.0.0.254
--	---

OK Close Help

Figure 50 Network Properties

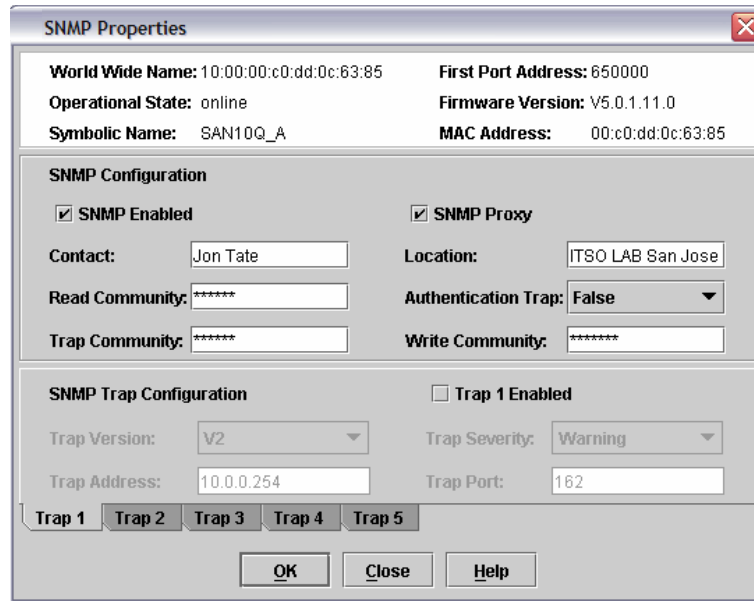
The factory default is set to 10.0.0.1 and the mask is 255.0.0.0.

When the Enable Remote Logging box is checked, the log entries are sent to the host IP address specified in this field.

Attention: If you change any settings on this window and click **OK**, you could lose connectivity to your switch.

SNMP

Figure 51 shows the window where we set up Simple Network Management Protocol (SNMP). SNMP is the protocol for network management and monitoring of network devices. SNMP security consists of a read community string and a write community string. The read community string *public* and write community string *private* are set at the factory to these well-known defaults and should be changed if SNMP is enabled. SNMP is enabled by default.



The image shows a window titled "SNMP Properties" with a close button in the top right corner. The window is divided into several sections:

- Header Information:**
 - World Wide Name: 10:00:00:c0:dd:0c:63:85
 - Operational State: online
 - Symbolic Name: SAN10Q_A
 - First Port Address: 650000
 - Firmware Version: V5.0.1.11.0
 - MAC Address: 00:c0:dd:0c:63:85
- SNMP Configuration:**
 - ☒ SNMP Enabled
 - ☒ SNMP Proxy
 - Contact: Jon Tate
 - Location: ITSO LAB San Jose
 - Read Community: *****
 - Authentication Trap: False (dropdown menu)
 - Trap Community: *****
 - Write Community: *****
- SNMP Trap Configuration:**
 - ☐ Trap 1 Enabled
 - Trap Version: V2 (dropdown menu)
 - Trap Severity: Warning (dropdown menu)
 - Trap Address: 10.0.0.254
 - Trap Port: 162
- Trap Tabs:** Trap 1, Trap 2, Trap 3, Trap 4, Trap 5 (Trap 1 is selected)
- Buttons:** OK, Close, Help

Figure 51 SNMP Properties

In the SNMP Configuration area, we can enable or disable SNMP, set our contact and location information, and then set up our community names.

In the SNMP Trap area, we can enable traps and set up the version of SNMP (V1 or V2), the severity of traps sent, the TCP port number used, and the IP address of our trap receiver. We can set up multiple traps and receivers using the Trap tabs.

Firmware update

In the sections that follow, we show how to obtain the latest firmware and upgrade the switch.

Obtaining the latest firmware

You can obtain the latest firmware as follows:

1. Download the latest firmware using the link from the IBM Web site:
<http://www-304.ibm.com/jct01004c/systems/support/supportsite.wss/supportresources?taskind=2&brandind=5000031&familyind=5329837>
2. This links you to the QLogic® Web site dedicated to IBM, from which you can download both the latest firmware and SANsurfer.
3. Download the firmware onto your management workstation.

Upgrading the switch

From the SANsurfer Topology window, we can see the current version of our switch, as shown in Figure 52.

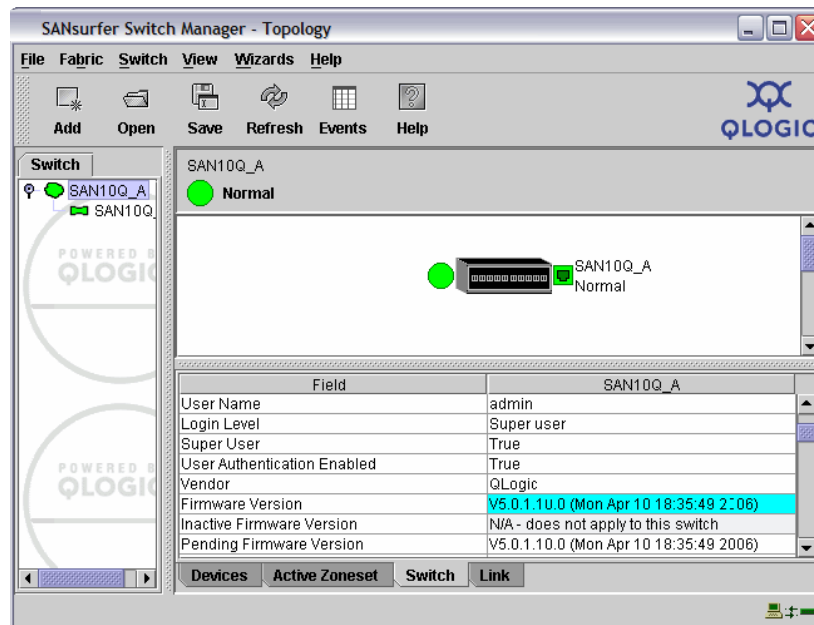


Figure 52 Check switch firmware level

Select the switch that you wish to upgrade in the fabric tree and then select **Switch** → **Load Firmware**.

The Load Firmware frame is now displayed, as shown in Figure 53. Select the **Browse** button.

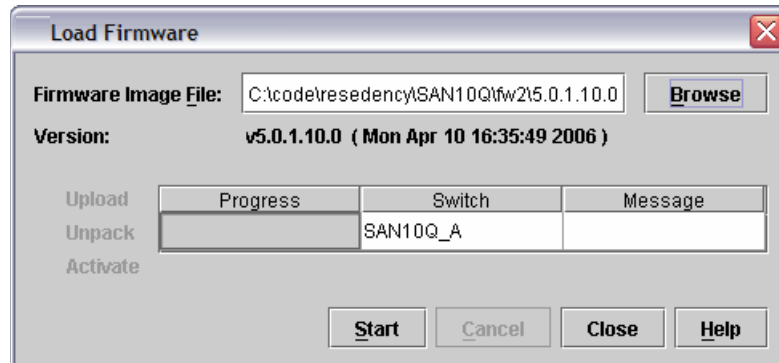


Figure 53 Load Firmware

Using the **Look In** button, shown in Figure 54, browse to the directory into which you downloaded the firmware. Select the correct firmware image and click the **Open** button.

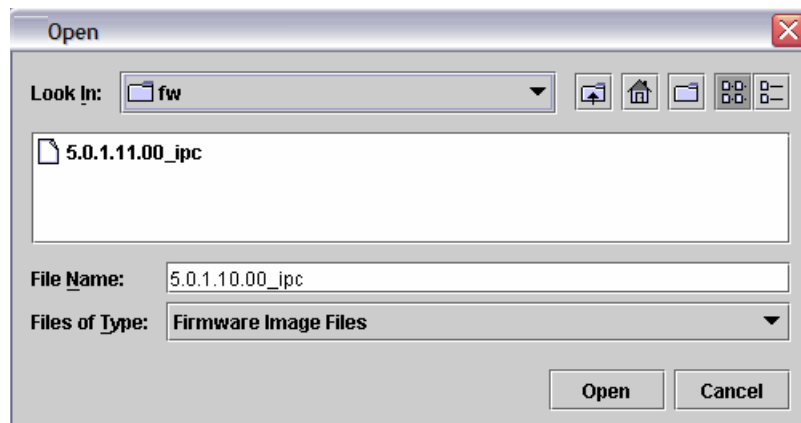


Figure 54 Open file

On the Load Firmware window, you now see the version that you selected displayed in the version field, shown in Figure 55. Click the **Start** button to begin the download.

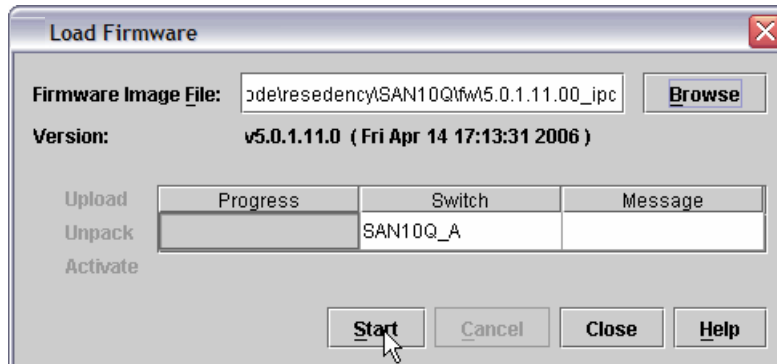


Figure 55 Load Firmware start

You now receive a warning message, as shown in Figure 56. Read the message and then click **OK** to continue.

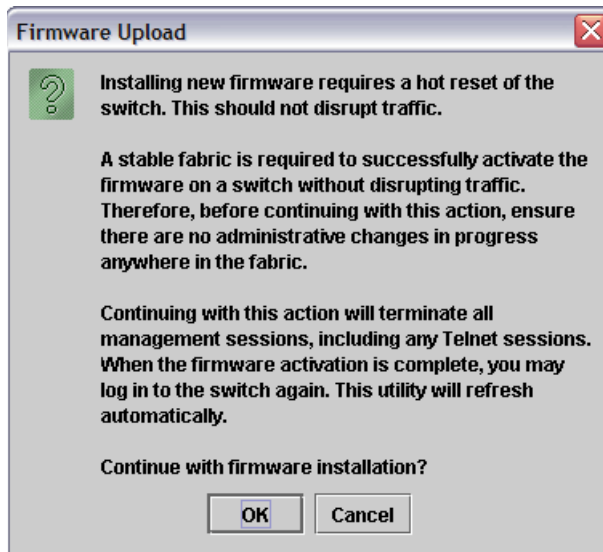


Figure 56 Warning message

The window shown in Figure 57 displays the progress of the activation process.

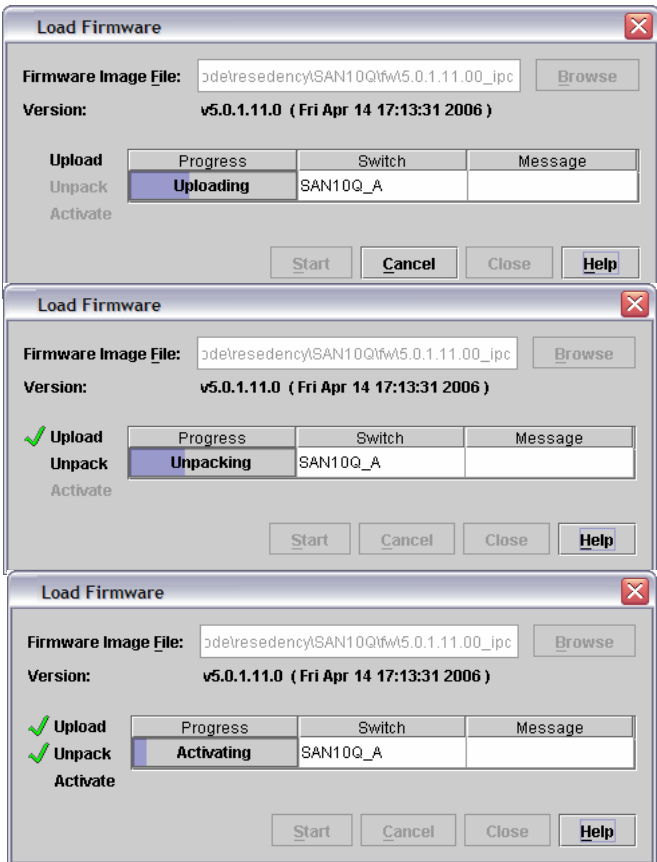


Figure 57 Activation progress windows

During the final phase, the switch performs a hot reset. Fabric services are unavailable for a short period (30–75 seconds). This is shown in Figure 58.

Note: To ensure that a *nondisruptive code load and activation* operation is successful, do not attempt to do any administrative changes to the fabric during a firmware update. If changes to the fabric are attempted during this process, this might disrupt the firmware activation process.

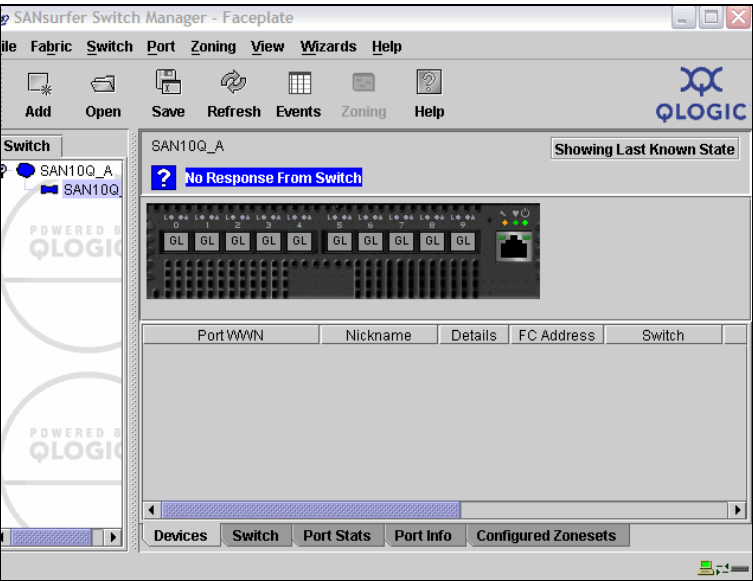


Figure 58 Hot reset of switch

Finally, you get the Activation Successful message, shown in Figure 59. Click the **Close** button to exit.

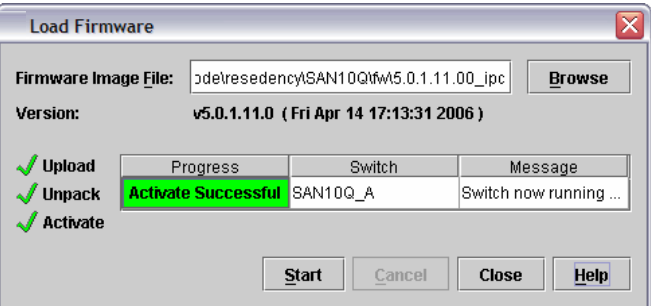


Figure 59 Activation successful

When the Firmware upgrade is complete, you can check your active level of the switch from the Topology display, as shown in Figure 60.

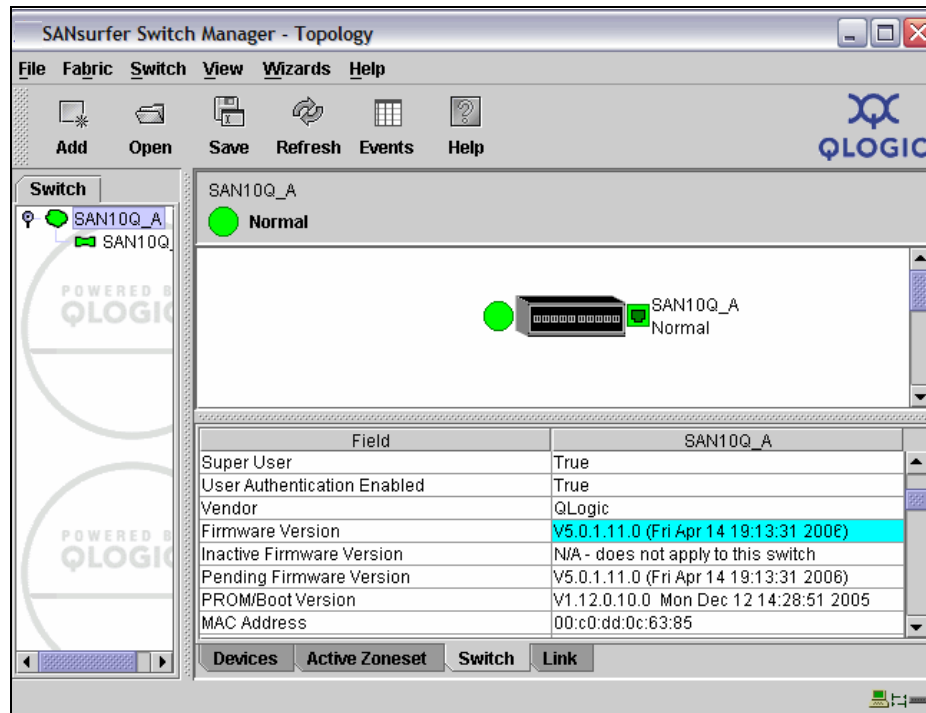


Figure 60 Firmware versions

Zoning

In the sections that follow we discuss zoning.

Zoning limits

These are the zoning limits for the QLogic:

- ▶ The maximum number of zone sets is 256.
- ▶ The maximum number of zones is 2,000.
- ▶ The maximum number of aliases is 2,500.
- ▶ The maximum number of total zone and alias members is 10,000.
- ▶ The maximum number of zone linkages to zone sets is 2,000. Every time a zone is added to a zone set, this constitutes a linkage.
- ▶ The maximum number of zone members is 2,000. Aliases are considered zone members when added to a zone.

- The maximum number of zone members that can be added to any alias is 2,000.

Zone types

The SAN10Q supports hard zoning and soft zoning.

Hard zoning is, as its name suggests, enforced by the hardware. Hard zoning membership can be defined only by domain ID and port number, and supports all port types.

Soft zoning, as its name suggests, is enforced by the name server. Soft zoning membership can be defined by Fibre Channel address, domain ID and port number, world wide name, or a combination. Soft zoning supports all port types.

With reference to Figure 61, we utilize two SAN10Q switches to create a redundant SAN.

The first step is to install and configure both switches using the previous topics in this book. We linked both switches together utilizing an ISL link and plugged all devices into the switches.

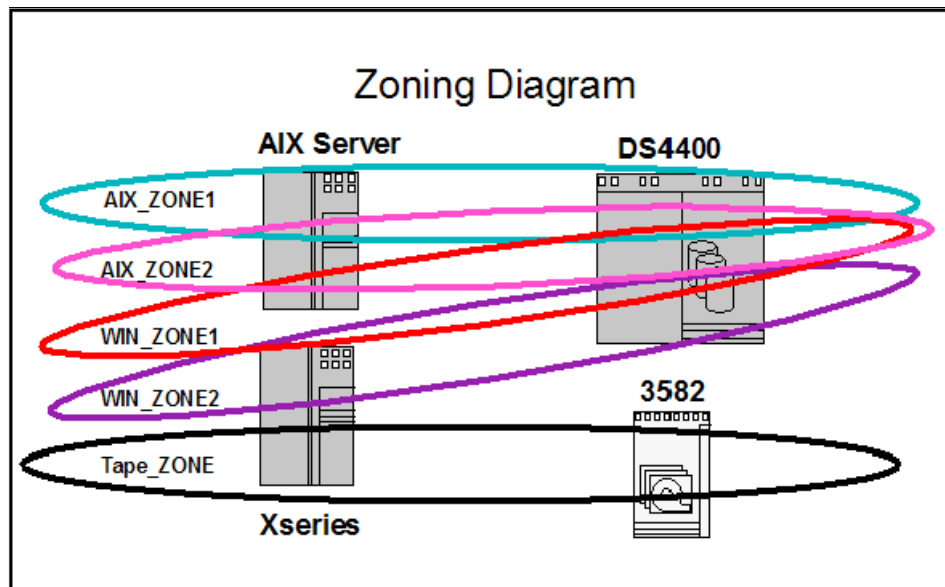


Figure 61 Zoning diagram

Zoning wizard

For small, simple installations, you can use the zoning wizard, which brings up a series of dialog windows that lead you through the process of zoning a fabric. To open the zoning wizard, select **Wizards** → **Zoning Wizard**. The wizard is only supported on Windows servers and is self-explanatory, as shown in Figure 62.

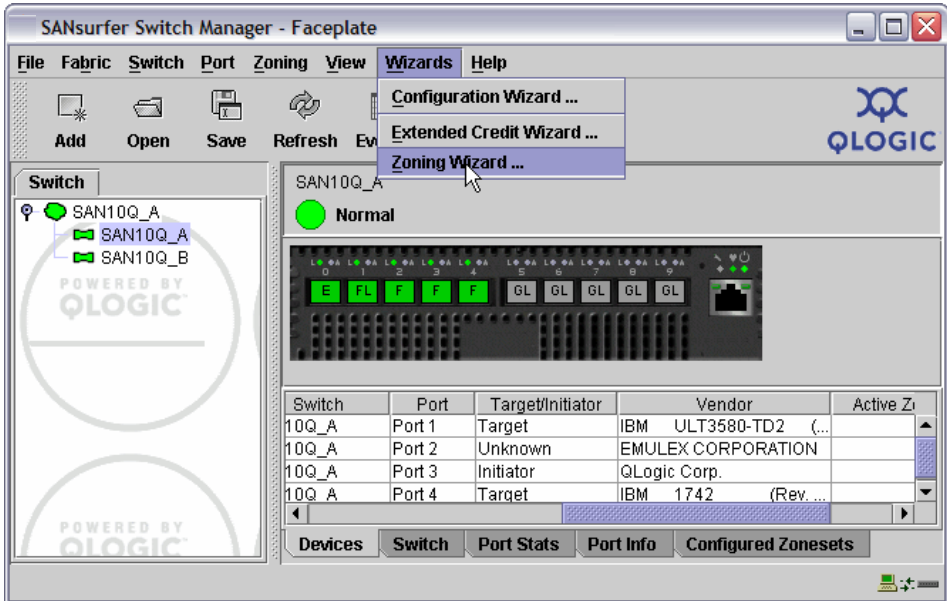


Figure 62 Zoning wizard

Zoning startup

To make zoning easier, we can give each WWN a nickname, and to do this, we double-click the nickname field in the devices menu, shown in Figure 63. This is not compulsory, but it can make managing the SAN less complicated.

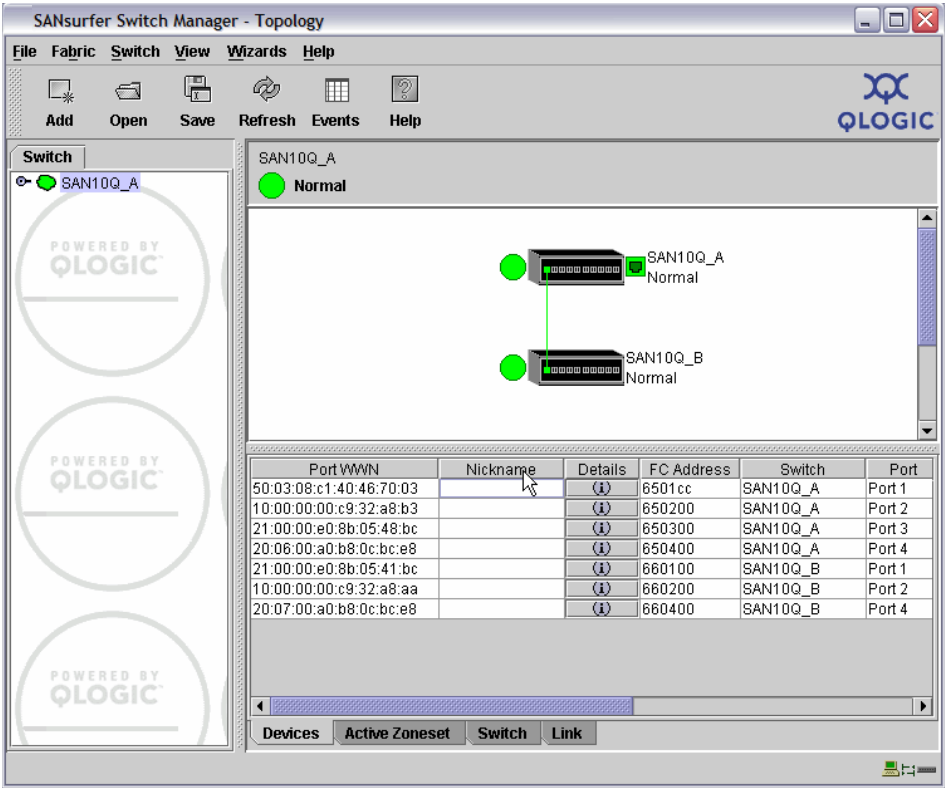


Figure 63 Topology display

We now give each of the attached WWNs a nickname, as shown in Figure 64.

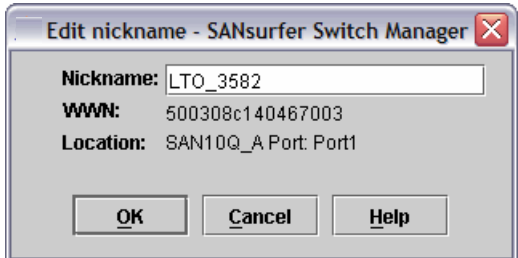


Figure 64 Adding nickname

From the Faceplate window of any switch, we select **Zoning** → **Edit Zoning**, as shown in Figure 65.

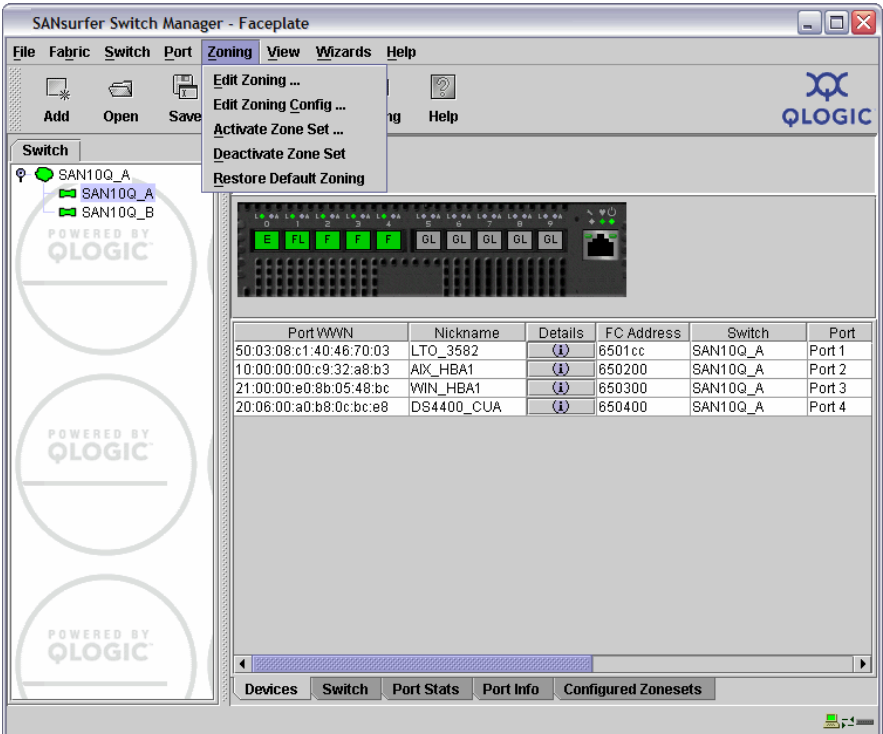


Figure 65 Starting Zoning configuration

The *Edit Zoning* window is now displayed, as shown in Figure 66. Notice that the nicknames that were set up previously are displayed in the Members window. If you do not set up nicknames, then you see the WWN of each device.

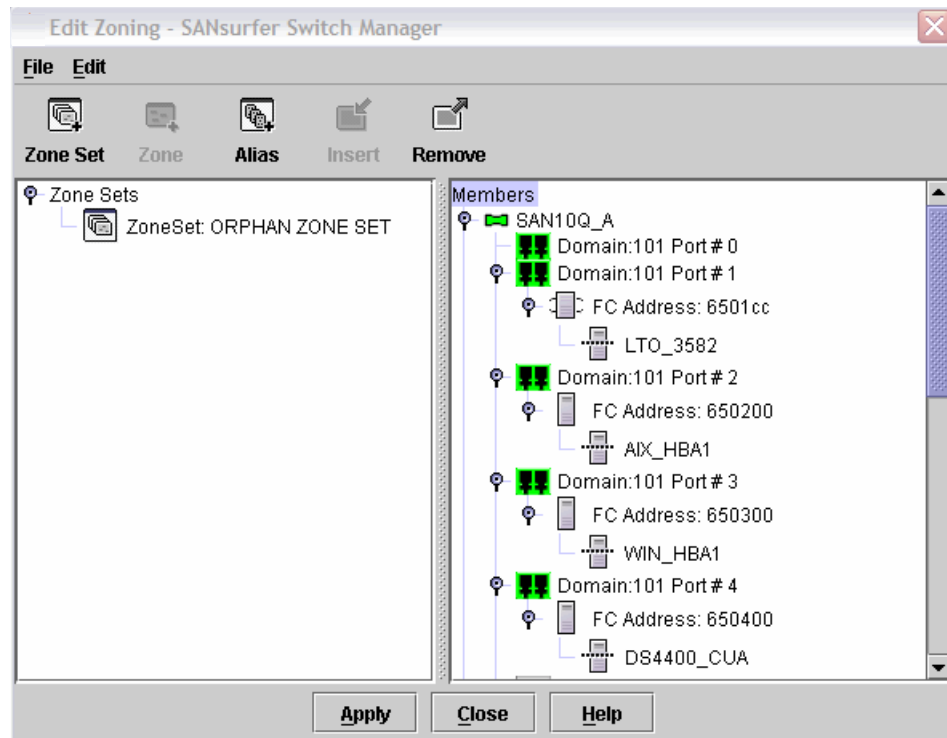


Figure 66 Edit Zoning window

Creating an alias

An alias is a named set of ports or devices that are grouped together for convenience. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias. To create an alias, from the window shown in Figure 66, select the **Alias** button.

Enter the alias name in the window shown in Figure 67, and repeat this step for all the alias names that you wish to create.

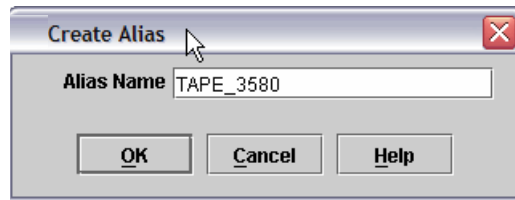


Figure 67 Create Alias

When this is done, you have a list under Zone Sets of all the alias names that you have defined, as shown in Figure 68.

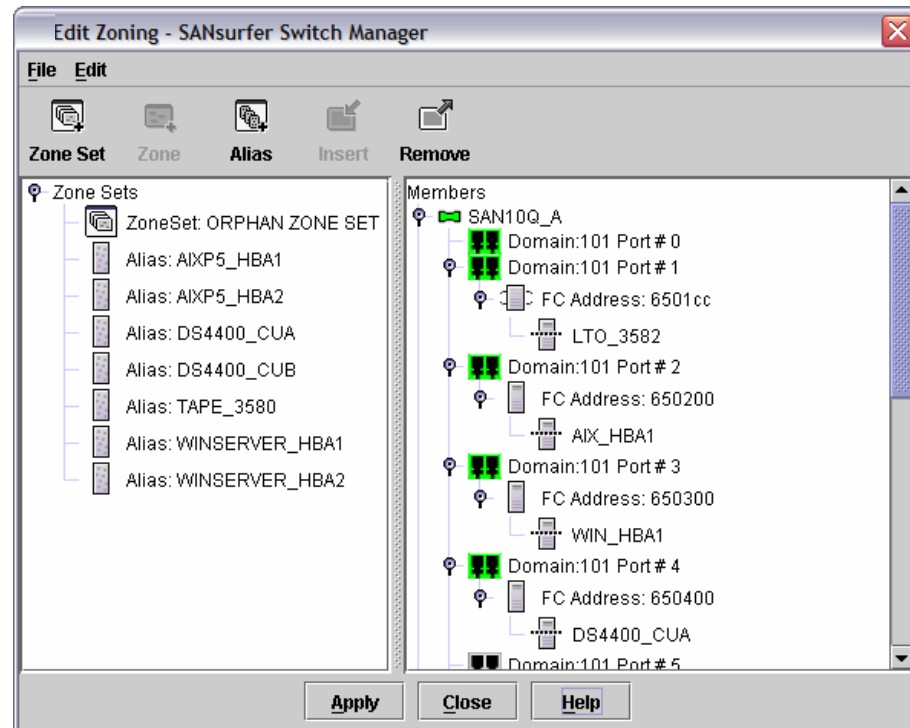


Figure 68 Alias names

There are three methods that you can use to add members to an alias:

- To use the drag-and-drop method, click and hold down the mouse button on the member to be added to the alias. Drag the selected member from the right pane to the alias in the left pane.

- ▶ Select the alias in the left pane and the member to add to that alias in the right pane, and then click **Edit** → **Add Members**.
- ▶ Select the alias in the left pane, select the member to add to that alias in the right pane, and click the **Insert** button.

Using one of these methods, add the members to the alias names, as shown in Figure 69.

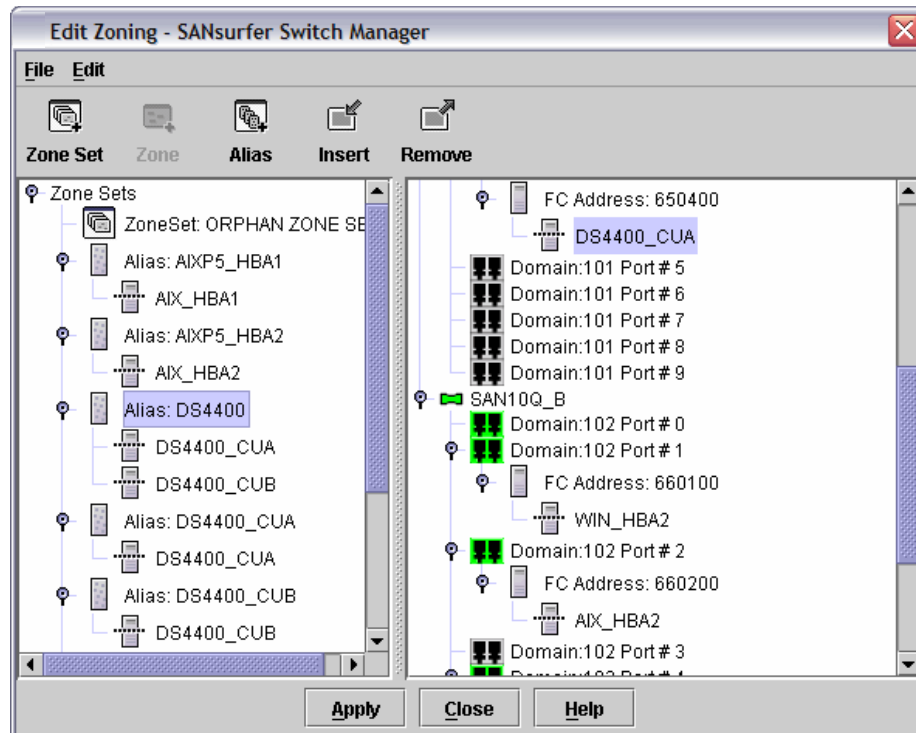


Figure 69 Adding a member to an alias

Creating a zone set and zones

By clicking the **Zone Set** icon, as shown in Figure 69 on page 49, you get a window to enter the zone set name, as shown in Figure 70. Enter your zone set name and click **OK**.

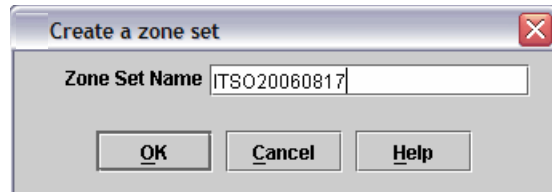


Figure 70 Create a zone set

Now click the zone set that you just created and click the **Zone** button, as shown in Figure 71.

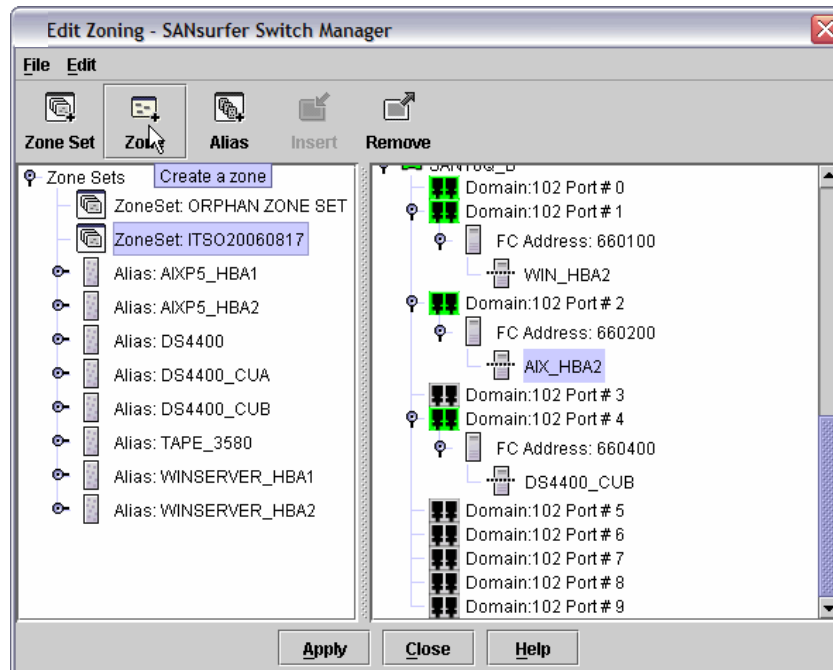


Figure 71 Zone set created

Enter the name of the zone that you wish to create, as shown in Figure 72, and repeat this step for all the zones you wish to create.

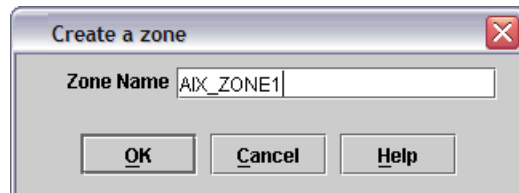


Figure 72 Create zone

Under the zone set you created, you see all the zone names that you just created, as shown in Figure 73.

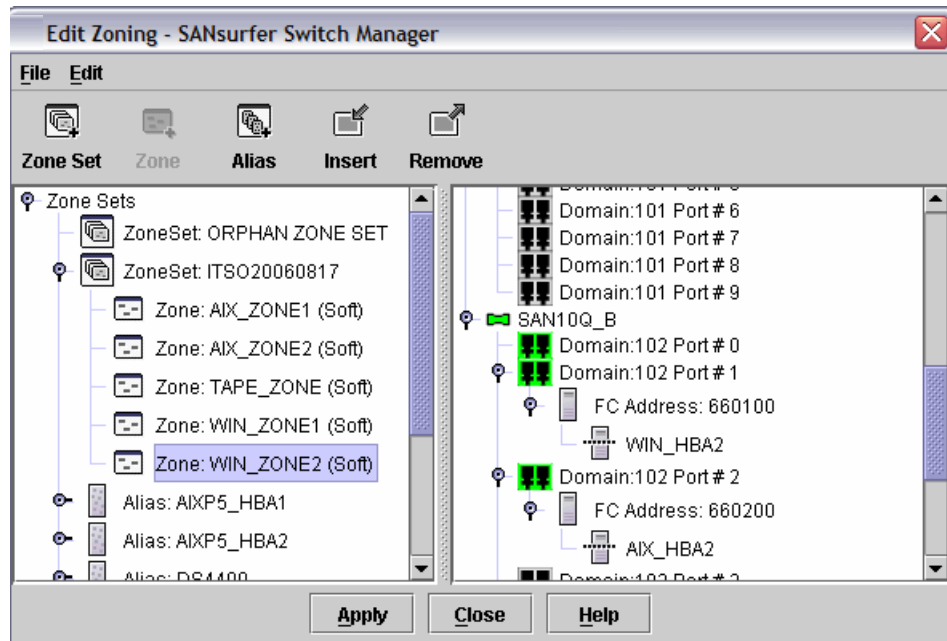


Figure 73 Zones created

By default, all zones are set up for soft zoning. To change any details of the zone that you created, such as zone type and name, right-click the zone and select the action from the menu options displayed, as shown in Figure 74.

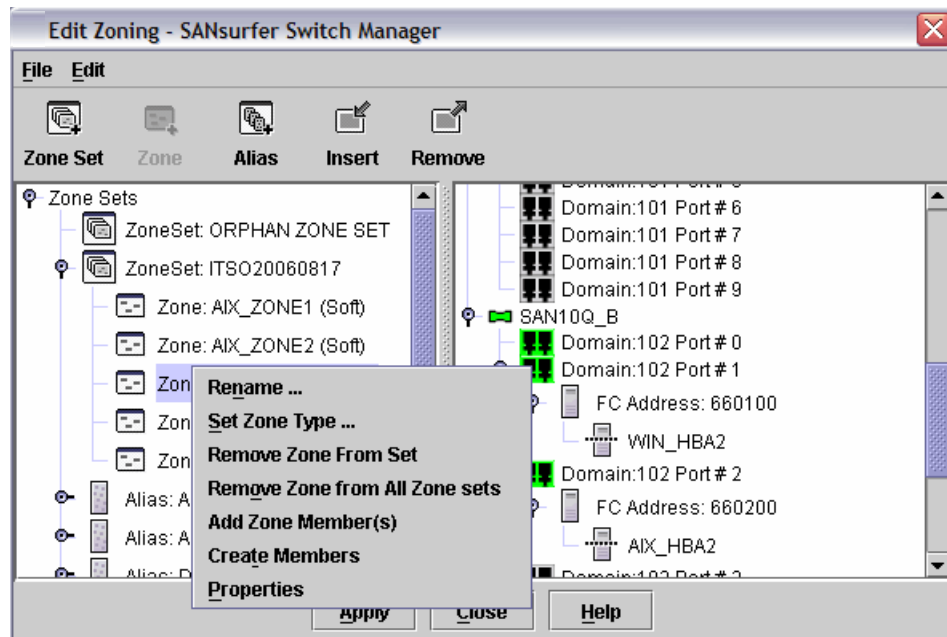


Figure 74 Zone modification

Adding members to a zone can be done in a number of ways:

- ▶ Select a member by alias name, and drag it into the zone.
- ▶ Select one or more members by port number, Fibre Channel address, or World Wide Name in the device tree. Then select the zone in which to add members, and select the **Insert** button, as shown in Figure 75 on page 53.
- ▶ Select a member by port number, Fibre Channel address, or World Wide Name in the device tree, and drag it into the zone. You can select and drag multiple ports or devices by clicking and holding the Ctrl key while dragging into the required zone.

Do this to configure all your zones and click the **Apply** button to save changes to the zoning database.

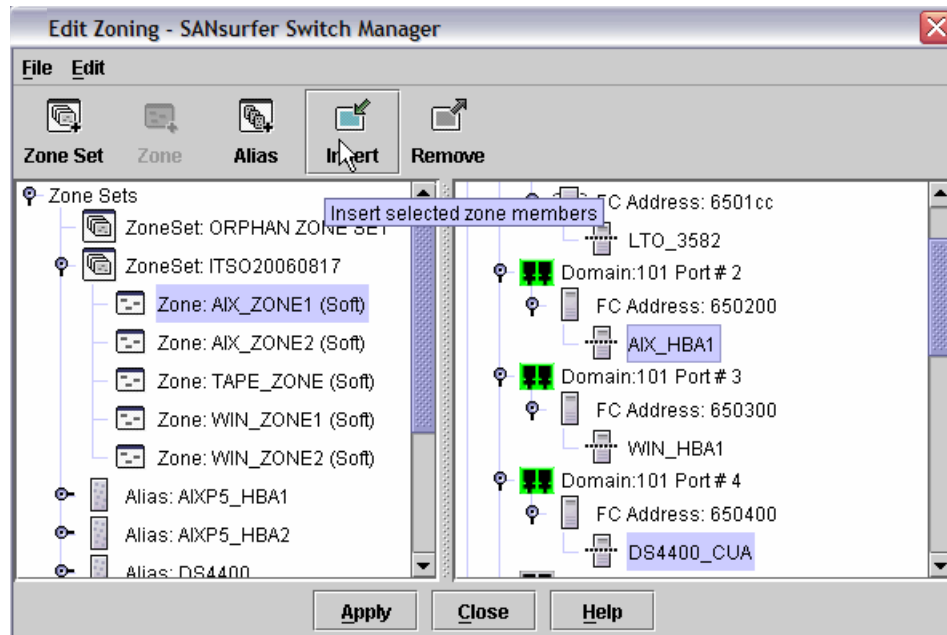


Figure 75 Adding zone members

Click the **Save Zoning** button in the window shown in Figure 76.

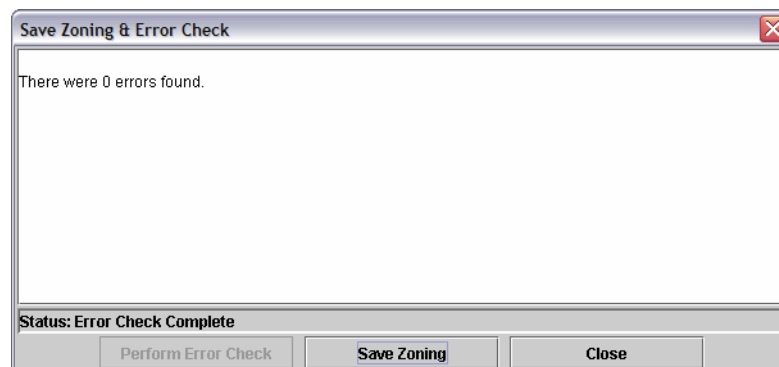


Figure 76 Save Zoning

Click **Yes** to activate from the window shown in Figure 77.

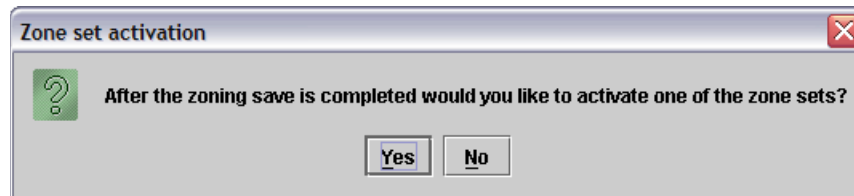


Figure 77 Zone set activation

Select the zone set you wish to activate and click **OK**, as shown in Figure 78.

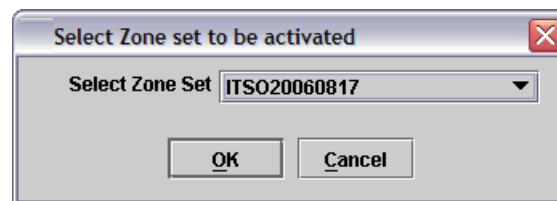


Figure 78 Zones set to be activated

Check the status line of the window shown in Figure 79 to see whether the zone set was activated.

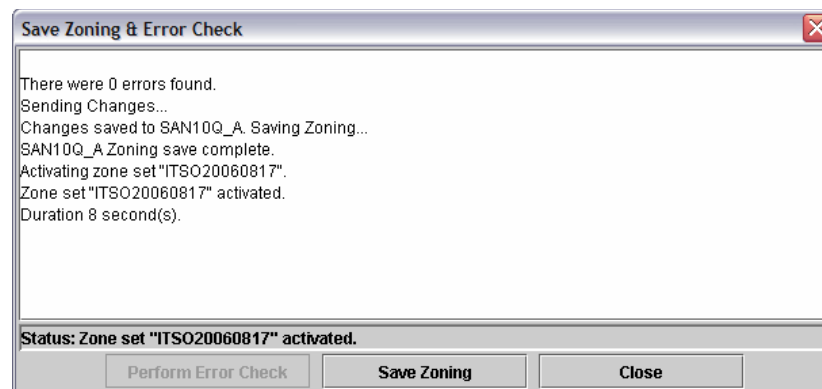


Figure 79 Zone set activation complete

Modifying zoning

Using the Edit Zoning window, as shown in Figure 80, you can add, delete, and modify all zoning information. You can create a new zone set using the previous steps and create new zones in this new zone set. You can also modify the active zone set.

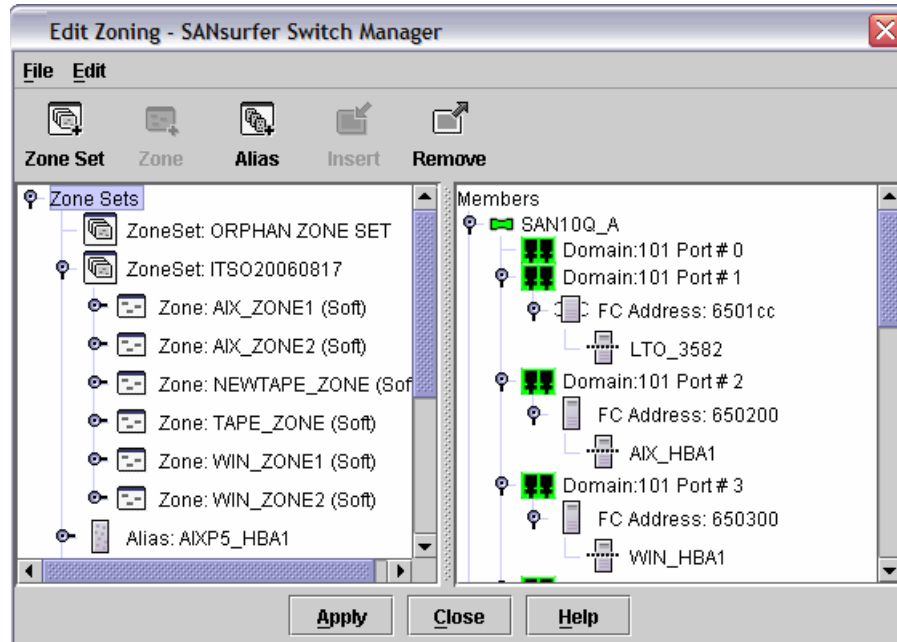


Figure 80 Edit zoning

As shown in Figure 81, we added a new zone to the active zone set, called NEW_TAPE in our example. We also added the members to this zone set. To activate the change, select the **Apply** button and activate the same zone set.

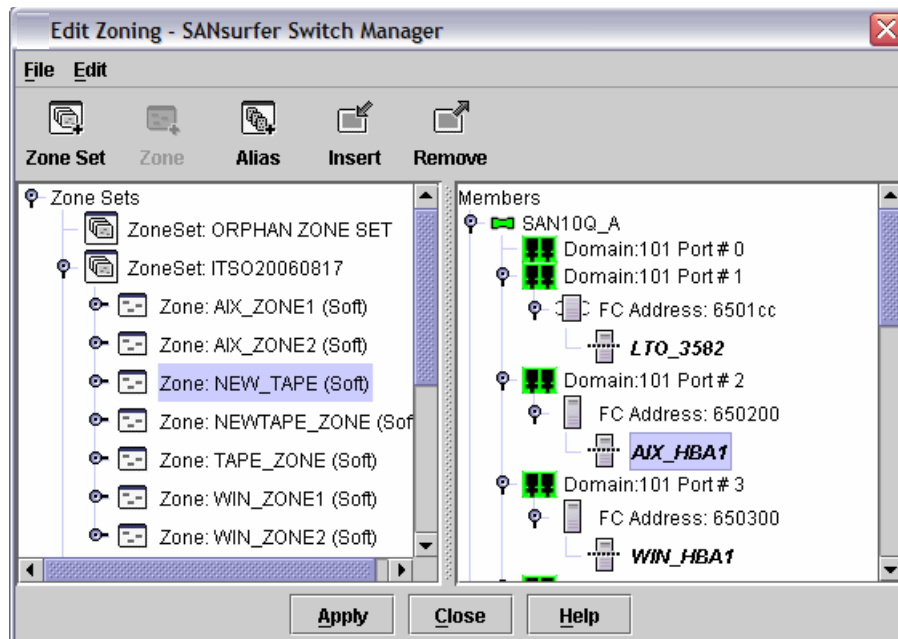


Figure 81 Zone addition

Performance viewer

The performance viewer application is a separate application from the switch management application that displays port performance using graphs.

The performance viewer provides a method to visually monitor the real-time traffic for each port on a switch. Traffic for a port is displayed in its own graph that is continually updated to reflect changes as they occur, and is based on the number of kilobytes (Kb) or on the number of frames that pass through that port per second.

To start the performance viewer from within the topology display, select **Fabric** → **Start Performance Viewer**, as shown in Figure 82.

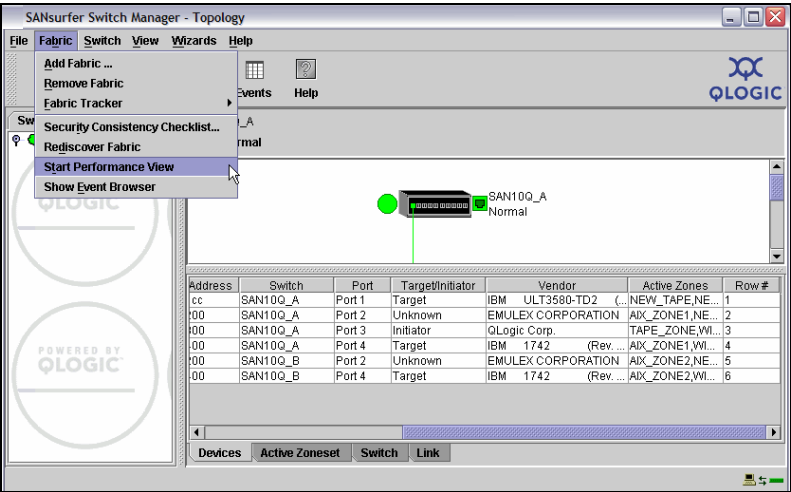


Figure 82 Starting performance viewer

On the left side of the window is a list of ports available for monitoring. Click the ports that you wish to monitor, and a graphical view of these ports appears in the right-hand side of the window, as shown in Figure 83.

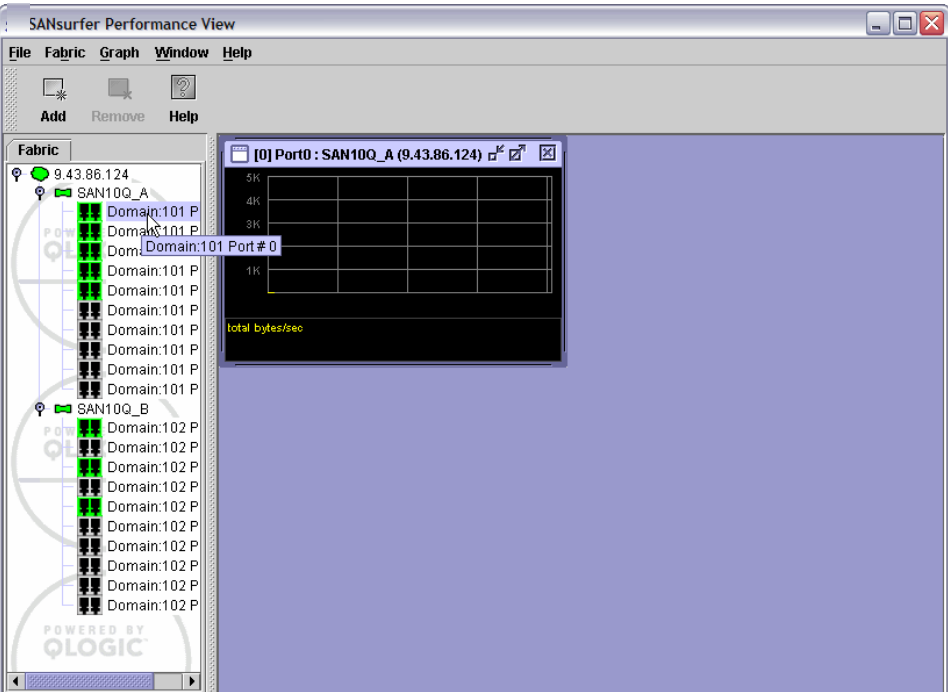


Figure 83 Performance view

Select **Graph** → **Modify Graph Options** from the tool bar. This opens the Default Graph Options dialog, shown in Figure 84. Here you can choose display options that affect what is to be plotted and how the graphs are displayed.

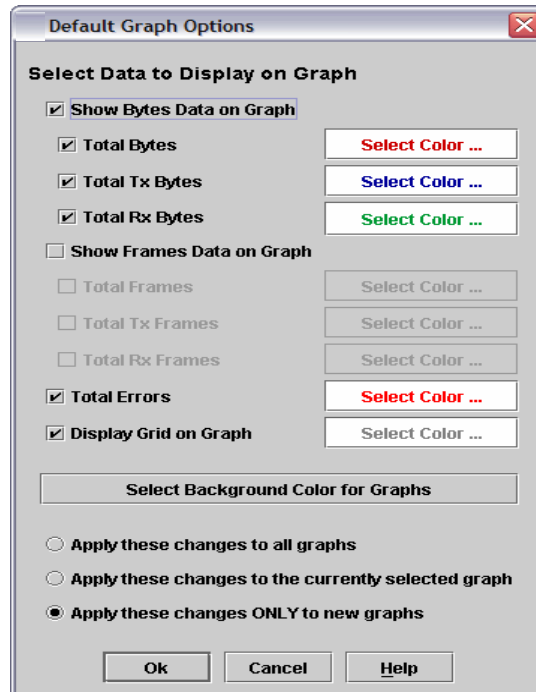


Figure 84 Default graph options

You can select to display the following data:

- ▶ Display either frames data or byte data on the graph. These can be plotted as one or all of the following, and you can also choose the color scheme for the graph:
 - Total frames/bytes transmitted and received (Total Frames/Bytes)
 - Total frames/bytes transmitted (Total Tx Frames/Bytes)
 - Total frames/bytes received (Total Rx Frames/Bytes)
- ▶ Display total errors by clicking the **Total Errors** check box.
- ▶ Display or hide the unit grid. Click the **Display Grid on Graph** check box to display the unit grid.
- ▶ Set your default graph options.
- ▶ Select one option and click an **OK** button to apply the color scheme changes to all graphs, to the currently selected graph, or to only new graphs.

Figure 85 shows an example of monitoring four ports. This includes monitoring E ports.

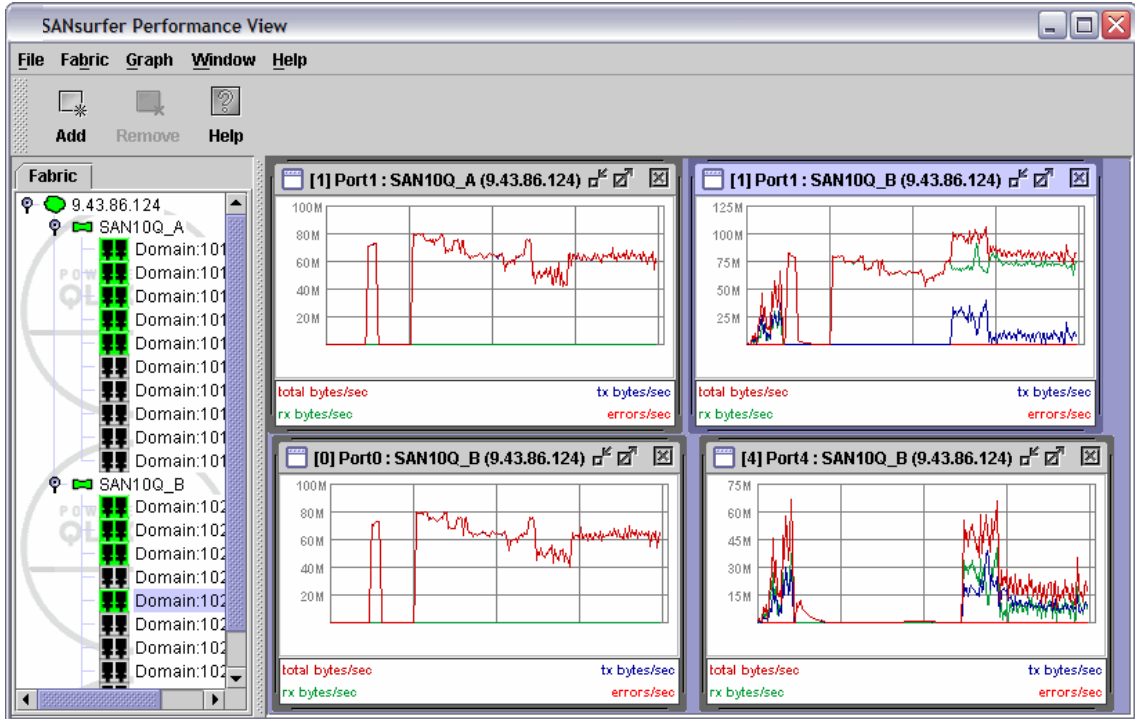


Figure 85 Performance line graph

Figure 86 shows an example of monitoring four ports using bar graphs. This includes monitoring E_Ports.

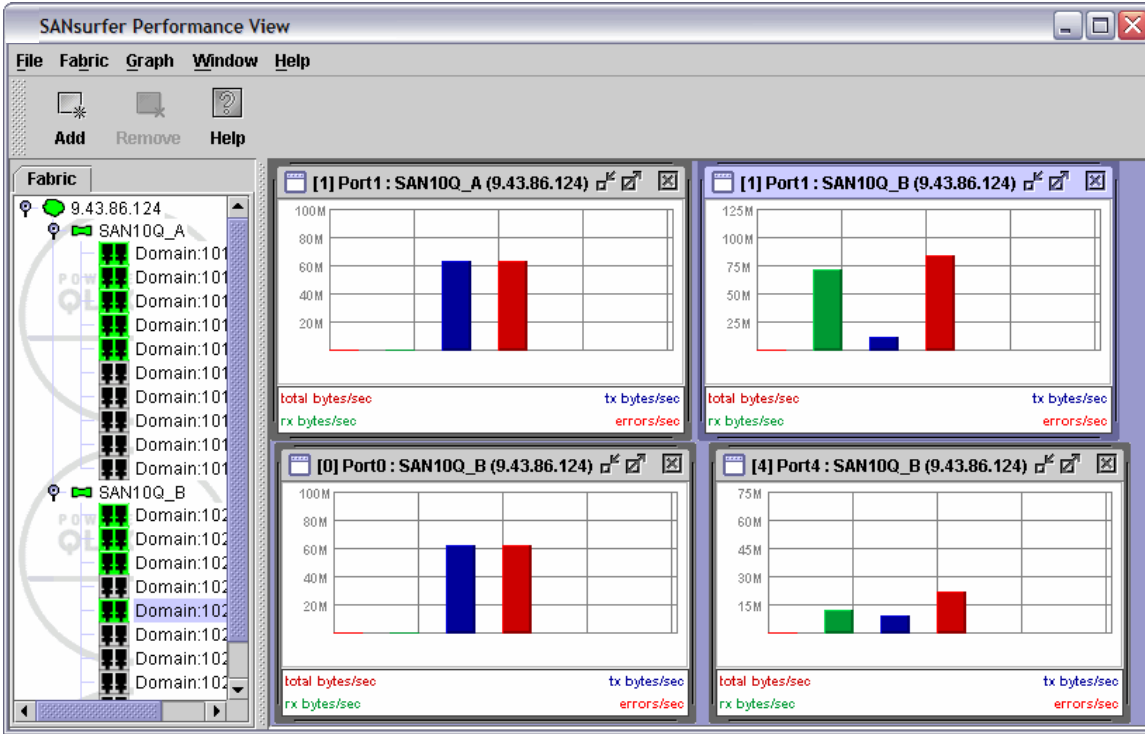


Figure 86 Performance bar graph

To change your view from bar graph to line graph, select **Graph** → **Set Global Graph Type**.

By selecting **File** → **Save Current Graph Statistics to file** from the performance view menu shown in Figure 87, you get the option to save a single graph to a file, or by selecting **File** → **Save All Graph Statistics to file**, you can save all graphs currently being monitored. This data is saved as a .csv file.

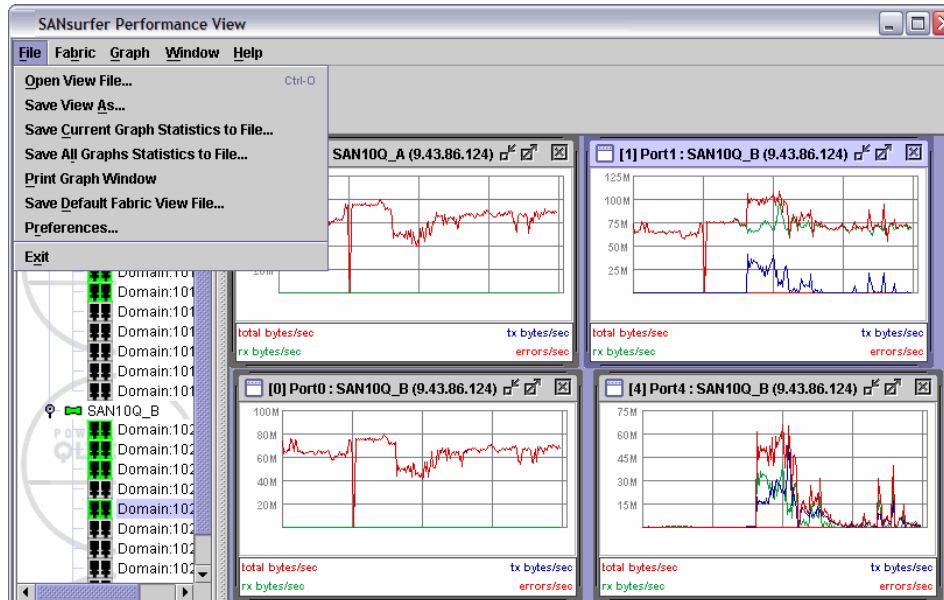


Figure 87 Saving performance data to file

By default, the polling frequency is set to one second. You can change this by selecting **Graph** → **Set Polling Frequency**. This option window is displayed in Figure 88.

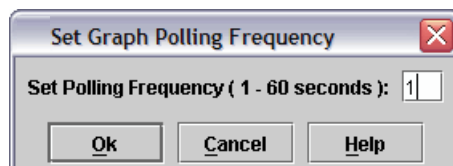


Figure 88 Polling frequency

Logs and troubleshooting

In these sections we show the logs and some basic troubleshooting information.

Event browser

The event browser displays a list of events generated by all of the switches in the fabric, as well as the switch management application. Events that are generated by the application are not saved on the switch, but can be saved to a file during the switch management session. To display the event browser, select **Fabric** → **Show Event Browser**, as shown in Figure 89.

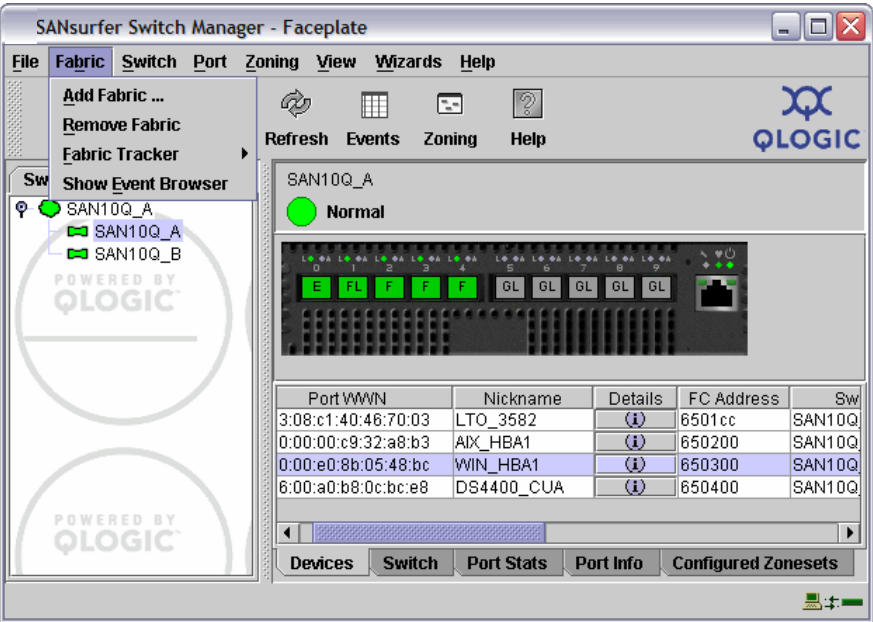


Figure 89 Event browser selection

If you cannot select the event browser option, you might have to enable the Show Event Browser option in the Fabric menu. Select **File** → **Preferences**, and from the window shown in Figure 90, enable the event browser.

Note: If the event browser is enabled using the Preferences dialog, the next time the application is started, all events from the switch alarm log are displayed. If the event browser is disabled when the application is started and later enabled, only those events from the time the event browser was enabled and forward from that time are displayed.

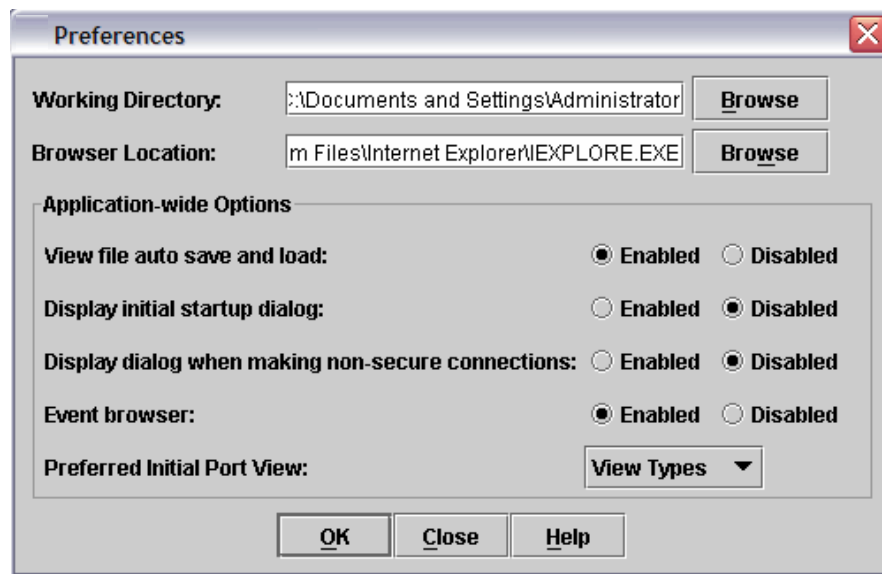
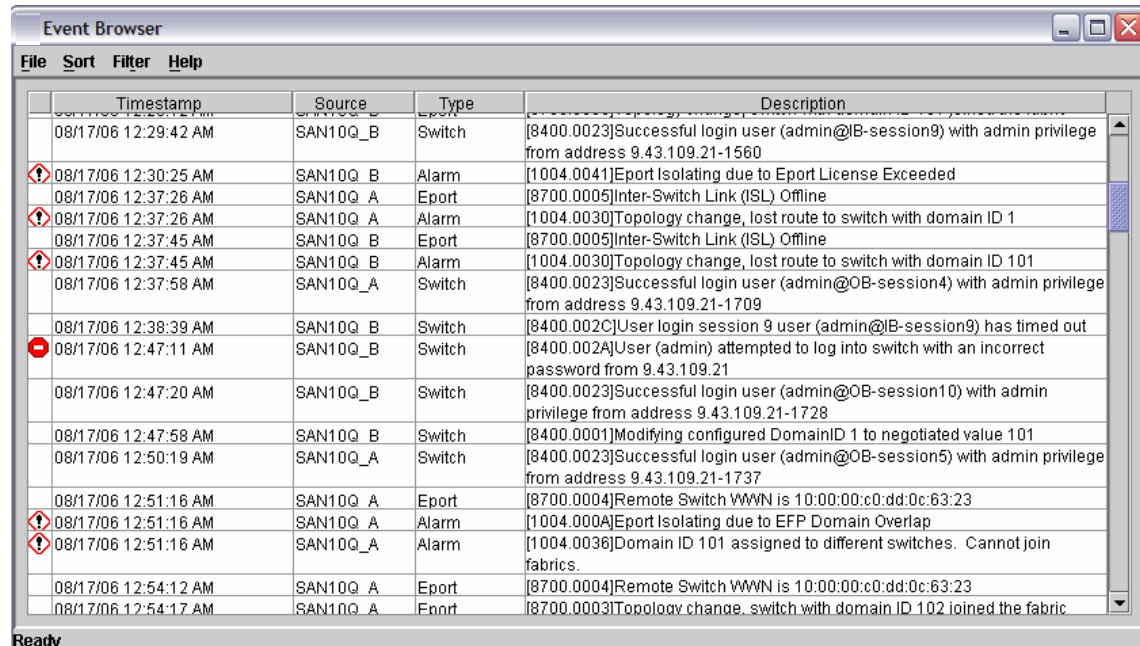


Figure 90 Preferences

Entries in the event browser, as shown in Figure 91, are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed in the event browser is 10,000. The maximum number of entries allowed on a switch is 1,200. When the maximum is reached, the event list wraps and the oldest events are discarded. The switch uses the switch time stamp, while event entries generated by the application have the workstation's time stamp.



Timestamp	Source	Type	Description
08/17/06 12:29:42 AM	SAN10Q_B	Switch	[8400.0023]Successful login user (admin@IB-session9) with admin privilege from address 9.43.109.21-1560
08/17/06 12:30:25 AM	SAN10Q_B	Alarm	[1004.0041]Eport Isolating due to Eport License Exceeded
08/17/06 12:37:26 AM	SAN10Q_A	Eport	[8700.0005]Inter-Switch Link (ISL) Offline
08/17/06 12:37:26 AM	SAN10Q_A	Alarm	[1004.0030]Topology change, lost route to switch with domain ID 1
08/17/06 12:37:45 AM	SAN10Q_B	Eport	[8700.0005]Inter-Switch Link (ISL) Offline
08/17/06 12:37:45 AM	SAN10Q_B	Alarm	[1004.0030]Topology change, lost route to switch with domain ID 101
08/17/06 12:37:58 AM	SAN10Q_A	Switch	[8400.0023]Successful login user (admin@OB-session4) with admin privilege from address 9.43.109.21-1709
08/17/06 12:38:39 AM	SAN10Q_B	Switch	[8400.002C]User login session 9 user (admin@IB-session9) has timed out
08/17/06 12:47:11 AM	SAN10Q_B	Switch	[8400.002A]User (admin) attempted to log into switch with an incorrect password from 9.43.109.21
08/17/06 12:47:20 AM	SAN10Q_B	Switch	[8400.0023]Successful login user (admin@OB-session10) with admin privilege from address 9.43.109.21-1728
08/17/06 12:47:58 AM	SAN10Q_B	Switch	[8400.0001]Modifying configured DomainID 1 to negotiated value 101
08/17/06 12:50:19 AM	SAN10Q_A	Switch	[8400.0023]Successful login user (admin@OB-session5) with admin privilege from address 9.43.109.21-1737
08/17/06 12:51:16 AM	SAN10Q_A	Eport	[8700.0004]Remote Switch WWN is 10:00:00:c0:dd:0c:63:23
08/17/06 12:51:16 AM	SAN10Q_A	Alarm	[1004.000A]Eport Isolating due to EFP Domain Overlap
08/17/06 12:51:16 AM	SAN10Q_A	Alarm	[1004.0036]Domain ID 101 assigned to different switches. Cannot join fabrics.
08/17/06 12:54:12 AM	SAN10Q_A	Eport	[8700.0004]Remote Switch WWN is 10:00:00:c0:dd:0c:63:23
08/17/06 12:54:17 AM	SAN10Q_A	Eport	[8700.0003]Topology change, switch with domain ID 102 joined the fabric

Figure 91 Event Browser

To save or export the events to a file during a session, select **File** → **Save As**, and enter a name for the XML file.

From the event browser you can get important information regarding the status of your switch or fabric. The event browser gives you detailed information regarding any errors that have occurred.

Severity is indicated in the severity column using icons. The meanings of these icons and their severity are shown in Figure 92.




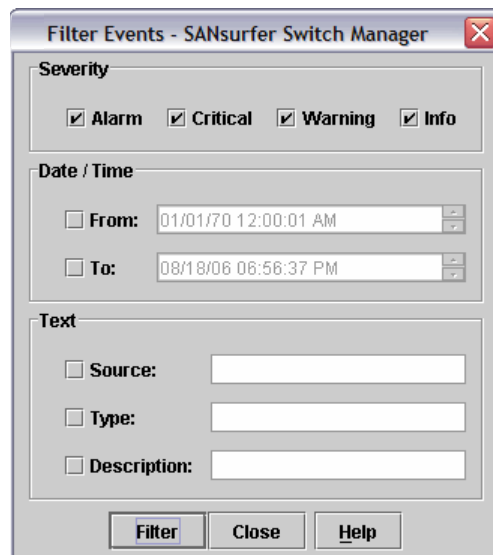
	Alarm	Alarm – An Alarm is a "serviceable event". This means that attention by the user or field service is required. Alarms are posted asynchronously to the screen and cannot be turned off. If the alarm denotes that a system error has occurred the customer and/or field representative will generally be directed to provide a "show support" capture of the switch.
	Critical	Critical event – An event that indicates a potential failure. Critical log messages are events that warrant notice by the user. By default, these log messages will be posted to the screen. Critical log messages do not have alarm status as they require no immediate attention from a user or service representative.
	Warning	Warning event – An event that indicates errors or other conditions that may require attention to maintain maximum performance. Warning messages will not be posted to the screen unless the log is configured to do so. Warning messages are not disruptive and, therefore, do not meet the criteria of Critical. The user need not be informed asynchronously.
None	Informative	An unclassified event that provides supporting information.

Figure 92 Event severity levels and icons

Filtering the event browser enables you to display only those events that are of interest based on the event severity, time stamp, source, type, and description. To filter the event browser, select **Filter** → **Filter** to open the Filter Events dialog, shown in Figure 93. The filter does not remove the events from the browser.



Filter Events - SANsurfer Switch Manager

Severity

☒ Alarm ☒ Critical ☒ Warning ☒ Info

Date / Time

☐ From: 01/01/70 12:00:01 AM

☐ To: 08/18/06 06:56:37 PM

Text

☐ Source:

☐ Type:

☐ Description:

Filter Close Help

Figure 93 Filter events dialog

Support files

The Download Support File menu option assembles all log files and switch memory data into a core dump file (dump_support.tgz). This file can be sent to technical support personnel for troubleshooting switch problems.

From SANsurfer, select the switch for which this is required. Then from the Faceplate menu, select **Switch** → **Download Support File**. You then select the desired location on your work station, and the name of the file you wish to save using the **Browse** button. Click the **Start** button and the file is saved to your workstation, as shown in Figure 94.

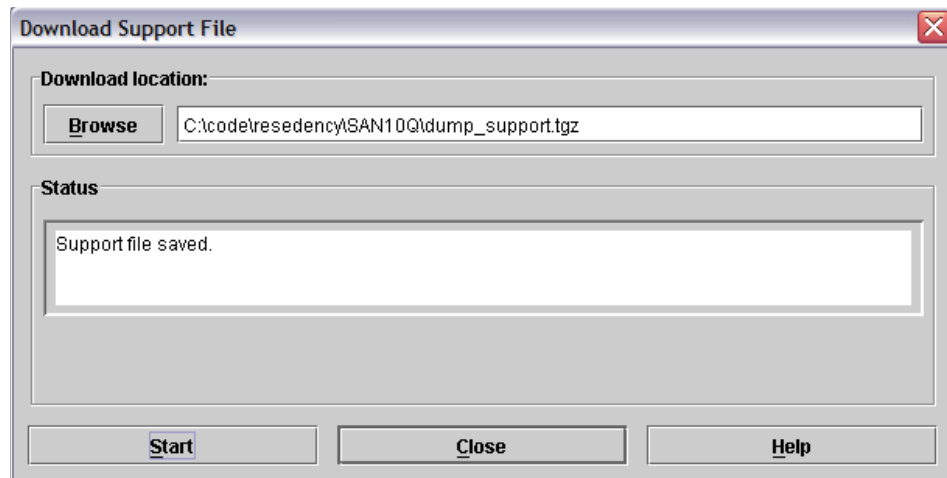


Figure 94 Support file download

Switch reset

There are three ways to reset a switch, as shown in Figure 95:

- ▶ Hot reset. This resets a switch without a power-on self-test. This reset activates the pending firmware, but does not disrupt switch traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
- ▶ Reset. This resets a switch without a power-on self-test. This reset activates the pending firmware and it is disruptive to switch traffic.
- ▶ Hard reset. This resets a switch with a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.

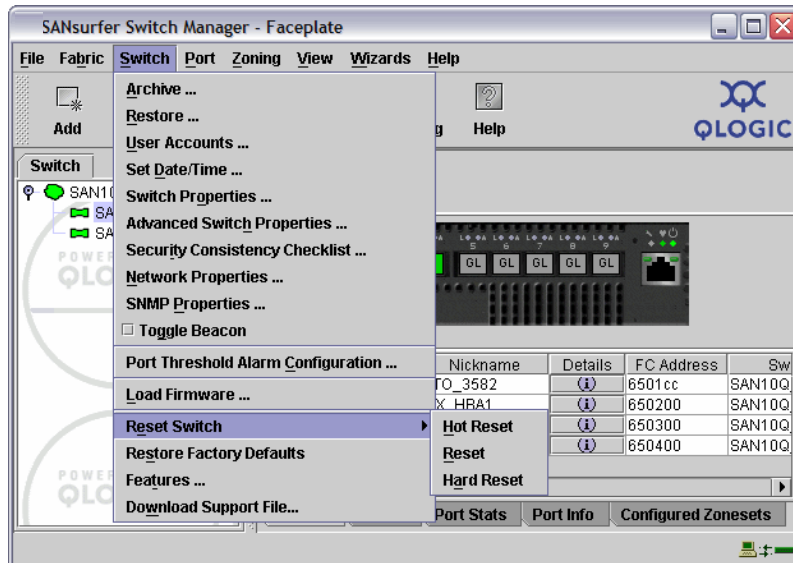


Figure 95 Switch reset

Maintenance mode

If there is a requirement to reset any switch setting to default, such as IP address or password, perform the following procedure using maintenance mode.

Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to perform the following tasks:

- ▶ Unpack a firmware image file.
- ▶ Restore the network configuration parameters to the default values.
- ▶ Remove all user accounts and restore the admin account name password to the default.
- ▶ Copy the log file.

- ▶ Restore factory defaults for all but user accounts and zoning.
- ▶ Restore all switch configuration parameters to the factory default values.
- ▶ Reset the switch.
- ▶ Update the system boot loader.

To place the switch in maintenance mode, perform the following steps:

1. Press and hold the maintenance button with a pointed tool, as indicated by the white arrow shown in Figure 96 on page 70.
2. All LEDs light up. Wait until *only* the heartbeat LED is lit, and release the button.
3. Establish a Telnet session with the switch by using the maintenance mode IP address 10.0.0.1, using a crossover cable to your workstation.
4. Enter the maintenance mode account name *prom* and password *prom*, and press Enter:

```
Switch login: prom
Password:xxxx
```

The menu shown in Example 1 is displayed.

Example 1 Account name and password

```
0) Exit
1) Image Unpack
2) Reset Network Config
3) Reset User Accounts to Default
4) Copy Log Files
5) Remove Switch Config
6) Remake Filesystem
7) Reset Switch
8) Update Boot Loader Option
```

5. You can now select a switch recovery option. Type the number corresponding to the option that you wish to select, and press Enter.

Front panel

On the front panel we have three status LEDs.

- ▶ The input power LED, which indicates the voltage status of the switch
- ▶ A heartbeat LED, which indicates the status of the internal switch processor and the results of the power-on self-test
- ▶ A system fault LED, which indicates an over-temperature condition or a POST error

We also have a reset button indicated by the white arrow in Figure 96.

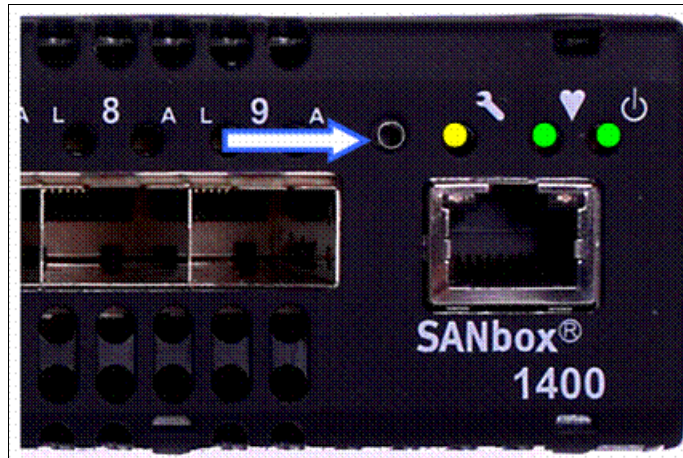


Figure 96 Front panel

LED diagnostics

In the following sections we describe the LED conditions.

Input Power LED

The input power LED is lit when the Fibre Channel switch logic circuitry is receiving the correct voltages. If the input power LED is off, complete the following steps:

1. Inspect the power cords and connectors. Is the cord disconnected or is the cord or connector damaged?
2. Inspect the ac power source. Is the power source delivering the correct voltage?
3. If the condition remains, contact your technical support representative.

System fault LED

The system fault LED is lit when the Fibre Channel switch logic circuitry is overheating or when there is a POST error. The system fault LED is always accompanied by a heartbeat LED error flash code. If the system fault LED is lit, identify the heartbeat LED error flash pattern, and take the necessary actions.

Heartbeat LED

The heartbeat LED indicates the operational status of the Fibre Channel switch. When the POST is complete with no errors, the heartbeat LED flashes at a steady rate of once per second.

When the Fibre Channel switch is in maintenance mode, the heartbeat LED is lit continuously. All other flash patterns indicate critical errors.

- ▶ Two flashes - internal firmware failure flash pattern
- ▶ Three flashes - system error flash pattern
- ▶ Four flashes - configuration file system error flash pattern
- ▶ Five flashes - over-temperature flash pattern

Port logged-in LED

Above each port is the port logged-in LED. This LED has the following three indications:

- ▶ Lit continuously - This means that a device is logged in to the port.
- ▶ Flashing once per second - This means that a device is busy logging in to the port.
- ▶ Flashing twice per second - This means that the port is down or offline, or an error has occurred. If a port logged-in LED is flashing twice per second, review the event browser for alarm messages about the affected port. You can also inspect the alarm log by using the Show Alarm command.

Note: For more detailed information regarding these LEDs, refer to Chapter 5 of the *System Storage SAN10Q 4 Gbps 10-Port Fibre Channel SwitchType 6918 Installation Guide*, 31R1632, on the CD supplied with the switch.

Port testing

The following sections cover the ways to test a port.

Resetting a port

The Reset Port option re-initializes the port using the saved configuration. From the Faceplate window, select the ports to be reset, then select **Port** → **Reset Port**. You get the confirmation message shown in Figure 97. Click **OK** to reset the port.

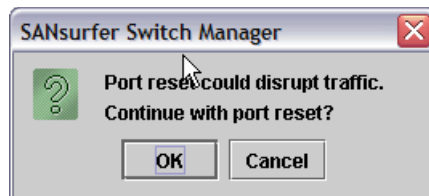


Figure 97 Resetting port

Testing ports

The port loopback tests verify correct port operation by sending a frame out through the loop, and then verifying that the frame received matches the frame that was sent. Only one port can be tested at a time for each type of test.

To run the internal, external, or online port loopback test on a port, select **Port** → **Port Loopback test**, and window shown in Figure 98 is displayed. From this window, you have the following panels available:

- ▶ Test Selection area: Here you can choose the type of loopback test to be run and select the port number:
 - Internal: The internal test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and is therefore disruptive.

Port Loopback Test

Symbolic Name: SAN10Q_B

Test Details

Internal loopback test can be performed only on a port set to the diagnostic state.

Internal loopback tests all the

Test Selection

Select Port: Port 3

Select Test:

☒ Internal ☐ External ☐ Online

Test Results

Test Status: Inactive

Frames Sent:

Failure Count:

Test parameters

Frame Count: 100

Frame Size [40-292]: 256

Test Pattern:

☒ Use Default Pattern ☐ User Defined Pattern [hex]: f5f5f5f5

☐ Terminate Test Upon Error

Start Test Stop Test Close Help

Figure 98 Port loopback test

- External: The external test sends a test frame from the ASIC through the SerDes chip, through the SFP module fitted with an external loopback plug (as shown in Figure 99), and back to the ASIC for the selected ports. The port passes the test if the test frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and is therefore disruptive.

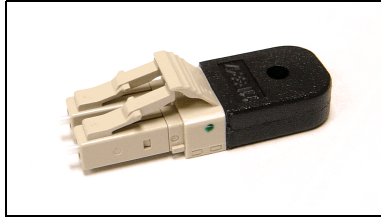


Figure 99 External loopback plug

- Online: The online test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes the test if the frame that was sent by the ASIC matches the frame that was received. This test does not disrupt communication on the selected port.
- Test Parameters:
- Enter the frame count.
 - Enter the frame size.
 - Enter the test pattern. You can use the default pattern or enter an 8-digit pattern (hex). For online test, you can select the Terminate Test Upon Error check box if you want the test to stop should it encounter an error. You click **Start Test** to begin the test. The Test Results area shows the test status, number of frames sent, and number of errors found.

Click **Start Test**, as shown in Figure 98 on page 72, to begin the test. You get a window like the one shown in Figure 100. Read this message and click **OK**. Then observe the results in the Test Results area of the window shown in Figure 98 on page 72.

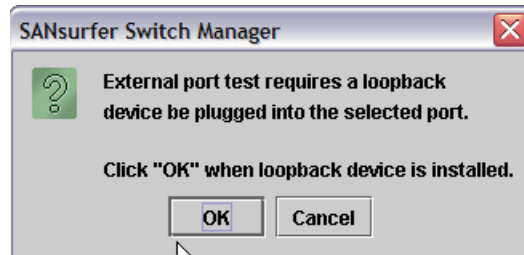


Figure 100 Start test dialog

Take the necessary actions based on the resultant feedback. If necessary, contact technical support for diagnostic help.

The team that wrote this IBM Redpaper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Michael Engelbrecht is a Senior IT Specialist in IBM Global Technical Services, ITS. He has worked with IBM for 26 years. For the last six years he has provided support for South Africa and Africa for storage products, including all SAN products. Before this, he was a Networking Specialist with many years of networking experience on a large range of networking equipment, specializing in ATM and Frame relay. He is currently level 1 and 2 support, Product Manager, and Educator for zSeries® tape storage, open system tape storage, as well as all SAN switch products for South Africa and Africa. The products are supported from South Africa.

Jon Tate is a Project Manager for IBM System Storage SAN Solutions at the International Technical Support Organization, San Jose Center. Before joining the ITSO in 1999, he worked in the IBM Technical Support Center, providing level 2 support for IBM storage products. Jon has 22 years of experience in storage software and management, services, and support, and is both an IBM Certified IT Specialist and an IBM SAN Certified Specialist.

Thanks to the following people for their contributions to this project:

Keith Burnett

Nasir Moinuddin

QLogic Corporation

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrates programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM application programming interfaces.

© Copyright International Business Machines Corporation 2008. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This document REDP-4370-00 was created or updated on January 2, 2008.


Send us your comments in one of the following ways:

- ▶ Use the online **Contact us** review Redbooks form found at:
ibm.com/redbooks
- ▶ Send your comments in an email to:
redbook@us.ibm.com
- ▶ Mail your comments to:
IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099, 2455 South Road
Poughkeepsie, NY 12601-5400 U.S.A.



Trademarks

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

Redbooks (logo) ®
zSeries®

IBM®
System Storage™

TotalStorage®

The following terms are trademarks of other companies:

SANsurfer, QLogic, and the QLogic logo are registered trademarks of QLogic Corporation. SANblade is a registered trademark in the United States.

Acrobat, and Portable Document Format (PDF) are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Internet Explorer, Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.