IBM TotalStorage SAN n–type Director Family

Enterprise Manager Installation and Operation Guide

Read Before Using

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

GC26-7720-00

IBM TotalStorage SAN n−type Director Family

Enterprise Manager Installation and Operation Guide

GC26-7720-00

First Edition (November 2004)

The following paragraph does not apply to any country (or region) 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 MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states (or regions) do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Order publications through your IBM® representative or the IBM branch office serving your locality.

© Copyright International Business Machines Corporation 2004. All rights reserved.
US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

© Copyright IBM Corp. 2004

© Copyright IBM Corp. 2004

Figures

© Copyright IBM Corp. 2004

Tables

© Copyright IBM Corp. 2004

About this document

This guide is intended to assist you with the installation and operation of the Enterprise Manager Software for the IBM TotalStorage SANn-type director family for Windows XP Pro, which is available for the CNT FC/9000™ Fibre Channel Switch and IBM TotalStorage SAN256N director 2045-N16. The software comes in server-based and client-based modules. This guide provides step-by-step instructions for installing the software.

The intended audience for this document is anyone involved in the installation and operation of the FC/9000 Fibre Channel Switch, SAN256N director, and Enterprise Manager Software.

- The Enterprise Manager Software should *only* be installed on a PC running Windows 2000® or Windows XP® . The Client software may be installed on a machine running the other listed operating systems.

IBM TotalStorage SAN switch library

The following documents contain information related to this product:

- IBM TotalStorage SAN n-type Director Series Enterprise Manager Installation and Operator Guide (GC26-7720) - this document
- IBM TotalStorage SAN256N Director 2045-N16 Installation and Maintenance Guide (GC26-7714)
- IBM TotalStorage SAN256N Director 2045-N16 Release Notes (GC26-7716)
- IBM TotalStorage SAN Director 2045 Statement of Limited Warranty (GC26-7718)
- IBM TotalStorage SAN n-type Director Series Site Planning Guide (GC26-7715)
- IBM TotalStorage Translated Safety Notices (GC26-7717)

Web sites

You can find additional information related to the software for this and other switches at the following Web site:

http://www.ibm.com/servers/storage/support/san

To get specific details about models and firmware that the switch supports, see the following Web site:

http://www.storage.ibm.com/ibmsan/

For detailed information about the Fibre Channel standards, see the Fibre Channel Industry Association (FCIA) Web site at:

www.fibrechannel.org/

For a directory of worldwide contact information, including technical support, see the following Web site:

www.ibm.com/contact/

© Copyright IBM Corp. 2004

Getting software updates

Contact IBM for software updates and maintenance releases.

Select the SAN support link at the following Web site:

http://www.storage.ibm.com/ibmsan/index.html

Getting help

Before contacting technical support, check for solutions in this guide or check with the network administrator.

Online

Contact technical support at the following Web site:

http://www.ibm.com/servers/storage/support/san/index.html

Telephone

Within the United States, call 1-800-IBM-SERV (1-800-426-7378).

Outside the United States, go to the following Web site to find the appropriate service number:

http://www.ibm.com/planetwide/

How to send your comments

Your feedback is important in helping us provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, you can send us comments electronically by using the following addresses:

- Internet: starpubs@us.ibm.com
- IBMLink™ from U.S.A.: STARPUBS at SJEVM5
- IBMLink from Canada: STARPUBS at TORIBM
- IBM Mail Exchange: USIB3VVD at IBMMAIL

You can also mail your comments by using the Reader Comment Form in the back of this manual or direct your mail to:

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona 85744-0001 U.S.A.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

Chapter 1. Introduction

This chapter discusses the Enterprise Manager Software for the IBM TotalStorage SANn-type director family package contents and system requirements, and provides an overview of the application. It also lists which actions an Enterprise Manager Software user can perform, based on their level of access.

Software package contents

The Enterprise Manager software package includes this software guide and a CD-ROM which contains the Server and Client software. Instructions for installation and control of both systems are included in this guide.

System requirements

Enterprise Manager Software workstation requirements

A designated Enterprise Manager Software Intel ® platform is an integral part of the SAN256N director operation, where the Enterprise Manager Software is installed and run by the operator.

IBM supports the Enterprise Manager Software that adheres to the requirements listed below.

The customer’s Enterprise Manager Software configuration meets the following requirements:

- The SERVER solution is listed on Microsoft's ® certified solutions web page (http://www.microsoft.com/whdc/hcl/default.mspx)
- Has the (“Designed For Windows 2003 or 2000") or (“Certified for Windows 2003 or 2000) stamp of approval
- O/S support has not been discontinued by Microsoft (http://support.microsoft.com/default.aspx?scid=fh;[ln];LifeWin)
- Meets resource requirements as identified below:
  - Operating System: Windows 2000 Professional ® or Windows XP Professional ®
  - Processor: One Intel Pentium 4 (1.8 GHz +)
  - Memory: See table below

Table 1. Memory required per number of port blocks

Number of Port Blocks	Maximum Number of Ports	Memory Required
FC/9000 1	256	256 MB
FC/9000 2	512	512 MB
SAN256N director 1	256	512 MB

© Copyright IBM Corp. 2004

Note: Memory requirements must be based upon the number of port blocks, and not based upon the number of ports.

- Other:
  - 4 MB video RAM
  - One 40 GB hard drive
  - One 1.44 MB diskette drive
  - One CD-ROM
  - One parallel port
  - Two Ethernet 10Base-T/100 Base-TX
  - One IBM or equivalent mouse
  - One external serial com port (external modem)
  - One internal com port (internal modem)
  - One 17-inch 1280 x 1024 x 256 SVGA monitor
  - Internal and external modem compatibility; analog, protocol support: V.90 5 6kbps ITU Standard

Note: Multi-Tech™ hardware compatible modems recommended (do not use Winmodem® software controlled modems)

Maintenance of a customer supplied Enterprise Manager Software Intel platform and Windows 2000 Professional or Windows XP Professional Operating System is a customer responsibility.

Enterprise Manager Software overview

The Enterprise Manager Software for the IBM TotalStorage SANn-type director family Switch management application is able to manage a variety of switch products (8-port, 16-port, 64-port, single-stage, multi-stage, etc.). The following description describes the functions of the application. The application grays-out or does not display functions that do not pertain to the selected switch chassis.

Fabric/switch interoperability

The Enterprise Manager Software manages fabrics made up of IBM TotalStorage SAN256N director 2045-N16 and FC/9000 director switches. In addition, the Enterprise Manager Software is capable of managing SAN256N director and FC/9000 Director fabrics that connect to FC/9000-8, FC/9000-16, and FC16-2 switches. Currently, the Enterprise Manager Software can control the SAN256N director, FC/9000 8- and 16-port switches and, 64-, 128- and 256-port directors. The Enterprise Manager Software allows you to view, but not control, the FC16-2 switch and switches from other vendors.

Fabric monitoring

The Enterprise Manager Software provides the following fabric and switch monitoring capabilities:

- View the fabric IP connection(s)
- View hardware and firmware version information for the selected chassis

- View switch names and World Wide Names (WWNs) of all chassis
- View port addresses on the selected chassis
- View Interswitch Links (ISLs) and their port addresses
- View dynamic statistics that display performance data for each online port on the selected chassis. Performance data includes traffic throughput and error counts.
- View Name Server data for each device connected to the selected chassis
- View the type of GBIC or SFP installed in each port on the selected chassis
- View the address, WWN, FC-4 type, and logged-in status of each loop device (FC/9000 only) connected to any port on the selected chassis
- View zoning currently active and inactive in the fabric

Fabric configuration

The Enterprise Manager Software provides the following switch and fabric configuration capabilities:

- Auto-discover and manage multiple fabrics
- Set up connection to the Ethernet ports on the switch chassis through which the fabrics are managed
- Configure the Switch Management interface with its IP network configuration parameters and SNMP configuration parameters
- Configure chassis switch name
- Configure the mode of each port on the selected chassis. Port modes include:
  - E_Port
  - F_Port (port forced to be an F_Port)
  - TL_Port (port forced to be a Private Translated Loop port) (FC/9000 1 Gig models)
  - Off Line (port forced offline)
  - Test (port forced into test mode)
- Configure loop devices (FC/9000 directors) including:
  - Place any NL_Port into Loop Bypass mode
  - Place any or all NL_Ports back into normal Loop mode
  - Reset the loop
  - Re-initializing the loop

Note: Loop capability is available and supported only on the FC/9000 models.

Fabric zoning

E_Port zoning divides the fabric for more efficient and secure communication among functionally grouped nodes.

Privileges

The following table lists the privileges a user is entitled to based on the system access level.

Table 2. Privilege descriptions

Privilege	Role: Viewer	Role: Operator	Role: Administrator
Fabrics	No Add, Delete, or Apply	No Add, Delete, or Apply	Full access
Fabrics-Topology	Full access	Full access	Full access
Fabrics-Zoning, saved zones	No Add, Delete, or Apply	Full access	Full access
Switch-General	Cannot change	Cannot change	Full access
Switch-Hard Zoning	Cannot change	Full access	Full access
Switch-Version	Full access	Full access	Full access
Switch-Code Load	Not visible	Not visible	Not visible
Switch-Event Log	Cannot delete	Full access	Full access
FIO/TFIO-General	Cannot change	Full access	Full access
FIO/TFIO-Name Service	Full access	Full access	Full access
Port-General	Cannot change	Full access	Full access
Port-Loop Devices	Cannot change	Full access	Full access
FCM/TCM	Cannot change	Cannot change	Cannot change
FC8/16-General	Cannot change	Cannot change	Can change name only
FC8/16-Version	Full access	Full access	Full access
FC8/16-Name Service	Full access	Full access	Full access
FC8/16-Event Log	No Delete	Full access	Full access
Traps-Acknowledge		Full access	Full access
Audit Trail	Full access	Full access	Full access
Trap Settings	Cannot change	Cannot change	Full access
Port Parameters, port configuration	Cannot change	Full access	Full access
User Admin	Cannot change	Can change only own password	Full access to Viewer, Operator, and Administrator IDs. Cannot see Maintenance IDs or Role.
Trap Settings	Cannot change	Cannot change	Can change
TOVs: IP Addr	Cannot change	Cannot change	Cannot change

Table 2. Privilege descriptions (Continued)

Privilege	Role: Viewer	Role: Operator	Role: Administrator
Domain ID, FICON Mode	Cannot change	Cannot change	Cannot change
Fab ID, Chassis ID	Cannot change	Cannot change	Cannot change
SNMP Param	Cannot change	Cannot change	Can change
Default Config (User, PW)	Viewer, Viewer	Operator, Operator	Administrator, Administrator
CUP Configs	Cannot change	Cannot change	Full access
Node Desc. View	Full access	Full access	Full access

Chapter 2. Installing and setting up Enterprise Manager Software

The correct Windows operating system should already be installed on the PC upon which you will install the Enterprise Manager Server, the Enterprise Manager Client, and the Java Runtime Environment (JRE). The Server and Client components are installed separately.

Note: When planning a fabric, you may only have one Enterprise Manager Software per fabric for control. Having more than one Enterprise Manager will cause serious conflicts among the various Enterprise Managers.

Installing the Enterprise Manager Software server

The following instructions show you how to install the Enterprise Manager Software Server software on a PC. Refer to the "System requirements" on page 1 if you are loading the software on a PC other than a IBM-supplied workstation.

Note: The 9.x version of the Enterprise Manager Software requires Java Runtime Environment (JRE) 1.4.2. You will need to uninstall previous versions of the JRE prior to installing the newer one.

To install the Enterprise Manager Software Server on a PC:

1. Double-click the **setup.exe** file to run the CD-ROM from the CD drive of your PC.
2. Click **Next** to begin the installation.
3. Read the License Agreement and then click **Next** to accept and proceed.
4. Click **Next** again to accept "English" as the prefered language.
5. From the next window, indicate whether you want to install the Enterprise Manager Software Server in the default directory or in a directory you specify. If you choose to install the software in your own directory, enter the path to the directory in the **Directory Name** field. Click **Next** to proceed.

   Note: IBM recommends that you use the default directory.
6. Review the install information that is displayed, and then click **Next**. If you disagree with the information, use the **Back** button to return to previous windows to make any changes.

   A progress bar begins to display the installation status.
7. Click **Next** when the download is complete.
8. The remaining window explains how to start the application. Click **Finish** to complete the installation.

© Copyright IBM Corp. 2004

Installing the Enterprise Manager Software client

Note: Supported client platforms at this time are Windows 95 ®, Windows 98 ®, Windows 2000 ® with Service Pack 2 or above, and Windows XP Pro ®; Linux ® (kernel 2.2.12 and above); and Solaris ® SPARC 8 and above.

Once the Enterprise Manager Software server application is loaded on the management workstation, you can configure the client(s) for use with the server. The client platform requires the Netscape 6.x or Internet Explorer 5.x browser and Adobe Acrobat Reader (version 5.0 or greater). It uses the Sun Java Runtime Environment and Java Web Start to provide a uniform Java distribution for the various supported Client platforms; this also improves performance by caching Java applet class and jar files on the local Client. The necessary files can be downloaded from the Server PC using a supported browser on the Client platform.

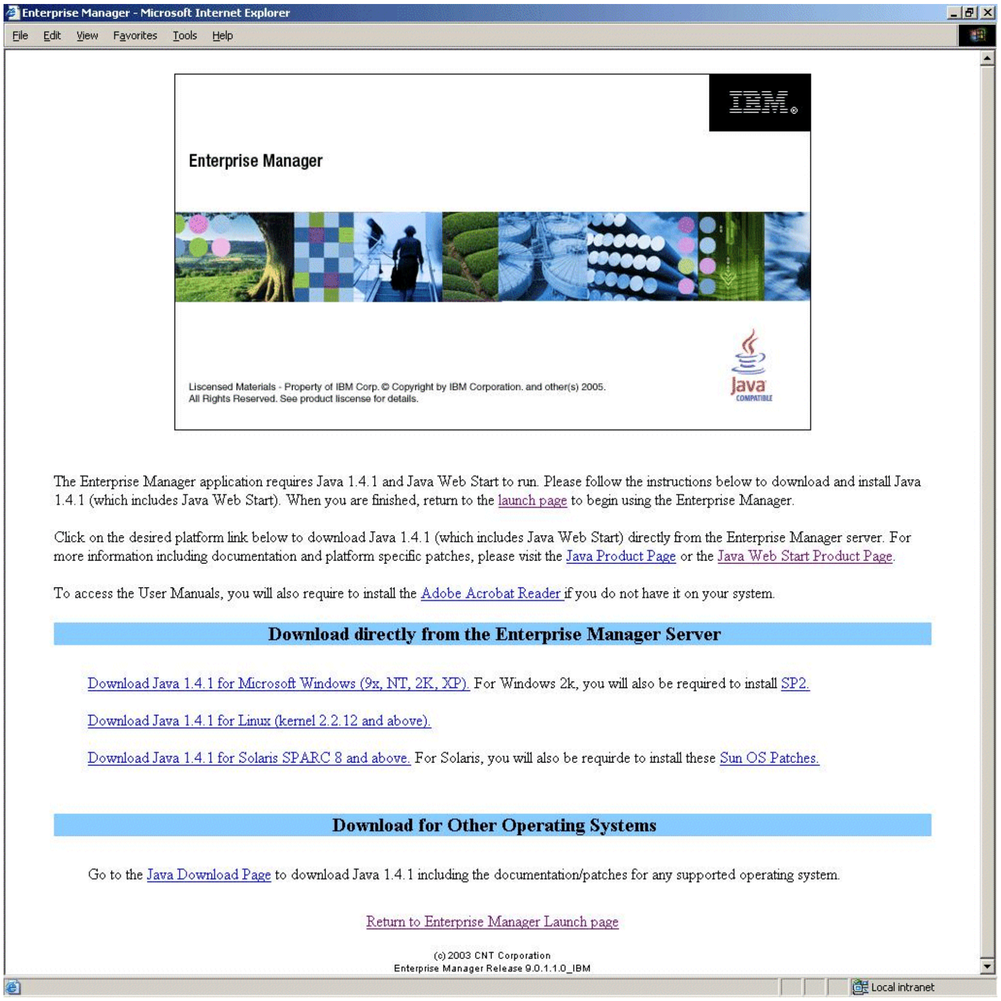
Note: If an earlier version of Java Runtime Environment/Java Web Start has been installed on the PC on which the client will reside, you should uninstall this previous version (if possible) before downloading the new version using these procedures.

Installing the Java Runtime Environment (JRE) software

To download the client software from the server PC (requires network access to the server PC):

1. Close all open applications on the client and then open a web browser.

2. Enter the IP address for the Server PC in the **Address** field of the browser and press the **Enter** key. When the web browser connects with the Server PC, the following window appears.



Enterprise Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
IBM.
Enterprise Manager
Java COMPATIBLE
Local intranet

Liscensed Materials - Property of IBM Corp. © Copyright by IBM Corporation. and other(s) 2005.
All Rights Reserved. See product liscense for details.

The Enterprise Manager application requires Java 1.4.1 and Java Web Start to run. Please follow the instructions below to download and install Java 1.4.1 (which includes Java Web Start). When you are finished, return to the launch page to begin using the Enterprise Manager.

Click on the desired platform link below to download Java 1.4.1 (which includes Java Web Start) directly from the Enterprise Manager server. For more information including documentation and platform specific patches, please visit the Java Product Page or the Java Web Start Product Page.

To access the User Manuals, you will also require to install the Adobe Acrobat Reader if you do not have it on your system.

Download directly from the Enterprise Manager Server

Download Java 1.4.1 for Microsoft Windows (9x, NT, 2K, XP). For Windows 2k, you will also be required to install SP2.

Download Java 1.4.1 for Linux (kernel 2.2.12 and above).

Download Java 1.4.1 for Solaris SPARC 8 and above. For Solaris, you will also be requirde to install these Sun OS Patches.

Download for Other Operating Systems

Go to the Java Download Page to download Java 1.4.1 including the documentation/patches for any supported operating system.

Return to Enterprise Manager Launch page

(c) 2003 CNT Corporation
Enterprise Manager Release 9.0.1.1.0_IBM

Figure 1. JRE download window

Downloading the JRE for a Windows platform

1. Select **Download Java 1.4.2 for Microsoft (9x, NT, 2K, XP)** from the list that appears on the **JRE Download** window. The File Download dialog box is displayed.

2. Click **Save** to save this program to your computer.

3. You will be prompted to identify the directory location for this download. Choose a known directory (e.g., **C:/Temp**) in which to save the executable file. Click **Save** and wait for the download to complete.

4. Log out of the web browser.

5. Access the directory in which you saved the executable file. Double-click the file **j2re*.exe** to load Java Web Start onto your PC.

6. A License Agreement for Java Web Start appears. Read the conditions and terms of this agreement and then click **Yes** to continue.

7. Accept the default **Typical** setup type on the following window by clicking **Next>**.

8. The remainder of the Java Web Start installation process is automated. When it is completed, a **Java Web Start** icon will appear on your desktop.

Downloading the JRE for a Linux platform

1. Login as root (at the Administrator level) and open a web browser.
2. Type in the IP address of the Server PC and press the **Enter** key.
3. The management software will recognize that you do not have the Java Runtime Environment (JRE) resident on the PC. Click **Do so now**. The download window appears.
4. Select **Download Java 1.4.2 for Linux (kernel 2.2.12 and above)** from the list that appears on the window.
5. Save the script file to the /opt directory and click **Save**.

   Note: You may choose /opt or any other directory to install Java.
6. Log out of the web browser.
7. Go to the /opt directory to access the file. Type `chmod 555 j2re*.sh` and then press the **Enter** key.
8. Type `./j2re*.sh` and then press the **Enter** key.
9. Scroll through the License Agreement, type `Yes` to accept, and press the **Enter** key at the end of the agreement. Files will now be placed on the PC.
10. Change directories to the **j2re1.4.x** directory.
11. Unzip the javaws*.zip file.
12. Type `./install.sh` and press the **Enter** key.
13. Once again, read through the License Agreement, type `Yes`, and press the **Enter** key to accept the License Agreement.
14. Type `/opt/j2re1.4.2`, press the **Enter** key, and open a web browser.
15. Type in the IP address of the server on which the Enterprise Manager Server software is located and press the **Enter** key.
16. Some browsers will not detect the JRE that you just installed. Click **Launch!** anyway. The Performance Vision client application will launch.

Downloading the JRE for a Solaris platform

1. Login as root (at the Administrator level) and open a web browser.
2. Type in the IP address of the Server PC and press the **Enter** key.
3. The management software will recognize that you do not have the JRE resident on the PC. Click **Do so now**. The download window will appear.
4. Select **Download Java 1.4.2 for Solaris SPARC 8 and above** from the list that appears on the window.
5. Save the script file to the /opt directory and click **Save**.
6. You may choose /opt or any other directory to install Java.
7. Log out of the web browser.
8. Go to the /opt directory to access the file. Type `chmod 555 j2re*.bin` and then press the **Enter** key.

9. Type `/opt/j2re*.bin` and then press the **Enter** key.
10. Read through the License Agreement, type `Yes` to accept, and press the **Enter** key at the end of the agreement. Files will now be placed on the PC.
11. Change directories to the **j2re1.4.x** directory.
12. Unzip the javaws*.zip file.
13. Type `./install.sh` and press the **Enter** key.
14. Once again, scroll through the License Agreement, type `Yes`, and press the **Enter** key to accept the License Agreement.
15. Type `/opt/j2re1.4.2`, press the **Enter** key, and open a web browser.
16. Type in the IP address of the server on which the Enterprise Manager Software server software is located and press the **Enter** key.
17. Some browsers will not detect the JRE that you just installed. Click **Launch!** anyway. The Performance Vision client application will launch.

Installing the JRE from the technical manuals CD

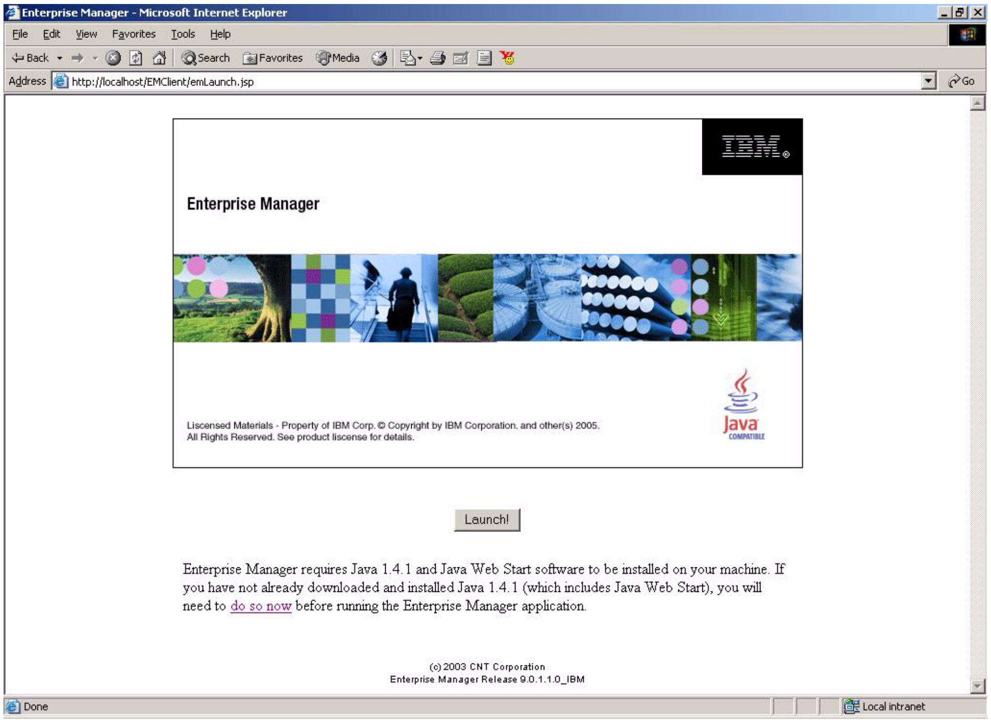
Your local network security configuration may prevent downloads of executable program files via an Internet browser. For this reason, the necessary Java Web Start files also are provide on the Enterprise Manager Software Technical Manuals CD supplied by IBM. To install Java Runtime Environment on the client from this CD:

1. Close all open applications on the client.
2. Insert the Technical Manuals CD (1014569-001-XX) into the CD drive of the client.
3. Navigate to the CD drive.
4. Copy the Java Runtime Environment executable file appropriate for your platform to a known directory and then follow the instruction above (for Windows, Linux, or Solaris platforms) to install the program onto the client.

Starting the Enterprise Manager Software client

After the Java Runtime Environment is loaded onto the client, you can download the Enterprise Manager Software client.

1. Enter the IP address of the Server PC in the **Address** field and press the **Enter** key. The following window appears..



Enterprise Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://localhost/EMClient/emLaunch.jsp
Go
IBM
Java COMPATIBLE
Launch!
Done
Local intranet

Enterprise Manager

Liscensed Materials - Property of IBM Corp. © Copyright by IBM Corporation. and other(s) 2005.
All Rights Reserved. See product liscense for details.

Enterprise Manager requires Java 1.4.1 and Java Web Start software to be installed on your machine. If you have not already downloaded and installed Java 1.4.1 (which includes Java Web Start), you will need to do so now before running the Enterprise Manager application.

(c) 2003 CNT Corporation
Enterprise Manager Release 9.0.1.1.0_IBM

Figure 2. Enterprise Manager launch window

Note: If you are using the Netscape browser, this page may display a warning `(Unable to detect the installation of Java 1.4.2)` when Java Runtime Environment version 1.4.2 is installed. If this warning appears on a Client with Java Runtime Environment 1.4.2 installed, click **Launch!** to load the Enterprise Manager Software application correctly.

2. Click **Launch!** to download the Enterprise Manager Software Java applet class and jar files to the client. A Security Warning dialog appears. Read this warning and then click **Start** continue the download process.
3. The Enterprise Manager Software Login dialog appears. It is recommended that you change the factory-default password for the system user account as soon as you have finished the initial configuration of the Enterprise Manager Software. Review the User Security information in Chapter 4 for information on passwords. Record the new password for future reference and keep it in a safe location.
4. When the login process is complete, the Enterprise Manager Software window appears.

Setting up the server and client

Use the following instructions to start the server and connect a client to the server.

Starting the server

At the CSM upon which the server software is loaded, start up the server by double-clicking the **Enterprise Manager Software** icon on the desktop.

Note: Icons are placed on the desktop when the software is installed. You must login to access server functionality or perform operations presented at the task bar.

Connecting a client to a server

Before you begin, make sure the server is running before you try and connect to it.

1. Connect to a server by opening a web browser and then typing in the IP address or machine name of the PC on which the server is located.

   Note: The second time you launch into a particular server, you will be asked whether you would like to create a shortcut on your PC to that server.

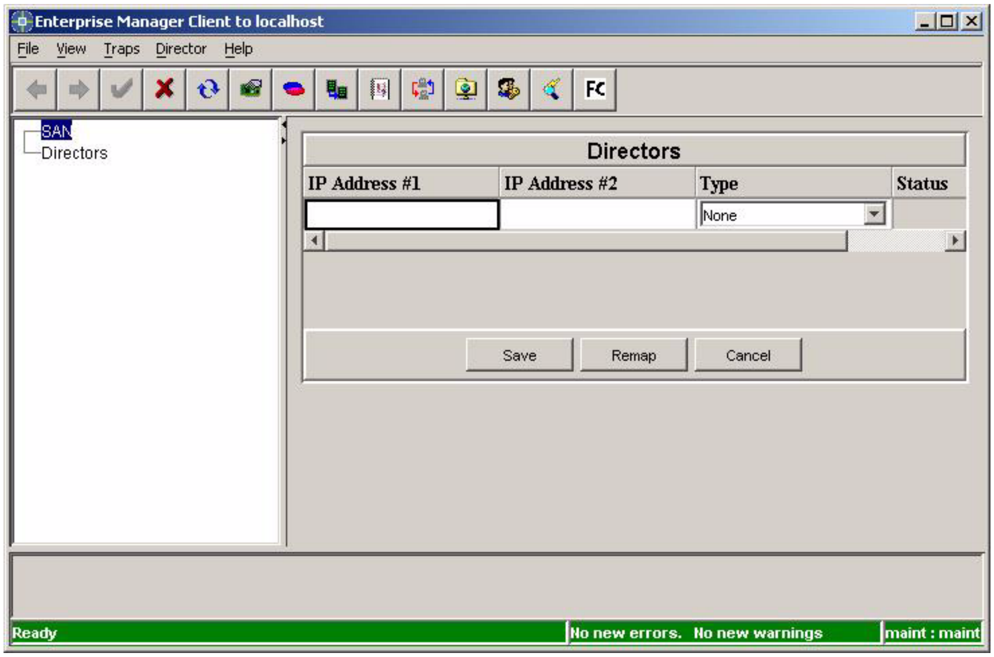
2. When prompted, type in your user ID and password. If the server to which you want to connect is located on the PC that is operating the Client, type `localhost` in the **Address** field on the browser and press the **Enter** key.

Setting up for fabric discovery

You must discover fabrics that contain the switches to which you want to connect ports, view statistics, create zones, or other such tasks.

To discover a fabric:

1. Start the client software.
2. Type in the username and the password, which will allow you to perform administrative tasks, typically the default admin level user. If User Security has been altered, then a user who has the ability to perform this task may also log in.



Directors

IP Address #1	IP Address #2	Type	Status
		None	

Ready | No new errors. No new warnings | maint : maint

Figure 3. Main Window

3. With an FC/9000, determine the first chassis or port block of the director. The first chassis of the director contains the primary and backup FCMs.

- In a 128-port director, it will be the bottom chassis and the Primary FCM will be on the right.
- In a 256-port director, the first chassis will be the left bottom chassis. The view is from the front of the director.

4. In a SAN256N director, the primary TCM is on the top and the secondary is on the bottom.
5. Determine the IP addresses of the Primary and Backup TCMs/FCMs of the director which you would like to add.
6. Select the type of director from the drop down list.
7. Type in the IP address of the primary TCM/FCM in the **IP Address #1** field.
8. Type in the IP address of the backup TCM/FCM (if there is one for the director) in the **IP Address #2** field.
9. Enter the IP addresses of the other directors and switches which will be a part of the fabric.
10. Click **Save**.

Using the entered IP addresses, the Enterprise Manager Software auto-discovers the fabric. Each discovered fabric is automatically named based on the principal switch for an E_Port fabric. The fabric should now appear under the Fabrics header in the Navigation Tree.

Fabric remap

Clicking the **Remap** button causes the fabric to be re-discovered and any directors to which Enterprise Manager has lost connection will be deleted.

Uninstalling the Enterprise Manager Software

If you find it necessary to uninstall the Enterprise Manager Software, use the following procedure.

1. From the Windows Desktop, click **Start | Control Panel** and then double-click the **Add/Remove Programs** option.
2. Click Enterprise Manager Software and then click the **Change/Remove** button. Follow the on-screen instructions.
3. Manually delete all other files.

Chapter 3. Operation Basics

This chapter presents information about:

- Enterprise Manager Software operation
- Enterprise Manager window features, icons, and function key applications
- Basic Enterprise Manager Software operation

Once you become familiar with these operating system elements, you will be able to use the Enterprise Manager Software effectively.

Connecting a client to a server

Use the following steps to connect to a server:

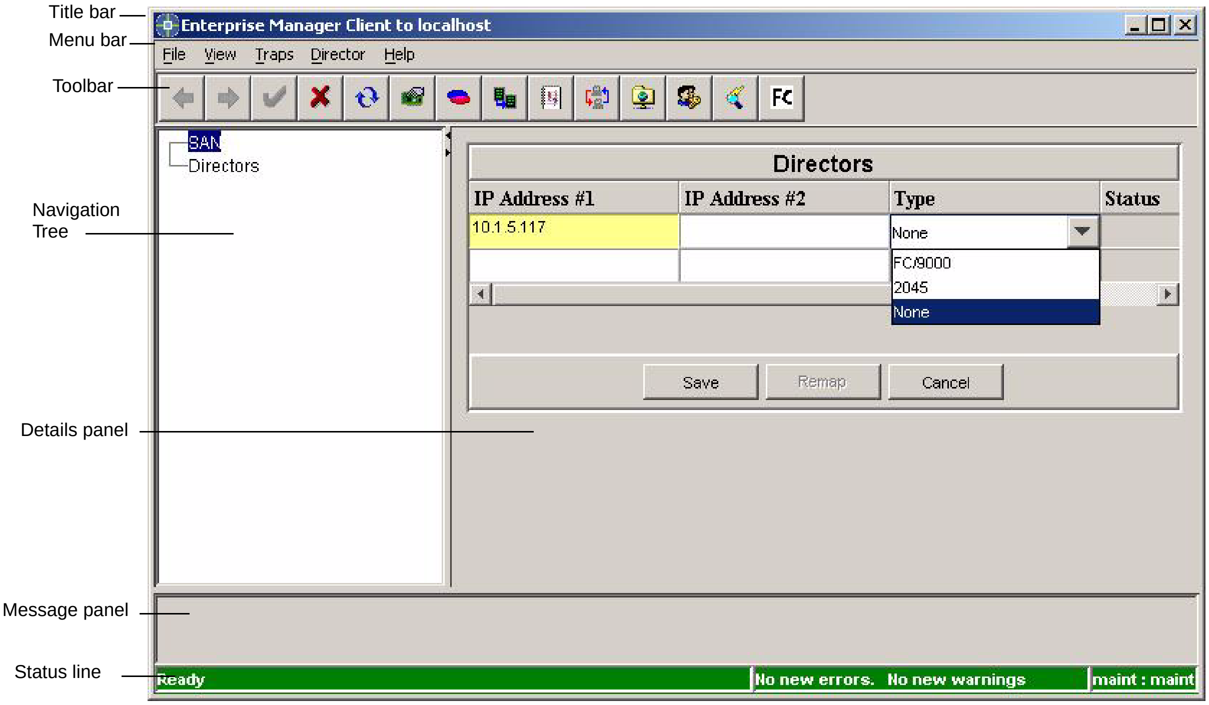
Note: The server to which you want to connect should be running before you attempt to connect to it.

4. Double-click the **Enterprise Manager Software** icon located on the desktop of your PC. The Enterprise Manager Software Logon dialog appears.
5. Type your user name in the **User Name** field.
6. Type your password in the **Password** field.
7. Type in the IP address or the computer name of the PC on which the server to which you want to connect is operating in the **Server** field. If the server you want to connect to is on the client PC, leave the local server address in the dialog.
8. Click **OK**.

© Copyright IBM Corp. 2004

Enterprise Manager window layout

The windows of the Enterprise Manager Software are divided into seven areas: the Title Bar, Menu Bar, Toolbar, Navigation Tree, Details Panel, Message Panel, and Status Line.



Directors

IP Address #1	IP Address #2	Type	Status
10.1.5.117		None	

Ready | No new errors. No new warnings | maint : maint

Figure 4. Enterprise Manager main display window

Title bar

The Title bar displays the Enterprise Manager Software tile.

Menu bar

Enterprise Manager provides five menus: File, View, Traps, Director, and Help. Following are descriptions of the five menus and the respective functions selectable from each.

File

- Port WWN Device Names: Select **Port WWN Device Names** to view devices attached to ports.
- Flow Group Sets: Select **Flow Group Sets** to configure and apply Flow Group Sets.
- Notification Preferences: Select **Notification Preferences** to configure preferences as to how admins are notified regarding traps and other such information.
- Event Notification Setting: Select **Event Notification Setting** to configure who gets informed when select events occur.
- Reset User Preferences: Select **Reset User Preferences** to set the Enterprise Manager User Preferences.
- Copy Codeset: To use for codeload.

- Debug Backup: Used to gather set of log files for debug purposes.
- Launch UCM: Select **Launch UCM** to launch the UCM application.
- Launch Applications: Select **Launch Application** to launch applications from the Enterprise Manager.
- Configure Applications: Select **Configure Applications** to configure the third party applications which may be launched from the Enterprise Manager.
- Logoff: Select **Logoff** to log off the client application.
- Exit: Select **Exit** to close the client application.

View

- Refresh: Select **Refresh** to update information on the window by refreshing what is being viewed.
- Events: Select **Events** to view the event log.
- Audit Trail: Select **Audit Trail** to view the audit trail.
- User Security: Select **User Security** to view the currently set user security and make changes.
- LRT: Select **LRT (L**ink **R**ate **T**est**)** to setup and perform link rate tests.

Traps

- Clear Port(s) Trap: Clear all port based traps for all ports.

Director

- Set Director Clock: Sets the clock of a Director. (for FC/9000 only)
- Auto Sense Arbitrated Loop Enable: Enables the Auto Sense feature. (for FC/9000 only)
- Auto Sense Arbitrated Loop Disable: Disables the Auto Sense feature. (for FC/9000 only)
- Take over System Primary: Select director which acts as primary director in fabric. (for FC/9000 only)
- Set All XFIO2 Blades Speed to Default (1G/2G-2G): Set speed of boards to default. (for FC/9000 only)
- Set All XFIO2 Blades Speed to 1G Optimized (1G-1G): Set blades to 1G. (for FC/9000 only)
- Clear All Ports Statistics: Clear port statistics. (for FC/9000 only)
- Director Serial Debug Commands: Displays selected debug information when requested. (for FC/9000 only)
- Device Binding: Selecting **Device Binding** pops up the Device Binding window. (for FC/9000 only)
- License: Invoke the license dialog with this command.

Help

- Contents: View on-line help information. When performing a search with the Java help, the help will return an empty search box if the search string is not found.
- About: View version information for the client.

Toolbar

The Toolbar provides thirteen buttons; you can move your cursor over each button to display the tool tip and learn which action each button performs.The text below briefly describes each of the buttons.

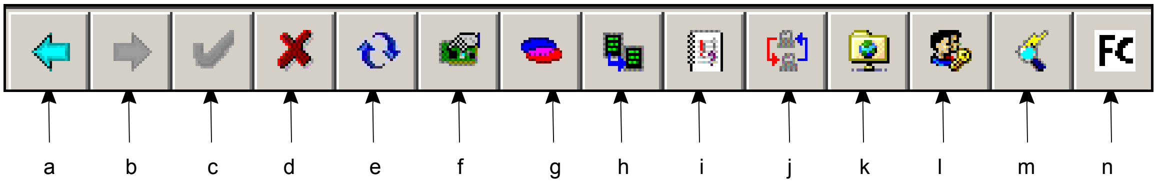


Figure 5. EM toolbar

A - Back

Returns you to the previous window.

B - Forward

Forwards you to the previous window.

C - Apply

Performs current action.

D - Cancel

Cancels an action.

E - Refresh

Refreshes the displayed window.

F - Port WWN Device Names

Displays the currently defined port WWN device nicknames and allows you to define new nicknames. Viewer level users may not create or delete device nicknames.

G - E Port Zoning

Displays E Port Zoning window.

H - One Button Code Load

Displays the One Button Code Load window.

I - Events

Displays the Event window.

J - Trace

Displays the Trace window.

K - SAN256N director FTP

Displays the SAN256N director FTP window.

I - User Security

Displays the User Security window.

M - LRT

Displays the Link Rate Test window.

N - FC Ping

Displays the IP Ping Configuration window.

Customizing the toolbar

You can customize the toolbar; right-click over the blank toolbar area, and a dialog will appear so you can modify which elements are displayed or not. You can also arrange the order of toolbar items by dragging them from one area of the dialog to the other. Click the **Apply** button to apply your changes.

Navigation tree

The Navigation tree displays information specific to the server module of the Enterprise Manager Software that is running. Use the Navigation tree to select and display information specific to SANs and Directors. Under the SAN heading, view board or port information of a particular director, switch or logical switch of a SAN256N director. Under the director heading, view physical attributes of a switch, director or SANC40 cabinet. Physical attributes include fan status, power supply status, etc.

Details panel

Information specific to the component you chose in the Navigation tree is displayed here. You may make changes to certain components, view and acknowledge traps, and perform other tasks related to switches and software.

Message panel

The Message panel is a scrolling display of the 25 most recent events of severity 3 or less.

Status line

The Status line is located below the Navigation tree and Details panel. It indicates the current status. Red or orange indicates an alert status, while green indicates all clear.

Switch views

The SAN Faceplate view shows a graphical representation of the selected switch in the details view of the window after you click on a switch at the left side Navigation Tree under the Switch heading:

- On the right side, a graphical representation of the switch appears.
- Right-click in the gray area next to the switch and Switch Configuration, Network Configuration, Trace Log and Version are all options you can choose for more switch info.

Details about the selected switch are also shown.

Color coding of items

Color coding of events, components and switches are used to alert users to situations present in the system.

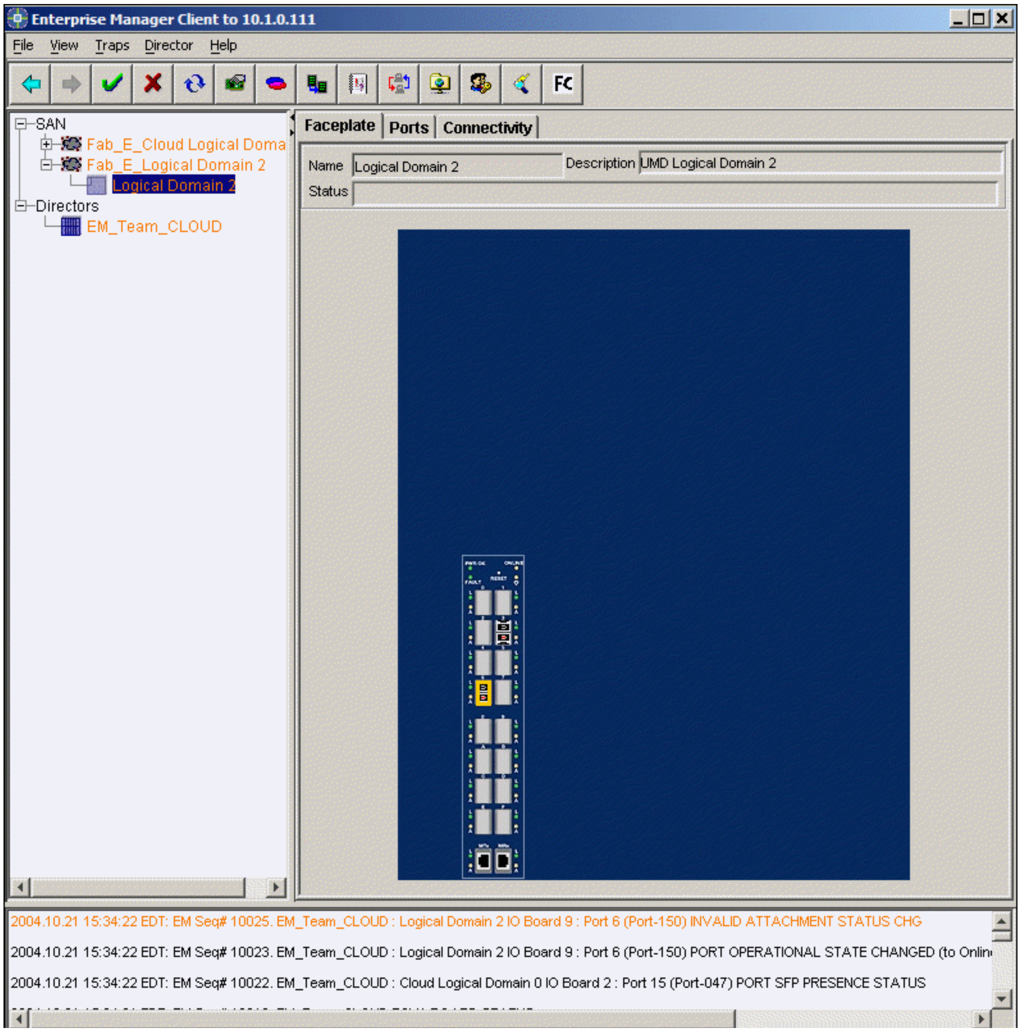
- If a representation of a switch at the topology level view is surrounded by a red box, it indicates a lost connection.
- A red ringed component at the face plate view indicates that the component has failed.
- If the Status line is red, it indicates that at least one level 1 event is present in the system.
- If the Status line is orange, it indicates that at least one level 2 event is present in the system.
- If the Status line is green, it indicates that no level 1 or level 2 events are present in the system or that all events have been acknowledged.

SAN view

While the Switch view allows you to see physical information about the switch, SAN views allow you to view board and port information.

SAN faceplate view

The **SAN Faceplate** view is what you see after clicking a switch under the SAN heading (click a logical portion of a SAN256N director switch to see board and port information about that particular partition of the switch or click on an FC/9000). It shows the faceplate view of the switch. It shows all the installed boards and some of the switch properties on the right side. By double-clicking the faceplate, you can zoom into the details of that particular board or component.



Name Logical Domain 2

Description UMD Logical Domain 2

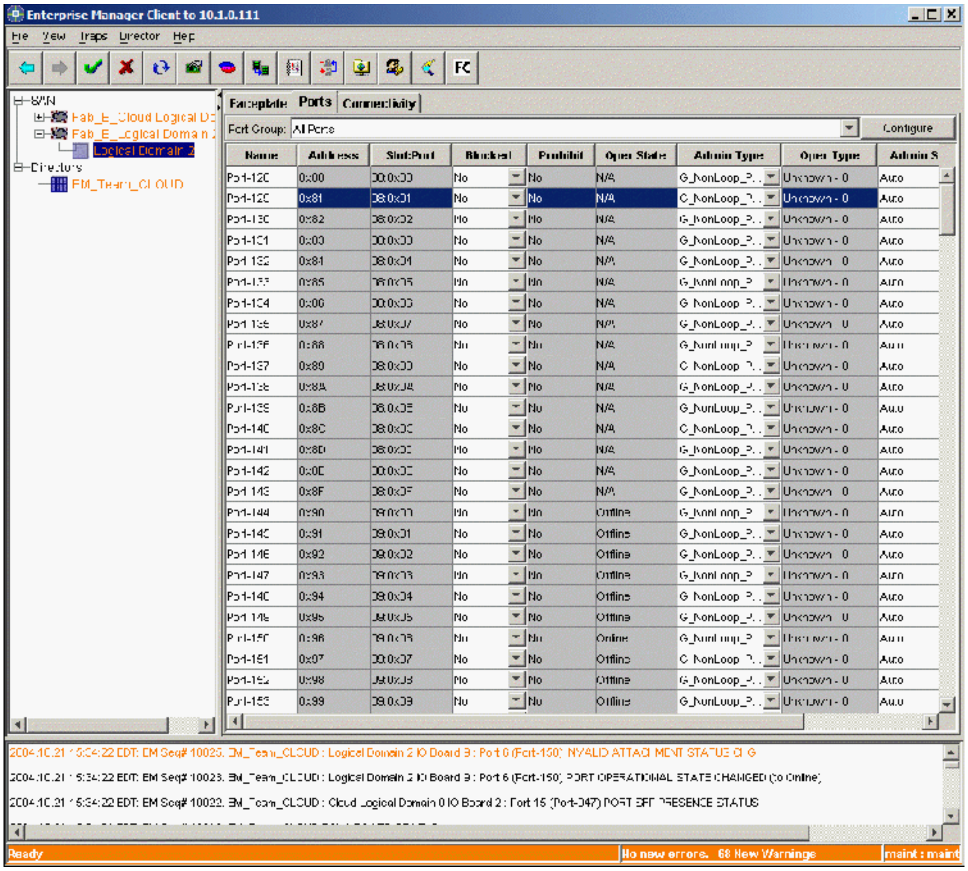
Status

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Onlin
2004.10.21 15:34:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port-047) PORT SFP PRESENCE STATUS
```

Figure 6. SAN view - faceplate tab

SAN ports view

You can display the SAN Ports view by clicking the **Ports** tab after selecting a switch under the SAN heading (click a logical partition of a SAN256N director switch to see board and port information about that particular partition of the switch or click an FC/9000). It shows the port information of the switch.



Port Group: All Ports

Name	Address	Slot:Port	Blocked	Prohibit	Oper State	Admin Type	Oper Type	Admin S
Port-128	0x80	08:0x00	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-129	0x81	08:0x01	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-130	0x82	08:0x02	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-131	0x83	08:0x03	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-132	0x84	08:0x04	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-133	0x85	08:0x05	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-134	0x86	08:0x06	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-135	0x87	08:0x07	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-136	0x88	08:0x08	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-137	0x89	08:0x09	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-138	0x8A	08:0x0A	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-139	0x8B	08:0x0B	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-140	0x8C	08:0x0C	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-141	0x8D	08:0x0D	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-142	0x8E	08:0x0E	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-143	0x8F	08:0x0F	No	No	N/A	G_NonLoop_P..	Unknown - 0	Auto
Port-144	0x90	09:0x00	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-145	0x91	09:0x01	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-146	0x92	09:0x02	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-147	0x93	09:0x03	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-148	0x94	09:0x04	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-149	0x95	09:0x05	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-150	0x96	09:0x06	No	No	Online	G_NonLoop_P..	Unknown - 0	Auto
Port-151	0x97	09:0x07	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-152	0x98	09:0x08	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto
Port-153	0x99	09:0x09	No	No	Offline	G_NonLoop_P..	Unknown - 0	Auto

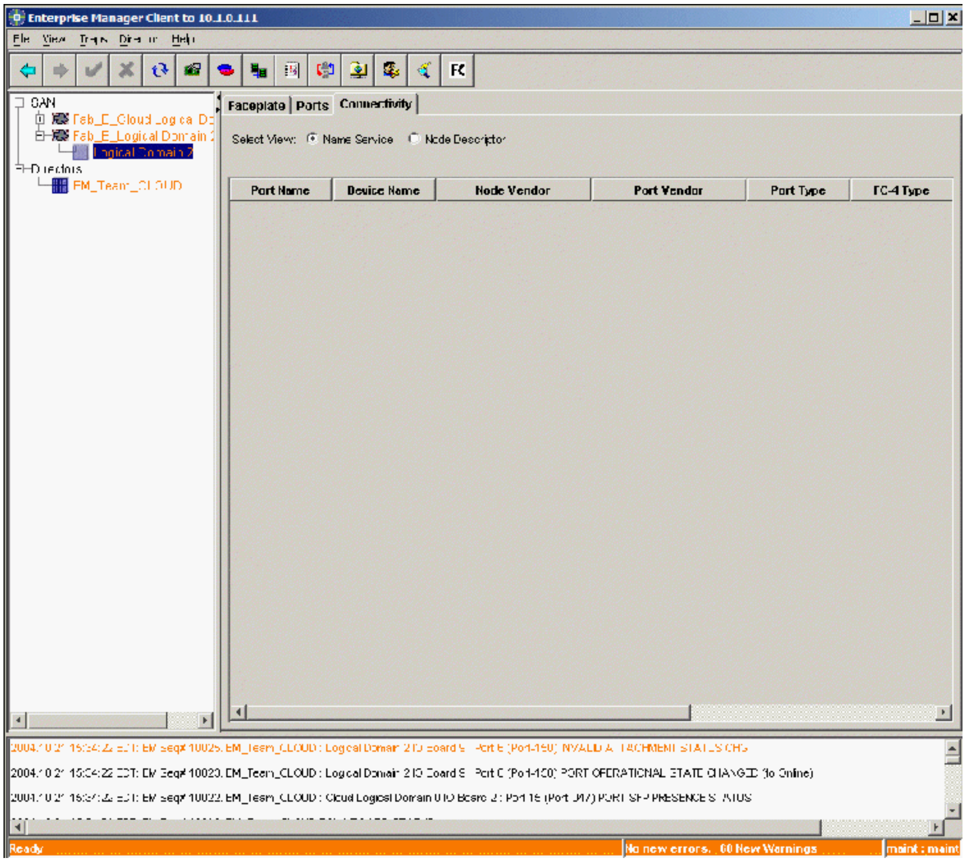
```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 3 : Port 0 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 3 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
2004.10.21 15:34:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port-047) PORT SFP PRESENCE STATUS
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 7. Ports tab view

SAN connectivity view

The SAN Connectivity view is displayed after clicking on a switch or logical switch partition under the SAN heading (click on a logical portion of a SAN256N director switch to see board and port information about that particular partition of the switch or click an FC/9000) and then clicking the **Connectivity** tab. It shows connectivity information as.



Select View: ● Name Service ○ Node Descriptor

Port Name	Device Name	Node Vendor	Port Vendor	Port Type	FC-4 Type

```
2004/10/21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 5 Port E (Port-150) INVALID ATTACHMENT STATUS CHG
2004/10/21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 5 Port C (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
2004/10/21 15:37:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port 047) PORT SFP PRESENCE STATUS
```

Figure 8. Connectivity tab view

In-band and out-of-band

Control of a director or switch by the Enterprise Manager Software is accomplished either in-band or out-of-band. Release 3.x and above of the Enterprise Manager Software supports in-band control of FC/9000 and SAN256N director and switches.

In-band

In-band control is accomplished when the Enterprise Manager controls a Director or switch via the IP address of another Director in the fabric. The Directors and switches communicate via Interswitch Links (ISLs).

In-band control is always enabled in the FC/9000.

By default, In-band control is disabled in the SAN256N director. Contact your IBM support representative before activating this feature. In-band control for the SAN256N director is accomplished by activating the functionality via a selectable option at the Enterprise Manager Server. Enable or disable in-band control by selecting the option from the EM Server and then selecting **Maintenance** from the toolbar. Click the **in-band**

and out-of-band control option. A dialog with a drop down list appears. Select the type of control you wish for the SAN256N director from the drop down list and then click on **OK**. Click through the verification windows.

Out-of-band

Out-of-band control is accomplished when director(s) or switch(es) are controlled via the FCME or TCM IP address(es).

External application launch and setup

The Enterprise Manager Software allows users to launch external applications for selected fabrics, switches or ports via a menu selection.

Setting up external application launches from the Enterprise Manager Software

1. At the Enterprise Manager client window, Select the **Configure Applications** function from the **File** menu.
2. Type the name of the application at the **Name** field.
3. At the **Path** field, type in or browse for the path to the application that will be launched.
4. At the **Level** drop-down list, select the Navigation Tree level from which the application may be launched.
5. When you are finished, click **Add** and then **Save** to save your work.

Launching an application from the Enterprise Manager Software

1. Select the fabric, switch, or port name from the Navigation Tree view you want to launch.
2. Select the **Launch Application** option from the **File** menu. A small window appears with a drop-down list of available applications.
3. Click the application you want to launch and then click **OK**.

Modifying an application launch

1. Open the Configure Applications window by selecting the **Configure Application** option from the **File** menu.
2. At the Configure Applications window, click the Application you want to modify.
3. Make any modifications; and then click **Modify,** and then **Save**. Close the window.

Deleting an application from the Launch Application window

1. Open the Configure Applications window by selecting the **Configure Application** function from the **File** menu.
2. At the Configure Applications window, select the Application that you want to delete.
3. Click **Delete,** and then **Save**. Close the window.

Launching UltraNet ConfigManager

You can launch the UltraNet ConfigManager (UCM) from the Enterprise Manager by selecting **Launch UCM** from the **File** menu. The UCM is for configuration and control of the UltraNet Edge Storage Router (Edge) product.

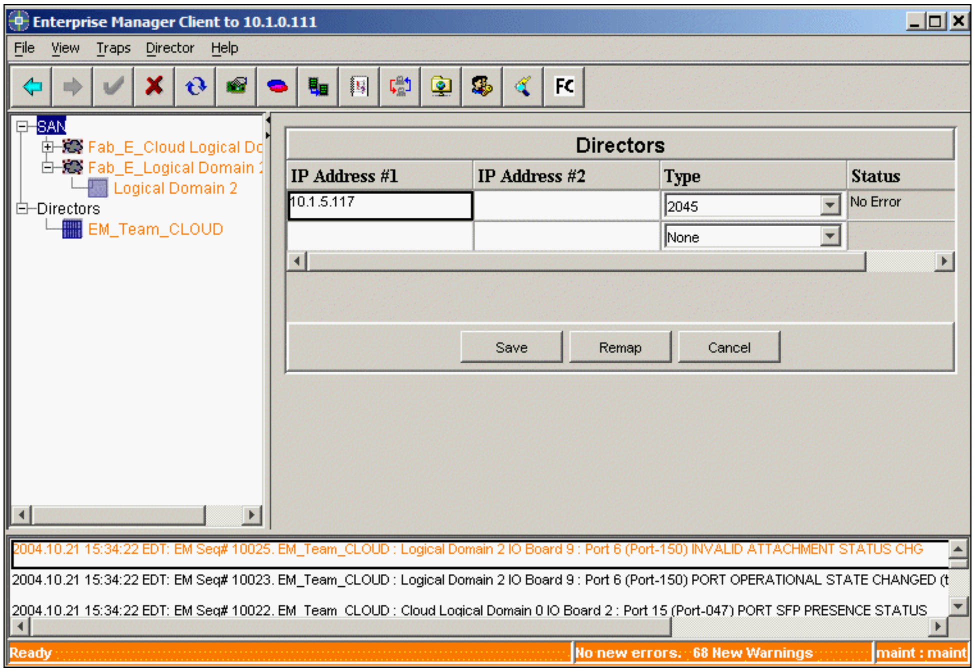
Chapter 4. Common switch functionality

This chapter presents information common to the different types of switches and directors controlled by the Enterprise Manager Software. Examples include the 128-port FC/9000 Director, 64-port FC/9000 Director, 16-port FC/9000 Switch, and 8-port FC/9000 Switch.

Note: The 256-, 128-, and 64-port FC/9000s are director class systems; the 8- and 16-port FC/9000s are simply switches. When describing the FC/9000 or SAN256N director in a broad sense, the term "switch" is used.

Enterprise Manager Software main window

After you log into a server, you are presented with the following window. From this main window, you can navigate to the directors window by clicking a director under the director list, or you can view information about directors and switches by clicking on a fabric under the SAN heading and then selecting a director, switch or logical partition of a SAN256N director. You can also add directors to fabrics here.



Directors

IP Address #1	IP Address #2	Type	Status
10.1.5.117		2045	No Error
		None	

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (t
2004.10.21 15:34:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port-047) PORT SFP PRESENCE STATUS
```

Figure 9. Enterprise Manager main window

To view the fabrics associated with the server into which you logged, double-click a **Fabric** under the SAN heading or single-click the plus sign (+). You can also view the physical information of selected directors and switches by clicking the switch of your choice under the **Directors** heading. You can view the IP addresses of directors and switches in the fabric at this window.

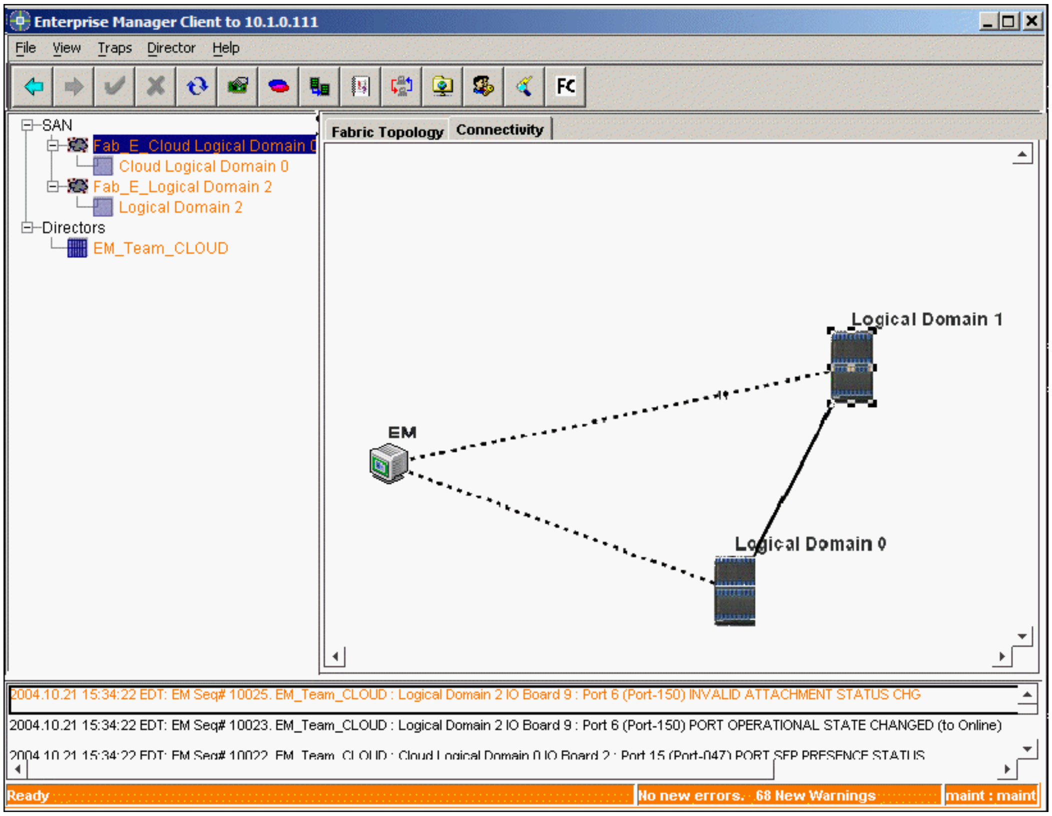
Discover a new switch or dIrector in the fabric

You can discover new directors and switches from this window. Refer to "Setting up for fabric discovery" on page 13 for instructions.

© Copyright IBM Corp. 2004

Fabric view

After clicking a fabric, you can see all the switches, directors and devices associated with it and connections between those switches and devices.



```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
2004.10.21 15:34:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port-047) PORT SFP PRESENCE STATUS
```

Figure 10. Fabric view

Switch links

Select a link for information. Note that the links are color coded: green for a good link, red for a lost link. Multiple links denote multiple ISLs between directors.

Connectivity

Click the **Connectivity** tab to view Fabric Wide Name Service information and also Node Descriptor information.

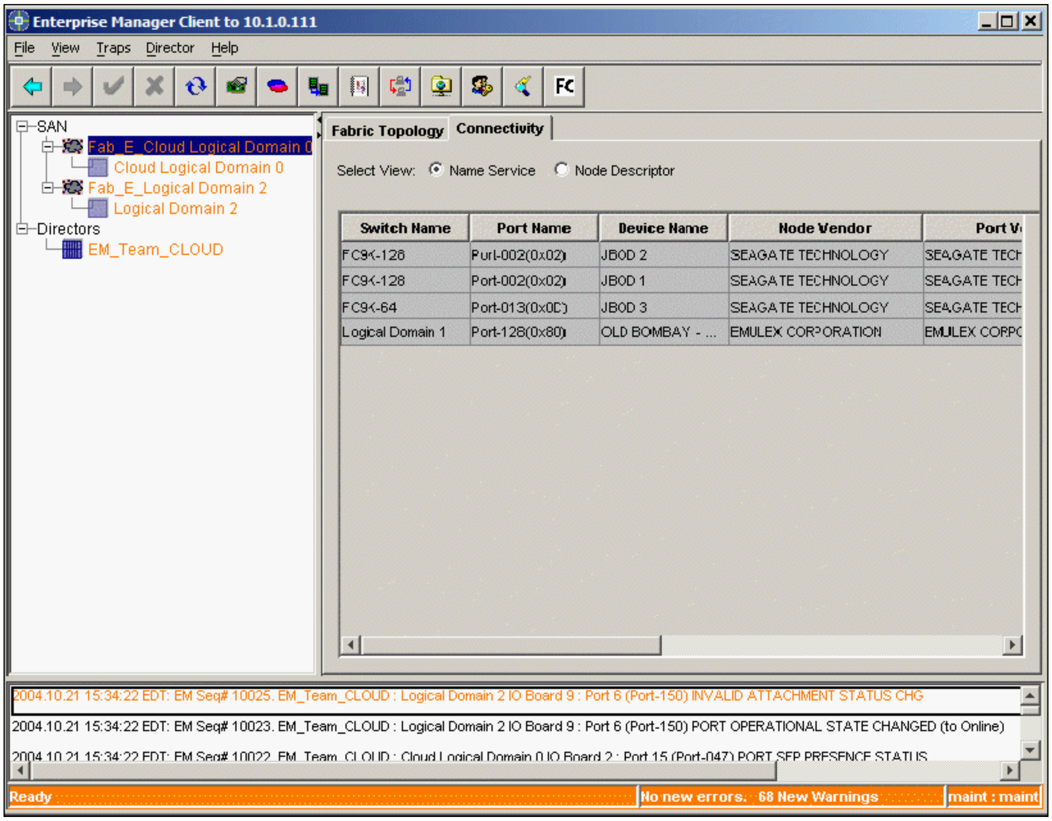
Fabric wide name service

Fabric wide name service information may be viewed by clicking the Connectivity tab. Name Service is the default choice, as evidenced by the filled in radio button. Name Service information for all of the switches and directors in a fabric are displayed. The information is valuable for use in creating zones and nicknames. The zoning tree will display the WWNs and FC addresses for switches of other vendors.

Non-IBM switches

In the tree view to the left, you will see the WWNs of non-IBM switches. Click the **+** next to the switch, and you will see the WWNs of devices attached to those switches.

Note: The information in this window does not automatically refresh. To ensure that you are viewing current information, click the **ReSynch** button.



Select View: ● Name Service ○ Node Descriptor

Switch Name	Port Name	Device Name	Node Vendor	Port V
FC9K-128	Purl-002(0x02)	JBOD 2	SEAGATE TECHNOLOGY	SEAGATE TECH
FC9K-128	Port-002(0x02)	JBOD 1	SEAGATE TECHNOLOGY	SEAGATE TECH
FC9K-64	Port-013(0x0D)	JBOD 3	SEAGATE TECHNOLOGY	SEAGATE TECH
Logical Domain 1	Port-128(0x80)	OLD BOMBAY - ...	EMULEX CORPORATION	EMULEX CORPC

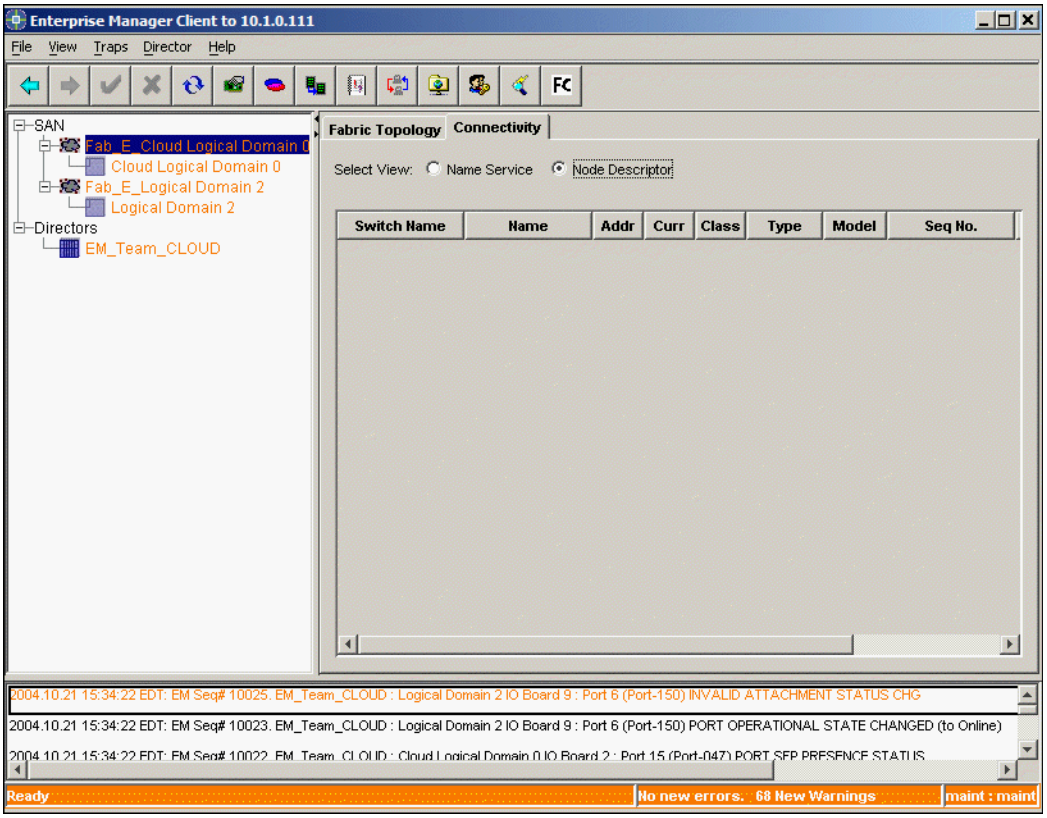
```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
2004.10.21 15:34:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port-047) PORT SFP PRESENCE STATUS
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 11. Fabric wide name service

Fabric Wide Node Descriptor information

Note: Fabric wide Node Descriptor information may be viewed by clicking the Connectivity tab. Node Descriptor is not the default choice, so you will have to select the radio button to see it. Click the Node Descriptor button and you will see the Node Descriptor information for all of the switches and Directors in a fabric.



Select View: ○ Name Service ● Node Descriptor

Switch Name	Name	Addr	Curr	Class	Type	Model	Seq No.

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
2004.10.21 15:34:22 EDT: EM Seq# 10022. EM_Team_CLOUD : Cloud Logical Domain 0 IO Board 2 : Port 15 (Port-047) PORT SFP PRESENCE STATUS
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 12. Fabric wide node descriptor information

Zoning

Zoning allows you to create inactive zonesets and zones on a switch/director basis. Each SAN256N director and FC/9000 director can have up to 256 inactive zonesets. In addition, any inactive zoneset can be activated. When a zoneset is activated, it gets propagated to all director/switches in the fabric of which the switch is currently a member.

A zone is created independently and can then be assigned to one or more zonesets. No changes may be made to an active zoneset. To change an active configuration, you must replicate the active configuration and change it. The changed zoneset may then be activated. Zoning tables auto-refresh every five seconds.

When determining whether you will create a hard zone or a soft zone with members from a SAN256N director, note that you create hard zones with Node FC address members only. A mix of Node FC address members and WWN members or simply WWN only members can be used to create only soft zones.

Guidelines for zoning and port prohibits while employing intermix mode

When running FICON and Open Systems simultaneously (Intermix Mode), there are some guidelines that should be followed.

Zoning guidelines:

- Enterprise Manager Software will restrict zone type to WWN only with a CS4.3.0. fabric that has ISLs to a FC9000 director running CS4.1.3 or below.
- Zone types include Type 2 and 3 Port zoning with CS4.3.0 or above.
  - Previous zoning type:
- Type 1 - WWN
  - Zoning types added:
- Type 3- FC address
- Enable domain locking when using Type 2 and 3 zoning.
- Zoning should be used for controlling connectivity among FCP N/NL-ports (“soft”, i.e. enforced at the name server level).
- Prohibits may be used for FCP N/NL-ports, however some FCP devices/HBAs have been found to have limitations with handling a prohibit RSCN containing multiple entries. When enabling or disabling prohibits, a RSCN will be sent to all affected prohibited port(s) even if a port is in a different a zone.
- Ports defined for FCP traffic can be placed within a maximum of 1024 unique zones totaling 5000 members with the SAN256N director director.
- Ports defined for FCP traffic can be placed within a maximum of 256 unique zones totaling 3600 members with the FC/9000.

Prohibit/Allows guidelines:

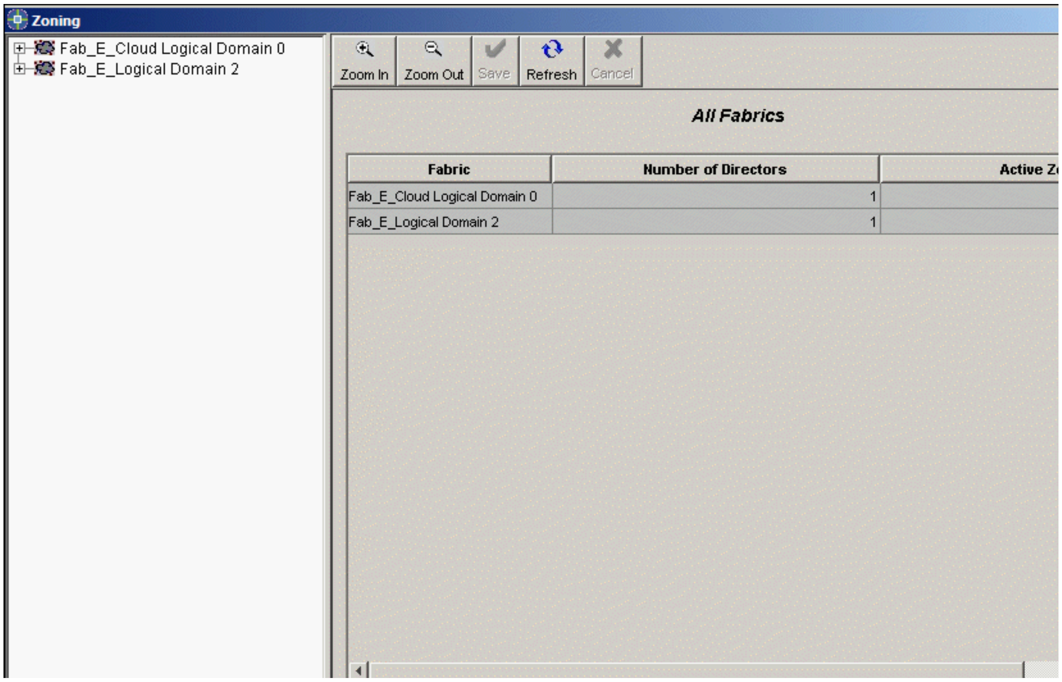
- Prohibits/Allows should be used for controlling connectivity among FICON N-ports (“hard”, i.e. enforced at a traffic frame level)
- FICON ports should be placed within a single zone; this provides nameserver separation of FICON ports from FCP ports, and ensures that FICON ports receive a RSCN for FICON port state changes.
- Port prohibits/allows should be limited to the ports defined in the FICON zone, and not used for ports in a FCP zone.
- Additional traffic separation of FICON ports, independently of zoning, is accomplished by prohibiting all FICON ports to all FCP ports. This may be performed via the Enterprise Manager by setting prohibits on columns corresponding to FICON ports. Then the intersection with FICON ports rows may be modified (Set) to allow FICON to FICON connectivity. See the information which follows on how to create and populate zones and zonesets.
- Prohibits shall not to be used for ISLs port connections.
- Prohibits/allows may be applied also from the System Automation console via Z/OS and CUP. Care should be taken to apply them to FICON ports only.

Viewing zones and zonesets

To view zones and zonesets created for the director:

1. Click the **Zoning** button on the Toolbar. The **All Fabrics** window appears.

From this window, you can access any fabric upon which you can choose a Director to begin to build zonesets. Notice that in the message area you are given instructions on how to get to the next level of the zoning window.

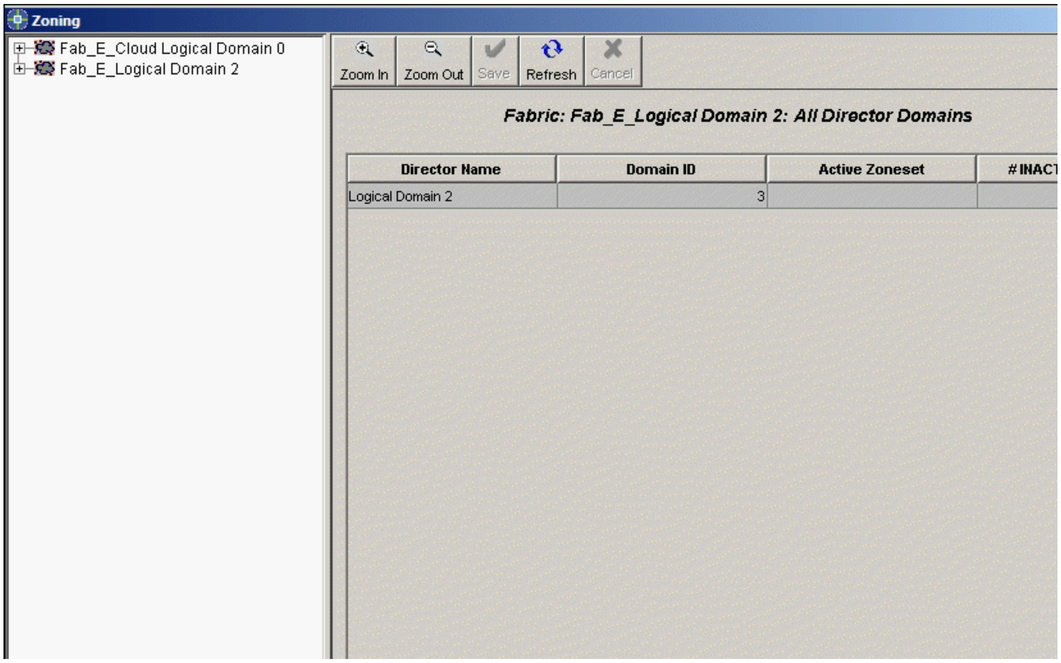


All Fabrics

Fabric	Number of Directors	Active Z
Fab_E_Cloud Logical Domain 0	1	
Fab_E_Logical Domain 2	1	

Figure 13. All Fabrics window

2. Access a fabric by either double-clicking it or highlighting it and clicking **Zoom In**. The All Director Domains window appears. This window shows Directors associated with the fabric you chose.



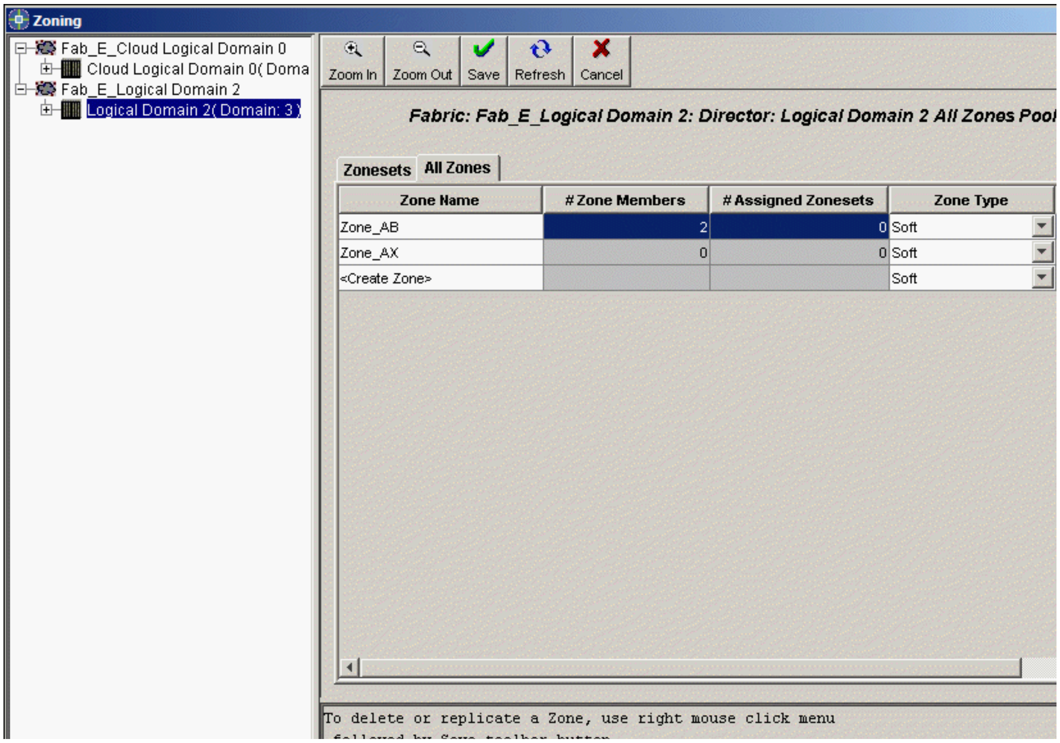
Fabric: Fab_E_Logical Domain 2: All Director Domains

Director Name	Domain ID	Active Zoneset	# INACT
Logical Domain 2	3		

Figure 14. All Director Domains window

3. Select the director with the zoning database that you need to access or update. Either double-click it or highlight it and then click **Zoom In**. The All Zonesets window appears.

4. Click the **All Zones** tab and you are now viewing the All Zones Pool window. All of the inactive zonesets which have been created for this director are listed here, along with any active zoneset which may be propagated to each director in the fabric.


Zoning
Fab_E_Cloud Logical Domain 0
Cloud Logical Domain 0(Doma
Fab_E_Logical Domain 2
Logical Domain 2(Domain: 3)
Zoom In
Zoom Out
Save
Refresh
Cancel
Zonesets
All Zones

Fabric: Fab_E_Logical Domain 2: Director: Logical Domain 2 All Zones Pool

Zone Name	# Zone Members	# Assigned Zonesets	Zone Type
Zone_AB	2	0	Soft
Zone_AX	0	0	Soft
<Create Zone>			Soft

```
To delete or replicate a Zone, use right mouse click menu
followed by Save toolbar button.
```

Figure 15. All Zones Pool window

Creating a zoneset for the first time

The following procedure will show you how to create a zoneset and a zone, add members to the zone, add the zone to a zoneset, and activate the zoneset.

1. Click the **Zoning** button on the Toolbar. The **All Fabrics** window appears. “

   The **All Fabrics** window is considered the first level of zoning. All of the fabrics monitored by the Enterprise Manager server are listed in this window.

2. Double-click on a Fabric, or select it and click **Zoom In**.

   The **All Director Domains** window appears.

3. From the **All Director Domains** window (level 2), select the director you want to set up by either double-clicking it or highlighting it and then clicking **Zoom In**.

   Level 3 window of the zoning window appears. From here, all zonesets resident in the director’s zoneset database are viewable.

4. Create the zones you need to populate your zoneset. To begin doing so, select the **All Zones** tab.

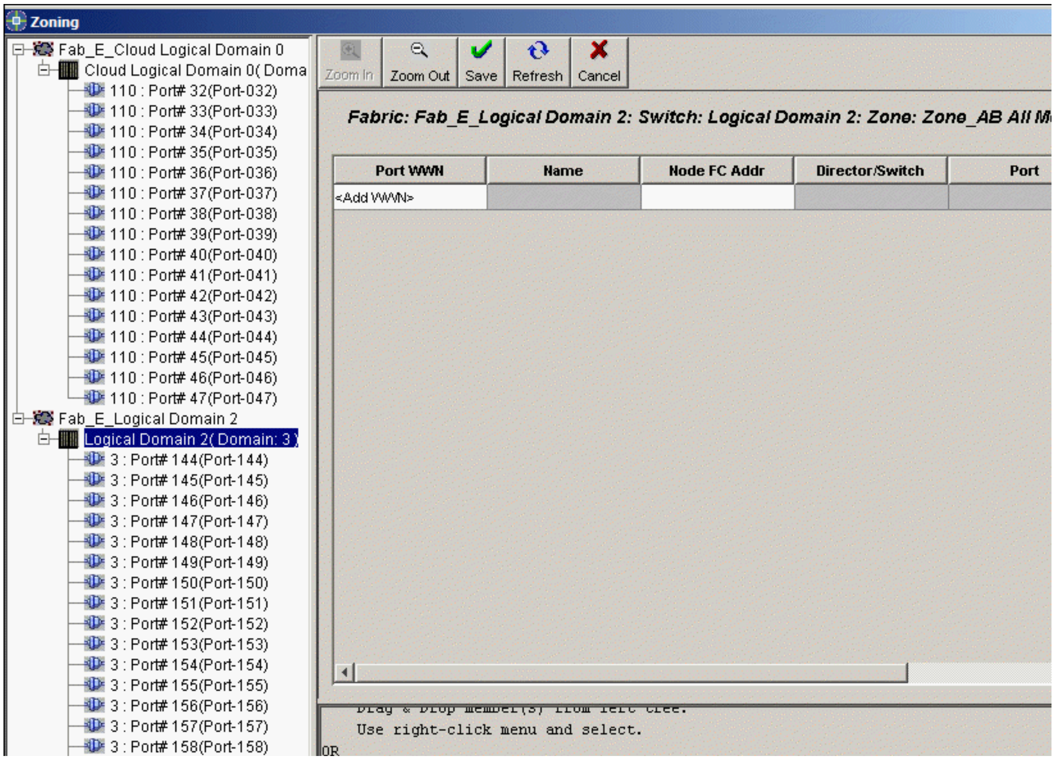
5. Highlight **<Create a Zone>** and type the name of the zone you would like to create in the fields.

6. After you type in the name, press the **Enter** key.

7. At this point, select whether the zone will be hard or soft. Remember, from the All Zones Pool window, you may only create hard zones with Node FC Address members from a SAN256N director. Soft is the default choice, select **Hard** from the drop down list if you plan on creating a hard zone.

8. Populate the zone with members. Highlight the zone you want to add zone members (device WWNs) to and click **Zoom In**, or double-click the zone

9. There are a couple of ways you can add zone members at this window. You can type them in, or you can drag and drop them from the Navigation Tree at the left (click the plus sign next to a director to expand the view and see the available ports for that director). You may also right-click over **<Add WWN>** and click **Add Zone Members**. A list of known WWNs and their nicknames, or Node FC Addresses will pop up..



Fabric: Fab_E_Logical Domain 2: Switch: Logical Domain 2: Zone: Zone_AB All M

Port WWN	Name	Node FC Addr	Director/Switch	Port
<Add WWN>				

```
Drag & Drop member(s) from left tree.
Use right-click menu and select.
OR
```

Figure 16. Add WWN and Add Zone Members window

10. Select the WWNs you wish to add, and then click **Add**.

Note: For the FC16-2, FC8-2, non-IBM switches and QLogic Sanbox2’s you will have to manually add their WWNs to the zone.

11. To expand the Navigation Tree to get to the port level, click the plus sign (**+)** to the left of the director. Then click on a port, and all the devices which are assigned to that port are listed beneath it.

    There are two types of zone members that can be added to a zoneset: WWN (note that the WWN type may also appear as the nickname for the device), and Node FC Address.

    Highlight and then drag the zone member to the next available line cell and drop it there. It will then be listed in the zone member list. You can also type in a member manually by clicking in the pertinent cell at the next available line and typing in the information.

12. When you are finished adding zone members, click **Save** to save the zone and then click **Zoom Out**. There is now zone information listed

13. Select the **Zonesets** tab to return to the Zonesets window and highlight **<Create Zonesets>.**

14. Type in the name of the zoneset and press the **Enter** key. Right-click over the newly-created zoneset.

15. Select the **Add Zones** option and a dialog listing all of the available zones appears.

16. Highlight the zones which you would like to add, and then click **Add**.

17. Click **Save** to save the zoneset configuration.

18. To activate the zoneset, right-click on the zoneset which you would like to activate and then select **Activate** from the pop-up menu that appears.

19. Confirm the **Activate** option by clicking **Yes** on the message that appears.

20. When you activated the zoneset, an inactive duplicate of the zoneset you created was made. This allows you to modify a *copy* of the activated zoneset, since you can not modify a zoneset which is itself active. You could then activate the copy with modifications. You may wish to change the name of the modified zoneset so that when you activate it you will not overwrite the old zoneset and lose its attributes.

21. Minimize or close the Zones window.

Creating a zone

1. Click the **Zones** button. Select the fabric for the director you would like to create a zone for.

2. Select the director you want to create a zone.

3. Select the **All Zones** tab.

4. Highlight **<Create Zone>** and type in the name of the new zone you want to create, then press the **Enter** key.

5. Double-click the zone or highlight it and click **Zoom In**.

6. Type in the WWNs of the devices you would like to add to the zone, or click on the plus sign (+) next to the Director at the left side of the window. Then click on a port to view the WWNs associated with it. Highlight the WWNs you would like to move and then click and drag them over a cell at the Add WWN panel to the right.

7. When you finish adding WWNs, click **Save**. Then click **Zoom Out**.

Deleting a zoneset

1. Highlight the zoneset which you would like to delete and then right-click over it.

2. Click the **Delete** option. In the Zoneset Status column, it now says “deleted” with an asterisk (*). This indicates the zoneset is in a delete, pending state.

3. Click **Save** to complete the deletion, or click **Cancel** to remove the zoneset from the delete, pending state.

4. Click **Apply**.

Replicating a zoneset

1. Select the **Zonesets** tab.

2. Right-click over the zoneset you would like to replicate and select **Replicate** from the pop-up menu. A dialog appears. Type in the name of the zoneset you would like to create and click **OK**.
3. You may now make any adjustments the zoneset.

Activating a zoneset

1. Highlight the zoneset to activate and then right-click over it.
2. Select the **Activate** function from the pop-up menu that appears.
3. Confirm your choice at the confirmation window.

Deactivating a zoneset

1. Highlight the zoneset to deactivate and then right-click over it.
2. Select the **Deactivate** function from the pop-up menu that appears.
3. Confirm your choice at the confirmation dialog.

Adding a zone to the zoneset

1. Highlight the zoneset which you would like to add a zone to and then right-click over it. The zoneset must be inactive.
2. Select **Add Zones** from the pop-up menu that appears.
3. A small dialog appears. Select the zones you would like to add and then click **Add**.
4. Click **Save**.

Deleting a zone from the zoneset

1. Highlight the zoneset from which you would like to delete a zone and right-click over it. The zoneset must be inactive.
2. Select **Remove Zones** from the pop-up menu that appears.
3. A small dialog appears. Select the zones you would like to remove from the zoneset and then click **Delete**.
4. Click **Save**.

Replicating an entire zoning database

1. Go to the All Directors Domain window.
2. Select the director with the zoning database you want to replicate.
3. Right-click over it and select Replicate **Zoning Database** from the pop-up menu that appears. This option replicates the entire inactive zoning database. A dialog appears which lists all of the switches of which the Enterprise Manager is aware.
4. From this dialog, select the director(s) to which you want to propagate the zoning database. You may select more than one.
5. Click **OK** to finish.

Deleting a zone

1. Select the **All Zones** tab.
2. Verify the zone you are about to delete is not a member of an active zoneset; right-click over the zone you would like to delete and select **Assigned Zonesets** from the pop-up menu. Deactivate the zoneset if necessary.
3. Right-click over the zone you would like to delete and select the **Delete** option from the pop-up menu that appears. The zone status changes to “deleted-pending apply.”

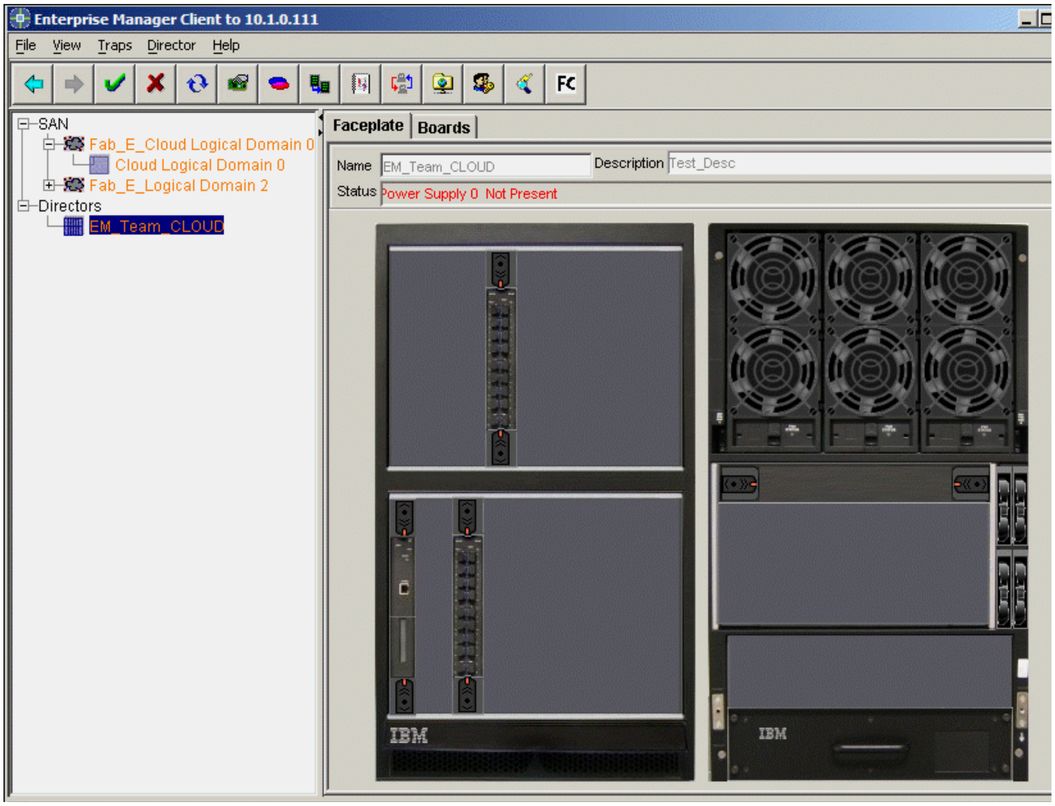
4. Click **Apply**.

Replicating a zone

1. Select the **All Zones** tab.
2. Right-click over the zone you would like to replicate and select **Replicate** from the pop-up menu that appears. A dialog appears.
3. Type in the name of the zone you would like to create and click **OK**.
4. You may now adjust the zone as you wish. The new zone will not automatically be a member of any zoneset. It must be added to the zonesets you want it to belong.

Port WWN Device Names button

Clicking the **Port WWN Device Names** button reveals information for devices across the fabric for which the Enterprise Manager Software has name service information. It is used to define nicknames for devices (servers and storage).



Name EM_Team_CLOUD
Description Test_Desc
Status Power Supply 0 Not Present

Figure 17. Devices button

Creating device nicknames

1. Click the **Devices** button to display the Creating Device Nicknames window.
2. Type in the nicknames which you would like to add (up to 64 characters).

   Note: Port WWNs of all know devices appear in the Port WWN columns.

3. After adding and/or editing nicknames, click **Save** to finish.

Port information

Port statistics are available at the port level, while visual indications of port failures are viewable at the port level, board level, and Director/switch level. See “SAN256N director switch configuration and control” on page 71 for more SAN256N director information.

Port failure indications

Port failure indications are evident at the port, board, and director/switch level. The port will be surrounded by a red box. The red indicator will disappear after the problem has been resolved.

Clearing port failure indicators

If the red indicator does not go away, you can manually shut it off by clicking the **Traps** button on the Toolbar and moving the mouse down to the **Clear Port(s) Failure Indicator** button. Click it and a dialog will appear, giving you the option to clear traffic and/or util traps. After choosing the option you wish, click **OK**. The red indicator will disappear.

- Doing this at the port level will clear the indicator for that port which you are viewing.
- Doing this at the board level will clear the indicators for all of the ports on that board, if there are multiple indicators.
- Doing this at the director/switch level will clear the indicators for all the ports on that director/switch, if there are multiple indicators.

Event Log View window

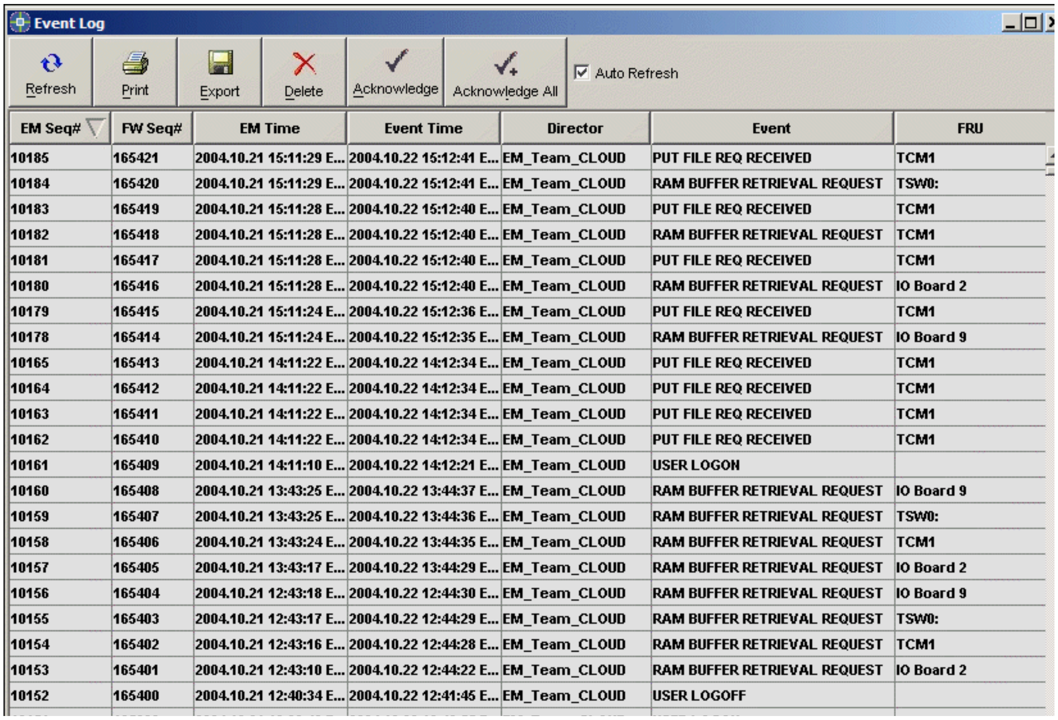
The Event Log View window appears when you double-click the error/warnings display at the bottom right of the window, or by clicking the **Events** button up top. The window shows event log information.

The Event Error/Warnings displayed at the bottom right of Enterprise Manager Software windows are color coded:

- Green means there are no new errors/warnings to report
- Red indicates level 1 errors
- Orange indicates a level 2 event

Clicking the message will open the Event Log window and take you to the first event which generated the color-coded message. In addition to the top level indication, the Fabrics tree will show the name of the corresponding director and fabric in red or orange when new error warning events occur. Bold events have yet to be acknowledged.

The Event Log View window shows event log information for everything controlled by this Enterprise Manager server (fabrics, switches, ports, etc.). Note that by checking the **Auto Refresh** option, the Enterprise Manager Software will automatically auto refresh the Event Log. Uncheck it to manually control the refresh rate by clicking the **Refresh** button when you want the events to be updated.



☑ Auto Refresh

EM Seq#	FW Seq#	EM Time	Event Time	Director	Event	FRU
10185	165421	2004.10.21 15:11:29 E...	2004.10.22 15:12:41 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10184	165420	2004.10.21 15:11:29 E...	2004.10.22 15:12:41 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	TSW0:
10183	165419	2004.10.21 15:11:28 E...	2004.10.22 15:12:40 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10182	165418	2004.10.21 15:11:28 E...	2004.10.22 15:12:40 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	TCM1
10181	165417	2004.10.21 15:11:28 E...	2004.10.22 15:12:40 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10180	165416	2004.10.21 15:11:28 E...	2004.10.22 15:12:40 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	IO Board 2
10179	165415	2004.10.21 15:11:24 E...	2004.10.22 15:12:36 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10178	165414	2004.10.21 15:11:24 E...	2004.10.22 15:12:35 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	IO Board 9
10165	165413	2004.10.21 14:11:22 E...	2004.10.22 14:12:34 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10164	165412	2004.10.21 14:11:22 E...	2004.10.22 14:12:34 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10163	165411	2004.10.21 14:11:22 E...	2004.10.22 14:12:34 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10162	165410	2004.10.21 14:11:22 E...	2004.10.22 14:12:34 E...	EM_Team_CLOUD	PUT FILE REQ RECEIVED	TCM1
10161	165409	2004.10.21 14:11:10 E...	2004.10.22 14:12:21 E...	EM_Team_CLOUD	USER LOGON	
10160	165408	2004.10.21 13:43:25 E...	2004.10.22 13:44:37 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	IO Board 9
10159	165407	2004.10.21 13:43:25 E...	2004.10.22 13:44:36 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	TSW0:
10158	165406	2004.10.21 13:43:24 E...	2004.10.22 13:44:35 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	TCM1
10157	165405	2004.10.21 13:43:17 E...	2004.10.22 13:44:29 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	IO Board 2
10156	165404	2004.10.21 12:43:18 E...	2004.10.22 12:44:30 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	IO Board 9
10155	165403	2004.10.21 12:43:17 E...	2004.10.22 12:44:29 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	TSW0:
10154	165402	2004.10.21 12:43:16 E...	2004.10.22 12:44:28 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	TCM1
10153	165401	2004.10.21 12:43:10 E...	2004.10.22 12:44:22 E...	EM_Team_CLOUD	RAM BUFFER RETRIEVAL REQUEST	IO Board 2
10152	165400	2004.10.21 12:40:34 E...	2004.10.22 12:41:45 E...	EM_Team_CLOUD	USER LOGOFF	

Figure 18. Event Log window

Initially, you view EM Seq, Time, Director Name, Event ID, FRU, Severity, and Event Code information. You can sort the information and how it is presented by clicking on the headers. For example, click the **Time** header to sort events by time or click on the **FRU** header to sort events by FRU.

Initial event log details

Event log details can be sorted by clicking the various headers.

Table 3. Initial Event Log details

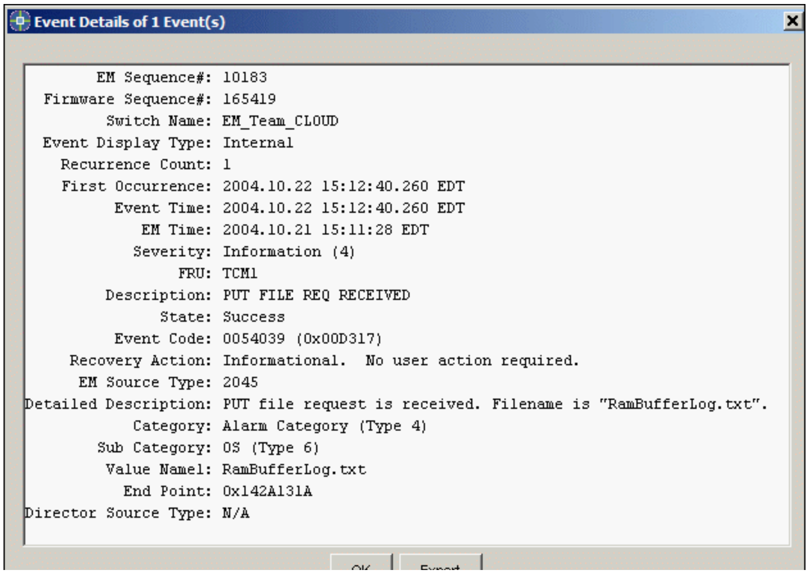
Header	Description
EM Seq #	Tracking number assigned to the event via the EM.
FW Seq #	Tracking number assigned to the event via the EM for firmware tracking.
EM Time	Time the event was recorded by the EM.
Event Time	Time the event was recorded.
Director	Name of the switch from where the event originated.
Event	Non-verbose description of the event.
FRU	Identifier of the Field Replaceable Unit which is/was affected by the event.

Table 3. Initial Event Log details (Continued)

Severity	A severity of 1 to 5 is listed, with 1 being the harshest.
Event Code	Numerical representation of the event for support staff.

Additional Event Log details

You can view additional information about selected events by right-clicking them.



```
       EM Sequence#: 10183
  Firmware Sequence#: 165419
        Switch Name: EM_Team_CLOUD
 Event Display Type: Internal
   Recurrence Count: 1
   First Occurrence: 2004.10.22 15:12:40.260 EDT
         Event Time: 2004.10.22 15:12:40.260 EDT
            EM Time: 2004.10.21 15:11:28 EDT
           Severity: Information (4)
                FRU: TCM1
        Description: PUT FILE REQ RECEIVED
              State: Success
         Event Code: 0054039 (0x00D317)
    Recovery Action: Informational.  No user action required.
     EM Source Type: 2045
Detailed Description: PUT file request is received. Filename is "RamBufferLog.txt".
           Category: Alarm Category (Type 4)
       Sub Category: OS (Type 6)
        Value Name1: RamBufferLog.txt
          End Point: 0x142A131A
Director Source Type: N/A
```

SAN256N
Event log details

Figure 19. Event log details windows for SAN256N director

Table 4. SAN256N director additional Event Log details

Header	**Description**
Event ID	Tracking number assigned to the event.
Fabric Name	Name of the fabric from where the event originated.
Switch Name	Name of the switch from where the event originated.
Event Type	An event of severity 5 is an alert; severity 4 is an alarm.
Time	Time the event was recorded.
FRU	Identifier of the Field Replacable Unit which is/was affected by the event.
Error	Non-verbose description of the event.
Trap Code Type	Type of trap reported: switch, Frame Bus, Port, etc.
Phone Home Code	Phone home code reported.
Error Code	Numerical representation of an event for support staff.
UserActionTime	Time user performed action.
UserActionBy	User ID of one who performed the action.
UserActionByIP	IP address of PC from which user performed action.
Severity	A severity of 1 to 5 is listed, with 1 being the most critical.

Table 4. SAN256N director additional Event Log details (Continued)

Detail Description	A more in-depth documenting of the event/error.
Acknowledge	Events are bold until acknowledged. Information regarding who acknowledged the event and when it was acknowledged is maintained. The type of alarm is also maintained.

Event Log buttons

The following buttons appear in the upper left corner of the Event Log window.

Refresh

Click **Refresh** to refresh the Event Log window.

Print

Click **Print** to print the contents of the Event Log window.

Delete

You can delete Event Log entries based on time or switch.

Export

You can save the contents of the Event Log by exporting it as a text (.txt) file to disk (hard drive, floppy diskette, zip disk, etc.). Follow the instructions below to capture the Event Log and save it to disk.

Acknowledge

You can acknowledge Event Log entries by highlighting them and then clicking **Acknowledge**. Once you acknowledge an event, it is no longer considered new. The count of new events listed in the bottom right corner of the window will reflect the change in status.

Acknowledge All

You can acknowledge all of the Event Log entries by clicking **Acknowledge All**. After acknowledging all errors, the color of the status shown in the bottom right corner of the window changes from red to yellow/green based on other unacknowledged events.

Exporting the Event Log

1. At the Navigation Tree, select the FC/9000 you want for the event log capture.
2. Click the **Event Log** icon from the tree view, and then click **Export**.
3. The file, by default, will be saved in the same folder as your Enterprise Manager Software client files as a .csv file (comma separated value) which may be imported into a spread sheet type program. You may also save it as a .txt file by selecting the .txt option from the **Files of type** drop-down list.

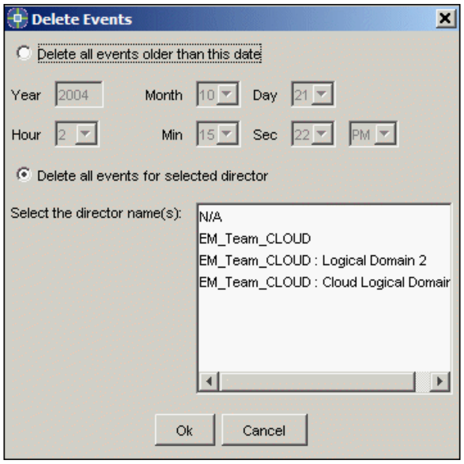
Printing the Event Log

1. At the Navigation Tree, click on the FC/9000 or SAN256N director for which you would like to print event log information.
2. Select the event log you want to print from the Navigation Tree.
3. Click the **Print** button to print the file.

Deleting the Event Log

You can delete the contents of the Event Log by switch or by time/date.

1. At the Navigation Tree, click the **Event Log** icon. The Event Log window appears.
2. Click **Delete.** The following dialog appears:



Delete Events

○ Delete all events older than this date

Year 2004 Month 10 Day 21

Hour 2 Min 15 Sec 22 PM

● Delete all events for selected director

Select the director name(s):

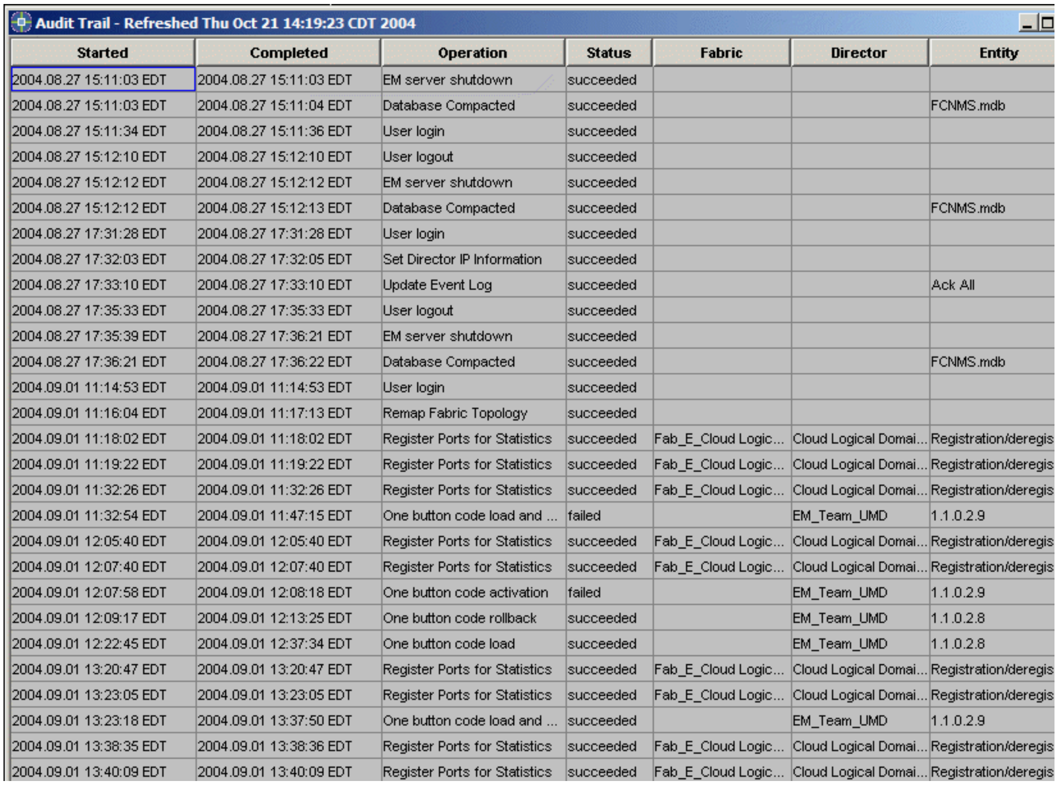
N/A
EM_Team_CLOUD
EM_Team_CLOUD : Logical Domain 2
EM_Team_CLOUD : Cloud Logical Domair

Figure 20. Delete Events window

3. To delete by date, select the **Delete all events older than this date** radio button and the date options will become enabled.
4. Click the arrow next to the month/day and select the desired month or day from the drop down list.
5. Choose the time from which you would like the events to be deleted.
6. To delete by Director, select the **Delete all events for selected director** radio button. The **Select the director name(s)** option is enabled.
7. Select the appropriate director and then click **OK** to delete its event logs.

Audit Trail

The Audit Trail provides information about the server you are connected to. To view this information, click the **Audit Trail** option under the **View** menu. Note that the Audit Trail will show information relevant to the FC/9000 as well as the SAN256N director.



Audit Trail - Refreshed Thu Oct 21 14:19:23 CDT 2004

Started	Completed	Operation	Status	Fabric	Director	Entity
2004.08.27 15:11:03 EDT	2004.08.27 15:11:03 EDT	EM server shutdown	succeeded			
2004.08.27 15:11:03 EDT	2004.08.27 15:11:04 EDT	Database Compacted	succeeded			FCNMS.mdb
2004.08.27 15:11:34 EDT	2004.08.27 15:11:36 EDT	User login	succeeded			
2004.08.27 15:12:10 EDT	2004.08.27 15:12:10 EDT	User logout	succeeded			
2004.08.27 15:12:12 EDT	2004.08.27 15:12:12 EDT	EM server shutdown	succeeded			
2004.08.27 15:12:12 EDT	2004.08.27 15:12:13 EDT	Database Compacted	succeeded			FCNMS.mdb
2004.08.27 17:31:28 EDT	2004.08.27 17:31:28 EDT	User login	succeeded			
2004.08.27 17:32:03 EDT	2004.08.27 17:32:05 EDT	Set Director IP Information	succeeded			
2004.08.27 17:33:10 EDT	2004.08.27 17:33:10 EDT	Update Event Log	succeeded			Ack All
2004.08.27 17:35:33 EDT	2004.08.27 17:35:33 EDT	User logout	succeeded			
2004.08.27 17:35:39 EDT	2004.08.27 17:36:21 EDT	EM server shutdown	succeeded			
2004.08.27 17:36:21 EDT	2004.08.27 17:36:22 EDT	Database Compacted	succeeded			FCNMS.mdb
2004.09.01 11:14:53 EDT	2004.09.01 11:14:53 EDT	User login	succeeded			
2004.09.01 11:16:04 EDT	2004.09.01 11:17:13 EDT	Remap Fabric Topology	succeeded			
2004.09.01 11:18:02 EDT	2004.09.01 11:18:02 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 11:19:22 EDT	2004.09.01 11:19:22 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 11:32:26 EDT	2004.09.01 11:32:26 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 11:32:54 EDT	2004.09.01 11:47:15 EDT	One button code load and ...	failed		EM_Team_UMD	1.1.0.2.9
2004.09.01 12:05:40 EDT	2004.09.01 12:05:40 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 12:07:40 EDT	2004.09.01 12:07:40 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 12:07:58 EDT	2004.09.01 12:08:18 EDT	One button code activation	failed		EM_Team_UMD	1.1.0.2.9
2004.09.01 12:09:17 EDT	2004.09.01 12:13:25 EDT	One button code rollback	succeeded		EM_Team_UMD	1.1.0.2.8
2004.09.01 12:22:45 EDT	2004.09.01 12:37:34 EDT	One button code load	succeeded		EM_Team_UMD	1.1.0.2.8
2004.09.01 13:20:47 EDT	2004.09.01 13:20:47 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 13:23:05 EDT	2004.09.01 13:23:05 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 13:23:18 EDT	2004.09.01 13:37:50 EDT	One button code load and ...	succeeded		EM_Team_UMD	1.1.0.2.9
2004.09.01 13:38:35 EDT	2004.09.01 13:38:36 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis
2004.09.01 13:40:09 EDT	2004.09.01 13:40:09 EDT	Register Ports for Statistics	succeeded	Fab_E_Cloud Logic...	Cloud Logical Domai...	Registration/deregis

Figure 21. Audit Trail

The Audit Trail displays audit trail information for everything controlled by this Enterprise Manager server (fabrics, switches, ports, etc.). You can also export and print audit trail information.

Audit Trail column headers

You can sort Audit Trail details by clicking on the various column headers. Table 5. provides descriptions of the column headers.

Table 5. Audit Trail details

Header	Description
Started	Time the operation was started.
Completed	Time the operation was finished.
Operation	Type of operation performed.
Status	Whether the operation succeeded or failed.
Fabric	Name of the fabric affected by the operation.
Director	Name of the Director affected by the operation.

Table 5. Audit Trail details (Continued)

Entity	Name of the item affected by the operation.
User	Name of the user performing the operation.
User IP	IP address of the user performing the operation.
Description	Description of the operation performed.
Additional Info	Other pertinent information.

User security

Those familiar with previous versions of the Enterprise Manager Software will notice that User Security has many new options and is much more robust. For example:

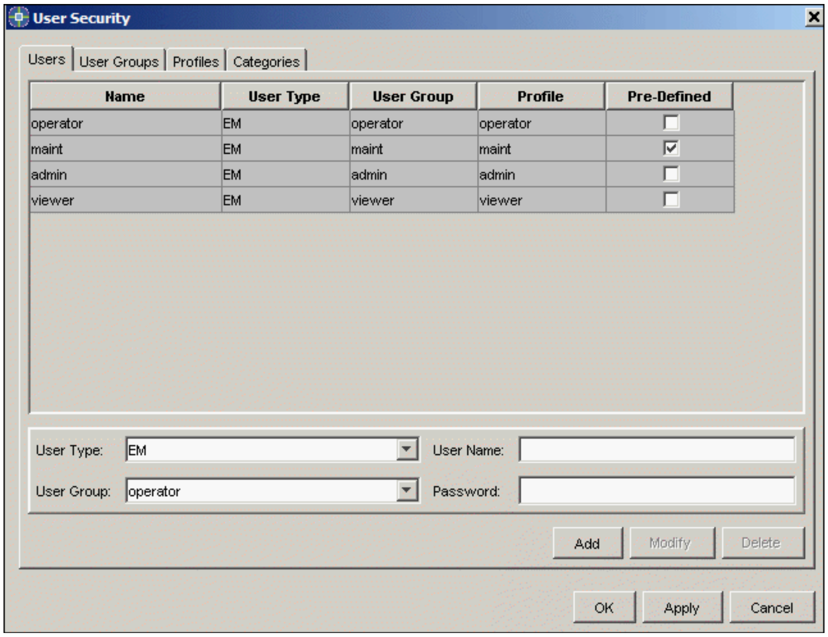
- Four adjustable areas exist: users, user groups, profiles, and categories.
- Users: assigned to user groups.
- User groups: users with common functionality assignments grouped together.
- Profiles: categories assigned and what operations may be performed; profiles assigned to user groups.
- Categories: hard coded options which may not be changed.

Note: User IDs and passwords are case sensitive.

Users

The User tab is the default opening view you see when you click the **User Security** button.

1. Create a User and then add a User to a User Group by clicking an existing User.
2. Type the new User name into the User Name box.
3. Select a User Type from the drop down list. Types include the various methods via which the SAN256N director or FC/9000s may be controlled: EM, SNMP Ver 1 & 2, SNMP Ver 3, Telnet, GS3 or GS4, CUP, FTP.
4. Assign them to a User Group by choosing a User Group from the drop down list.
5. Type the password for the user into the Password area. Click the **Add** button.



Name	User Type	User Group	Profile	Pre-Defined
operator	EM	operator	operator	□
maint	EM	maint	maint	☑
admin	EM	admin	admin	□
viewer	EM	viewer	viewer	□

User Type: EM

User Group: operator

User Name:

Password:

Figure 22. User security: users

User groups

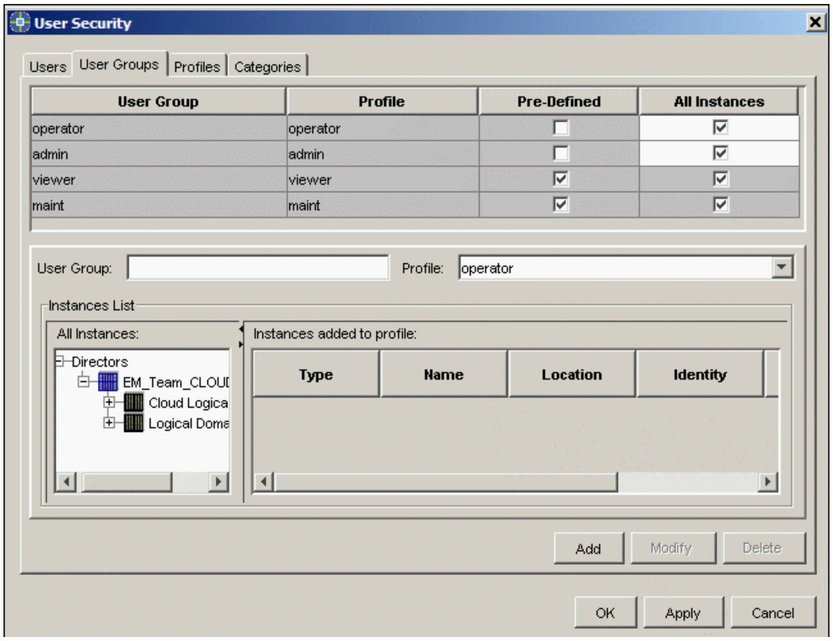
There are four predefined User Groups: operator, admin, viewer, maint. Each of them has a single member, consisting of a Profile of the same name. See the table onpage -47 for default permission information of the profiles assigned to the Users in the User Group. Initially, only Maintenance and Admin level users may create new User Groups.

To create another user group, highlight one which already exists, then type in the name of the new user group in the User Group text box.

Select the profile which you would like to assign to this User Group. (Note that you may create new Profiles at the Profile window if you wish. Profiles, the window for the Profile tab, and how to create them are in the following section.)

Select the director and/or Logical Domains and/or ports which the User Group will be able to access.

From the All Instances list, drag and drop the director into the Instances added to profile list at the right. Checking the box at the All Sub-components included column means all boards and ports associated with that director will be accessible by the User Group. Uncheck the box, and drag a Logical Domain from the left window to the right window. Same rule applies, if the check box is checked under the All Sub-components column, then all ports associated with that Logical Domain will be accessible by the user group. Uncheck the box and then drag individual ports from the left window to the Instances added window to allow the user group to access only the ports listed in that window. Click the **Add** button to add the new User Group.



User Group	Profile	Pre-Defined	All Instances
operator	operator	□	☑
admin	admin	□	☑
viewer	viewer	☑	☑
maint	maint	☑	☑

User Group:

Profile: operator

Instances List

All Instances:

- Directors
  - EM_Team_CLOUI
    - Cloud Logica
    - Logical Doma

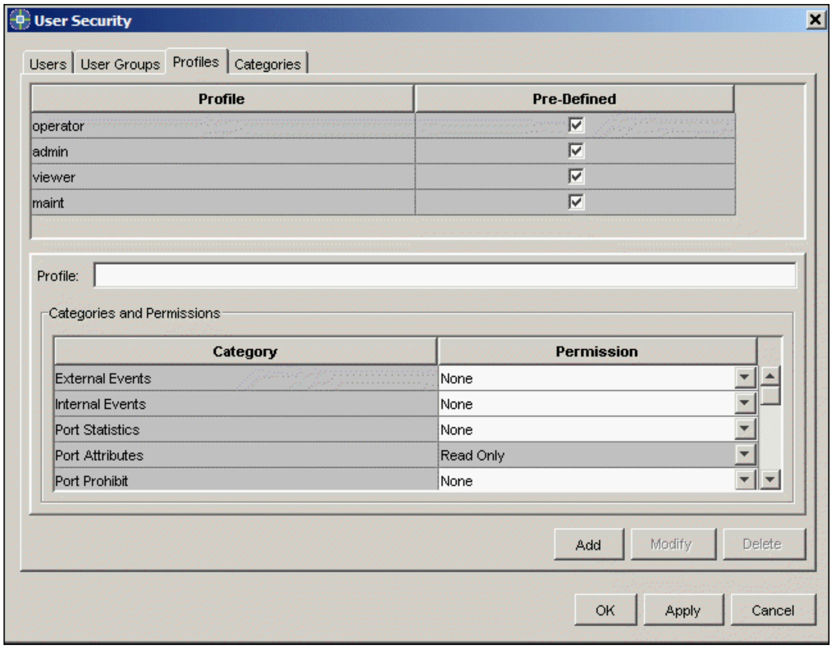
Instances added to profile:

Type	Name	Location	Identity

Figure 23. User Security: user groups

Profiles

There are four predefined profiles: operator, admin, viewer, maint. Each of them has different write (control) and read permissions. See the table onpage -47 for default permission information. Initially, only Maintenance and Admin level users may create new profiles. Once new profiles are created, other users may be given permission to make changes. To create a new Profile, click an existing one and then type the name of the new profile into the Profile text area. If you want to adjust the attributes of the new Profile, do so at the Permission drop down list next to the category you want to change by clicking the arrow next to the drop down list and highlighting your choice: Read/Write, Read Only, or None. Then click the **Add** button to add the profile to the list. You may now assign that profile to a User Group.



Profile	Pre-Defined
operator	☑
admin	☑
viewer	☑
maint	☑

Profile:

Categories and Permissions

Category	Permission
External Events	None
Internal Events	None
Port Statistics	None
Port Attributes	Read Only
Port Prohibit	None

Figure 24. User Security: profiles

Table 6. Profile Permissions

Category	operator	admin	viewer	maint	Description
External Events	R/W	R/W	R	R/W	Events visible to the user
Internal Events	N/A	N/A	N/A	R/W	Engineering debug events
Port Statistics	R	R	R	R/W	Cumulative port performance information
Port Attributes	R/W	R/W	R	R/W	Port performance settings
Port Prohibit	R/W	R/W	R	R/W	Disallow ports from connecting to other specified port(s)
Port Swap	R/W	R/W	R	R/W	Ability to swap a failing port for one which is operational
Sub Switch FC Attributes	R/W	R/W	R	R/W	Fibre channel attributes of the sub switch
Sub Switch Attributes	R/W	R/W	R	R/W	Non fibre channel attributes of the sub switch.
Fabric Security	R/W	R/W	R	R/W	Port and switch binding
Zoning	R/W	R/W	R	R/W	Zone devices and switches
Network Attributes	R/W	R/W	R	R/W	Network connectivity information for directors
SNMP Configuration	R/W	R/W	R	R/W	SNMP configuration for directors
Platform Attributes	R/W	R/W	R	R/W	

Table 6. Profile Permissions (Continued)

Category	operator	admin	viewer	maint	Description
Sensor Data	R	R	R	R/W	
Sub Switch Reconfigure	R	R	R	R/W	
Maintenance	R/W	R/W	R/W	R/W	
Platform Diagnostics	N/A	N/A	N/A	R/W	
User Management	R	R/W	R	R/W	Ability to assign and alter user attributes
Fabric Configuration for GS3	R/W	R/W	R	R/W	
EM Attributes	R/W	R/W	R	R/W	Ability to configure the look and feel of the Enterprise Manager

User groups

At the User Group level, assign a profile to the group and then choose the directors, Boards and Ports the group will have the ability to control from the Instance List

Force ports down

The director has the ability to take a front port off line if the attached device is behaving abnormally. This is done to prevent the director port from being flooded with erroneous data. If a front port is forced down, the user can use the Enterprise Manager Software to place the port administratively off line and then on line which will restore operation.

A backlink can also be forced down if improper behavior is detected. A backlink can also be restored via the Enterprise Manager.

Typical reasons that a port can be forced down:

- More than four log-ins within 10 seconds
- Excessive LOS occurrences within 10 seconds
- Various frame-error events within 10 seconds

The forcedown feature is turned on by default, but it can be disabled for the entire director via the Enterprise Manager.

To enable or disable force ports down

1. Select the director at the SAN tree view upon which you would like to enable or disable the Force Ports Down feature.
2. Right-click in the gray area next to the graphic of the director, and select the **System Configuration** option.
3. Select **Disable** or **Enable** from the drop down list at the **Force Ports Down** option.
4. Click **Apply**, and then click **OK** at the confirmation windows which follow.

Backing up a database

The database backup feature allows you to back up files from the server window. All necessary files will be backed up.

1. Log into the server.
2. Select the **Backup** function from the **File** menu. The Backup dialog appears.
3. Type in the name of the backup file in the **File name** field if you want to change it from the default file name. Then click the **Backup** button to complete the process. When the file has been successfully backed up, you will get a confirmation message.

   Note: If you have a backup file with the same name as the file you are trying to add, you will have to click **OK** to overwrite the older version.

Setting Auto Backup

The Auto Backup feature allows you to automatically back up files that you deem important. This function is performed at the Server window.

1. Log into the server.
2. Select the **AutoBackup** function from the **Configuration** menu. The Auto Backup Settings dialog appears.
3. Click the **Auto Backup Enabled** box. The Auto Backup Settings window appears.
4. Use Windows Explorer to locate the file you want to back up.
5. After selecting the file, click **Backup**.
6. The cursor is now in the **Every** field. The value entered in this field determines the frequency in hours by which you backup the file. Type in a number.
7. Click **OK** to continue.

Restoring a database

Note: Do not attempt to restore a database without first consulting a IBM-qualified service person.

1. Shutdown the Enterprise Manager Software server and client host software.
2. From the desktop, click the **Enterprise Manager DB-Restore** icon.
3. From the Restore dialog, select the database file you want to restore or browse to the selected folder that contains the database you want to restore and select one from there.
4. Click **Restore** to restore the selected database.

Licensing optional features

Fabric security and CUP are a licensable features that can be added via the License Wizard.

Using the license wizard

1. From the Enterprise Manager, connect to the director you want to license.
2. From the **Director** menu, select the **License** function to display the **Product License Client** window.

3. Select the check box for each feature(s) you want to license. If this is an upgrade, recheck features that had previously been enabled in addition to features being added.
4. Refer to the SAN256N director Software License document(s) you received in the original, if applicable, and upgrade shipment(s) to obtain the License Key and enter it (them).
5. Click **Apply**. The Validation prompt is displayed.
6. Click **OK** to validate and apply the License Keys.

Copying a codeset

The copy codeset functionality is available from the client window.

To copy a codeset, select **File | Copy Codeset** to display a window where you can browse to the codset you want to copy.

Port Groups

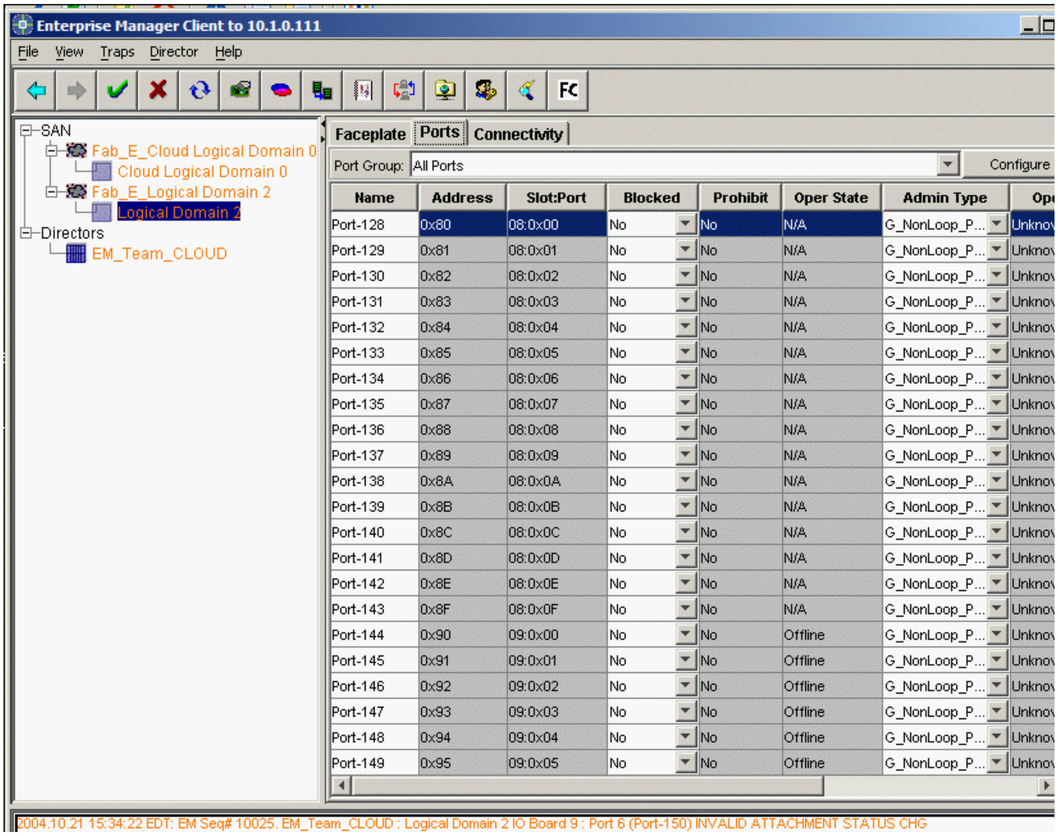
Port Groups are a collection of ports. In larger Directors and Logical Domains, grouping ports will allow for smaller matrixes of blocking and prohibiting assignments.

Creating a Port Group

Use the following procedure to create a Port Group.

1. At the SAN view window select a director or Logical Domain in which you would like to create a port group, the select the **Ports** tab.

2. Click the **Configure** button. The Port Group window appears.



Port Group: All Ports

Name	Address	Slot:Port	Blocked	Prohibit	Oper State	Admin Type	Ope
Port-128	0x80	08:0x00	No	No	N/A	G_NonLoop_P...	Unknov
Port-129	0x81	08:0x01	No	No	N/A	G_NonLoop_P...	Unknov
Port-130	0x82	08:0x02	No	No	N/A	G_NonLoop_P...	Unknov
Port-131	0x83	08:0x03	No	No	N/A	G_NonLoop_P...	Unknov
Port-132	0x84	08:0x04	No	No	N/A	G_NonLoop_P...	Unknov
Port-133	0x85	08:0x05	No	No	N/A	G_NonLoop_P...	Unknov
Port-134	0x86	08:0x06	No	No	N/A	G_NonLoop_P...	Unknov
Port-135	0x87	08:0x07	No	No	N/A	G_NonLoop_P...	Unknov
Port-136	0x88	08:0x08	No	No	N/A	G_NonLoop_P...	Unknov
Port-137	0x89	08:0x09	No	No	N/A	G_NonLoop_P...	Unknov
Port-138	0x8A	08:0x0A	No	No	N/A	G_NonLoop_P...	Unknov
Port-139	0x8B	08:0x0B	No	No	N/A	G_NonLoop_P...	Unknov
Port-140	0x8C	08:0x0C	No	No	N/A	G_NonLoop_P...	Unknov
Port-141	0x8D	08:0x0D	No	No	N/A	G_NonLoop_P...	Unknov
Port-142	0x8E	08:0x0E	No	No	N/A	G_NonLoop_P...	Unknov
Port-143	0x8F	08:0x0F	No	No	N/A	G_NonLoop_P...	Unknov
Port-144	0x90	09:0x00	No	No	Offline	G_NonLoop_P...	Unknov
Port-145	0x91	09:0x01	No	No	Offline	G_NonLoop_P...	Unknov
Port-146	0x92	09:0x02	No	No	Offline	G_NonLoop_P...	Unknov
Port-147	0x93	09:0x03	No	No	Offline	G_NonLoop_P...	Unknov
Port-148	0x94	09:0x04	No	No	Offline	G_NonLoop_P...	Unknov
Port-149	0x95	09:0x05	No	No	Offline	G_NonLoop_P...	Unknov

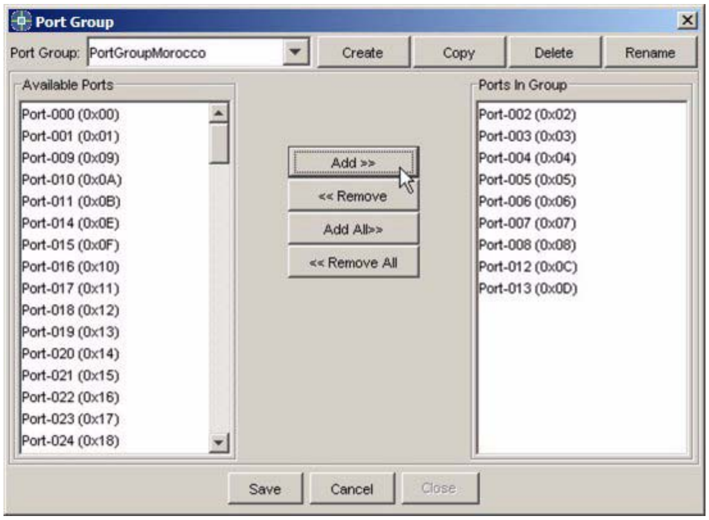
```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
```

Figure 25. Port Group window

3. Click **Create**. The Create Port Group window appears.

4. Type in the name you want to give the group and then click **OK**. Available ports associated with the specified group now appear in the Port Group window.

5. Select the ports that you want to add to a Port Group from the Available Ports list, then click **Add**. The ports you selected now appear in the Ports in Group list.



Port Group: PortGroupMorocco

Available Ports

Port-000 (0x00)
Port-001 (0x01)
Port-009 (0x09)
Port-010 (0x0A)
Port-011 (0x0B)
Port-014 (0x0E)
Port-015 (0x0F)
Port-016 (0x10)
Port-017 (0x11)
Port-018 (0x12)
Port-019 (0x13)
Port-020 (0x14)
Port-021 (0x15)
Port-022 (0x16)
Port-023 (0x17)
Port-024 (0x18)

Ports In Group

Port-002 (0x02)
Port-003 (0x03)
Port-004 (0x04)
Port-005 (0x05)
Port-006 (0x06)
Port-007 (0x07)
Port-008 (0x08)
Port-012 (0x0C)
Port-013 (0x0D)

Figure 26. Port Group: create, copy, delete, or rename window

6. If you are finished adding ports to the group, click **Save** to save the group and then click **OK** on the confirmation message dialog that appears.
7. Click **Close** when you are finished.

Removing ports from a Port Group

Use the following procedure to remove ports from a port group.

1. At the SAN view, select the Director or Logical Domain from which you would like to remove ports in a port group.
2. At the **Ports** drop-down list, select the port group from which you wish to remove ports and then click the **Configure** button to the right of the list. The Port Group window appears.
3. Select the ports that you want to remove from the port group and then click **Remove**.
4. Click **Save** to save the changes to the port group and then click **OK** at the confirmation dialog.
5. Click **Close** to close the Port Group window if you are finished.

Deleting a Port Group

Use the following procedure to delete a port group from a selected director.

1. At the SAN view, select the Director or Logical Domain from which you would like to delete a port group.
2. At the **Ports** drop-down list, select the port group you wish to delete and then click the **Configure** button to the right of the list.
3. Click **Delete** to delete the Port Group and then click **Yes** on the confirmation dialog.
4. Click **Save** and then click **OK** on the confirmation dialog.
5. Click **Close** to close the Port Groups window.

Copying a Port Group

Use the following procedure to copy a Port Group and then rename it as another Port Group.

1. At the SAN view, select the Director or Logical Domain at which you would like to copy a port group.
2. At the **Port Group** drop-down list, select the port group you want to copy and then click **Configure**.
3. Click **Copy**.
4. Type in the name of the new Port Group in the **Copy Port Group** window, and then click **OK**.
5. Click **Save** after you make any changes (adding or removing ports) that you wish to accomplish with the new Port Group and then click **OK** at the confirmation dialog.
6. Click **Close** when you are finished with the **Port Group** window.

Port and switch binding

Port and switch binding allows users to restrict access to a director and its individual ports from other nodes in a fabric. It could also be called Device Connection Control (DCC). When binding is disabled, any node is permitted access through any port in the switch.

Note: Port and switch binding are only available for the FC/9000 8- and 16- port switches and 64-, 128- and 256- port directors.

Switch binding initial setup

1. Highlight an FC/9000 switch or director at the SAN list of the navigation tree.
2. Click **Director** at the menu bar and select the **Device Binding** option.
3. At the Device Binding configuration window, the default view is Switch Binding.
4. To bind devices to a switch, simply choose them from the left panel by either selecting them individually by using standard windows selection procedures or use the **Add/Remove All** button to add all devices, and then move them to the right panel by by clicking on the **Add Selected** button.

   Note: Note that the radio buttons above the available device list allow you to toggle the view of devices from all devices in the fabric to devices currently connected to the switch at which you are attempting to bind devices.

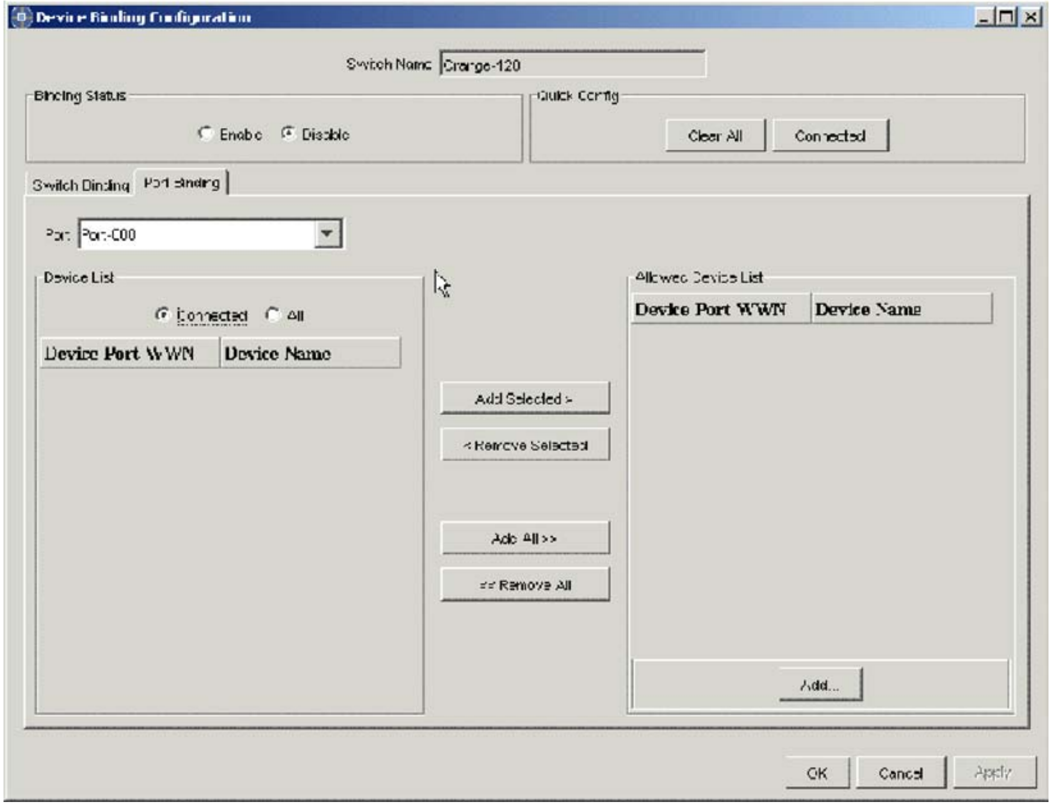
5. After you have moved the devices you want to bind to this switch, you can click the **Apply** button. This will move the list of devices to the switch.

   Any device that attempts to log into the switch, such as new attachments, that is not part of the switch binding list will be rejected, and the attached port is isolated with “Invalid Attachment.”

6. Click the **Enable** radio button, and then click **OK** at the confirmation window. This enables the list as the devices which may attach to this switch.

Port binding

Clicking the **Device Binding** tab opens the Device Binding window.



Switch Name: Orange-120

Binding Status: ○ Enable ● Disable

Port: Port-C00

Device List: ● Connected ○ All

Figure 27. Device Binding Configuration window

Initial port binding

Port binding is a way to ensure that devices communicate through a particular port on a director.

1. After invoking the Device Binding Configuration window, click the **Port Binding** tab.
2. At the Port drop down list, select the port to which you will bind devices by scrolling through the list of port and highlighting the port of your choice.
3. At the Devices list, determine whether you want to view all devices in the fabric, or only those currently connected to the director at which you will be binding the devices, by clicking either the **Connected** or **all** radio button.
4. Use standard Windows selection procedures to select the devices you would like to bind to the port you selected earlier.
5. Click the **Add Selections** button to move the ports you selected to the list at the right panel. You may also click on the **Add All** button to move all of the devices listed in the panel at the left to the list on the right.
6. Click the **Apply** button to send the list to the switch.

7. Click the **Enable** radio button, and then click **OK** at the confirmation window. This enables the list to the switch and binds the devices you chose to the port you chose.

   Any device that attempts to log into the switch via the specified port , such as new attachments, that is not part of the port binding list will be rejected, and the attached port is isolated with Invalid Attachment.

Adding devices to the switch binding list

1. Invoke the Device Binding Configuration window.
2. In the panel on the left, highlight the devices you wish to add. Use the All or Connected button to show the devices you wish to add.
3. Click the **Add Selected** button.
4. Click **Apply**.
5. Click the **Enable** button, and then click **OK** at the confirmation window to complete the task.

Removing devices from the switch binding list

1. Invoke the Device Binding Configuration window.
2. In the panel on the right, highlight the devices you wish to remove.
3. Click the **Remove Selected** button.
4. Click **Apply**.
5. Click on the **Enable** radio button, then click **OK** at the confirmation window to complete the task.

   When the last device is removed from the switch binding list, only devices that have been configured in a specific port binding list will be permitted access to the switch, and only through an attachment on that specific port.

Adding devices to the port binding list

1. Invoke the Device Binding Configuration window.
2. Click the **Port Binding** tab.
3. Use the Port drop down list to choose the port to which you would like to bind devices.
4. In the panel on the left, highlight the devices you wish to add. Use the All or Connected button to show the devices you wish to add.
5. Click the **Add Selected** button.
6. Click **Apply**.
7. Click the **Enable** button, and then click **OK** at the confirmation window to complete the task.

Removing devices from the port binding list

1. Open the **Device Binding Configuration** window.
2. Click the **Port Binding** tab.
3. Use the Port drop down list to choose the port from at you would like to remove bound devices.
4. In the panel on the right, highlight the devices you wish to remove.
5. Click the **Remove Selected** button.

6. Click **Apply**.
7. Click the **Enable** button, and then click **OK** at the confirmation window to complete the task.

   When the last device is removed from a specific post binding list, then all devices attached to that port will be enforced from the switch binding list.

Combined switch/port binding for entire switch

1. Open the **Device Binding Configuration** window.
2. Use the Quick Configure panel (upper right section of the Device Binding Configuration window).
3. Clicking **Connected** and then **Apply** would stage the switch/ports bound list in the switch.
4. Clicking **Clear All** and then **Apply** would clear the switch/ports bound list in the switch.
5. Click the **Enable** button, and then click **OK** at the confirmation window to complete the task.

Globally disable all bindings

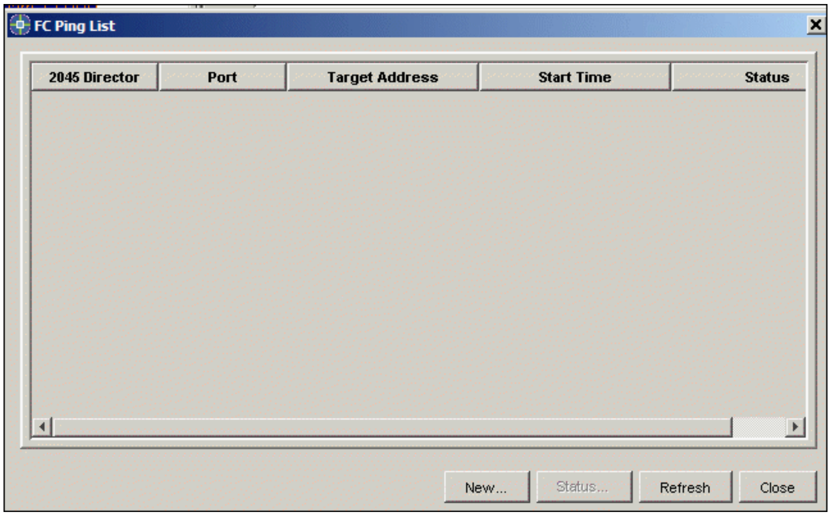
To disable all bindings, open the **Device Binding Configuration** window and click **Clear All**.

FC Ping

The FC Ping functionality allows you to check the route or physical link between a source port and a device connected to the switch.

Performing FC Ping test

1. Click the **FC** button on the Enterprise Manager Software toolbar. The FC Ping List window appears:

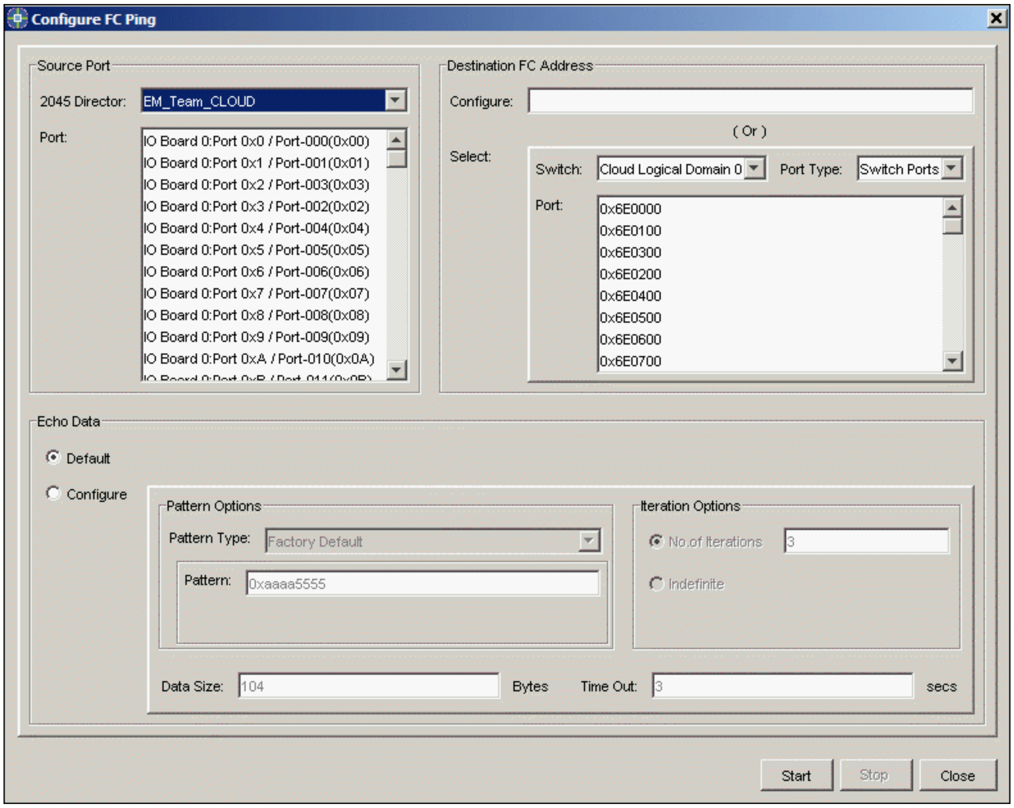


FC Ping List

2045 Director	Port	Target Address	Start Time	Status

Figure 28. FC Ping List window

2. To begin a new FC Ping test, click **New.** The Configure FC Ping window appears:



Configure FC Ping

Source Port

2045 Director: EM_Team_CLOUD

Port:

IO Board 0:Port 0x0 / Port-000(0x00)
IO Board 0:Port 0x1 / Port-001(0x01)
IO Board 0:Port 0x2 / Port-003(0x03)
IO Board 0:Port 0x3 / Port-002(0x02)
IO Board 0:Port 0x4 / Port-004(0x04)
IO Board 0:Port 0x5 / Port-005(0x05)
IO Board 0:Port 0x6 / Port-006(0x06)
IO Board 0:Port 0x7 / Port-007(0x07)
IO Board 0:Port 0x8 / Port-008(0x08)
IO Board 0:Port 0x9 / Port-009(0x09)
IO Board 0:Port 0xA / Port-010(0x0A)
IO Board 0:Port 0xB / Port-011(0x0B)

Destination FC Address

Configure:

(Or)

Select:

Switch: Cloud Logical Domain 0

Port Type: Switch Ports

Port:

0x6E0000
0x6E0100
0x6E0300
0x6E0200
0x6E0400
0x6E0500
0x6E0600
0x6E0700

Echo Data

● Default

○ Configure

Pattern Options

Pattern Type: Factory Default

Pattern: 0xaaaa5555

Iteration Options

● No.of Iterations 3

○ Indefinite

Data Size: 104 Bytes

Time Out: 3 secs

Figure 29. Configure FC Ping window

3. On the left side of the window, begin by selecting the director on which the board and port the the source of the FC Ping test will reside. That is, the port which will send out the ping.

4. Then from the drop down list below the source director, select the source port. Note that the port you choose can not be the port from which the ping originates.

5. Now shift your attention to the right side of the window. Choose the director (if an FC/9000) or Logical Domain upon which the port through which the device is connected. Choose the port type from the Port Type drop down list, and then choose the port.

6. You then have the choice of either using the default Echo Data option (three pings) or setting up a custom configuration. To set up a custom configuration, perform the following:

   – Select the pattern type from the drop down list.

   – Select the Pattern

   – Select either the number of iterations or indefinite iterations by clicking on the radio button of your choice. If you select the number button, you should then type in the number of iterations you want the test to run.

   – Select the Data Size you would like to run by entering in a number.

   – Enter a Time Out value.

7. Click the **Start** button to begin the test. When the test is finished, a **Detail Status** button will appear at the window:

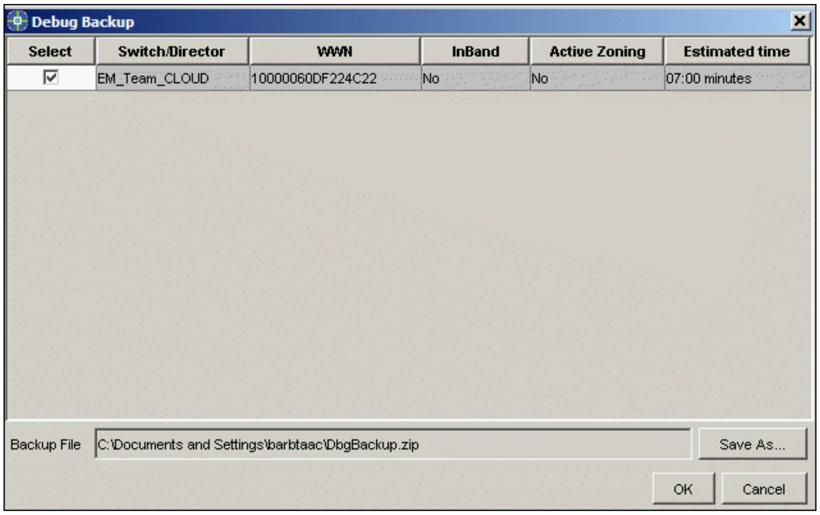
8. Click **Detail Status** to view information about the test

Debug Backup

Debug Backup function allows you to collect debug backup information about the SAN256N director and FC/9000 directors.

Perform a Debug Backup

1. Click **File | Debug Backup** from the drop down list. The Debug Backup window appears:



Select	Switch/Director	WWN	InBand	Active Zoning	Estimated time
☑	EM_Team_CLOUD	10000060DF224C22	No	No	07:00 minutes

Backup File: C:\Documents and Settings\barbtaac\DbgBackup.zip

Figure 30. Debug Backup window

2. Select which directors upon which you would like the backup performed by checking the boxes next to them. Note that the boxes are checked by default.
3. Direct where you would like the backup files to be placed by clicking on the **Save As** button and indicating a directory, or accept the default directory by doing nothing, and then click on **OK**.

One button code load

One button code load via the Enterprise Manager Software allows maintenance level users the ability to load code into an FC/9000 director or switch.

One button code load for FC/9000

1. Click the **Code Load** button.
2. After clicking the **Code Load** button, the **One Button Code Load** window is displayed.
   - Hard reset boards after application code move: Enterprise Manager by default does a soft reset after an application code move to boards. By selecting this option, Enterprise Manager will perform hard resets to those boards. By default, this option is not selected.
   - Hard reset board(s) after FPGA code move:
   - Move code to failed boards: User has option to select if they want to move code to failed boards. If selected, an attempt will be made to move FCM flash code to

failed boards (Application as well as FPGA). The board will be hard reset after move code. By default this option is selected.

– Stop after first error (for each director): User can select if they want to stop/ continue after any error has encountered. By default this option is selected.

3. Select the code load set from the drop down box at the right by clicking the arrow and then clicking the code set you want to load. Note that you must choose a code set for each director into which you want to load code. Also note that you may choose a different available code set for directors and concurrently complete those code loads when you click the Start button.

4. Select the director(s) to which you wish to download code by clicking on them. Note that all directors known by the Enterprise Manager Software will be listed.

   Note: Inband and out of band directors must be loaded in separate sessions. Upgrade out of band directors first. Then Inband directors secondly.

5. Select the options you wish to apply and click the **Start** button. Click the **OK** button at the confirmation window to continue the process. Note that if you wish to stop the process, click the **Abort** button and not the **Close** button. Clicking the **Close** button simply closes the window but does not stop the process. Clicking the **Detail Status** button shows progress of the code load.

One button code load for SAN256N director

1. Click the **Code Load** button.

2. After clicking the **Code Load** button, click the SAN256N director tab to see the following window.

3. Select the code load set from the drop down box at the right by clicking on the arrow and then clicking on the code set you want to load. Note that you must choose a code set for each director into which you want to load code.

4. Select the director(s) to which you wish to download code by clicking on them. Note that all directors known by the Enterprise Manager will be listed.

   Note: Inband and out of band directors must be loaded in separate sessions. Upgrade out of band directors first. Then Inband directors secondly.

5. Click the **Load and Activate** button, or click Load if you want to only load the code at this time and want to manually choose **Activate**. Click the **OK** button at the confirmation window to continue the process. Note that if you wish to stop the process, click on the **Abort** button and not the **Close** button. Clicking the **Close** button simply closes the window but does not stop the process. Clicking on the Detail Status button shows progress of the code load.

Chapter 5. 8- and 16-port switch configuration and control

The Enterprise Manager Software is composed of a set of windows with each window managing a different aspect of switch/fabric configuration.

This chapter covers information which is relevant to the 8- and 16-port FC/9000 switches. Some information which is generic to the 8-, 16-, 64-, and 128-port switches and directors may be found in “Common switch functionality” on page 27 of this guide.

- The first window that the application displays following login is the Main Display window. From this window, you can navigate to other windows which will allow you to configure and control any FC/9000 switch to which you have access. Fabrics to which you have access are displayed.
- Choose a fabric and the application displays a list of switches for a multiple switch fabric. For multiple switch fabrics, the Fabric window allows you to select and manage any switch in the fabric.
  - Choose any switch icon and the application displays a switch front view display for the selected switch.
- The switch front view display is composed of a graphical representation of the switch and information pertaining to that switch. The **General** tab is the default view displayed.
  - Choose the **Event Log** tab to view event log information about various boards installed on the previously selected switch. The following pages describe the general procedures for each of these.

Note: There are three levels of access: Viewer, Operator and Administrator. The procedures and examples on the following pages are in Administrator mode. Items and procedures not available in Viewer and Operator mode will be noted as such.

FC8-2 and FC16-2 notes

The FC8-2 and FC16-2 are the 2-Gigabit versions of the 8- and 16-port FC/9000 switch. The Enterprise Manager Software will allow you to view them at the fabric view, but will not bring up a switch view of them. Control of them and viewing their statistics may be accomplished via the FC-2 EM. After double-clicking one of their icons in the Fabric view, the FC-2 EM will launch.

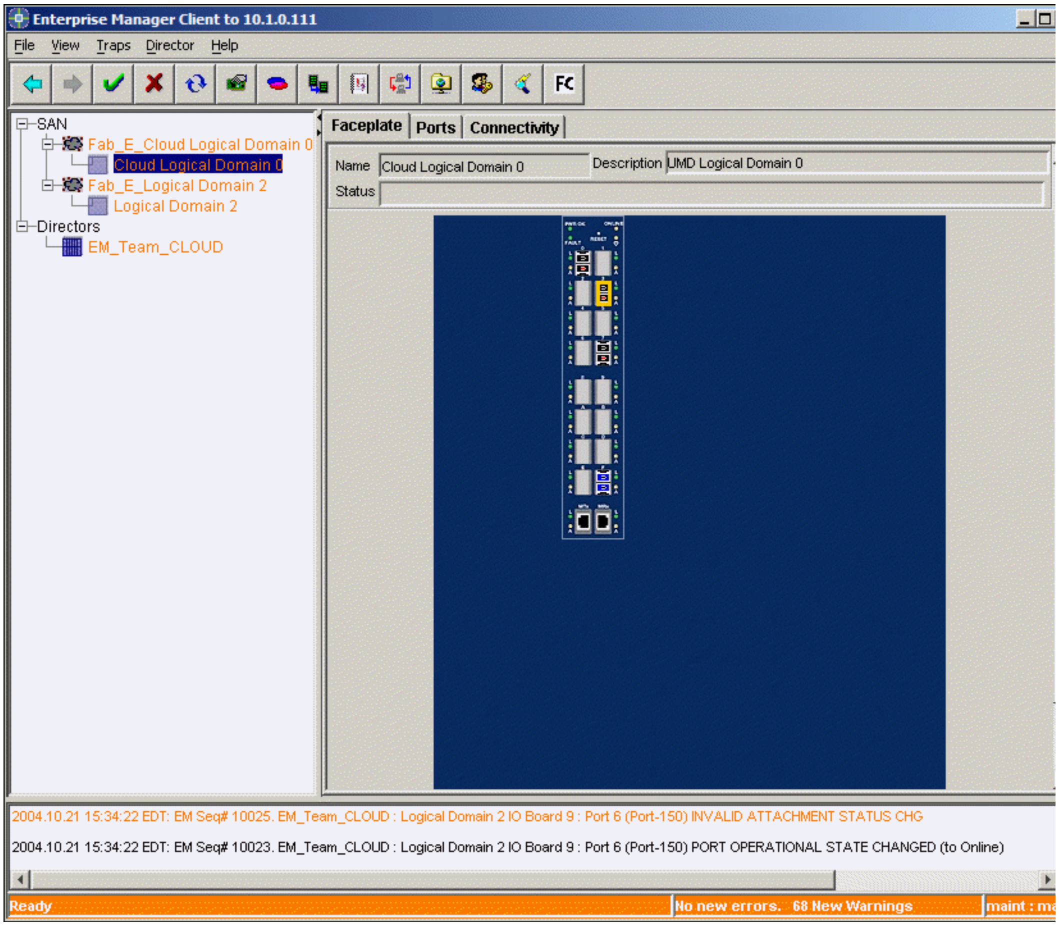
Each FC8-2 or FC16-2 which you wish to view and/or control must be connected via an Ethernet connection to the Enterprise Manager server. The IP address for each switch you wish to view and/or control must be included in the fabric definition in the Enterprise Manager. The switch will appear in the Fabric Topology view of the Enterprise Manager Software.

The FC-2 Enterprise Manager Software must be installed on the EM server along with the Enterprise Manager in their default directories. When you double-click or call up the FC-2 or SANBox2 within the Fabric View of the Enterprise Manager, the FC-2 EM will automatically hot launch. You can then view statistics and make changes to the FC-2 switch using the FC-2 EM software. For more external application information, see the “External application launch and setup” on page 24.

© Copyright IBM Corp. 2004

SAN view

After clicking a switch under the SAN header, you see the information for the Faceplate tab.



Name: Cloud Logical Domain 0
Description: UMD Logical Domain 0
Status:

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Figure 31. Faceplate view

The **Faceplate** view is displayed by default. It provides the face view of the switch. It shows all the installed GBICS and some of the switch properties. By mousing over the graphic of the faceplate, you can view information relevant to the SFP.

Faceplate view details

The following fields are displayed when the **Faceplate** tab is selected:

- **Name**

  The name of the switch viewed.

- **Temp**

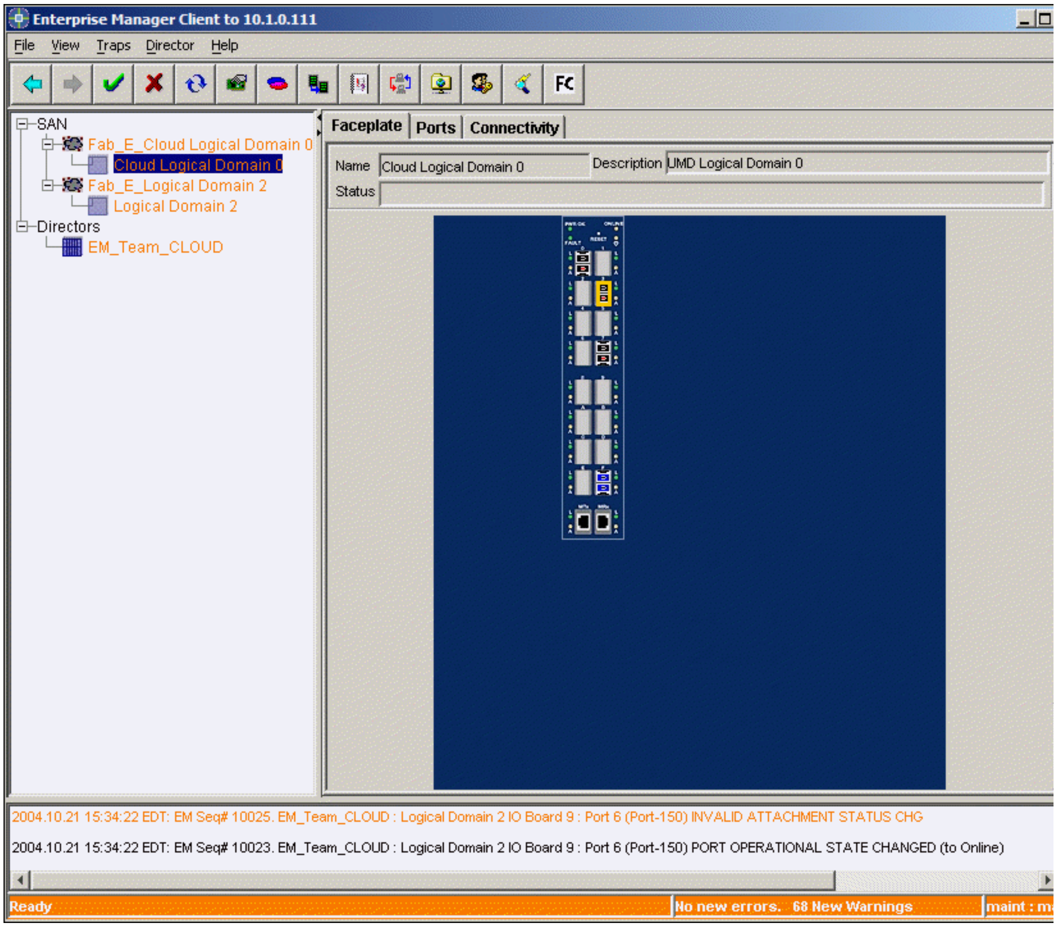
  The temperature of the unit.

- **Description**

  Information provided by the user.

Ports tab

The **Ports** tab shows port information for the selected switch. Note that the Online Configuration view is the default.



Name: Cloud Logical Domain 0

Description: UMD Logical Domain 0

Status:

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Ready | No new errors. 68 New Warnings | maint : m

Figure 32. Switch view - Port Config tab

Ports tab details

The following fields are displayed when the **Ports** tab is selected:

Table 7. Port tab fields

Field	Description
Name	Name of the port.
Description	User-provided description of the port.
Status	Indication of whether the port is online or offline.

Table 7. Port tab fields (Continued)

Save Statistics	If checked, ports associated will be sampled every five minutes and the information will be saved to a .csv file. The file will be named xxx_portstatistics.csv (with xxx equaling the switch WWN) and may be found in the directory in which the Enterprise Manager server resides. Additions to the file will append to the file, until the file becomes 20 megabytes in size. At that time, a backup file will be created and all the old information will be stored in that backup file (xxx_portstatistics.bak.csv). New information will be stored in the xxx_portstatistics.csv file until the 20 megabyte limit is again reached. A backup file will again be created, which will overwrite the old backup file. Right-click to get device information which shows the type of device connected through port.

Ports right-click information

Right-click over a port and a menu gives you the following options.

Offline port configuration information

For Offline Port Configuration information, click on the **Offline Port Configuration** radio button**.** Information about port configuration settings, and allows you to create new port configurations, save created port configurations, and copy port configurations using the **Save As...** button.

Save a port configuration

1. Select a configuration from the **Configurations** drop-down list.
2. Click **Save**.

New port configuration

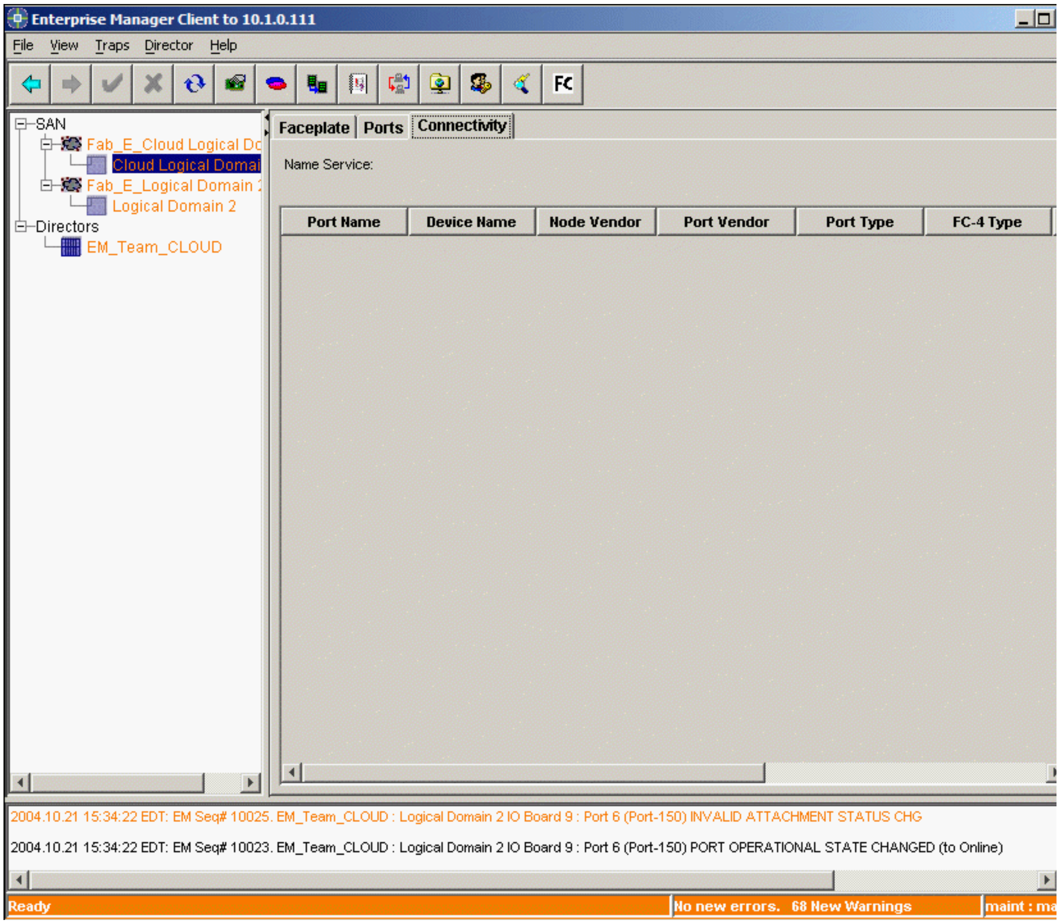
1. Click the **New** button to create a new port.
2. Type a name in the **Name** field and click **OK**.
3. Click **Save** to save the port.

Save configuration as

1. Use the **Save As...** button to save a current configuration.
2. You can then change the configuration if you wish.

SAN view - Connectivity tab

The **Connectivity** tab shows Name Service information about the system configuration of the selected FC-16 switch.



```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Ready | No new errors. 68 New Warnings | maint : ma

Figure 33. SAN view - Connectivity tab

Name Service details

The following fields are displayed when the **Name Service** tab is selected:

Table 8. Name Service tab fields

Field	Description
Port Name	Name of the port for which you are viewing information.
Device Name	Name of the device for which you are viewing information.
Vendor	Vendor of the equipment connected to the port.
Port Type	Type of port for which you are viewing information.
FC-4 Type	Device fibre channel protocol types.
FC Physical Address	Physical address of the port.
Node WWN	World Wide Name (WWN) of the piece of equipment connected to the port. Private devices will not be listed.

Table 8. Name Service tab fields (Continued)

Port WWN	World Wide Name of the port via which the equipment is connected.

Right-click information

Right-clicking over a gray area in the SAN or director view of the switch will pull up a menu of four items:

- System Configuration
- Network Configuration
- Trace Log
- Version

SAN view - System Configuration details

Right-click in a gray area of the SAN or switch view and you see a menu. Select the **System Configuration** option to view System Configuration details.

Note: TOV values must be the same for all directors and switches across the fabric.

The following fields are displayed when **System** is selected as the Configuration Type.

Table 9. System field

Field	Description
Inter Switch Link Type	Shows whether the fabric is in E_Port mode.
WWN	World Wide Name (WWN) assigned to the Director.
Ser. No.	Serial number assigned to the Director in manufacturing.
RT TOV	The RT_TOV field controls the Receiver_Transmitter_Timeout value for all ports on the chassis. Select the field, type the new value. The number is in ms (2000 = 2 seconds). The numbers may be changed with the help of a IBM-qualified service person.
RA TOV	The RA_TOV field controls the Resource_Allocation_Timeout value for all ports on the selected chassis. Select the box, type the new value. The number is in ms (2000 = 2 seconds). The numbers may be changed with the help of a IBM-qualified service person.
ED TOV	The ED_TOV field controls the Error_Detect_Timeout value for all ports on the chassis. Select the box, type the new value. The number is in ms (2000 = 2 seconds). The numbers may be changed with the help of a IBM-qualified service person.
MFS TOV	The MFS TOV field controls the Multi Frame Sequence Time-out Value for all ports on the selected switch. The numbers may be changed with the help of a IBM-qualified service person.

Table 9. System field (Continued)

Director Domain ID	The domain ID is a unique fibre channel identifier for the switch. The domain ID must be unique for each switch in the fabric. In a SAN with redundant paths, the Domain IDs have to be unique even if the two fabrics are not ISL'd together. (shown when in E_Port mode).
WWN of Principal Switch	WWN of the Principal Switch of the fabric in which this director resides (shown when in E_Port mode).

Network Configuration details

Right-click in a gray area of the SAN or switch view and you see a menu. Select the **Network Configuration** option to view Network Configuration details.

Table 10. Network Configuration fields

Field	**Description**
IP Address	The IP network address of the selected Director.
Net Mask	The IP subnetwork mask.
IP Gateway	The IP address of the network gateway.
Ethernet Mac	The Mac address of the selected Director.
arpTimeout	The time in seconds to expire entries in the arp cache. By default this is set to 30000 (about 8 hours).
snmpName	The value of the SNMP Systems Group SysName variable. This is usually identical to the host name, for example, “switch001”. The default value for this parameter is the empty string, “”.
snmpLocation	The value of the SNMP Systems Group SysLocation variable. This is usually set to identify the physical location of the Switch, for example, “Wiring Closet B, 3rd floor, East”. The default value for this parameter is the empty string, “”.
snmpContact	The value of the SNMP Systems Group SysContact variable. This is usually set to identify the person or organization responsible for maintaining the host, for example, “John Chaney, x0123”. The default value for this parameter is the empty string, “”.
Snmp Read Community	The SNMP community name to be recognized for SNMP Get and GetNext requests. By default this is the string “public”.
Snmp Write Community	The SNMP community name to be recognized for SNMP Set requests. By default this is the string “private”.
Snmp Trap Community	The SNMP community name to be used in SNMP Trap messages. By default this is the string “public”.
Trap Address 1 through 5	IP addresses of PCs or workstations running SNMP manager to which SNMP trap information may be sent by the Director.

Table 10. Network Configuration fields (Continued)

Trap Authorization	A check indicates that trap information will be sent to the indicated IP address.

Version tab details

Right-click in a gray area of the SAN or switch view and you see a menu. Select the **Version** option to view Version details.

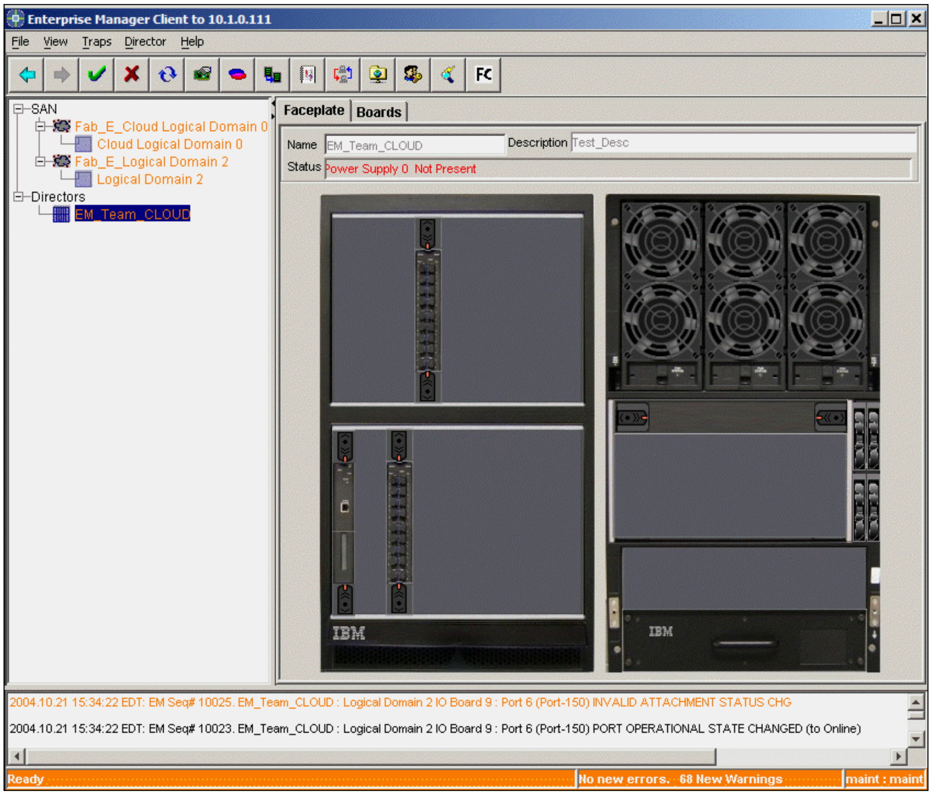
The following fields are displayed when the **Version** tab is selected.

Table 11. Version tab fields

Field	Description
FLASH REV	Version information of the Flash firmware.
PROM HW	Version information of the PROM hardware.
FLASH SW	Version information of the Flash firmware.
PROM SW	Version information of the PROM software.
UTIL MSG	Util version, typically 0 or 1.
Long PROM HW	Version information of the PROM hardware.

Directors view

Click a director under the **Directors** heading in the treeview, and you see the front and back of the director can be viewed.



Name EM_Team_CLOUD Description Test_Desc

Status Power Supply 0 Not Present

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 34. Directors View - Facplate tab

Take a port offline

Note: Viewer level users may not apply changes.

You can take the selected port offline from this view.

1. Select the **Offline** radio button.
2. Click the **Apply** button on the Toolbar to perform the action.

Arbitrated loop

Note: Viewer level users may not apply changes.

You can designate an Arbitrated Loop port in the FC/9000 by clicking on a box and then clicking the **Apply** button. A checkmark indicates activation.

Enabling auto sense arbitrated loop

1. Click the box next to **Auto Sense Arbitrated Loop Enabled** to place the selected port into Auto Sense Arbitrated Loop mode.
2. Click the **Apply** button on the Toolbar to complete the action.

Disabling auto sense arbitrated loop

1. Click the box next to **Auto Sense Arbitrated Loop Enabled** to remove the selected port from Auto Sense Arbitrated Loop mode.
2. Click the **Apply** button on the Toolbar to complete the action.

Point-to-point

Note: Viewer level users may not apply changes.

You can designate a port as Point-to-Point in the FC/9000.

1. Click the **Point-to-Point** radio button to place the selected port into Point-to-Point mode.
2. Click the **Apply** button at the Toolbar to complete the action.

Admin type

Note: Viewer level users may not apply changes.

This option allows you to change the Admin Type of a port from Normal (default) to a TL_Port. Changing the port to TL will allow you to assign World Wide Name(s) (WWN) of a device to it. The WWN is a 64-bit address composed of the 48-bit MAC address and 16-bit NAA address.

Refer to Appendix D. for instructions on changing a port Admin Type from Normal to TL.

Port tuning

In most circumstances, tuning of an individual port is not desirable and the default setting (Normal) should be left unchanged. However, certain Host-Bus-Adapters (HBAs) perform better with tuning. To support optimum performance with these HBAs, the Switch allows individual ports to be tuned based on the characteristics of a particular HBA. Tuning modes supported are:

Non-I - Non-interleaved
This option prevents sequences from different sources and bound for a single destination from being interleaved. Once a sequence has begun, the Switch will not transmit frames from any source other than the one which began the sequence.

This mode is recommended only for Tachyon-based adapters being used for IP traffic. It is not recommended in any other circumstance. If the fabric consists of multiple switches, Non-I must also be selected on any Cross Connect port that will be used as a route to the Tachyon.

Min-I - Minimize-interleave
This option, while not preventing interleaved sequences, minimizes their extent. Once a sequence has begun, the switch will continue to transmit from the same source as long as frames are available for transmission or end-of-sequence occurs. If no frames are available for transmission, then a new source will be started and held until it has no frames to transmit or end-of-sequence occurs. This mode is recommended for Qlogic 2xxx HBAs.

Frame-L - Frame limit
This option limits the number of frames that can be transmitted during a single loop tenancy to 32. This option is recommended for JNI HBAs based on the Adaptec ASIC, and Adaptec HBAs.

Normal
No tuning applied. Recommended for all situations.

Chapter 6. SAN256N director switch configuration and control

The Enterprise Manager Software is composed of a set of windows with each window managing a different aspect of director/fabric configuration.

- The first window that the application displays following login is the Main Display window. From this window, you can navigate to other windows which will allow you to configure and control any SAN256N director switch to which you have access. Fabrics to which you have access are displayed.
  - Choose a fabric and the application displays a list of switches for a multiple switch fabric. For multiple switch fabrics, the Fabric window allows you to select and manage any switch in the fabric.
  - Choose any switch icon and the application displays a switch front view display for the selected switch.
- The switch front view display is composed of a graphical representation of the switch and information pertaining to that switch. The **General** tab is the default view displayed.
  - Choose the **Event Log** option to view event log information about various boards installed on the previously selected switch.
  - Select a TFIO board for information.
- The Board Management portion of the window may control/view any of the following for the selected switch:
  - General (default)
  - Name Service

The following pages describe the general procedures for each of these.

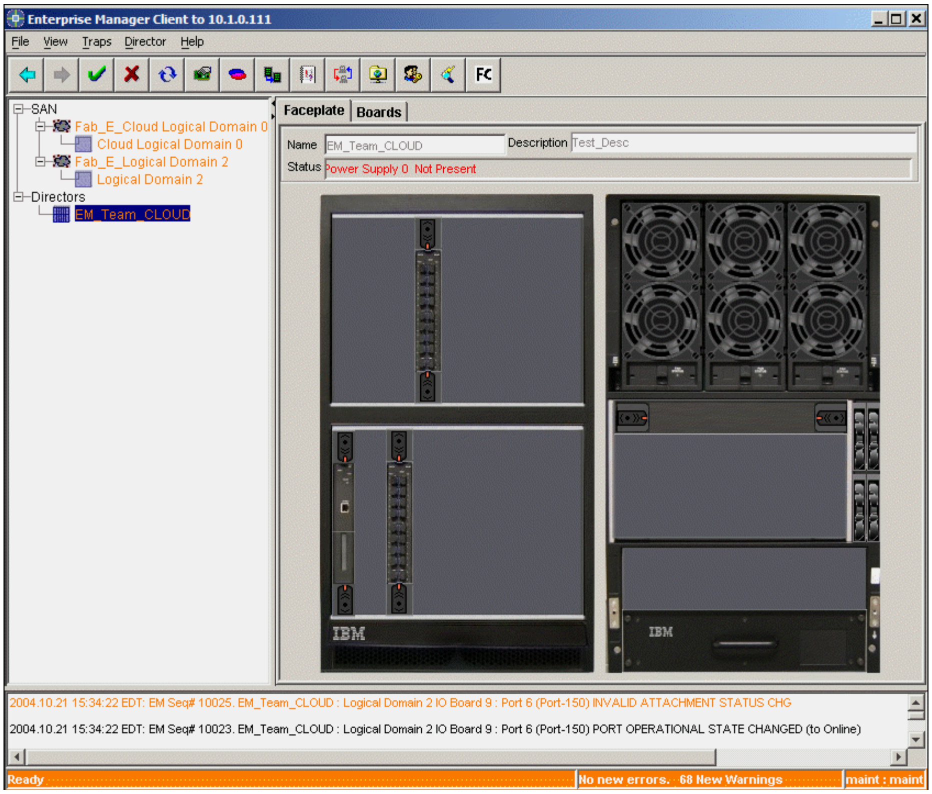
Note: There are four levels of access: Viewer, Operator, Administrator, and Maint. The procedures and examples on the following pages are shown in Maint mode. See the User Security section in Chapter 4 for information on setting up user groups and accessibility options.

Faceplate view

There are now two separate faceplate views at which you can look. One at the SAN view level, the other at the director view level. Each has different attributes which may be viewed by right-clicking different areas of the window.

© Copyright IBM Corp. 2004

Director faceplate view



Name EM_Team_CLOUD
Description Test_Desc
Status Power Supply 0 Not Present

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 35. Director faceplate view

The **Faceplate** tab is displayed by default. It provides the front and rear views of the Director and all the installed boards, fans and power supplies. By right-clicking on the grey area to the left of the graphic, you will display a new menu.

Version
Select Version from the right-click menu to display the **Version Information of the Director** window.

Current Primary

Information for the Current Primary SAN256N director Control Module.

Current Secondary

Same information as in the Current Primary View, but applicable to the secondary SAN256N director Control Module

Previous Primary

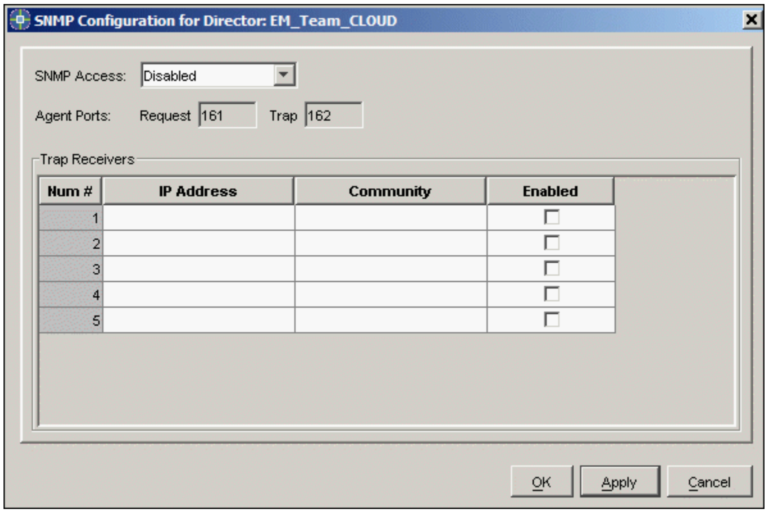
Previous primary TCM code version.

Previous Secondary

Previous secondary TCM code version.

SNMP configuration

This window displays the SNMP Configuration information and configuration options for the selected director.



SNMP Configuration for Director: EM_Team_CLOUD

SNMP Access: Disabled

Agent Ports: Request 161 Trap 162

Trap Receivers

Num #	IP Address	Community	Enabled
1			□
2			□
3			□
4			□
5			□

Figure 36. SNMP Configuration for Director window

SNMP access

Disable and enable SNMP access to the director via the drop down list at the top of the page.

Agent ports

IP ports of SNMP agent involved with requests and trap information.

Trap receivers

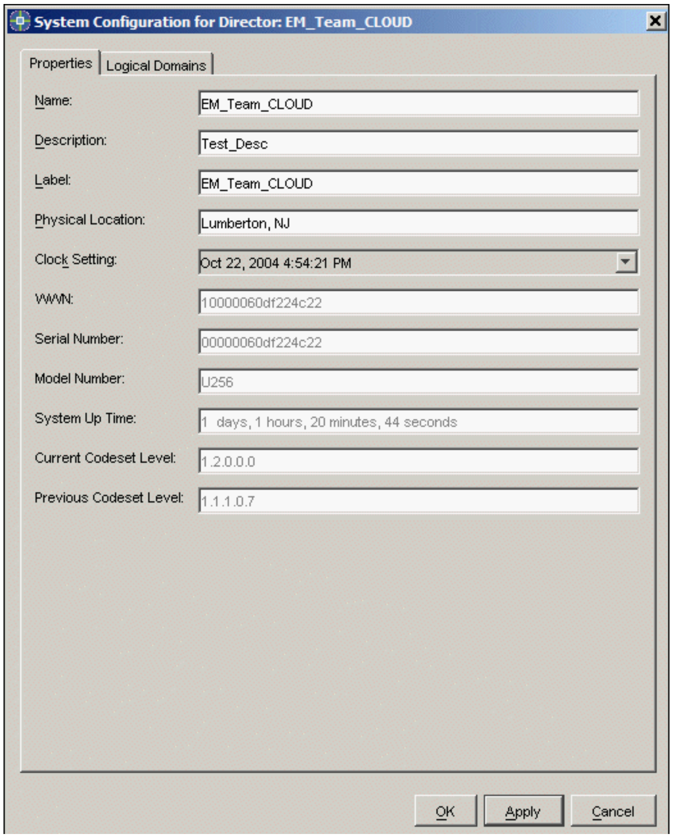
Trap Receivers may be set by simply typing in the IP address of the PC at which trap information may be viewed and typing in the appropriate community name. You can then enable or disable those addresses by clicking the check box in the Enabled column. A checked box indicates enablement.

System restart

Simply stated, this will restart the system. Select the System Restart option and then click **OK** at the warning window.

Director view system configuration

Selecting the **System Configuration** option pulls up the Director View System Configuration window for the director. Note that this System Configuration view shows director identification information.



System Configuration for Director: EM_Team_CLOUD

Properties | Logical Domains

Name: EM_Team_CLOUD

Description: Test_Desc

Label: EM_Team_CLOUD

Physical Location: Lumberton, NJ

Clock Setting: Oct 22, 2004 4:54:21 PM

WWN: 10000060df224c22

Serial Number: 00000060df224c22

Model Number: U256

System Up Time: 1 days, 1 hours, 20 minutes, 44 seconds

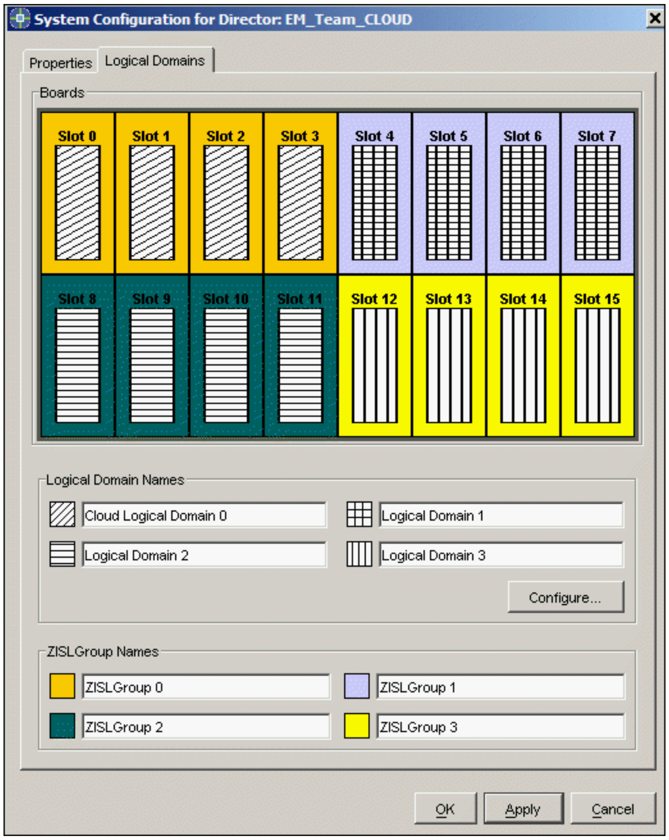
Current Codeset Level: 1.2.0.0.0

Previous Codeset Level: 1.1.1.0.7

Figure 37. Director View System Configuration window

Logical domains

Selecting the Logical Domains tab displays the **System Configuration for Director: SAN256N director** window.



System Configuration for Director: EM_Team_CLOUD

Logical Domain Names

▨ Cloud Logical Domain 0	▦ Logical Domain 1
▤ Logical Domain 2	▥ Logical Domain 3

ZISLGroup Names

🟧 ZISLGroup 0	🟪 ZISLGroup 1
🟦 ZISLGroup 2	🟨 ZISLGroup 3

Figure 38. System Configuration for Director window

The default configuration is that everything is in logical domain 0, and Zero Cost ISL (ZISL) Group Network 0. All have the diagonal lines and mustard color.

Note: The ability to change the logical domain configuration is a licensed option. Please call your support representative for information on how to obtain a license for logical domain functionality.

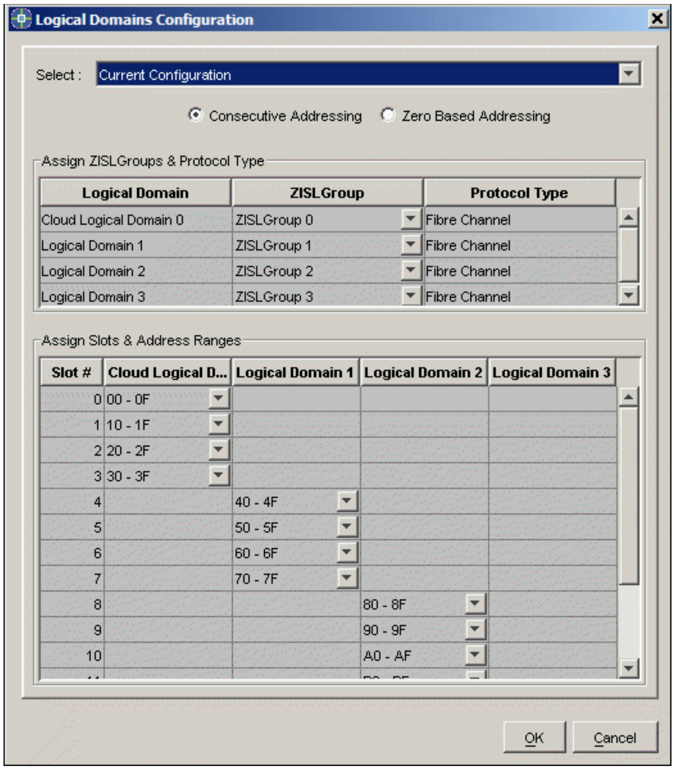
You may create three other logical domains and three other ZISL Groups.

Configure logical domain

Configure logical domains as a means of creating two separate logical directors within one physical director.

1. Click the director at the director view where you would like to create a logical domain. Right-click in the grey area to the left of the director view and then select the **System**

Configuration option. Then click on the **Logical Domains** tab. Click the **Configure** button



Logical Domains Configuration

Select : Current Configuration

● Consecutive Addressing ○ Zero Based Addressing

Assign ZISLGroups & Protocol Type

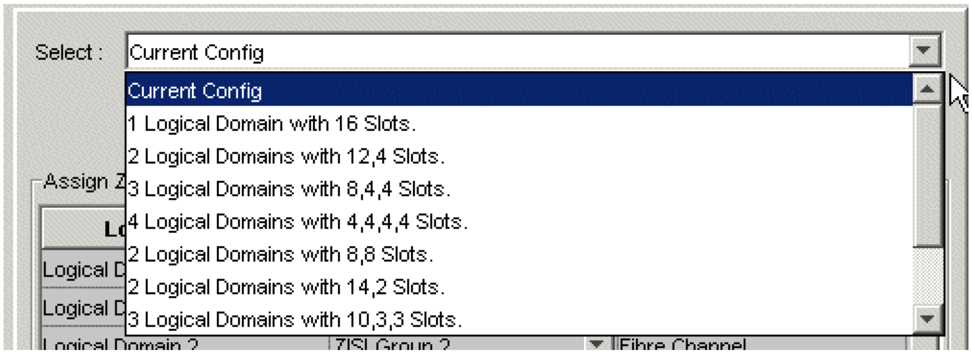
Logical Domain	ZISLGroup	Protocol Type
Cloud Logical Domain 0	ZISLGroup 0	Fibre Channel
Logical Domain 1	ZISLGroup 1	Fibre Channel
Logical Domain 2	ZISLGroup 2	Fibre Channel
Logical Domain 3	ZISLGroup 3	Fibre Channel

Assign Slots & Address Ranges

Slot #	Cloud Logical D...	Logical Domain 1	Logical Domain 2	Logical Domain 3
0	00 - 0F			
1	10 - 1F			
2	20 - 2F			
3	30 - 3F			
4		40 - 4F		
5		50 - 5F		
6		60 - 6F		
7		70 - 7F		
8			80 - 8F	
9			90 - 9F	
10			A0 - AF	

Figure 39. Logical Domains Configuration window

2. Select the the pre-configured option which fits how you want to set up the logical domains of the director. Determine how many logical domains you will have, and the slot count of each of them. Note that there are sixteen ports per slot or board.



Select : Current Config

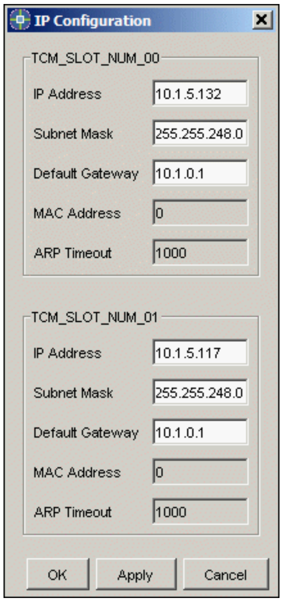
Current Config
1 Logical Domain with 16 Slots.
2 Logical Domains with 12,4 Slots.
3 Logical Domains with 8,4,4 Slots.
4 Logical Domains with 4,4,4,4 Slots.
2 Logical Domains with 8,8 Slots.
2 Logical Domains with 14,2 Slots.
3 Logical Domains with 10,3,3 Slots.

Figure 40. Drop-down menu options

3. Zero cost InterSwitch Links is a way to set up an ISL between logical partitions without having to physically cable them together.
4. When finished, click **OK**.
5. After the configuration, click **Apply.**
6. Click **OK** at the confirmation windows which appear.

IP addresses

The last entry on the right-click list contains IP Addresses of the control modules (TCMs). Click it and you see the following window. In it, you can view the IP addresses of the TCMs, along with their Subnet mask, Default Gateway, MAC Address and ARP timeout. The first three may be changed by typing in new values and clicking **Apply**.



TCM_SLOT_NUM_00

IP Address	10.1.5.132
Subnet Mask	255.255.248.0
Default Gateway	10.1.0.1
MAC Address	0
ARP Timeout	1000

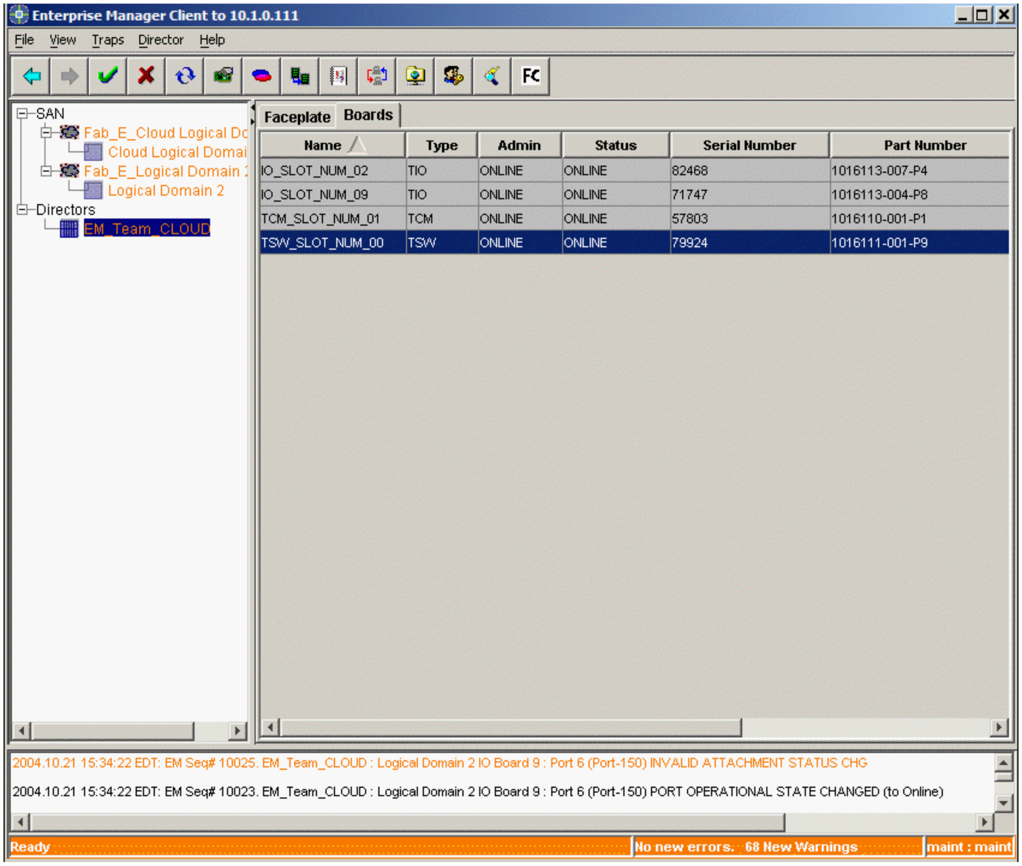
TCM_SLOT_NUM_01

IP Address	10.1.5.117
Subnet Mask	255.255.248.0
Default Gateway	10.1.0.1
MAC Address	0
ARP Timeout	1000

Figure 41. IP Settings window

Director boards view

To see board information for a particular director, click a particular director under the directors heading and then click the Boards tab. You will see the name of the board, board type, board serial number, admin state and the status of the board.



Name	Type	Admin	Status	Serial Number	Part Number
IO_SLOT_NUM_02	TIO	ONLINE	ONLINE	82468	1016113-007-P4
IO_SLOT_NUM_09	TIO	ONLINE	ONLINE	71747	1016113-004-P8
TCM_SLOT_NUM_01	TCM	ONLINE	ONLINE	57803	1016110-001-P1
TSW_SLOT_NUM_00	TSW	ONLINE	ONLINE	79924	1016111-001-P9

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 42. Director board view

Highlight a board and then right-click over it to display the following menu options:

Search...
Perform a search at the board window within the information presented at that window via options selected by the user.

Filter...
Filter the board information according to the parameters which you set at the Filter menu.

Print...
Print board information.

Export...
Export board information.

Customize
Customize the information presented at the boards window via the parameters set at the Customize menu.

Soft Reset

Perform a soft reset on the selected board. To do so, simply click on the **Soft Reset** option and click the **OK** buttons at the confirmation windows which follow.

Hard Reset

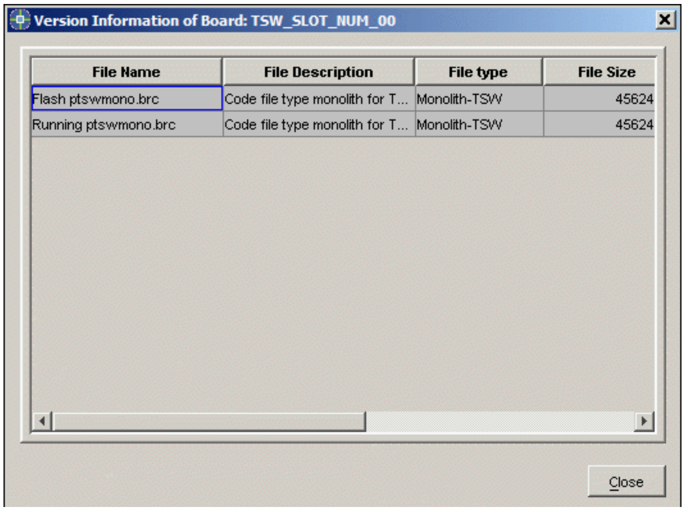
Perform a hard reset on the selected board. To do so, simply click on the **Hard Reset** option and click the **OK** buttons at the confirmation windows which follow.

Beacon

Enable and disable a beacon of the selected board.

Versions...

Right-click over a highlighted board, and see the **Versions** window:



Version Information of Board: TSW_SLOT_NUM_00

File Name	File Description	File type	File Size
Flash ptswmono.brc	Code file type monolith for T...	Monolith-TSW	45624
Running ptswmono.brc	Code file type monolith for T...	Monolith-TSW	45624

Figure 43. Version Information window

Table 12. Version Information window fields

Field	**Description**
File Name	File name of the code.
File Description	Description of the code.
File Type	The type of code.
File Size	Size of the code present.
File Version	Version of the code.
Timestamp	Code timestamp.
Valid	Valid or Invalid

Configuration...

The Configuration window includes the name of the board, the state of the board (online, offline) and the chosen admin mode of the board.

Board admin mode

Taking a board offline

Note: Viewer level users may not apply changes.

You can take the selected board offline from this view.

1. Select the **Offline** radio button.
2. Click the **Apply** button on the Toolbar to complete the action.

Placing a board online

Note: Viewer level users may not apply changes.

You can place the selected board online from this view.

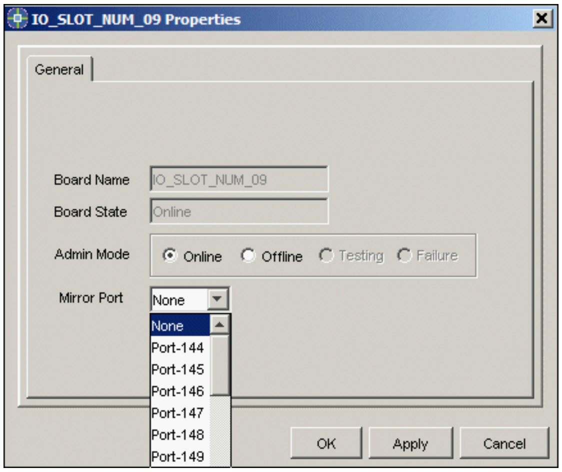
1. Select the **Online** radio button.
2. Click the **Apply** button on the Toolbar to complete the action.

Note: The Testing and Failure options are only available to those with maintenance level access to the Enterprise Manager.

Mirror port

You can perform the mirror port function at this window.

Setting mirror ports with the Enterprise Manager Software takes a little preparation. You may need to research the blades (TFIO boards) and corresponding ports through which the information is being passed, if you don't already know. One way to get that information is shown in the graphic below. You can then select the two ports which you would like mirrored.



IO_SLOT_NUM_09 Properties

Board Name: IO_SLOT_NUM_09

Board State: Online

Admin Mode: ● Online ○ Offline ○ Testing ○ Failure

Mirror Port: None

Figure 44. IO Slot Properties window with mirror port information

Set a mirror port

1. To view name service information for a TFIO board, click on the plus sign (+) next to the SAN heading to expand the list of subswitches, if it isn't already.
2. Select the subswitch in which the physical TFIO board is located and then click on the **Connectivity** tab. Name Service information is the default view.

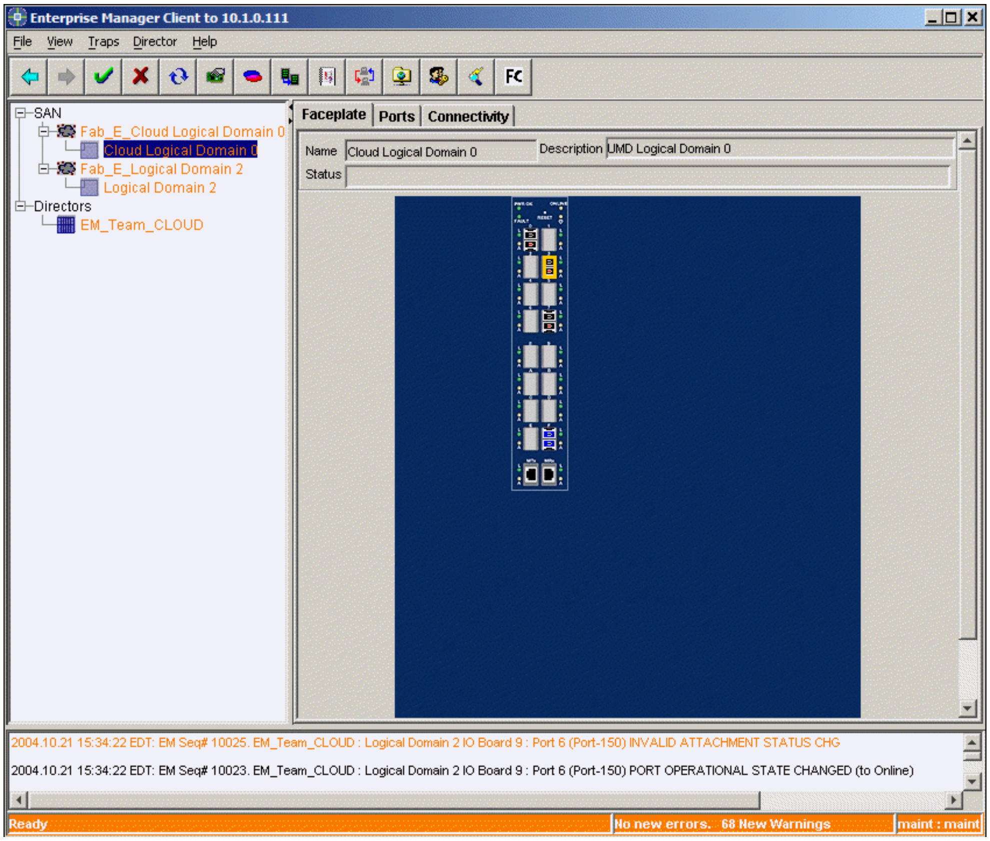
3. Find the port address of the devices whose information you wish to monitor and write them down.
4. To set the mirror ports you have selected, at the director heading at the left panel click on the **+** to expand the list of directors, if it isn’t already.
5. Select the director on which the boards reside by clicking on it at the left panel.
6. Click the **Boards** tab.
7. Click the TFIO board on which the first port resides.
8. Right-click over the chosen board and select **Properties** from the menu.
9. At the **Mirror Port** drop-down list, select the first port you would like to mirror and then click **Apply**.
10. Click the TFIO board on which the second port resides.
11. At the **Mirror Port** drop-down list, select the second port you would like to mirror and then click **Apply**.
12. You can now hook up an analyzer between the two MTX ports to view the data.

Set director clock

Allows you to set the clock in a SAN256N director. The director clock will be set to the time of the PC from which you performed the procedure.

1. At the Navigation Tree under the **Director** heading, click the SAN256N director for which you would like to set the clock.
2. Right-click in the grey area and click on **System Configuration**.
3. Click the drop down arrow next to the **Clock Setting** listing.
4. Either key in the director time, or set the time via the clock which resides on the PC from which you performed this procedure.

SAN faceplate view



Name: Cloud Logical Domain 0
Description: UMD Logical Domain 0
Status:

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Ready | No new errors. 68 New Warnings | maint : maint

Figure 45. SAN View

The **Faceplate** tab is displayed by default. It provides the face view of the boards associated with the logical view you chose. It shows all the associated boards.

Faceplate at SAN view details

The following fields are displayed when the **Faceplate** tab is selected at the SAN view.

Name

- The name of the Subswitch viewed.

Description

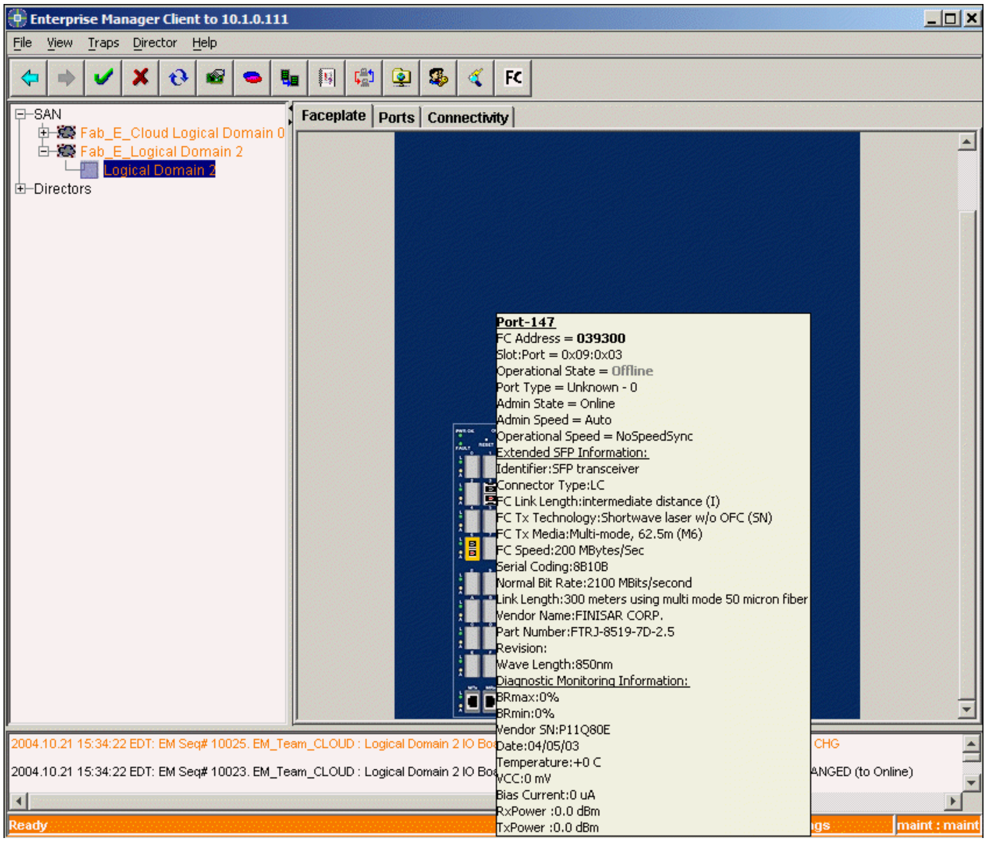
- The user-supplied description of the Subswitch.

Status

- The status of the currently selected Subswitch.

Mouse-over information

Mouse over ports in the SAN view of the SAN256N director, and you see information about the port and the SFP itself. Note that certain SFPs yield more information than others. The extra information is called Digital Diagnostics and can help avoid problems with the SFPs and, ultimately, the director.



```
Port-147
FC Address = 039300
Slot:Port = 0x09:0x03
Operational State = Offline
Port Type = Unknown - 0
Admin State = Online
Admin Speed = Auto
Operational Speed = NoSpeedSync
Extended SFP Information:
Identifier:SFP transceiver
Connector Type:LC
FC Link Length:intermediate distance (I)
FC Tx Technology:Shortwave laser w/o OFC (SN)
FC Tx Media:Multi-mode, 62.5m (M6)
FC Speed:200 MBytes/Sec
Serial Coding:8B10B
Normal Bit Rate:2100 MBits/second
Link Length:300 meters using multi mode 50 micron fiber
Vendor Name:FINISAR CORP.
Part Number:FTRJ-8519-7D-2.5
Revision:
Wave Length:850nm
Diagnostic Monitoring Information:
BRmax:0%
BRmin:0%
Vendor SN:P11Q80E
Date:04/05/03
Temperature:+0 C
VCC:0 mV
Bias Current:0 uA
RxPower :0.0 dBm
TxPower :0.0 dBm
```

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Bo            CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Bo            ANGED (to Online)
Ready                                                                                     gs   maint : maint
```

Figure 46. SAN view, mouse-over view

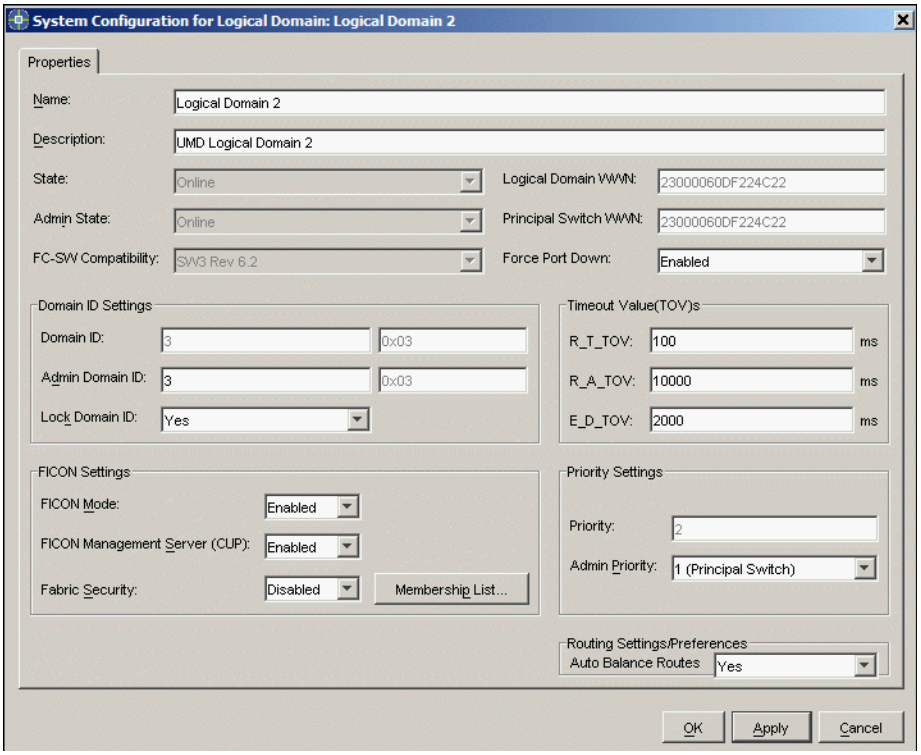
SAN view right-click

Right-click over the gray area to the left of the graphic, and you see a menu with the following options:

- System configuration
- FICON management server (CUP)
- Clear all port statistics

System configuration

Right-click in the gray area of a SAN view of the director and then click System Configuration and you see the following window:



System Configuration for Logical Domain: Logical Domain 2

Properties

Name: Logical Domain 2

Description: UMD Logical Domain 2

State: Online

Logical Domain WWN: 23000060DF224C22

Admin State: Online

Principal Switch WWN: 23000060DF224C22

FC-SW Compatibility: SW3 Rev 6.2

Force Port Down: Enabled

Domain ID Settings

Domain ID: 3 0x03

Admin Domain ID: 3 0x03

Lock Domain ID: Yes

Timeout Value(TOV)s

R_T_TOV: 100 ms

R_A_TOV: 10000 ms

E_D_TOV: 2000 ms

FICON Settings

FICON Mode: Enabled

FICON Management Server (CUP): Enabled

Fabric Security: Disabled

Priority Settings

Priority: 2

Admin Priority: 1 (Principal Switch)

Routing Settings/Preferences

Auto Balance Routes: Yes

Figure 47. System Configuration for Logical Domain: Logical Domain 0

System configuration information

Name

Name of the switch.

Description

Description of the switch.

State

Current state of the switch, online or offline.

Admin State

Current admin state of the switch, online or offline.

Logical Domain WWN

WWN of the particular Logical Domain which you are viewing.

Principal Switch WWN

World Wide Name of the Principal Switch of the fabric in which this director resides (shown when in E_Port mode).

FC-SW Compatibility

Set an SAN256N director to operate in SW2 Rev 4.9 mode or Rev 5.3 mode. After selecting the option you want to choose, click the green **Apply** button.

Force port down
Force ports to disengage and go into an offline state after reaching a defined error threshold.

Domain ID settings

Domain ID
The domain ID is a unique fibre channel identifier for the switch. The domain ID must be unique for each switch in the fabric. In a SAN with redundant paths, the Domain IDs have to be unique even if the two fabrics are not ISL'd together (shown when in E_Port mode).

Admin domain ID

Lock domain ID
Lock Domain ID of this director so it may not be altered by the principal switch. (shown when in E_Port mode). This setting must be enabled in FICON environments.

Timeout value (TOV)s

RTTOV
The RT_T_OV field controls the Receiver_Transmitter_Timeout value for all ports on the chassis. Select the field, type the new value. The number is in ms (2000 = 2 seconds). The numbers may be changed with the help of a IBM-qualified service person.

RATOV
The R_A_TOV field controls the Resource_Allocation_Timeout value for all ports on the selected chassis. Select the box, type the new value. The number is in ms (2000 = 2 seconds). The numbers may be changed with the help of a IBM-qualified service person.

EDTOV
The E_D_TOV field controls the Error_Detect_Timeout value for all ports on the chassis. Select the box, type the new value. The number is in ms (2000 = 2 seconds). The numbers may be changed with the help of a IBM-qualified service person.

FICON settings

FICON mode
Select to enable FICON mode. See the definition for FICON Mode in the Glossary for more information. Only maintenance-level users may set this option.

FICON management server (CUP)
Must be enabled for Control Unit Port (CUP). Only maintenance level users may set this option. This feature may *not* be enabled from this window. This is a licensed feature and must be purchased to be enabled.

Fabric security
Include or exclude Directors to be ISL'd. Create a list of directors which can be directly attached through ISL cabling. Directors not in the list are excluded. This setting is required when cascading FICON directors and is optional for open system ISLs. It is also a licensed feature and must be purchased to be enabled.

Priority settings

Priority
Read only, current operational priority in the switch for the purpose of determining/ assigning a domain ID.

Admin priority
The priority used in the CF-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.

Fabric security

The Fabric Security option (also referred to as Fabric Binding) allows you to enable or disable the ability to control the Interswitch Links (ISLs) of Directors within a fabric. Fabric security is a licensable option and is required in a FICON Cascade implementation. Using Fabric Security in open systems configurations is optional.

Enabling fabric security

Enable fabric security at the System Configuration window called at the SAN view.

1. Select **Enabled** from the **Fabric Security** drop-down list.
2. Click **Apply** to complete the process.

Disabling fabric security

Disable fabric security at the System Configuration window.

1. Select **Disabled** from the **Fabric Security** drop-down list.
2. Click **Apply** to complete the process.

Creating a membership list

To be Interswitch Linked with other members of a list, the Fabric Binding Membership List of a Director must match the list of every other director in that grouping.

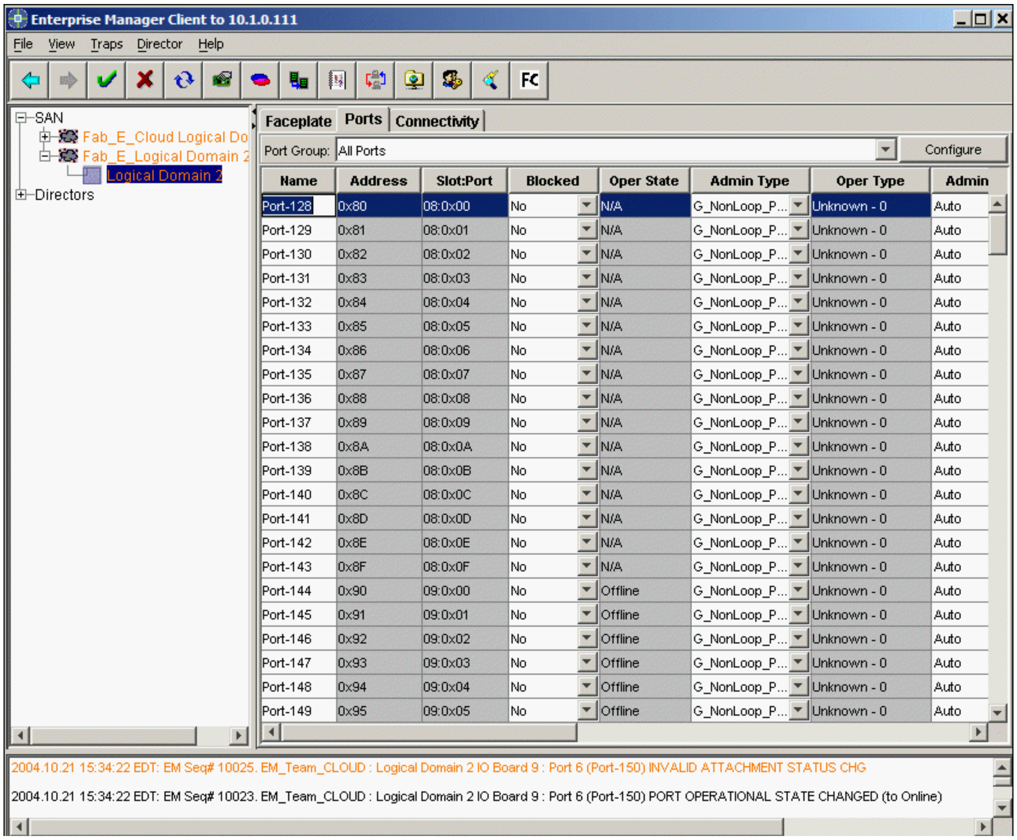
1. Click the **Membership List** button at the System Configuration window of the director with which you would like to create a membership list. The Fabric Binding Membership List dialog appears.
2. Do one of the following to add switches to the list.
   - Enter the **Domain ID** and **WWN** of each switch that you would like to add.
   - Click the **Known Switches** button. The Known Directors List dialog appears. Select the switches you would like to add, and then click **Add**.
3. Click **Add**.
4. Click **OK**.

   Note: If any director that is not on the Membership List is connected to this director, the ISL will not go online. Instead, an “invalid attachment” is reported on the isolated E_Port. This is called out via a yellow border around the port.

Once the Membership List is correct and Interswitch Links are attached, they will come online. For FICON devices, you can now vary online devices which are defined correctly in the Input/Output Configuration Program (IOCP).

Ports tab

The **Ports** tab displays port information about the selected SAN256N director.



Port Group: All Ports

Name	Address	Slot:Port	Blocked	Oper State	Admin Type	Oper Type	Admin
Port-128	0x80	08:0x00	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-129	0x81	08:0x01	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-130	0x82	08:0x02	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-131	0x83	08:0x03	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-132	0x84	08:0x04	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-133	0x85	08:0x05	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-134	0x86	08:0x06	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-135	0x87	08:0x07	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-136	0x88	08:0x08	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-137	0x89	08:0x09	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-138	0x8A	08:0x0A	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-139	0x8B	08:0x0B	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-140	0x8C	08:0x0C	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-141	0x8D	08:0x0D	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-142	0x8E	08:0x0E	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-143	0x8F	08:0x0F	No	N/A	G_NonLoop_P...	Unknown - 0	Auto
Port-144	0x90	09:0x00	No	Offline	G_NonLoop_P...	Unknown - 0	Auto
Port-145	0x91	09:0x01	No	Offline	G_NonLoop_P...	Unknown - 0	Auto
Port-146	0x92	09:0x02	No	Offline	G_NonLoop_P...	Unknown - 0	Auto
Port-147	0x93	09:0x03	No	Offline	G_NonLoop_P...	Unknown - 0	Auto
Port-148	0x94	09:0x04	No	Offline	G_NonLoop_P...	Unknown - 0	Auto
Port-149	0x95	09:0x05	No	Offline	G_NonLoop_P...	Unknown - 0	Auto

```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Figure 48. Switch View - Ports tab

Ports tab details

The following fields are displayed when the **Port Config** tab is selected.right-click.

Table 13. Port Config tab field descriptions

Field	Description
Name	Name of the port.
Trap/Alarm	Icon indicates if a trap or alarm is present on port.
Number	The port number.
Status	Indication or operational status of a port: online or offline.
Admin State	If checked, the port is blocked. Click in the box to check and activate blocking.
Oper Speed	The percentage of the maximum throughput currently being transmitted.
Admin Speed	Choose from 1 Gbps, 2 Gbps, or 1G/2G Auto. After setting the speed at which you would like traffic to pass, click the Apply button at the upper left of the Enterprise Manager Client window to apply the setting. For 1 Gig blades, the speed will be automatically set at 1 Gbps and the option to set the speed will be disabled/grayed out.

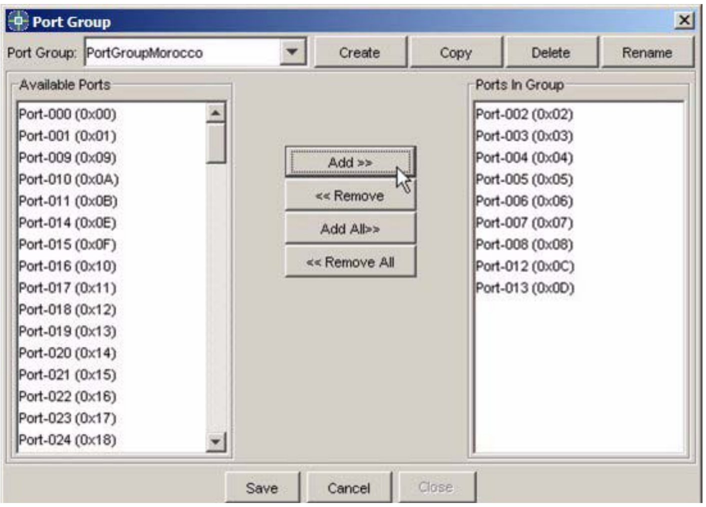
Table 13. Port Config tab field descriptions (Continued)

Capable Speed	
Port Type	If checked, monitor utilization feature is enabled. Click to toggle enabled and disabled aspect. This feature monitors throughput of a port in Megabytes per second.
SFP Type	Type of installed SFP.
WWN	World Wide Number of the port.
Board:Port	Board address and port address.

Configure port group

You can configure a port group at the Ports window.

1. Click the **Configure** button to the right of the **Port Group** drop down list. The **Port Group** window appears.



Port Group: PortGroupMorocco

Available Ports:
Port-000 (0x00)
Port-001 (0x01)
Port-009 (0x09)
Port-010 (0x0A)
Port-011 (0x0B)
Port-014 (0x0E)
Port-015 (0x0F)
Port-016 (0x10)
Port-017 (0x11)
Port-018 (0x12)
Port-019 (0x13)
Port-020 (0x14)
Port-021 (0x15)
Port-022 (0x16)
Port-023 (0x17)
Port-024 (0x18)

Ports In Group:
Port-002 (0x02)
Port-003 (0x03)
Port-004 (0x04)
Port-005 (0x05)
Port-006 (0x06)
Port-007 (0x07)
Port-008 (0x08)
Port-012 (0x0C)
Port-013 (0x0D)

Figure 49. Port Group

2. Click **Create** and type the name of the port group into the box. Click **OK**.
3. Highlight the ports you would like to add to the group, and click **Add>>**.
4. Click **Save** to save the port group and then **Close** to close the Port Group configure window.
5. The port group you created now appears in the port group drop down list at the Ports view window.

Ports view options

Highlighting a port and then right-clicking over a line at the **Ports** tab displays a pop-up menu providing several options.

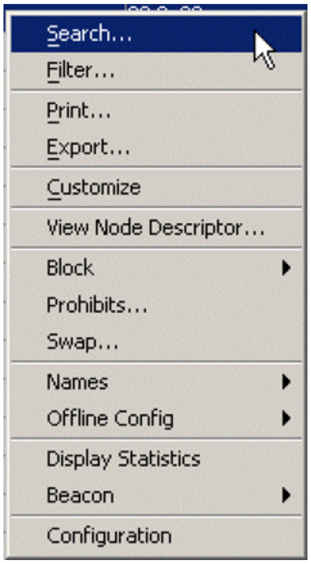


Figure 50. Port Config right-click menu

Search
A user configurable function which allows you to search the ports window table.

1. Right-click anywhere on the **Port Config** window. The menu shown in Figure 50. appears.
2. Click the **Search** function from this menu. The Search Ports window appears.
3. Search by entire list or a selected column. Choose the column from the drop down list.
4. Type your search criterian, select that attributes of the search, and then click the **Search Next** button.
5. If your search criteria ia found, the port will be highlighted.

Filter ports
The filter ports option allows you to view ports based on parameters you choose. For instance, choose the Blocked filter and have all blocked ports move to the top of the ports view list.

Filtering ports

1. Select a director under the **director** heading of the fabric tree whose ports you would like to filter and then click on the **Ports** tab. Right-click over the ports and select **Filter...**

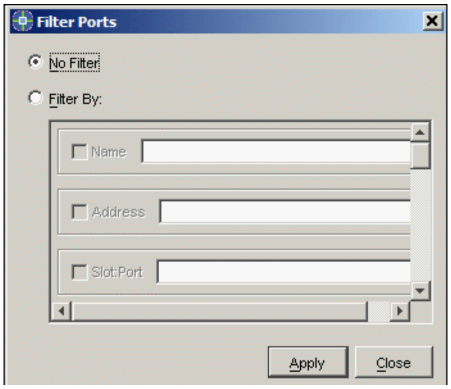


Figure 51. Filter Ports window

2. Choose the attribute via which you wish to filter the way the ports are presented in the ports view window by clicking in the check box to the left of that attribute.

   Note: The attributes via which you filter ports are the same ones you see on the ports view window and are presented in the same order.

3. You may also type in additional parameters in the box located to the right of the attribute. For example, if you choose the **Port Name** attribute by clicking in the check box and then type Port-01 into the box, you can view ports that only have Port-01 in their name.
4. Click **Apply** to activate the filtering. Note that you will only see ports which comply with the filter.

Print ports

Select to print a graphic representation of the ports view window.

Export

Export the port list in a .txt or .csv file format for viewing.

Customize

Allows you to customize the look of the Ports View list. Move columns. Determine which columns are visible and which are hidden. Determine which columns are frozen for viewing.

View Node descriptor

View the node descriptor information for a particular port.

Port prohibits and blocks (E_Port mode only)

Guidelines for zoning and port prohibits while employing intermix mode

When running FICON and Open Systems simultaneously (Intermix Mode), there are some guidelines or best practices which should be followed.

Zoning guidelines:

- Enterprise Manager will restrict zone type to WWN only with a CS1.1.0. fabric that has ISLs to a FC9000 director running CS4.1.3 or below.
- Zone types include Type 1 and 3 zoning with CS1.1.0 or above.
  - Previous zoning type:
- Type 1 - WWN, Type 2 and Type 3
  - Zoning types subtracted:
- Type 2 - Domain and Port Id
- Enable Domain locking when using Type 3 zoning.
- Zoning should be used for controlling connectivity among FCP N/NL-ports (“soft”, i.e. enforced at the Name Server level).
- Prohibits may be used for FCP N/NL-ports, however some FCP devices/HBAs have been found to have limitations with handling a prohibit RSCN containing multiple entries. When enabling or disabling prohibits, an RSCN will be sent to all affected prohibited port(s) even if a port is in a different a zone.
- Ports defined for FCP traffic can be placed within a maximum of 256 unique zones totaling 3600 members.

Prohibit/Allows guidelines:

- Prohibits/Allows should be used for controlling connectivity among FICON N-ports (“hard”, i.e. enforced at a traffic frame level)
- FICON ports should be placed within a single zone; this provides nameserver separation of FICON ports from FCP ports, and ensures that FICON ports receive a RSCN for FICON port state changes.
- Port prohibits/allows should be limited to the ports defined in the FICON zone, and not used for ports in a FCP zone.
- Additional traffic separation of FICON ports, independently of zoning, is accomplished by prohibiting all FICON ports to all FCP ports. This may be performed via the Enterprise Manager by setting prohibits on columns corresponding to FICON ports. Then the intersection with FICON ports rows may be modified (Set) to allow FICON to FICON connectivity. See the information which follows on how to set port prohibits and blocks.
- Prohibits shall not to be used for ISLs port connections.
- Prohibits/allows may be applied also from the System Automation console via z/OS and CUP. Care should be taken to apply them to FICON ports only.

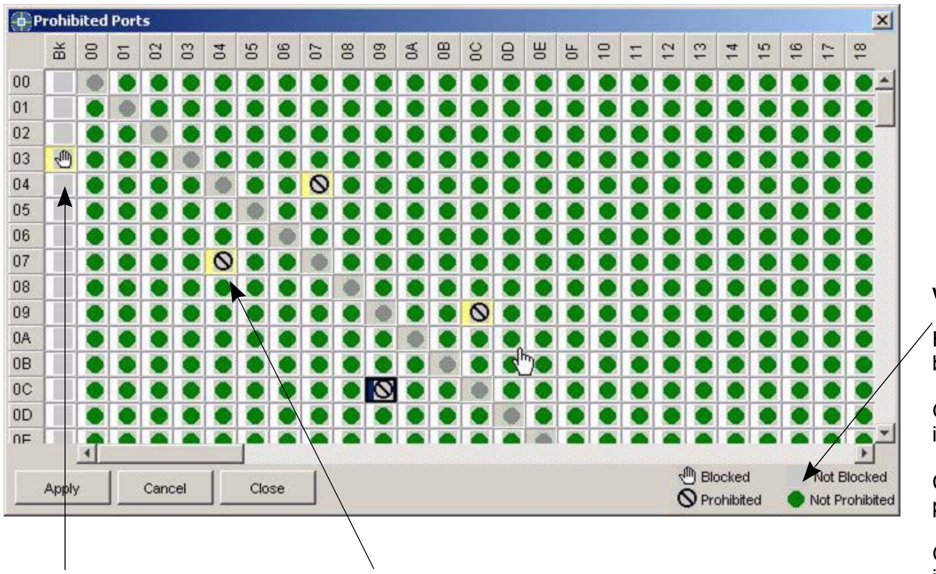
Employing port prohibits and blocks

Note: Port prohibits are only honored by FICON ports and should not be applied to open system ports.

Operators may prohibit ports from connecting to specified port(s) using the Prohibited Ports window. All ports may be blocked or unblocked using the right-click menu pick, or by right-clicking over the Prohibit Ports window. You may also block individual ports using the Port Config window.

To view the Prohibit Ports window, right-click on the Ports tab window and select **Prohibits** from the pop-up menu.

The Prohibited Ports window appears.



window Key:

Hand in left column indicates blocked port state.

Grey box in far left column indicates unblocked state.

Circle with line indicates prohibited state.

Green circle in matrix indicates unprohibited state.

Hand indicates blocked state for port.

Yellow around area indicates change in status. After Apply button is used, yellow goes away.

Figure 52. Prohibited ports window

Right-clicking anywhere on the Prohibited Ports window displays a pop-up menu providing several options.

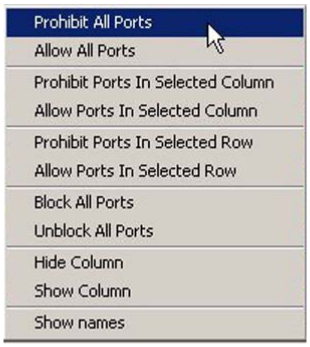

Prohibit All Ports
Allow All Ports
Prohibit Ports In Selected Column
Allow Ports In Selected Column
Prohibit Ports In Selected Row
Allow Ports In Selected Row
Block All Ports
Unblock All Ports
Hide Column
Show Column
Show names

Figure 53. Prohibited ports right-click menu

Prohibiting port connections

1. To prohibit one port from connecting with another, select the box which intersects the two ports. A circle with a line through it with a yellow background appears, indicating that a Prohibit state is pending.
2. Click all ports that you would like to prohibit.
3. Click **Apply**. The yellow goes away to indicate that the change has been completed.

Rescinding port prohibits

1. From the Prohibited Ports window, de-select the boxes of the ports which you would like to be available to each other. The lined circle is removed.
2. Click **Apply** to remove the yellow status indication and free up the port.

Prohibiting all ports

1. Right-click anywhere on the Prohibited Ports window. A pop-up menu appears.
2. Select the **Prohibit all ports** menu option. All ports are now in a Prohibit pending state.
3. Click **Apply** to complete the process.

Allowing all ports

1. Right-click anywhere on the Prohibited Ports window. A pop-up menu appears.
2. Select the **Allow all ports** menu option. All boxes are now in a pending unprohibited state.
3. Click **Apply** to complete the process.

Prohibiting ports in a selected column

1. From the Prohibited Ports window, right-click over the header of the column in which you would like to prohibit all ports. A pop-up menu appears.
2. Select the **Prohibit ports in selected column** menu option. All boxes in the selected column are now in a prohibited pending state.
3. Click **Apply** to complete the process.

Allowing ports in a selected column

1. From the Prohibited Ports window, right-click over the header of the column in which you would like to allow all ports. A pop-up menu appears.
2. Select the **Allow ports in selected column** menu option. All boxes in the selected column are now in a pending state of being unprohibited.
3. Click **Apply** to complete the process.

Prohibiting ports in a selected row

1. From the Prohibited Ports window, right-click over the header of the row in which you would like to prohibit all ports. A pop-up menu appears.
2. Select the **Prohibit ports in selected row** menu option. All boxes in the selected row are now in a prohibit pending state.
3. Click **Apply** to complete the process.

Allowing ports in a selected row

1. From the Prohibited Ports window, right-click over the header of the row in which you would like to allow all ports. A pop-up menu appears.
2. Select the **Allow ports in selected row** option. All boxes in the selected row are now in a pending unprohibited state.
3. Click **Apply** to complete the process.

Blocking individual ports

1. From the Prohibited Ports window, select the boxes in the far left column adjacent to the ports you would like to block. A hand outlined in yellow appears, indicating a pending block state for the ports.
2. Click **Apply** to complete the process.

Unblocking individual ports

1. From the Prohibited Ports window, select the boxes in the far left column adjacent to the ports you would like to unblock. The hand disappears and a grey block outlined in yellow appears, indicating a pending unblocked state for the ports.
2. Click **Apply** to complete the process.

Port swap

Note: Port prohibits are only honored by FICON ports and should not be applied to open system ports.

This feature gives an Administrator level and above operator the ability to swap a failing FICON attached port with a port that is operational.

1. From the SAN option, highlight the subswitch which contains the ports you wish to swap, and then select the **Ports** tab.
2. Right-click anywhere on the Ports window. A pop-up menu appears.
3. Select the **Swap** menu option.
4. Select the failing port from the **Failing Port** drop-down list.
5. Select the operational port you want to swap from the **Spare Port** list.
6. Click **OK** on the dialog.
7. Click **OK** at the confirmation windows.
8. Click the **Apply** button on the Toolbar of the Port Config window to complete the process.

Names

You can clear port names or revert the names to their default value with this option.

Clear names

Administrator level and above operators clear port names via this command.

1. From the SAN option, highlight the subswitch on which the ports you wish to clear names resides and then select the **Ports** tab.
2. Right-click anywhere on the Ports window. A pop-up menu appears.
3. Select the **Names** menu option and then choose the **Clear Names** command.
4. Click **Yes** at the confirmation windows to confirm that you want the names cleared.
5. Click the **Apply** button on the Toolbar of the Port Config window to complete the process.

Default names

Administrator level and above operators restore port names to their default state via this command.

1. From the SAN option, highlight the subswitch on which the ports you wish to restore default names resides and then select the **Ports** tab.
2. Right-click anywhere on the Ports window. A pop-up menu appears.
3. Select the **Names** menu option and then select the **Default Names** command.

4. Click **Yes** at the confirmation windows.
5. Click the **Apply** button on the Toolbar of the Port Config window to complete the process.

Offline config

Save or retrieve a port configuration using this option.

Save config

This feature gives an Administrator level and above operator the ability to save an existing port configuration.

1. From the SAN option, highlight the subswitch on which the ports you wish to save the configuration resides and then select the **Ports** tab.
2. Right-click anywhere on the Ports window. A pop-up menu appears.
3. Select the **Offline Config** option.
4. Drag the mouse to **Save** and click. The **Save Config** window appears.
5. Select a filename from the drop-down list.
6. Click **Save**.

Retrieve port configuration

This feature allows you to retrieve a port configuration.

1. From the SAN option, highlight the subswitch on which the ports you wish to Retrieve a Configuration for resides and then select the **Ports** tab.
2. Right-click anywhere on the Ports window. A pop-up menu appears.
3. Select the **Offline Config** menu option and drag the mouse pointer to **Retrieve** and click. The following dialog appears.
4. Select a configuration file from the **Select a File** drop-down list from which you would like to retrieve the attributes available at the window.
5. By default, all available parameters are checked. If you don’t want to retrieve one, simply un-check the box.
6. Select the attribute(s) you would like to retrieve and then click **Retrieve**.
7. Click the **Apply** button on the Toolbar to complete the process.

Display statistics

This option allows you to view port statistics in a graph format. There, you may track trends over time. Drag the mouse over an area of the graph to zoom in on the area when you want to see greater detail.

Beacon

The beacon feature lets you set the port LED to continuously flash. This is helpful when you want to find a particular port on a board and are not sure where it physically resides. Simply start the beacon by right-clicking over the board you want to beacon, drag the mouse pointer down to the Beacon command and then choosing Start Beacon from the drop down list. Go to the director and board on which the port resides and then find the port by looking for the blinking light. To shut the beacon off, perform the above mentioned procedure and select Stop Beacon from the drop down list.

Clear trap/alarm

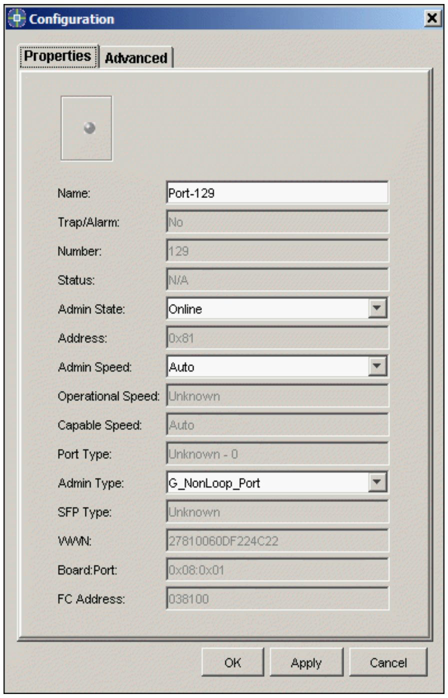
This feature gives an Operator level and above user the ability to clear traps and alarms. For information on clearing port failure indicators and traps at the board and Director level, refer to the “Port failure indications” section in Chapter 4..

1. From the SAN option, highlight the subswitch on which the ports you wish to Clear Traps/Alarms reside and then select the **Ports** tab.
2. Right-click anywhere on the Ports window. A pop-up menu appears.
3. Select the port for which you would like to clear a port or alarm by clicking on it.
4. Right-click over the port you selected. A pop-up menu appears.
5. Select the **Clear Trap/Alarm** menu option.
6. A dialog appears with the following options:
   - – traffic trap
   - – util trap

   Choose one or both by clicking in the checkboxes.
7. Click **OK** to clear the trap(s) you chose to clear.

Configuration

At the Configuration window you can view information about the port on which you right-clicked Simply right-click over a port and then select the **Configuration** option at the bottom of the menu.



Name: Port-129
Trap/Alarm: No
Number: 129
Status: N/A
Admin State: Online
Address: 0x81
Admin Speed: Auto
Operational Speed: Unknown
Capable Speed: Auto
Port Type: Unknown - 0
Admin Type: G_NonLoop_Port
SFP Type: Unknown
WWN: 27810060DF224C22
Board:Port: 0x08:0x01
FC Address: 038100

Figure 54. Configuration window

Configuration Properties tab

The Properties tab is the default view. At this view you see the following details:

Table 14. SAN256N director Port Config Properties details

Statistic	Description
Name	Port name.
Trap/Alarm	Is there a trap or alarm currently associated with the port. Yes or no.
Number	Port number.
Status	Current status of the port: Online or Offline.
Admin State	Current Admin State of the Port: Online or Offline.
Address	Hex address of the port.
Admin Speed	Choose from 1 Gbps, 2 Gbps, or 1G/2G Auto. After setting the speed at which you would like traffic to pass, click the Apply button at the upper left of the Enterprise Manager Software client window to apply the setting. For 1 Gig blades, the speed will be automatically set at 1 Gbps and the option to set the speed will be disabled/grayed out.
Operational Speed	Current Operational speed of the port: 1 Gbps, 2Gbps or Auto.
Capable Speed	Highest speed at which port may function.
Port Type	Current Port type.
Admin Type	Current Admin type of the board: Normal or TL. Typically, the port is set at Normal. To set up a port as a TL_Port, please review appendix D of this manual.
SFP Type	Information about the SFP for this port.
WWN	WWN of the Port.
Board:Port	Current Board and Port address information.
FC Address	FC address of the port
Auto Sense Arbitrated Loop	Whether Auto Sense Arbitrated Loop is enabled or disabled.

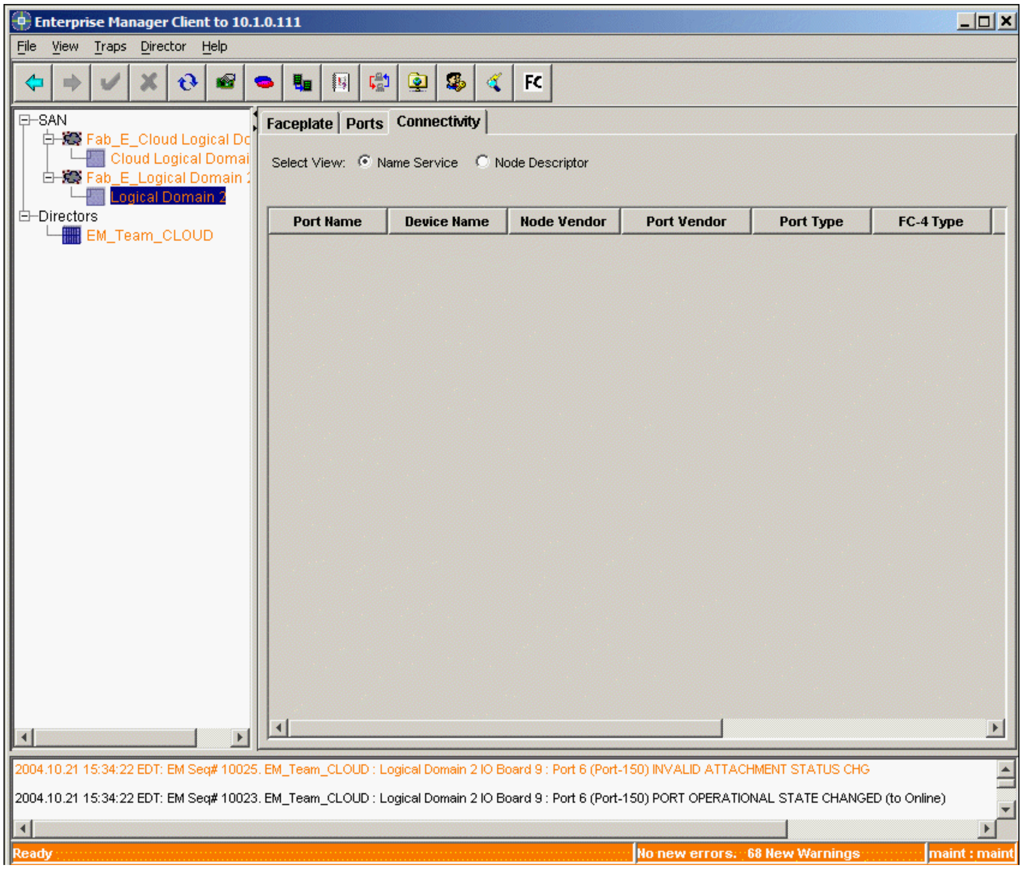
Configuration window Advanced tab

View all devices attached to a port with this option.

1. Right-click anywhere on the Port Config window, and select the **Configuration** function from the pop-up menu that appears.
2. Click the Advanced tab to see the Device List information.
3. When you are finished viewing the list, click **OK**.

Connectivity tab

The **Connectivity** tab default view shows Name Service information about the selected Director.



```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Figure 55. SAN view - Connectivity tab

Name Service details

The following fields are displayed when the **Name Service** tab is selected.

Table 15. Name Service tab field descriptions

Field	Description
Port Name	Name of the port for which you are viewing information.
Device Name	Nickname of the device, if entered.
Node Vendor	Vendor name of the piece of equipment connected to the port. Private devices are not listed.
Port Vendor	Vendor name of the device port via which the equipment is connected.
Port Type	Type of port for which you are viewing information.
FC-4 Type	Device fibre channel protocol types.
Address	Switch position of the fibre channel address.

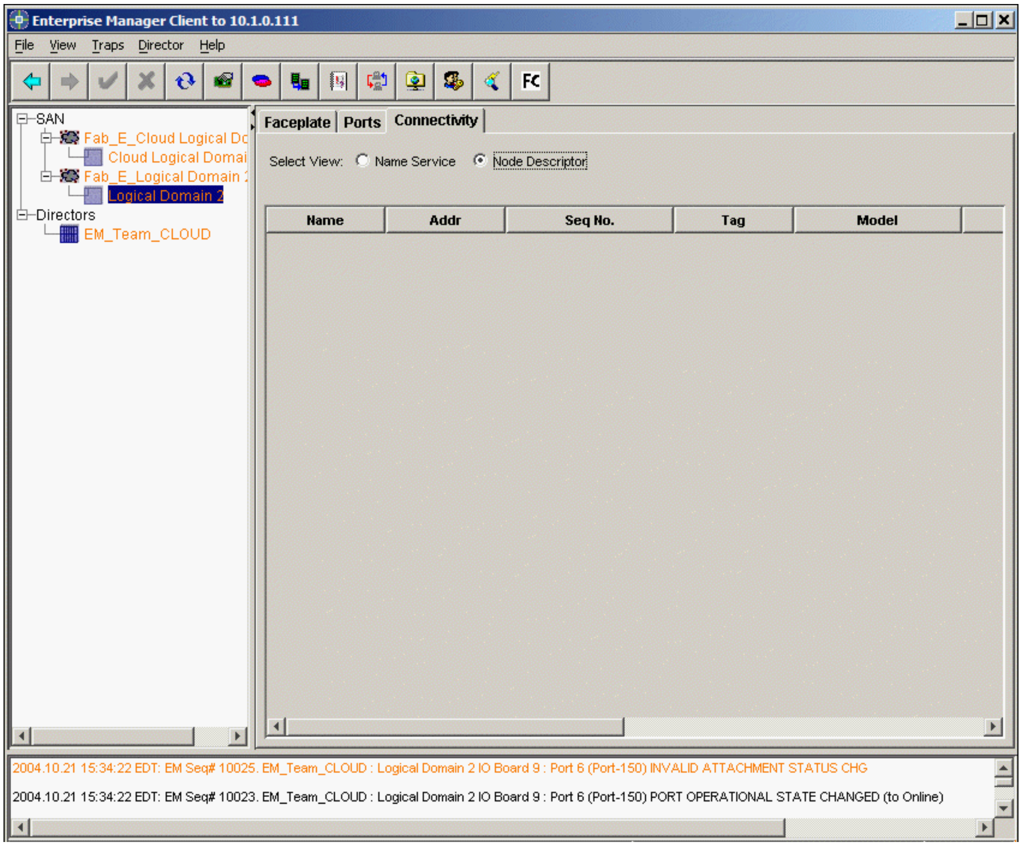
Table 15. Name Service tab field descriptions (Continued)

Port WWN	World Wide Name of the device port via which the equipment is connected.
Node WWN	World Wide Name (WWN) of the piece of equipment connected to the port.

Connectivity tab - Node Descriptor information

Selecting the Node Descriptor radio button at the Connectivity Tab window will show you node descriptor information for the ports of the logical domain you chose. The **Node Descriptor** displays details presented by the device logged into the port. Node descriptors typically pertain to FICON attached ports but may display useful data for non-FICON attachments.

Note: Blue text indicates a current node descriptor, while black text indicates a node descriptor which is not current. Node Descriptors, which are considered not current, are those devices which are no longer attached to a port



```
2004.10.21 15:34:22 EDT: EM Seq# 10025. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) INVALID ATTACHMENT STATUS CHG
2004.10.21 15:34:22 EDT: EM Seq# 10023. EM_Team_CLOUD : Logical Domain 2 IO Board 9 : Port 6 (Port-150) PORT OPERATIONAL STATE CHANGED (to Online)
```

Figure 56. Connectivity tab, Node Descriptors view

Trace

The Trace functionality in the Enterprise Manager Software allows the user to set triggers and filters which then may be used as guidelines to capture information flowing through the SAN256N director. This information is important in troubleshooting link problems, as information surrounding the triggers can be captured which will allow engineering and field support to determine what may have led to the trigger condition being met. Three categories of traces may be performed: hardware, firmware, and firmware startup.

For the hardware trace, trigger control combinations are “and”, “or” and “the ”with the ability to specify different directions for the trigger. For firmware, only the trigger control combinations of “and” and “or” are available. Direction is required to be the same for the “and” combination to work correctly.

Although similar in some respects to the hardware trace, the firmware trace is different in some ways. While the hardware trace records all frames once the settings in the trigger have been met, only frames meeting the given trigger condition defined by the filter are stored.

The Firmware Startup trace depends on the base firmware capturing current and historical FCP state register change information along with other firmware state trace information which is recorded via the internal firmware.

The recommended software to view the Trace Buffer file is Finisar xgigaViewer. This software is available via download at: www.finisar.com After you get to the Finisar home page, type **`xgigaviewer`** into the search box and click on **Search**. Follow the instructions to download the software onto the PC. Note that the software is an evaluation copy and should be purchased once the evaluation period ends.

Allows you to set two triggers at a time for a SAN256N director. The trace config may then be exported. Trace configs may also be imported. You have the option to use the defined triggers, or define new ones.

Preconfigured trigger combinations

When configuring a trace, you may use the set up your own trigger configuration or use the preconfigured trigger combinations. The preconfigured combinations are described in the table below:

Table 16. Trace preset options

Trigger Combination	**Description**
LS_RJT - Link Service Reject	The Link Service Reject (LS_RJT) notifies the transmitter of a Link Service request that the Link Service request Sequence has been rejected. This typically forces the link to be reset.
LS_ACC - Link Service Accept	The Link Service Accept (LS_ACC) ELS reply Sequence shall notify the transmitter of an ELS request that the ELS request Sequence has been completed.
PLOGI - N_Port Login	The PLOGI frame provides the means by which an Nx_Port may request Login with another Nx_Port prior to other Data frame transfers.
FLOGI - F_Port Login	The FLOGI frame provides the means by which an Nx_Port may request Login with the Fabric.
LOGO - Logout	The LOGO ELS, when sent to an N_Port, shall request invalidation of the Service Parameters and N_Port_Name that have been saved by an Nx_Port, freeing those resources.

Table 16. Trace preset options (Continued)

Trigger Combination	Description
ABTX - Abort Exchange	The ABTX ELS is used to request abnormal termination of an open Exchange.
RCS - Read Connection Status	The RCS ELS is a request to the Fabric Controller to return the current dedicated connection status for the Nx_Port_specified in the Payload of the RCS frame.
RES - Read Exchange Status Block	The RES ELS Request Sequence requests an Nx_Port to return the Exchange Status Block for the RX_ID or OX_ID originated by the S_ID specified in the Payload of this Request Sequence.
RSS - Read Sequence Status Block	The RSS ELS is a request to an Nx_Port to return the Sequence Status Block for the SEQ_ID specified in the Payload.
RSI - Request Sequence Initiative	The RSI ELS is used to request that Sequence Initiative be passed to the Sequence Recipient of an Exchange in progress.
ESTS - Establish Streaming	The ESTS ELS requests a temporary allocation of Credit known as Streaming Credit large enough to perform continuous streaming of Data frames.
ESTC - Estimate Credit	The ESTC ELS is used to estimate the minimum Credit required to achieve the maximum bandwidth for a given distance between an Nx_Port pair.
ADVC - Advise Credit	The ADVC ELS shall be used to advise the destination Nx_Port of the estimated end-to-end Credit that the source Nx_Port requests to be allocated.
RTV - Read Timeout Value	The RTV ELS is a request to an FC_Port to return the R_A_TOV and the E_D_TOV in the LS_ACC.
RLS - Read Link Error Status Block	The RLS ELS is a request to an FC_Port to return the Link Error Status Block associated with the Port_ID specified in the Payload.
ECHO	The Echo ELS is a single frame requesting the Recipient to transmit the Payload contents, following the LS_Command, back to the Initiator of the Echo command.
TEST	The TEST ELS is a single Sequence being transmitted from the Sequence Initiator to the Sequence Recipient.
RRQ - Reinstate Recovery Qualifier	The RRQ ELS is used to notify the destination Nx_Port that the Recovery_Qualifier shall be available for reuse.
REC - Read Exchange Concise	The REC (Read Exchange Concise) Extended Link Service requests an Nx_Port to return Exchange information for the RX_ID and OX_ID originated by the S_ID specified in the Payload of the request Sequence.
PRLI - Process Login	The PRLI ELS is used to establish the operating environment between a group of related processes at the originating Nx_Port and a group of related processes at the responding Nx_Port.

Table 16. Trace preset options (Continued)

Trigger Combination	**Description**
PRLO - Process Logout	The PRLO ELS is used to request invalidation of the operating environment between an image at the initiating Nx_Port and an image at the recipient Nx_Port.
SCN - State Change Notification	Obsolete.
TPLS - Test Process Login State	The TPLS ELS is used to determine whether image pairs are established for the image pairs specified by the combination of the S_ID || Originator Process_Associator || D_ID || Responder Process_Associator.
TPRLO - Third Party Process Logout	The TPRLO ELS is used to invalidate the operating environments between the specified image(s) at the recipient Nx_Port and the specified image(s) in the specified Nx_Port(s) that have performed Process Login with the recipient Nx_Port for the specified TY
LCLM- Login Control List Management	The LCLM ELS supports the management of a Login Control List (LCL) for Login Control.
GAID - Get Alias_ID	The GAID ELS is sent to the Fabric Controller by the Alias Server to request a unique Alias_ID to be associated with the Alias Group indicated in the passed Alias_Token.
FACT - Fabric Activate Alias_ID	The FACT ELS is sent to the Fabric Controller by the Alias Server to cause it to assign the passed Alias_ID as an Alias_ID for the passed Nx_Ports.
FDACT - Fabric Deactivate Alias_ID	The FDACT ELS is sent to the Fabric Controller by the Alias Server to request that it de-assign the indicated Alias_ID as an Alias Group identifier for the passed Nx_Ports.
NACT - N_Port Activate Alias_ID	The NACT ELS is sent to an Nx_Port by Alias Server to cause it to assign the passed Alias_ID as an Alias_ID.
NDACT - N_Port Deactivate Alias_ID	The NDACT ELS is sent to an Nx_Port by Alias Server to cause it to deactivate the passed Alias_ID as an Alias_ID.
QoSR - Quality of Service Request	The QoSR ELS is a request to setup of a Class 4 circuit and that the requested level of service be granted by the Quality of Service Facilitator (QoSF) for this Class 4 circuit.
RVCS - Read Virtual Circuit Status	The RVCS ELS is a request to the Virtual Circuit Status in the QoS Facilitator.
PDISC - Discover N_Port Service Parameters	The PDISC ELS is a transfer of Service Parameters from the initiating Nx_Port to the Nx_Port associated with the D_ID without affecting the operating environment between the two ports.
FDISC - Discover F_Port Service Parameters	The FDISC ELS is a transfer of Service Parameters from the initiating Nx_Port to the Fx_Port at well-known F_Port_ID (i.e., hex 'FF FF FE').
ADISC - Discover Address	The ADISC ELS is an exchange of addresses and identifiers of communicating Nx_Ports.

Table 16. Trace preset options (Continued)

Trigger Combination	Description
RNC - Report Node Capability	Obsolete
FARP_REQ - Fibre Channel Address Resolution Protocol Request	The FARP_REQ ELS is used to resolve Port_IDs of communicating Fibre Channel devices.
FARP_REPL - Fibre Channel Address Resolution Protocol Reply	A FARP_REPLY ELS communicates the information solicited by a previously received FARP_REQ ELS.
RPS - Read Port Status Block	The RPS ELS is a request to an FC_Port to return port status associated with the port specified in the Payload of this frame.
RPL - Read Port List	The RPL ELS provides internal node port identification information.
RPBC - Report Port Buffer Condition	The RPBC ELS provides a method for a Port to report its buffer conditions.
FAN - Fabric Address Notification	The FAN ELS is sent by an FL_Port (hex 'FF FF FE') to all known previously logged in (via FLOGI) attached NL_Ports following an initialization event.
RSCN - Registered State Change Notification	A RSCN ELS is sent to registered Nx_Ports when an event occurs that may have affected the state of one or more Nx_Ports, or the ULP state within the Nx_Port.
SCR - State Change Registration	The SCR ELS is a request the Fabric Controller or Nx_Port to add the Nx_Port that is sending the SCR Request to the list of Nx_Ports registered to receive the RSCN ELS.
RNFT - Report Node FC-4 Types	The RNFT ELS provides for the exchange of supported FC-4 protocol lists.
CSR - Clock Synchronization Request	The CSR ELS is used to request the Clock Synchronization Server to either send or to quit sending periodic Clock Synchronization Update (CSU) ELS frames or clock synchronization primitives, depending on the method implemented.
CSU - Clock Synchronization Update	The CSU ELS is used by the Clock Synchronization Server to send its current clock value to its clients.
LINIT - Loop Initialize	The LINIT ELS shall request the start of Loop Initialization on a designated loop.
LPC - Loop Port Control (Obsolete)	Obsolete
LSTS - Loop Status	The LSTS ELS is used to request the Fabric Controller to report on the state of the specified loop.
RNID - Request Node Identification Data	The RNID ELS is an ELS for acquiring Node Identification Data.
RLIR - Registered Link Incident Report	The RLIR ELS is a method for a reporting Nx_Port to send a Link Incident Record to a registered Nx_Port.

Table 16. Trace preset options (Continued)

Trigger Combination	**Description**
LIRR - Link Incident Record Registration	The LIRR ELS is a request to the recipient to add or remove this source Nx_Port to or from the list of Nx_Port's registered to receive the Registered Link Incident Report (RLIR) ELS.
SRL - Scan Remote Loop	The SRL ELS shall require a switch to scan attached loops to determine if any L_Ports have been disabled or removed.
SBRP - Set Bit-error Reporting Parameters	Set SBRP ELS is used to communicate a set of bit error reporting parameters to a Port or to all Ports in a particular Domain in a Fabric.
RPSC - Report Port Speed Capabilities	The RPSC ELS is a method for a Port to report its current and potential link operating speeds.
#Basic Link Services NOP - No Operation	The No Operation (NOP) Basic Link Service frame is used with delimiters appropriate to the class in which it is being used.
ABTS - Abort Sequence	The ABTS frame shall be used by the Sequence Initiator to request that the Sequence Recipient abort one or more Sequences or Sequence Recipient to request that the ABTS Recipient abort the entire Exchange.
BA_ACC - Basic Accept	BA_ACC is a single frame Link Service Reply Sequence that notifies the transmitter of a Basic Link Service Request frame that the request has been completed.
BA_RJT - Basic Reject	BA_RJT is a single frame Link Service Reply Sequence that notifies the transmitter of a Basic Link Service Request frame that the request has been rejected.
Any / All Frames	
D_ID or S_ID is CUP Address (FE)	Trigger on any frame with a D_ID or S_ID equal to 0xFFFFFE.
D_ID or S_ID is Management Server (FA)	Trigger on any frame with a D_ID or S_ID equal to 0xFFFFFA.
D_ID or S_ID is Directory Server (FC)	Trigger on any frame with a D_ID or S_ID equal to 0xFFFFFC.
D_ID or S_ID is Fabric Controller (FD)	Trigger on any frame with a D_ID or S_ID equal to 0xFFFFFD.
Any Well-Known Address	Trigger on any frame destined for a Well-Known Address.
Any ELS Request or Reply	Trigger on any frame with a R_CTL of 0x02 which identifies the frame as an Extended Link Service.
Exchange Link Parameters (ELP)	The Exchange Link Parameters Switch Fabric Internal Link Service requests the exchange of Link Parameters between two Interconnect_Ports connected via an ISL.
Switch Fabric Internal Link Service Reject (SW_RJT)	The Switch Fabric Internal Link Service Reject shall notifies the transmitter of an SW_ILS request that the SW_ILS request Sequence has been rejected.

Table 16. Trace preset options (Continued)

Trigger Combination	Description
Switch Fabric Internal Link Service Accept (SW_ACC)	The Switch Fabric Internal Link Service Accept reply Sequence notifies the transmitter of an SW_ILS request that the SW_ILS request Sequence has been completed.
Exchange Fabric Parameters (EFP)	The Exchange Fabric Parameters Switch Fabric Internal Link Service requests the exchange of Fabric Parameters between two E_Ports connected via an ISL.
Domain Identifier Assigned (DIA)	The Domain Identifier Assigned Switch Fabric Internal Link Service indicates that a Principal Switch has been selected, and that the upstream neighbor Switch has been assigned a Domain Identifier.
Request Domain_ID (RDI)	The Request Domain_ID Switch Fabric Internal Link Service is sent by a Switch to request a Domain_ID from the Domain Address Manager.
Hello (HLO)	The Hello Switch Fabric Internal Link Service is used to determine when two way communication is established with a neighbor Switch.
Link State Update (LSU)	The Link State Update Switch Fabric Internal Link Service requests the transfer of one or more Link State Records from one Switch to another Switch.
Link State Acknowledgement LSA	The Link State Acknowledgement Switch Fabric Internal Link Service is used to acknowledge the receipt of an LSR.
Build Fabric BF	The Build Fabric Switch Fabric Internal Link Service requests a non-disruptive reconfiguration of the entire Fabric.
Reconfigure Fabric RCF	The Reconfigure Fabric Switch Fabric Internal Link Service requests a disruptive reconfiguration of the entire Fabric.
Inter-Switch Registered State Change Notification SW_RSCN	The Fabric shall distribute RSCNs between Switches using the Inter-Switch RSCN payload.
Distribute Registered Link Incident Records DRLIR	Distribute Registered Link Incident Records (DRLIR) Switch Fabric Internal Link Service provides a method for a Fabric built RLIR to be distributed to every Switch in the Fabric.
Disconnect Class 1 Connection DSCN	The Disconnect Class 1 Connection Switch Fabric Internal Link Service requests that the receiving E_Port abort an existing Class 1 Connection.
Merge Request MR	The Merge request Switch Fabric Internal Link Service requests that the recipient merge any zoning data with the zoning data supplied in the MR payload.
23 00 xx xx Acquire Change Authorization ACA	Acquire Change Authorization requests are SW_ILSs addressed from the Domain Controller of the Managing Switch to the Domain Controller of a Managed Switch.
Release Change Authorization RCA	Release Change Authorization requests are SW_ILSs addressed from the Domain Controller of the Managing Switch to the Domain Controller of a Managed Switch.

Table 16. Trace preset options (Continued)

Trigger Combination	Description
Stage Fabric Configuration SFC	Stage Fabric Configuration Update requests are SW_ILSs addressed from the Domain Controller of the Managing Switch to the Domain Controller of a Managed Switch.
Update Fabric Configuration UFC	Update Fabric Configuration requests are SW_ILSs addressed from the Domain Controller of the Managing Switch to the Domain Controller of a Managed Switch.
Exchange Switch Capabilities ESC	The Exchange Switch Capabilities SW_ILS defines a mechanism for two Switches to exchange vendor and protocol information.
Exchange Switch Support ESS	The Exchange Switch Support (ESS) SW_ILS defines a mechanism for two switches to exchange vendor and support information relative to various supported features within the Fabric services and switch link services payloads.
Merge Request Resource Allocation MRRA	The Merge Request Resource Allocation (MRRA) SW_ILS defines a mechanism for switches to request resources to be allocated for the transfer of a Merge Request SW_ILS. MRRA enables buffer management in the Fabric Controller.

Setting up a trace in a SAN256N director

1. From the Enterprise Manager Software toolbar, click the **Trace** button.
2. The T**race List** window appears. At this window you can view any of the available traces. You can also configure new traces, configure trigger combinations, and get the status of existing traces,.

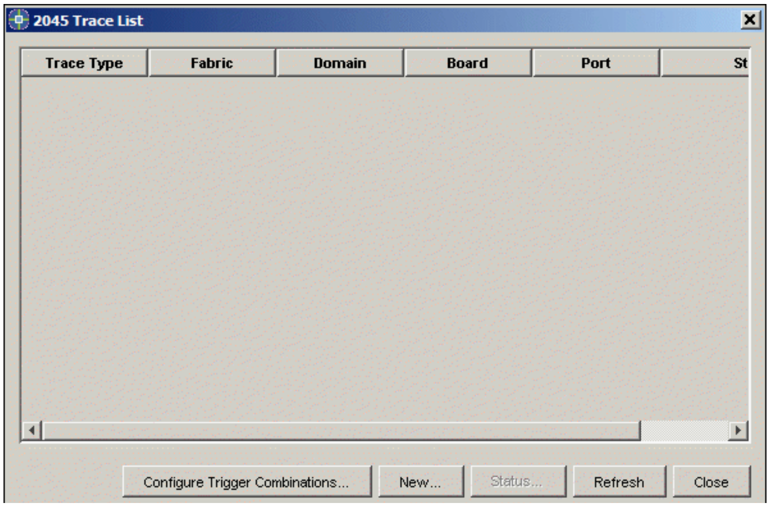
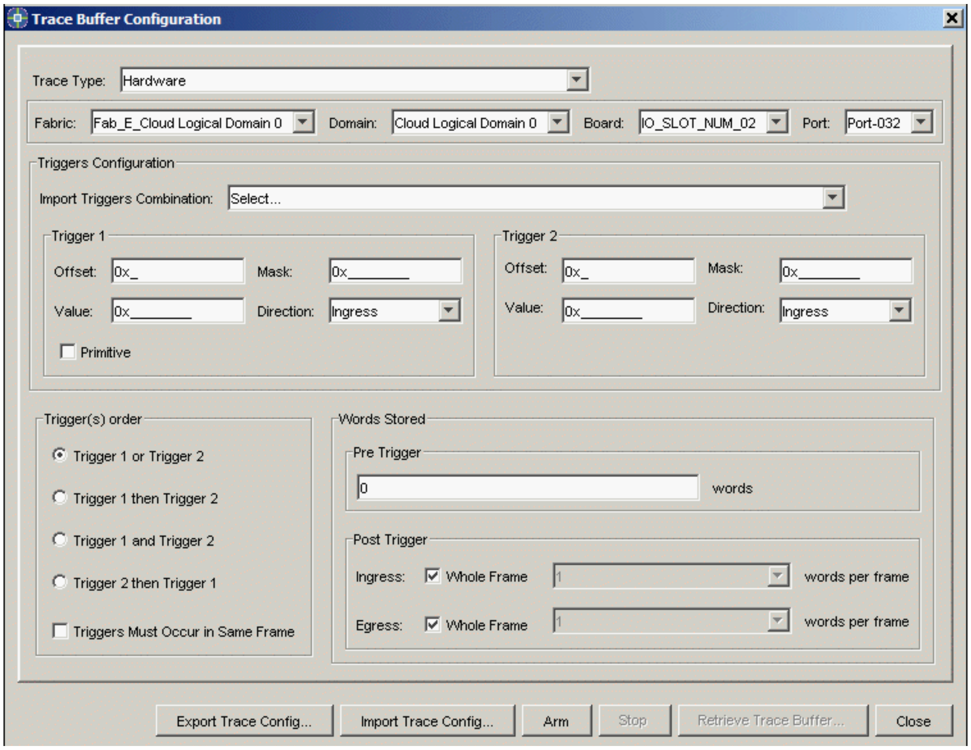


Figure 57. Trace List window

Configuring a new hardware trace

Note: **T**he port upon which the trace will be run should be set up as a mirror port. If you don’t do so prior to beginning this procedure, after you choose the port upon which the test will be run, the Enterprise Manager will set the port up as a mirror port for you. If a port already is in a mirror state and you choose a different port upon which to run the trace, you will receive an error message from the Enterprise Manager that another port is already set up as a mirror port. You will then have to remove that port from the mirror state and then begin the trace procedure again.

1. A new hardware trace may be configured by clicking the **New...** button on the **SAN256N director Trace List** window. At the drop down list at the top of the window, hardware is the default selection.



Trace Buffer Configuration

Trace Type: Hardware

Fabric: Fab_E_Cloud Logical Domain 0 Domain: Cloud Logical Domain 0 Board: IO_SLOT_NUM_02 Port: Port-032

Triggers Configuration

Import Triggers Combination: Select...

Trigger 1

Offset: 0x_ Mask: 0x______

Value: 0x______ Direction: Ingress

□ Primitive

Trigger 2

Offset: 0x_ Mask: 0x______

Value: 0x______ Direction: Ingress

Trigger(s) order

● Trigger 1 or Trigger 2

○ Trigger 1 then Trigger 2

○ Trigger 1 and Trigger 2

○ Trigger 2 then Trigger 1

□ Triggers Must Occur in Same Frame

Words Stored

Pre Trigger

0 words

Post Trigger

Ingress: ☑ Whole Frame 1 words per frame

Egress: ☑ Whole Frame 1 words per frame

Figure 58. Trace Buffer Configuration window

2. Select a Fabric from the **Fabric** drop down list.
3. Select a Domain from the **Domain** drop down list.
4. Select a Board from the **Board** drop down list.
5. Select a port from the **Port** drop down list. Note that ports which are to have the Trace run on them should be set up as a mirror port.
6. From the **Import Triggers Combination:** drop down list, you can select a preconfigured trigger combination. For a list and descriptions of the preconfigured options, see table *Trace preset options* on page 6-100.
7. If you want to capture Primitives, check the box next to **Primitive** to enable their capture. Un-check the box to disable that feature.
8. If you choose to create a new combination, you may choose to populate any or all of the following options for each trigger: Offset, Mask, Value, Direction.
9. You may then select the Trigger(s) order by clicking the radio button of your selection.

10. At the **Triggers Must Occur in Same Frame** option, click on the box to activate or deactivate that option. If the option is enabled, only words within a frame in which the trigger was met are captured. If the option is disabled, words in previous or subsequent frames other than the frame in which the trigger was met may be captured.

11. At the **Words Stored** Per Trigger option, you can type in at the Pre Trigger option how many words are captured.

12. At the **Post Trigger** area, choose **Whole Frame** by checking the box, if you want the entire frame captured or, if you don't want the entire frame captured at Ingress or Egress, select the amount of **words stored** from a frame from the drop down list. Note that the Whole Frame check box must be un-checked for you to enter a value.

13. Click **Arm** to begin the trace.

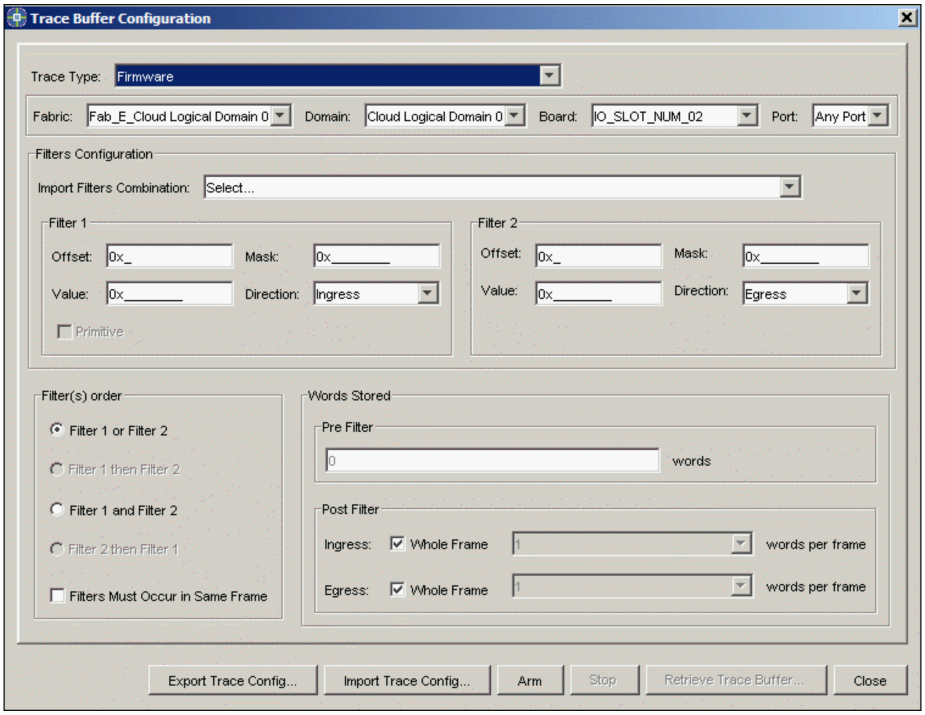
14. Clicking the **Stop** button stops gathering trace buffer information if a trigger has been met. If a trigger has NOT been met, clicking **Stop** ends the trace.

15. Click Retrieve **Trace Buffer...** and save the files to disk. Note that the Enterprise Manager automatically converts the files into a format that is readable via Finisar software.

Configuring a new firmware trace

The firmware version of the trace functionality is performed at the firmware level. Only frames sent to the board processor are scanned. Also, when a trigger is met, only the filter condition is saved. You may also set the filters through the CUP or domain controller boards and all of the boards associated with them are checked. Unlike the hardware trace, no port mirroring is necessary.

1. A new firmware trace may be configured by clicking on the **Trace** button at the toolbar, and then clicking the **New...** button on the SAN256N director Trace List window. At the drop down list at the top of the window, select **Firmware**.



Trace Buffer Configuration

Trace Type: Firmware

Fabric: Fab_E_Cloud Logical Domain 0 Domain: Cloud Logical Domain 0 Board: IO_SLOT_NUM_02 Port: Any Port

Filters Configuration

Import Filters Combination: Select...

Filter 1

Offset: 0x_ Mask: 0x_______

Value: 0x_______ Direction: Ingress

□ Primitive

Filter 2

Offset: 0x_ Mask: 0x_______

Value: 0x_______ Direction: Egress

Filter(s) order

● Filter 1 or Filter 2

○ Filter 1 then Filter 2

○ Filter 1 and Filter 2

○ Filter 2 then Filter 1

□ Filters Must Occur in Same Frame

Words Stored

Pre Filter

0 words

Post Filter

Ingress: ☑ Whole Frame 1 words per frame

Egress: ☑ Whole Frame 1 words per frame

Figure 59. Trace Buffer Configuration window

2. Select a Fabric from the **Fabric** drop down list.
3. Select a Domain from the **Domain** drop down list.
4. Select a Board from the **Board** drop down list.
5. From the **Import Triggers Combination:** drop down list, you can select a preconfigured trigger combination.
6. If you want to capture Primitives, check the box next to **Primitive** to enable their capture. Un-check the box to disable that feature.
7. If you choose to create a new combination, you may choose to populate any or all of the following options for each trigger:Offset, Mask, Value, Direction.
8. You may then select the Trigger(s) order by clicking the radio button of your selection.
9. At the **Triggers Must Occur in Same Frame** option, click on the box to activate or deactivate that option. If the option is enabled, only words within a frame in which the trigger was met are captured. If the option is disabled, words in previous or subsequent frames other than the frame in which the trigger was met may be captured.
10. At the **Words Stored Per Trigger** option, you can type in at the Pre Trigger option how many words are captured.
11. At the Post Trigger area, choose **Whole Frame** by checking the box, if you want the entire frame captured or, if you don't want the entire frame captured at Ingress or Egress, select the amount of **words stored** from a frame from the drop down list. Note that the Whole Frame check box must be un-checked for you to enter a value.
12. Click **Arm** to begin the trace.
13. Clicking the **Stop** button stops gathering trace buffer information if a trigger has been met. If a trigger has NOT been met, clicking **Stop** ends the trace.
14. Click Retrieve **Trace Buffer...** and save the files to disk. Note that the Enterprise Manager automatically converts the files into a format that is readable via Finisar software.

Configuring a new firmware Startup trace

The firmware startup version of the trace functionality is performed at the firmware level. When boards are brought online, they begin storing information. The Firmware Startup trace captures that information and allows you to pull it into a format which can then be read via Finisar software.

1. A new firmware startup trace may be configured by clicking the **Trace** button at the toolbar, and then clicking on the **New...** button on the SAN256N director Trace List window. At the drop down list at the top of the window, select **Firmware Startup**.
2. Select a Fabric from the **Fabric** drop down list.
3. Select a Domain from the **Domain** drop down list.
4. Select a Board from the **Board** drop down list.
5. Note that a vast majority of the options are grayed out. This is because the Firmware Startup trace captures anything and everything since a board was brought online.
6. Click **Arm** to begin the trace.
7. Clicking the **Stop** button stops gathering trace buffer information.

8. Click Retrieve **Trace Buffer...** and save the files to disk. Note that the Enterprise Manager automatically converts the files into a format that is readable via Finisar software.

Trap Configuration window

A trap is defined as a configurable software function that will send out an alarm when a particular event or condition occurs. Types of traps you may encounter are:

- **Chassis Hardware**

  Indicates a chassis hardware problem, such as a power supply or fan failure.

- **Fabric**

  Indicates a problem in the fabric, most likely between the Director and one or more N/NL-Ports.

- **Internal H/W**

  Indicate a potentially serious internal hardware error condition relating to the routing of frames within a Director.

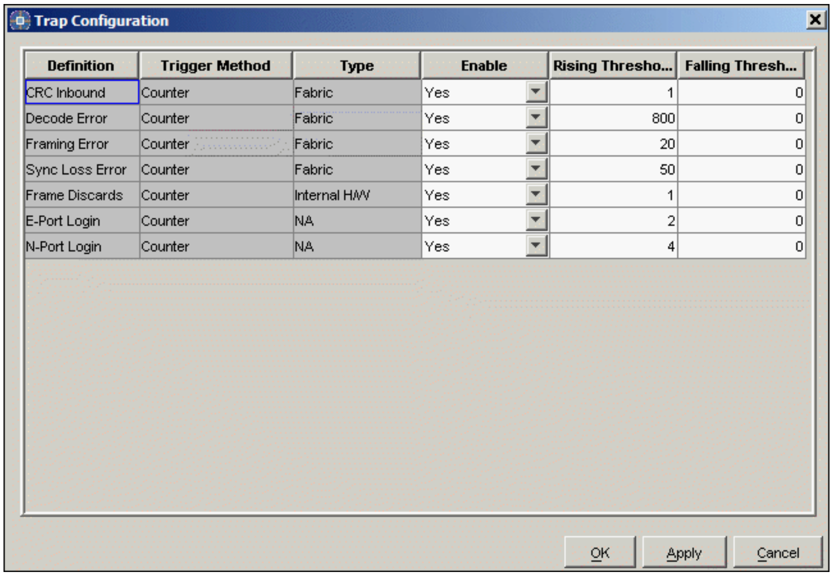
The **Trap Configuration** window presents conditions for which traps will be reported, and whether particular traps are enabled. This view allows you to enable or disable trap reporting and allows traps to be configured.

Viewing trap configurations

To view and adjust trap configurations follow the steps below.

1. Select by clicking the SAN256N director Logical View for which you would like to view the Trap Configuration window
2. Right-click in the gray area to the left of the logical director view and select **Trap Configuration** from the menu.

   Note: Traps are pre-set to factory levels and should only be adjusted and/or enabled or disabled if advised by an authorized IBM Field Service Representative.



Definition	Trigger Method	Type	Enable	Rising Thresho...	Falling Thresh...
CRC Inbound	Counter	Fabric	Yes	1	0
Decode Error	Counter	Fabric	Yes	800	0
Framing Error	Counter	Fabric	Yes	20	0
Sync Loss Error	Counter	Fabric	Yes	50	0
Frame Discards	Counter	Internal H/W	Yes	1	0
E-Port Login	Counter	NA	Yes	2	0
N-Port Login	Counter	NA	Yes	4	0

Figure 60. Trap Configuration window

Trap Configuration window details

The following fields are displayed when the **Trap Setting** tab is selected.

Table 17. Trap Setting tab field descriptions

Field	**Description**
Definition	Definition of the trap.
Trigger Method	There are two methods of triggering a trap, those being the pass/fail conditions and the counter thresholds. The pass/fail traps are driven by the pass/fail states of specific conditions whereas the counter threshold type traps key on specific event counts. The counter type traps have configurable rising and falling thresholds.
Type	There are several different trap types. The first is the Chassis HW traps which indicate a chassis hardware problem such as a power supply or fan failure. The Fabric traps indicate a problem in the fabric, most likely between the switch and one or more N_Ports. And finally, the Internal H/W traps indicate a potentially serious internal hardware error condition relating to the routing of frames within the switch.
Enable	Checked indicates that trap reporting is enabled; unchecked means reporting is disabled.
Rising Threshold	Uppermost threshold at which the trap will trigger.
Falling Threshold	Lowermost threshold at which the trap will trigger.

LRT button

The Link Rate Test (LRT) is a diagnostic tool that will test ports, modules and the switching capabilities of the SAN256N director. You must administratively set ports offline for testing. The test is run in two parts: part one is setting up and configuring the test (multiple tests can be setup and run) and part two is to run the test.

Clicking the **Link Rate Test (LRT)** button pops up the LRT List Dialog. From it, you can go to the testing form at which you may develop new tests, import test scenarios previously set up, export information and run the tests.

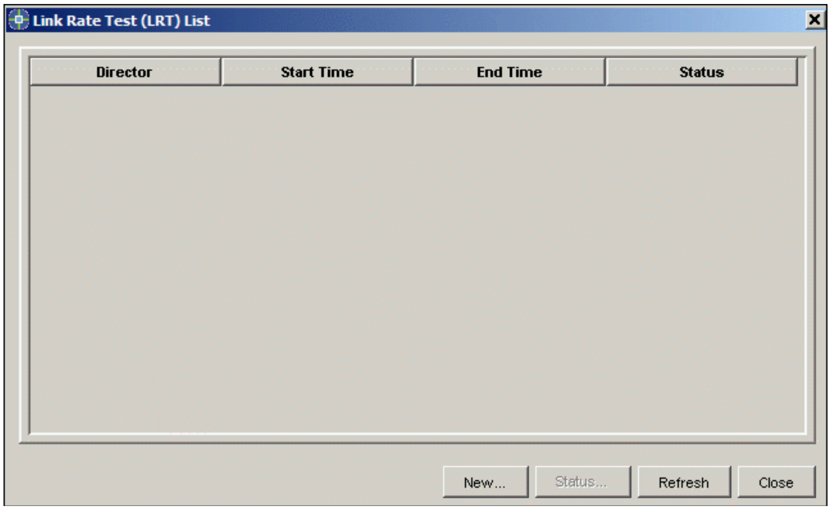
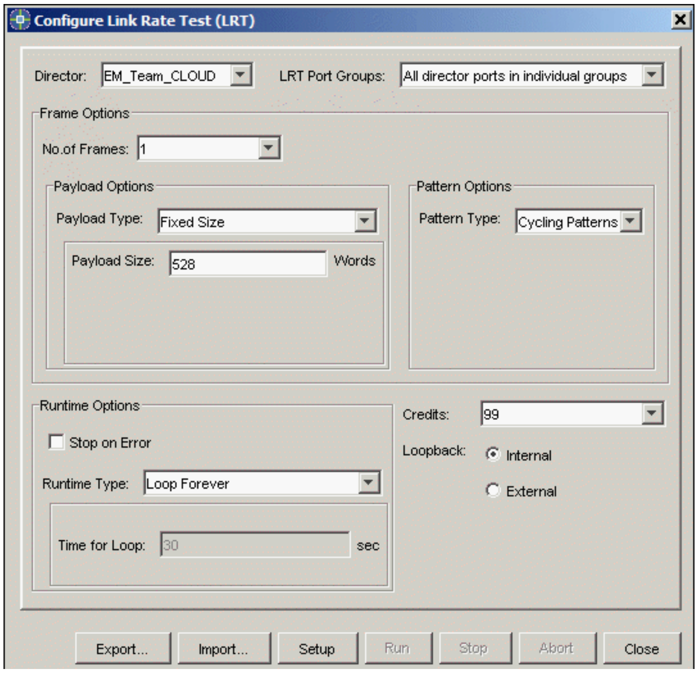


Figure 61. LRT List dialog

Configure a Link Rate Test

Note: All Ports in a director need to be taken offline prior to performing the Link Rate Test on them.

1. Click the **New...** button and the following dialog appears:



Director: EM_Team_CLOUD

LRT Port Groups: All director ports in individual groups

No.of Frames: 1

Payload Type: Fixed Size

Payload Size: 528 Words

Pattern Type: Cycling Patterns

□ Stop on Error

Runtime Type: Loop Forever

Time for Loop: 30 sec

Credits: 99

Loopback: ● Internal ○ External

Figure 62. Configure Link Rate Test dialog

2. Select the Director(s) on which the test will be run by choosing from the drop down list at the Director list in the upper left corner.

3. At the **LRT Port Groups** drop down list, choose the ports or port groups upon which the test will be run. Options are: All director ports in individual group, All director ports in one group, Single Board, Standard Paired, Sliding Paired, Random Paired, Custom Paired, Custom Port Groups.

Table 18. LRT Port Groups drop-down menu options

Option	**Description**
All director ports in individual groups	Each port is in its own group.
All director ports in one group	Test frames will circulate between all the director's ports in a daisy chain fashion.
Single Board	Perform test on a selected board. Test frames will circulate between all the ports on the board.
Standard Paired	Ports paired up into two per group.
Sliding Paired	Ports paired up such that after enough cycles every port will have been paired with every other port
Random Paired	Ports paired up randomly. Random pairs change with every cycle.
Custom Paired	Select one or more pair of ports of your choice from a dialog which pops up if this option is chosen.
Custom Port Groups	Create one or more groups of ports at a dialog upon which the test may be run.

4. Choose and set the number of frames at the **No. of Frames:** drop down list.
5. Next you can set the Payload Options. Choose the **payload type** and **payload size** from the drop down lists.
6. Select a pattern from the Pattern Type: drop down list.

Table 19. Pattern Type options

Option	**Description**
Fixed	Assigned 32 bit word specified by the value will be repeated throughout the frame.
Alternating	Pattern made up of two 32 bit words will be repeated throughout the frame.
Random	Random words are used throughout the frame.
Incrementing	Incrementing values are used throughout the frame.
CJ Jitter	Pattern that aggravates jitter difficulties.
Cycling Patterns	Cycles through different patterns including the CJ Jitter pattern every cycle.

7. If the Checkbox Stop on Error is checked, the test will stop when an error is detected. If unchecked, the test will run based on the Runtime Type selection.

8. You may also choose Runtime Options at the **Runtime Type:** drop down list Options are as follows:

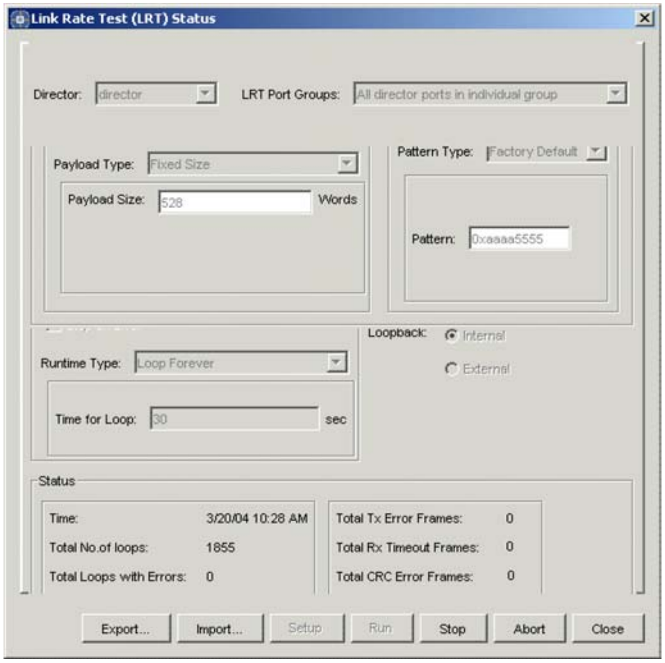
Table 20. Runtime Type options

Option	Description
Forever	Test runs until stopped by user
Fixed Type	Run the test for a specified time frame.
Loop Forever	Run the test for thirty seconds and then stop the test to gather information. Display the information and then start the test again.
Timed Loop	Run a specified number of loops, each for a specified amount of time.

9. At the Loopback option, select whether the test will run with an Internal or External loopback. Do so by clicking on the radio button of the option you wish to choose.
10. Click the **Setup** button and then **Yes** at the confirmation window. Click **OK** at the next window and then **OK** again at the “Successfully performed setup operation” window.
11. When you are finished making the option selections, click on **Run** to begin the test. At the confirmation window, click **Yes**. The status will update as the test is running.
12. You may close the LRT windows without affecting a running LRT.
13. To view the LRT status after closing the windows, click the **LRT** button. The list dialog appears. Click once on a test to select it, then click on **status** to view the progress of the test.

LRT status

Click the **Status** button and the following dialog appears:



Director: director

LRT Port Groups: All director ports in individual group

Payload Type: Fixed Size

Payload Size: 528 Words

Pattern Type: Factory Default

Pattern: 0xaaaa5555

Runtime Type: Loop Forever

Time for Loop: 30 sec

Loopback: ● Internal ○ External

Status

Time:	3/20/04 10:28 AM	Total Tx Error Frames:	0
Total No.of loops:	1855	Total Rx Timeout Frames:	0
Total Loops with Errors:	0	Total CRC Error Frames:	0

Figure 63. Link Rate Test status window

The status window indicates how the Link Rate Test is progressing.

LRT Status window buttons
Click the relevant buttons to perform the following tasks.

Table 21. LRT Status window buttons

Button	Description
Export...	Save the Link Rate Test parameters
Import...	Pull in the parameters of a previously Exported LRT
Setup	Setup the parameters of a LRT
Run	Run the currently “set up” LRT
Stop	Stop the LRT
Abort	Abort the LRT
Close	Close the LRT Status window

Status statistics
The following statistics are available at the LRT Status window

Table 22. LRT Status window statistics

Statistic	Description
Total No. of loops	Total number of loops run during the test period captured in the status window
Total Loops with Errors	Total number of loops run during the test period captured in the status window that returned errors.
Total Tx Error Frames	Number of frames not transmitted.
Total Rx Timeout Frames	Number of frames not received.
Total CRC Error Frames	Number of frames received with CRC error indications.

Export a Link Rate Test

At the Link Rate Status window, use the **Export...** button to save a configuration. Click the button and save the config file to a directory or removable storage.

Import a Link Rate Test

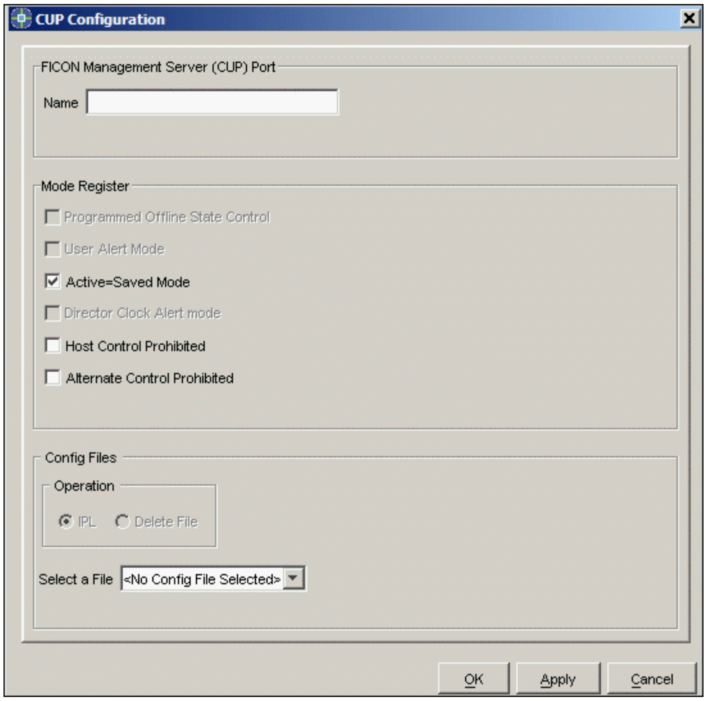
At the Link Rate Status window, use the **Import...** button to import a previously saved configuration. Click the button and import the config file from a directory or removable storage.

Chapter 7. FICON management server control unit port (CUP) feature

The FICON Management Server Control Unit Port (CUP) feature is optionally available for the SAN256N director, 64-, 128- and 256-port FC/9000 directors.

Note: This option may be enabled and disabled from the Enterprise Manager Software.

Click a director or SAN256N director Logical Domain in the SAN Navigation Tree and then right-click in the gray area next to the Faceplate view. Click the **FICON Management Server (CUP)** option to view the following dialog.



CUP Configuration

FICON Management Server (CUP) Port

Name

Mode Register

□ Programmed Offline State Control

□ User Alert Mode

☑ Active=Saved Mode

□ Director Clock Alert mode

□ Host Control Prohibited

□ Alternate Control Prohibited

Config Files

Operation

● IPL ○ Delete File

Select a File <No Config File Selected>

Figure 64. Control Unit Port (CUP) Configuration dialog

FICON Management Server (CUP) port

In this section, enter the name of the CUP port in the **Name** field.

Mode register

A check mark next to a mode indicates that the mode is selected and active.

Programmed offline state control

When selected, programmed control of the offline state is allowed. When deselected, control is prohibited and commands that cause entry into the director offline state are rejected with Unit Check status.

© Copyright IBM Corp. 2004

User alert mode

When enabled, a warning is displayed to the user whenever they attempt an action that writes director parameters. The user may override the warning. When disabled, a warning is not displayed.

Active=saved mode

This mode controls updating of the IPL configuration file. This file is enabled by default. The current state (configuration) is saved across power on-off cycles.

When enabled:

- A copy of the file will be saved as the IPL configuration file.
- Changes made to the active connectivity attributes or port address names by host programming or the Enterprise Manager user will also be saved to the IPL configuration file.
- The Enterprise Manager user and the host program will not be allowed to save configuration files with the name IPL.

When disabled:

- The current IPL configuration file is not changed.
- Changes made to the active connectivity attributes or port address names by host programming or the Enterprise Manager user will *not* be saved in the IPL configuration file.
- The Enterprise Manager user and the host program may save configuration files with the name ‘IPL.’

The default state is enabled. The current state is saved across power on-off cycles.

Director clock alert mode

If this mode is selected, it indicates that the Director Clock Alert mode is enabled. If it is not selected, this option is disabled.

When enabled, Director Clock Alert mode causes the Enterprise Manager Software to display a warning to the user when they attempt to set the Time-Stamp clock of the Director. They may override this warning. The mode also causes the Enterprise Manager to display an error message whenever the user attempts to activate any function which would automatically set the Time-Stamp clock. Functions which automatically set the Time-Stamp clock may only be enabled when Director Clock Alert mode is disabled.

When disabled, warning and error messages will not be presented.

By default, Director Clock Alert mode is disabled.

Host control prohibited

When disabled (unchecked), host programming is the controlling manager. Alternate Manager commands which alter the state of the director connectivity parameters will be accepted by the Management Server.

When enabled (checked), host programming has not been selected as the controlling manager and commands which alter director connectivity parameters will not be accepted from host programming.

Alternate control prohibited

When disabled (unchecked), alternate programming is the controlling manager. Host Manager commands which alter the state of the director connectivity parameters will be accepted by the Management Server.

When enabled (checked), alternate programming has not been selected as the controlling manager and commands which alter director connectivity parameters will not be accepted from alternate programming.

Config files

This option lets you IPL or delete config files.

IPL file

This operation is used to initialize the connectivity attributes and port address names of the ports in the director.

When the system is initially installed, the config file named DEFAULT is activated and contains a configuration which allows any-to-any communication. The default configuration contains no blocked ports and allows dynamic communication between all ports with which communication is allowed. The file also specifies 24 blank characters as the port address name for each implemented port.

Delete file

Selecting this option deletes the selected Config file.

Select a file

Select a Config file from this drop-down list.

Enabling the CUP feature

To enable the CUP feature, you must be logged in as an Administrative level or above user. Since CUP has an additional cost above the value of the base software, enablement of the feature is password protected. To obtain a password, contact your IBM Field Service Engineer. The Field Service Engineer will have to verify the purchase of the CUP feature.

1. Make sure that you have a valid password for enablement of the CUP feature. These passwords must be used within the time frame specified by your IBM Field Service Engineer. Make sure that you are logged in as an Administrative level or above user.
2. Select a Director at the SAN view of the navigation tree in which you wish to activate the CUP feature and right-click in the gray area next to the Faceplate view. Choose **System Configuration** from the list.
3. Select **Enabled** from the drop-down list next to CUP.
4. Click **Apply**.
5. Click **OK** at the confirmation window.
6. At the password pop-up dialog, type in the password you received from your IBM Field Service Engineer and then click **OK**.
7. If successful, the following message is displayed:

   ```
   The changes were applied successfully.
   ```

8. Click **OK** on the confirmation dialog.

9. If you do not receive the confirmation message, contact your IBM Field Service Representative.

Disabling the CUP feature

To disable the CUP feature, you will need to be logged in as an Administrative level or above user.

1. Make sure that you are logged in as an Administrative level or above user.
2. Select a director at the SAN view of the navigation tree in which you wish to disable the CUP feature and right-click in the gray area next to the Faceplate view. Choose **System Configuration** from the list.
3. Select **Disabled** from the drop-down list next to CUP.
4. Click **Apply**.
5. Click **OK** at the confirmation window.
6. If successful, the following message is displayed:

   ```
   The changes were applied successfully.
   ```
7. Click **OK** at the confirmation dialog.
8. If you do not receive the confirmation message, contact your IBM Field Service Representative.

Appendix A. Telnet

Each SAN256N director and FC-9000 director contains a Telnet server. This server allows a Telnet client to establish a Telnet session with it to retrieve information or to configure parameters. A command line interface enables you to perform a variety of fabric and switch management tasks through an Ethernet or a serial connection to a switch.

Starting a Telnet session using Windows

Note: Telnet must be enabled in the Enterprise Manager Software for the selected director.

1. From the **Start** menu, select **Run**. The Run dialog appears.
2. Type `telnet` in the **Open** field and click **OK**.
3. When the Telnet window appears, click **Connect** and then click **Remote System**.
4. At the Connect box, type the IP address of the FCM (for an FC/9000) or TCM (for a SAN256N director) in the **Host Name** area. “Telnet” should be displayed in Port box, and “VT100” should be displayed in the Terminal box.
5. Click **Connect**. The Telnet session will start, and you will be asked to enter your user name and password.

Note: For this procedure to work, the FCM's or TCM’s IP address must be accessible from the network of your computer.

Prompt client for login and password

When you want to initiate a Telnet session, you will be prompted for a user name and a password.

Currently, any user name is acceptable; the passwords that are accepted at this time, are “guest” or “admin”. Guest password allows the client very limited access to switch information. A guest is able to view some of the switch parameters, but is unable to set, reset, or delete any of the parameters. An Administrator level user, on the other hand, is able to view, set, reset, and delete any of the parameters that are available through the command line interface developed so far.

Command line interface

Upon a successful login to the FC/9000 or SAN256N director Telnet Server, the Telnet client will be in the CLI mode. You can immediately request CLI services from the switch. These commands are entered on one line ending with a new line character.

Note: Available commands may be viewed by typing `??` at the command line.

© Copyright IBM Corp. 2004

Appendix B. FC16-2, FC8-2, and QLogic SANbox2 zoning

The following instructions assume that you are familiar with the proper operation of the IBM Enterprise Manager Software.

Note: All zoneset creation, modification, and activation should be done from the Enterprise Manager Software. Do not use the SANbox Manager or FC-2 Enterprise Manager for any of these functions.

1. Define the devices that are attached to the SANbox2 by manually typing their worldwide names and descriptions into the Enterprise Manager Port WWN Devices Names Configuration window.
2. Use the Enterprise Manager Software to create a zoneset that contains zones that could consist of devices that are attached to either the FC/9000 and/or SANbox.
3. Make sure that these is no active zoneset on the SANbox.
4. Make an Interswitch Link (ISL) connection between the FC/9000 director and SANbox switch.
5. Activate the newly-created zoneset. This action will cause the zoneset to be merged into the SANbox and become the active zoneset of the fabric.
6. Zones can be added, deleted, or modified by using the Enterprise Manager Software to edit the *inactive* copy of the *active* zoneset. Activate the *inactive* zoneset when the changes are complete. There is no need to de-activate a zoneset to make changes to any of its zones.

© Copyright IBM Corp. 2004

Appendix C. Setup and activation of the SN-API API interface

The Enterprise Manager Software must be configured to allow the SN-API API interface to be used by third-party applications. This configuration process requires Administrator privileges.

Changing the default Enterprise Manager port

By default, the Enterprise Manager server uses TCP/IP port number 4000 to listen for any SN-API library commands. To change this default value:

1. Follow appropriate shutdown procedures to close the Enterprise Manager server.
2. Access the Enterprise Manager installation directory and locate the **ProductionInfo.ini** file.
3. Open this file into any text editor.
4. Search for the *SnapiPortNumbe*r entry in this file and modify the existing value (*e.g.*, the default value of 4000) to the required port number.
5. Save the file and close the text editor.
6. Restart the Enterprise Manager server.
7. Create an SN-API user account.

Note: It is recommended that a separate user account of username “SNAPI” and role “Operator” be created for the SN-API API interface. Refer to the “User security” section in Chapter 4. for instructions on how to do this.

© Copyright IBM Corp. 2004

Appendix D. TL_Port procedures

This appendix contains procedures for changing an Admin Type of a port to TL and to add, move, or remove devices on TL_Ports.

Note: TL_Port and arbitrated loop are available for the FC/9000 directors using 1 Gb/s I/O boards.

Changing a Port Admin type to TL

Note: Viewer level users may not apply changes.

This option allows you to change the Admin Type of a port from Normal (default) to a TL_Port. Changing the port to TL will allow you to assign World Wide Name(s) (WWN) of a device to it. The WWN is a 128-bit address composed of the 48-bit MAC address and 16-bit NAA address. This change can only be accomplished with 1 GB boards.

1. Under the SAN heading of the fabric tree, select the director on which the port resides that you wish to change to a TL_Port. Click the **Ports** tab and then right-click over the port which you wish to change. Then select **Configuration** at the list.
2. From the Configuration window, select the **TL_Port** option from the **Admin Type** drop-down list.
3. Click the **Advanced** tab, and note the **TL Cfg** button is enabled.
4. Click **TL Cfg** to display the **TL Port Configuration** window. By default, the TL_Port configuration is a private target. Private target has no WWNs assigned.
5. To assign WWNs, select the **Private initiator** option.
6. Click **Add...** to add WWNs or **Add From List...** to select available WWNs.

Note: Private devices are not listed. To add private devices, use the **Add...** button and type them in manually.

7. Type in the WWN number(s) you wish to add and then click **OK**, or if you chose to select from the list, highlight the WWNs you wish to add and then click **OK**.
8. The WWN(s) you added are now listed in the current WWN window.
9. Click the **Apply** button to apply the addition of the WWN number(s). This action sends the information to the director.
10. Click the **Apply** button on the Toolbar to complete the task.
11. When you are asked to set the port type, click **OK**.
12. When the changes have been applied, click **OK**.
13. The port type portion of the display now shows the port as a TL_Port.

Adding, moving, and removing devices on TL_Ports

Changes to devices specified on TL_Ports can be the result of adding a device, removing a device, or moving a device from one hard zone to another. If a device is a target, residing on a port defined solely for targets, the application will self-discover the device. If the device is an initiator, the port it resides on must be manually defined.

© Copyright IBM Corp. 2004

Moving an initiator

To move an initiator:

1. At the Ports view, right-click over the port from which the device is being moved.
2. Select **Configuration**, and then click the **Advanced** tab. Click the **TL Cfg** button. The TL_Port Configuration dialog appears.
3. If not already selected, select the **Private Initiator** radio button.
4. Select the WWN of the device being removed.
5. Click **Del**. The device is removed from the list.
6. Click the **Apply** button on the TL_Port Configuration dialog. Respond to any messages by clicking the appropriate option.
7. Click the **Apply** button on the Toolbar to save this port configuration. Respond to any messages by clicking the appropriate option.
8. At the Ports view, right-click over the port to which the device is being moved.
9. Select **Configuration**, and then click on the **Advanced** tab. Click the **TL Cfg** button. The TL_Port Configuration dialog appears.
10. If not already selected, select the **Private Initiator** radio button.
11. Click **Add**. The WWN entry dialog appears.
12. Enter the WWN for the device being added and click **OK**. The WWN is added to the list of devices.
13. Click the **Apply** button on the TL_Port Configuration dialog. Respond to any messages by clicking the appropriate option.
14. Click the **Apply** button on the Toolbar to save this port configuration. Respond to any messages by clicking the appropriate option.

Adding an initiator

1. At the Ports view, right-click over the port to which the device is being moved.
2. Select **Configuration**, and then click on the **Advanced** tab. Click the **TL Cfg** button. The TL_Port Configuration dialog appears.
3. If not already selected, select the **Private Initiator** radio button.
4. Click **Add**. The WWN entry window appears.
5. Enter the WWN for the device being added and click **OK**. The WWN is added to the list of devices.
6. Click the **Apply** button on the TL_Port Configuration dialog. Respond to any messages by clicking the appropriate option.
7. Click the **Apply** button on the Toolbar to save this port configuration. Respond to any messages by clicking the appropriate option.

Removing an initiator

1. At the Ports view, right-click over the port from which the device is being removed.
2. Select **Configuration**, and then click on the **Advanced** tab. Click the **TL Cfg** button. The TL_Port Configuration dialog appears.

3. If not already selected, select the **Private Initiator** radio button.
4. Select the WWN of the device being removed.
5. Click **Del**. The device is removed from the drop-down list.
6. Click the **Apply** button on the TL_Port Configuration dialog. Respond to any messages by clicking the appropriate option.
7. If no other devices are listed for this port, it is recommended that you change the **Admin Type** field back to **Normal** to facilitate auto-discovery of any future devices attached to this port.
8. Click the **Apply** button on the Toolbar. Respond to any messages by clicking the appropriate option.

Appendix E. IP broadcast

Introduction

This appendix provides a basic theory of operation of Fibre Channel Broadcast in IBM Directors, and defines how to configure a fabric including FC/9000 directors for an IP over Fibre Channel application. Address Resolution Protocol (ARP) in the IP layer is supported by broadcast frames in the Fibre Channel layer.

This document describes Broadcast mechanisms implemented in E_Port mode. Broadcast is supported in E_Port mode in Firmware Releases 4.3 and later.

Terms

Broadcast scope

Broadcast Scope, as used here, refers to the set of node ports to which a received broadcast frame is repeated. Broadcast Scope, as such, is not an entity that is configurable or viewable on a director. It is a term used for discussion purposes.

Broadcast scope is influenced by Domain-Port Zoning and also by whether zoning is active. The three possible values of broadcast scope are:

- If zoning is active, and the issuing node port is a member of an active Domain-Port zone, then the broadcast scope includes those node ports that share Domain-Port membership with the issuing node port.
- If zoning is active, and there are no Domain-Port zones or the issuing node port is not a member of an active Domain-Port zone, then the broadcast scope is NULL.
- If there is no active zoneset then the broadcast scope is the fabric.

Broadcast community

The term Broadcast Community is used here to refer to a set of node ports that are desired to have IP communications with each other. Broadcast Community is not an entity that is configurable on a director. The concept is for purposes of this discussion.

FC9000 broadcast theory of operation

Broadcast Enablement and Domain-Port Zoning are the two mechanisms provided in the IBM E_Port implementation to support Broadcast. The IBM design provides mechanisms to affect the processing of broadcast frames (D_ID = FFFFFF), at the point where the fabric receives the frame. Frames destined to addresses other than well-known addresses are not affected by these mechanisms.

Broadcast enablement

Broadcast enablement is a new port attribute that is configurable at the Enterprise Manager Software. This attribute affects how an F_Port processes a broadcast frame received from the fabric. If broadcast enablement is true (enabled) then the F_Port will pass the broadcast frame to its attached node port, otherwise the frame will be

© Copyright IBM Corp. 2004

discarded. An F_Port that receives a broadcast frame from its attached node port will repeat the broadcast frame to the other ports in its broadcast scope, independent of broadcast enablement settings.

Broadcast enablement is used to control, at the destination, the delivery of broadcast frames.

RSCN is not issued as a result of changing the broadcast enablement setting of a port. RSCN is the trigger for F_Ports to rediscover the nameserver (and for the soft zone to be enforced). Changing the Broadcast Enablement prior to applying a zoning change ensures that a port will have its proper enablement setting at the time the RSCN is issued for the zoning change.

FL_Port not supported

The broadcast enablement attribute is not supported for FL_Ports, therefore all ports desired to be in a broadcast community should be configured in non-loop mode. This may be accomplished by disabling loop at the F_Port, and if necessary reconfiguring the N_Port to operate in fabric topology, sometimes referred to as “point-to-point” (sic).

In an IP over Fibre Channel application, it is possible for an FL_Port that is inadvertently included in a broadcast community to establish communications with another F_Port, provided that it was the FL_Port that pinged the other F_Port. This is because the broadcast enablement attribute is enforced when an F/FL_Port receives a broadcast frame from the fabric that is headed to the attached node port. Specifically, an FL_Port that receives a broadcast frame from the fabric will unconditionally discard the frame. In contrast, an FL_Port that receives a broadcast frame from its attached node port will repeat the broadcast frame to the other ports in its broadcast scope; this is how communications with another F_Port might be established.

Domain-port zoning

A node’s membership in a Domain-Port zone is based on the Domain and Area fields of the Fibre Channel Address assigned by the fabric to that node. Domain-Port Zoning supports IP Broadcast in two ways:

- Domain-Port Zoning groups and separates nodes. The zoning is soft, as it is enforced at the level of the nameserver query. The response prepared by the directory server will contain references to only those nodes that share membership in a zone with the requesting node, and which meet the criteria of the query. When no zoneset is active, references to all nodes that meet the query criteria are included in the reply.
- Domain-Port Zoning defines the scope of ports to which a Broadcast frame is delivered. A fabric port, which receives a broadcast frame (D_ID = FFFFFF) from its node port, will send the frame out to the fabric. The frame will only be delivered to the node ports in the broadcast scope.

Fabric configuration for IP over Fibre Channel

This section discusses how to configure a fabric in support of an IP application, and how to change the configuration to achieve certain desired results. Unzoned operations and the affect of the IP/ARP table in the host are also discussed.

Creating broadcast communities

Set Broadcast Enablement to ‘enabled’ for each port in the broadcast community. Note that you may do so at the Port Configuration window of the Enterprise Manager. See the example of the Port Configuration window on page -87.

Given the nature of broadcast, it is typically desired to limit the broadcast scope. This is accomplished by configuring a zoneset with one Domain-Port zone for each broadcast community. The members of each Domain-Port zone should correspond to the members of the respective broadcast community. Then the zoneset should be activated.

Adding a broadcast community to an existing set of broadcast communities is accomplished by creating a replica of the existing active zoneset, adding a new Domain-Port zone in the inactive replica, then activating the replica. For information on how to create Zonesets and Zones and how to configure them and activate them, see , Zoning on page -30.

Unzoned considerations

When the broadcast scope is unbounded, i.e. the scope is the fabric, then all ports with Broadcast Enabled set to ‘enabled’ will receive a copy of every broadcast frame. Regardless of broadcast scope, there will be a small internal fabric load associated with every broadcast frame sent into the fabric by an attached node port.

Remove a node from a broadcast community

A node port is removed from an active broadcast community by setting Broadcast Enablement to ‘disabled’ for the port, and then removing it from the respective Domain-Port zone, by the following steps. Replicate the active zoneset, modify the appropriate zone to remove the node from the zone’s membership, and activate the modified zoneset.

For communications to stop, it is also necessary to clear the removed node’s IP address from the ARP tables of all other nodes in the broadcast community.

Add a node to a broadcast community

A node port is added to an active broadcast community by setting Broadcast Enablement to ‘enabled’ for the port, and then adding it to the respective Domain-Port zone, by the following steps. Replicate the active zoneset, modify the appropriate zone to add the node to the zone’s membership, and activate the modified zoneset.

Move a node from one community to another

One may move a node from one broadcast community to another broadcast community by removing it from the first community then adding it to the next community. One change to zoning is needed if, when removing the node from the current zone, it is also added to the desired zone. Then the modified zoneset may be activated. It is still necessary to delete the moving node’s IP address from the ARP tables of all other nodes in the original broadcast community, to prevent continued communications with the original community.

Preventing communications

Preventing all communications requires disabling the node for broadcast, as well as removing it from any active Domain-Port zones, while keeping zoning active. Clearing ARP tables is required as well.

Host IP / ARP considerations

A node’s IP layer will retain an entry in the ARP table for a discovered IP address until it is removed from the ARP table. Another way for an ARP entry to be scrubbed is when the IP layer fails in a point-to-point attempt, resorts to pinging, and times-out after not receiving a reply. ARP table resiliency must be properly considered when reconfiguring the fabric for IP Broadcast, otherwise undesired communications may occur between ports (because in a prior configuration they were communicating as desired, and they retain their point-to-point address in their ARP tables in the changed configuration.)

Overlapping zones

An HBA may be defined in overlapping zones, for example, it is a Domain-Port member of more than one zone. In this configuration, the Broadcast Scope for Broadcast frames issued by that HBA is the set of Domain-Port members of the zones of which that HBA is a member. Conversely, if enabled, the HBA will receive Broadcast frames issued by any HBA in that scope.

Mixing FCP (SCSI) and IP

A Domain-Port zone may be defined for a set of N/NL ports participating in FCP traffic, e.g. SCSI. A subset of the F_Ports may be enabled for broadcast. When queried, the nameserver will report all the entries satisfying the query criteria, and which share a zone with the querying device. Broadcast frames issued by any Domain-Port member will be received by the broadcast-enabled ports in that zone.

Comparison of 4.3 and 2.1 firmware

The method for configuring IP over Fibre Channel in the 4.3 firmware has changed significantly with respect to the 2.1 firmware. 4.3 uses E_Port interswitch links with Domain Port Zoning (soft) and Broadcast Enablement for configuring broadcast scope. ARP table scrubbing is required for stopping communications. In contrast, the 2.1 firmware implemented broadcast over propriety T_Port interswitch links. T_Port mode included three types of zoning, all with membership based on physical port number on the director: hard zoning, name server zoning, and broadcast zoning. Broadcast zones were the means of configuring the broadcast.

Configuring Broadcast Scope - Comparison

- 4.3 Firmware: Domain-port zoning, Broadcast enablement
- 2.1 Firmware: Broadcast zoning

HBA cConfiguration and test results

HBA configuration recommendations

Emulex HBA (Windows environment)

Select **Emulex Adapter** option from the available adapter list for configuration. After making the recommended selection, apply the changes by selecting the **Apply** tab from File Menu. Reboot the PC after applying the changes.

1. Ensure that the selection boxes next to the following options are checked at the Emulex Configuration Tool window:
   - Query name server for N_Ports
   - Allow multiple paths for SCSI targets
   - Register for state change
   - Use report LUNs
   - Use name server after RSCN
   - LUN mapping
   - Use PLOGI instead of PDISC after LIP
   - Scan in Device ID order
   - Enable Class2 for SCSI devices
   - Retry PLOGI open failures
   - Enable FCP-2 recovery
2. Enable networking by selecting **Networking** from Tools menu and select Class of Service as **Class 2**. Leave the “Disable FCP Poll” box unchecked, i.e. FCP Poll is enabled. IBM has found that when this box is checked, the HBA will not register to receive RSCNs, i.e. it will not send SCR. Click **OK**.
3. Select **Link Control** tab from Tuning menu and select **Point to Point Topology** with **AUTO** Link Speed. Click **OK**
4. Select the **Set** tab from the Configuration Menu and check the box for **Fabric/Point to Point**. Click. **OK**.

HBA test results

Emulex HBA

Table 1. Emulex HBA

Vender	Model	Platform	FW Version	Driver Version	Emulex Case #	Known Problem
Emulex	LP8000	NT 4.0 SP6, Win 2K SP3	3.82a1	5-2.11a2	47961	HBA changes its S_ID to 0x000001 after login
Emulex	LP8000 & LP9000	NT 4.0 SP6, Win 2K SP3	3.90a7	5-2.20a12	48222	Zoning Problem in windows environment (Broadcast messages not sent after Zoneset activation/de-activation)
Emulex	LP9000	Solaris 5.8	3.90a7	5.01e	48039	Zoning Problem in Solaris environment (Broadcast messages not sent after Zoneset activation/de-activation)
Emulex	LP8000 & LP9000	NT 4.0 SP6, Win 2K SP3, Solaris 5.8	3.90a7	5-2.13a4, 5-2.20a12, 5.01e	48222	PC Reboot problem (After Rebooting a PC with HBA, cause all HBA to stop communication)

Appendix F. Event codes

Event codes

EC = Event Code; Type = Property Type

Table 24. Event codes

EC	Name	Type	Severity	Description	Action
1	AC_CONDITION	E	EV_SEVERITY _WARNING	A change in AC power condition has been detected.	
2	DC_CONDITION	E	EV_SEVERITY _WARNING	A change in DC power condition has been detected.	
3	DEFAULT_SERIAL_NUM_ BEING_USED	E	EV_SEVERITY _CRITICAL	Backplane serial number cannot be read. Default serial number is being used. Default serial number is valueName1.	Call technical support.
4	FAN_CONDITION	I	EV_SEVERITY _WARNING	A change in fan condition has been detected.	
5	POWER_SUPPLY_PRES ENCE	E	EV_SEVERITY _WARNING	Power supply status event. On power up, a missing power supply is indicated with status = EV_FAIL. Insertion of missing power supply is indicated by this event with a status = EV_SUCCESS.	
6	FI_REPLACE_FRU_FAN	E	EV_SEVERITY _ERROR	Fault Isolation has determined that a fan needs to be replaced. The number of failed fans is failedValue.	Replace fan.
7	FI_REPLACE_FRU_POW ER_SUPPLY	E	EV_SEVERITY _CRITICAL	Fault Isolation has determined that a POWER SUPPLY needs to be replaced.	Replace power supply.
8	FI_FAN_MAINTENANCE	E	EV_SEVERITY _CRITICAL	Fault Isolation has detected a critical fan failure. The failure is valueName1. Number of failed fans is failedValue.	Replace failed fan module(s).

© Copyright IBM Corp. 2004

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
9	FI_CABINET_OVERHEAT	E	EV_SEVERITY_CRITICAL	Fault Isolation has detected critical cabinet heat condition. The failure is valueName1. Number of failed temperature sensors is failedValue.	Take immediate action to lower temperature. Call technical support.
10	FI_SECONDARY_CLOCK_ARM_FAILED	E	EV_SEVERITY_CRITICAL	The secondary clock ARM process failed. The number of boards in a failed state is failedValue. The failure is valueName1. Engineering level failure specific information is valueName2.	Replace failed board(s).
11	FI_INCOMPLETE_CLOCK_FAILOVER	E	EV_SEVERITY_CRITICAL	Incomplete clock failover. Not all TSW/TIO boards have successfully switched TCM clocks. The number of boards in a failed state is failedValue. The failure is valueName1. Engineering level failure specific information is valueName2.	
12	FI_NO_PRIMARY_CLOCK_ASSIGNED	E	EV_SEVERITY_CRITICAL	A TCM failed to assume the Primary clock role after boot-up or fail-over. The number of boards in a failed state is failedValue. The failure is valueName1. Engineering level failure specific information is valueName2.	
13	FI_INVALID_SECONDARY_CLOCK	E	EV_SEVERITY_BUG	An event used during Secondary clock assignment was received when only one TCM was detected in the system. The number of boards in a failed state is failedValue. The failure is valueName1. Engineering level failure specific information is valueName2.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
14	FI_SECONDARY_CLOCK_DISARM_FAIL	E	EV_SEVERITY_CRITICAL	All boards failed to disarm after the secondary TCM was removed. The number of boards in a failed state is failedValue. The failure is valueName1. Engineering level failure specific information is valueName2.	
15	SYSTEM_BEACON_TIMEOUT	E	EV_SEVERITY_INFO	System beaconing is stopped due to beacon time expiration.	
16	WATCHDOG_TRIGGERED	E	EV_SEVERITY_CRITICAL	Watchdog has triggered. Board is slotOrFruNum. Time in milliseconds is valueName2.	Retrieve debug backup logs and call technical support.
2001	BOARD_START_CONDITION	E	EV_SEVERITY_WARNING	Event generated upon board startup to indicate cause for start/restart.	If watchdog timeout reset cause, gather system logs and monitor for subsequent BoardStartCondition event from this board.
3001	BOARD_STATUS	E	EV_SEVERITY_ERROR	System Primary TCM Config process reports the state of the board that has either succeeded or failed the initialization process. Board status is failedValue. Additional info is valueName1.	Replace board if status is EV_FAIL.
3002	BOARD_REMOVED	E	EV_SEVERITY_WARNING	Board has been removed.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
3003	BOARD_FLASH_FAILURE	E	EV_SEVERITY_ERROR	Board flash failure is reported when the code load service is unable to update the board's flash. The Primary code load service will declare the board in 'Warning State' and issue a warning state event for the board. Filename for failed file is valueName1	Replace failed board.
3004	FI_REPLACE_FRU_BOARD	E	EV_SEVERITY_CRITICAL	Fault Isolation has determined that a board needs to be replaced. Cause of board failure is failedValue.	Replace failed board.
3005	BOARD_BEACON_TIMEOUT	E	EV_SEVERITY_INFO	Board beaconing is stopped due to beacon time expiration.	
3006	OVER_HEAT_CONDITION	E	EV_SEVERITY_ERROR	This event reports overheat or return to normal temperature range as indicated in the status field. The 2 byte temperature in degrees Centigrade is failedValue.	Replace failed board.
3007	EV_BOARD_RESTART_CONDITION	E	EV_SEVERITY_WARNING	Board has been restarted. Restart cause is valueName1.	
3008	NON_DEFAULT_DIPSWITCH_SETTINGS	E	EV_SEVERITY_ERROR	Board dip switches not set to default settings.	Confirm dip switch settings with technical support.
4001	PORT_SFP_PRESENCE_STATUS	E	EV_SEVERITY_WARNING	Current port connector (SFP) status. Additional info is valueName1.	
4002	PORT_HARDWARE_STATUS	E	EV_SEVERITY_ERROR	Change in Port Hardware Status. If port is reported failed, failure cause is valueName1.	Retrieve debug backup logs and call technical support.
4003	PORT_BEACON_TIMEOUT	E	EV_SEVERITY_INFO	Port beaconing is stopped due to beacon time expiration.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
4004	PORT_SFP_TEMPERATURE_STATUS	I	EV_SEVERITY_ERROR	Failure indicates the SFP internal temperature is outside of tolerance levels. Success indicates return to normal level.	On failure condition, place port offline. Disconnect SFP.
4005	PORT_SFP_SUPPLY_VOLTAGE_STATUS	I	EV_SEVERITY_ERROR	Failure indicates the SFP internal supply voltage is outside of tolerance levels. Success indicates return to normal level.	On failure condition, place port offline. Disconnect SFP.
4006	PORT_SFP_BIAS_CURRENT_STATUS	I	EV_SEVERITY_ERROR	Failure indicates the SFP internal bias current is outside of tolerance levels. Success indicates return to normal level.	On failure condition, place port offline. Disconnect SFP.
4007	PORT_SFP_XMIT_POWER_STATUS	I	EV_SEVERITY_ERROR	Failure indicates the SFP transmit power is outside of tolerance levels. Success indicates return to normal level.	On failure condition, place port offline. Disconnect SFP.
4008	PORT_SFP_LOW_RCV_POWER_STATUS	I	EV_SEVERITY_WARNING	Failure indicates the SFP receive power is below tolerance levels. Success indicates return to normal level.	On failure condition, check optical cables, connections, and distances for sources of signal loss. Replace cables or SFP if problem cannot be corrected.
4009	PORT_SFP_HIGH_RCV_POWER_STATUS	I	EV_SEVERITY_ERROR	Failure indicates the SFP receive power is above tolerance levels. Success indicates return to normal level.	On failure condition, place port offline. Disconnect SFP.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
4010	FI_RPLACE_FRU_SFP	E	EV_SEVERITY_CRITICAL	Fault Isolation has determined that a port SFP needs replacement. Fault Isolation has put the failed port offline. Failure cause is failedValue.	Replace SFP and put port administratively online.
16001	NO_CFG_FILE_CFG_SET_TO_DFLT	E	EV_SEVERITY_WARNING	Config File was not found. The configuration was set to default. Configuration filename is valueName1.	
16002	SYS_CFG_FILE_CORUPT_RST_TO_DFLT	E	EV_SEVERITY_WARNING	System config file corrupt; default settings applied. Configuration filename is valueName1.	
16003	CFG_CHG_PLATFORM_REALTIME_CLOCK	E	EV_SEVERITY_INFO	Real time clock has been set. Realtime clock value is valueName1.	.
16004	CFG_CHG_PLATFORM_TEXT_NAME	E	EV_SEVERITY_INFO	Platform text name has been changed. Old Platform text name is valueName1. New platform text name is valueName2.	.
16005	CFG_CHG_PLATFORM_DESCRIPTION	E	EV_SEVERITY_INFO	Platform description has been changed. First 64 characters of old Platform description is valueName1. First 64 characters of new platform description is valueName2.	.
16006	CFG_CHG_PLATFORM_LABEL	E	EV_SEVERITY_INFO	Platform label has changed. Old Platform label is valueName1. New platform label is valueName2.	.
16007	CFG_CHG_PLATFORM_PHYS_LOCATION	E	EV_SEVERITY_INFO	Platform physical location has been changed. Old Platform location is valueName1. New platform location is valueName2.	.
16008	CFG_CHG_SNMP_ENABLED_STATUS	E	EV_SEVERITY_INFO	SNMP platform service has been enabled or disabled.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
16009	CFG_CHG_SNMP_TRAP_REG_UPDATE	E	EV_SEVERITY_INFO	SNMP trap registry update. Update type is newValue. IP address affected is valueName1.	
16010	CFG_CHG_SNMP_IP_REGISTRY_UPDATE	E	EV_SEVERITY_INFO	SNMP IP registry update. Update type is newValue. IP address affected is valueName1.	
16011	CFG_CHG_SUBSW_RECONFIG_SLOTS	E	EV_SEVERITY_INFO	Logical domain has been reconfigured to assign IO boards to logical domains (logical domain partitions). Slot assignments are valueName2.	.
17001	CFG_CHG_NETWORK_RTTOV	E	EV_SEVERITY_INFO	RTTOV value has changed. RTTOV values should match for all connection units in the fabric. Old RTTOV is previousValue. New RTTOV is newValue.	
17002	CFG_CHG_NETWORK_EDTOV	E	EV_SEVERITY_INFO	EDTOV (Error Detect Timeout Value) has changed. EDTOV values should match for all connection units in the fabric. Old EDTOV is previousValue. New EDTOV is newValue.	
17003	CFG_CHG_NETWORK_RATOV	E	EV_SEVERITY_INFO	RATOV (Resource Allocation Timeout Value) has changed. RATOV values should match for all connection units in the fabric. Old RATOV is previousValue. New RATOV is newValue.	
17004	CFG_CHG_NETWORK_TEXT_NAME	E	EV_SEVERITY_INFO	zISL group text name has been changed. Old zISL group text name is valueName1. New zISL group text name is valueName2.	.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
17005	CFG_CHG_FABRIC_BINDING	E	EV_SEVERITY_INFO	Fabric binding has changed. The configuration change is valueName1. Configuration bitmap is valueName2.	
17006	CFG_CHG_SUBSW_TO_NETWORK_ASSIGN	E	EV_SEVERITY_INFO	Config changed for logical domain to zISL group assignment. The assigned logical domain is newValue.	.
18001	CFG_CHG_CUP_ENABLED_STATUS	E	EV_SEVERITY_INFO	CUP feature has been enabled or disabled.	
18002	CFG_CHG_SUBSWITCH_TEXT_NAME	E	EV_SEVERITY_INFO	Logical domain text name has been changed. Old logical domain text name is valueName1. New logical domain text name is valueName2.	.
18003	CFG_CHG_SUBSWITCH_INFO	E	EV_SEVERITY_INFO	Logical domain information has been changed. Old logical domain info is valueName1. New logical domain info is valueName2.	.
18004	CFG_CHG_SUBSWITCH_ADMIN_STATE	E	EV_SEVERITY_INFO	Logical domain state has been changed. All boards in the logical domain will be modified to reflect the new state. Old logical domain admin state is previousValue. New logical domain admin state is newValue.	
18005	CFG_CHG_SUBSWITCH_DOMAIN_ID	E	EV_SEVERITY_INFO	Admin domain Id has been changed for the logical domain. This is a disruptive change to the fabric in which this logical domain participates. Old domain Id is previousValue. New domain Id is newValue	.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
18006	CFG_CHG_SUBSW_DOMAIN_ID_NEGOT	E	EV_SEVERITY_INFO	Domain Id negotiable boolean configuration setting has been changed. Old domain ID negotiable is previousValue. New domain id negotiable is newValue	
18007	CFG_CHG_SUBSW_ADMIN_PRIORITY	E	EV_SEVERITY_INFO	Logical domain admin priority has changed. This value indicates the administrative priority for acting as Principal Switch. Old admin priority is previousValue. New admin priority is newValue.	.
18008	CFG_CHG_SUBSW_ADMIN_PRIOR_NEGOT	E	EV_SEVERITY_INFO	Admin Priority negotiable boolean configuration setting has been changed. Old admin priority negotiable is previousValue. New admin priority negotiable is newValue.	
18009	CFG_CHG_SUBSW_FICON_MODE_STATUS	E	EV_SEVERITY_INFO	FICON MODE has been enabled or disabled.	
18010	CFG_CHG_CUP_USER_ALERT_MODE	E	EV_SEVERITY_INFO	User Alert Mode has been changed. User Alert mode configured is newValue.	
18011	CFG_CHG_CUP_FILE_BLOCK_WRITE	E	EV_SEVERITY_INFO	CUP Config file block has been written. Block number is newValue. Filename is valueName1. This event occurs when active = save is off.	
18012	CFG_CHG_SUBSWITCH_REALTIMECLOCK	E	EV_SEVERITY_INFO	Real time clock has been set. Realtime clock value is valueName1, where format is yyyymmddhhmmssts.	
18013	CFG_CHG_CUP_MODE_REGISTER	E	EV_SEVERITY_INFO	CUP mode register has been changed. Command type is previous value. Old mode register command mask is valueName2. New mode register is newValue.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
18014	CFG_CHG_CUP_PRIMARY_REPORT_PATH	E	EV_SEVERITY_INFO	CUP primary report path has changed. New path source logical path is newValue.	
18015	CFG_CHG_CUP_ALLEGIANCE_PATH	E	EV_SEVERITY_INFO	CUP allegiance path has been transferred. New source path is newValue.	
18016	CFG_CHG_SUBSW_PORT_FORCE_DOWN	E	EV_SEVERITY_INFO	Change in configuration of port force down for all ports on the logical domain. Port will be put offline when error threshold exceeded.	
18017	CFG_CHG_CUP_IPL_APPLIED	E	EV_SEVERITY_INFO	CUP IPL file selected at EM has been applied. IPL filename is valueName1.	.
18019	CMD_CLEAR_STATS_LOGICAL_DOMAIN	E	EV_SEVERITY_WARNING	User has cleared statistics for all ports in the logical domain.	
18020	CFG_CHG_MULT_PORT_EXTERNAL_NAME	I	EV_SEVERITY_INFO	Event generated when more than one port name is changed. Number of port names changed is newValue.	None, internal informational event.
18023	CFG_CHG_SUBSW_STAT_THRESHOLDS	E	EV_SEVERITY_INFO	Port statistics threshold setting has been changed for all ports in a logical domain.	
19001	CFG_CHG_BOARD_ADMIN_STATE	E	EV_SEVERITY_INFO	Board admin state has changed. All ports on the board will be modified to reflect the new state. Old board admin state is previousValue. New board admin state is newValue.	
19002	CFG_CHG_BOARD_TEXT_NAME	E	EV_SEVERITY_INFO	Board text name has changed. Old board text name is previousValue. New board text name is newValue	.
20001	CFG_CHG_PORT_ADMIN_STATE	E	EV_SEVERITY_INFO	Port administrative state has changed. Old port admin state is previousValue. New port admin state is newValue.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
20002	CFG_CHG_PORT_PROHIBIT	E	EV_SEVERITY_INFO	Port prohibit mask for a port has changed. Bitmap payload: 1st word ignore, next 8 words are port prohibit mask, followed by 8 words of port map is valueName2.	.
20003	CFG_CHG_PORT_STATS_CFG_THRESHOL	E	EV_SEVERITY_INFO	Port statistics threshold setting has been changed. The statistic is valueName1.	.
20004	CFG_CHG_PORT_EXTERNAL_NAME	E	EV_SEVERITY_INFO	Port text name has changed. Old port text name is valueName1. New port text name is valueName2.	
20005	CFG_CHG_PORT_SWAP	E	EV_SEVERITY_INFO	Port Swap is processed. All attributes related to port A have been swapped with port B, and vice versa. Port A is previousValue; port B is newValue.	
20006	CFG_CHG_PORT_ADMIN_TYPE	E	EV_SEVERITY_INFO	Administrative port admin type has been changed. Old port admin type is previousValue. New port admin type is newValue.	
20007	CFG_CHG_PORT_PROHIT_ALL	E	EV_SEVERITY_INFO	This event generated when all ports are prohibited to all other ports in the logical domain	
20008	CFG_CHG_PORT_PROHIBIT_CLEAR_ALL	E	EV_SEVERITY_INFO	This event generated when port prohibit is cleared for all ports in the logical domain.	
20009	CFG_CHG_PORT_PROHIBIT_RANGE	E	EV_SEVERITY_INFO	Port prohibit mask for a range of ports has changed. This event reports how many ports are changed in newValue. Subsequent events for each port are reported with CFG_CHG_PORT_PROHIBIT. First port in range is logical domainPortNum.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
20010	CFG_CHG_CUP_PORT_NAME_RANGE	E	EV_SEVERITY_INFO	Port address names for a range of ports has changed. This event reports how many ports are changed in newValue. Subsequent events for each port are reported with CFG_CHG_PORT_EXTERNAL_NAME. First port in range is logical domainPortNum.	
20011	CFG_CHG_PORT_SPEED	E	EV_SEVERITY_INFO	Administrative port speed configuration change. Old port speed is previousValue. New port speed is newValue.	
20012	CMD_CLEAR_STATS_PORT	E	EV_SEVERITY_INFO	User has cleared statistics for a port.	
23001	CFG_INACTIVE_ZONING_DATA_CHANGE	E	EV_SEVERITY_INFO	Inactive zoneset is changed. Zoneset/Zone name is Value Name1.	
23002	CFG_CHG_ACTIVE_ZONESET_STATE	E	EV_SEVERITY_INFO	Active zoneset state has changed.	
23003	CFG_ZONESET_MERGED	E	EV_SEVERITY_WARNING	Zoneset merge has occurred. Zoneset name is valueName1. The resultant zoneset after merge is newValue.	
32001	ROUTABLE_PLATFORM_UPDATE	I	EV_SEVERITY_INFO	Change in the routable SAN256N director platforms list. Status of EV_SUCCESS means an addition to the list; EV_FAIL means subtraction from the list. Platform WWN of the remote SAN256N director is valueName2.	
33001	UPSTREAM_ISL_SELECTED	E	EV_SEVERITY_INFO	Upstream ISL selected. This occurs when new ISL is established, or removed. Additionally, removal of the IO board hosting the primary net config service will result in upstream ISL selection.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
33002	PRINCIPAL_SWITCH_SELECTED	E	EV_SEVERITY_INFO	Principal switch selected due to fabric reconfiguration. This occurs when new ISL is established, or removed. Additionally, removal of the IO board hosting the primary net config service will result in principal switch selection.	
33003	FABRIC_TOPOLOGY_UPDATE	E	EV_SEVERITY_INFO	Fabric topology has changed. Status of EV_SUCCESS means an addition to the fabric; EV_FAIL means removal from the fabric. The Domain Id in question is newValue.	
33004	FABRIC_ISL_OPER_STATE_CHANGE	I	EV_SEVERITY_INFO	A change in the fabric has been detected. An ISL may have come up or have been removed.	.
33005	DOMAIN_NAME_SERVER_UPDATE	I	EV_SEVERITY_INFO	Name Server information update for a remote domain. Domain Id is	.
33006	IN_OPERATIONAL_STATE_CHANGED	E	EV_SEVERITY_WARNING	This event is reported when the last board in an internal zISL group is removed, thus effectively putting the internal zISL group in an offline state. It is also reported when the first board is inserted into any slot of the internal network.	
34001	DOMAIN_ID_CHANGED	E	EV_SEVERITY_WARNING	Domain id of logical domain has changed due to Fibre Channel domain id reassignment by Principal Switch. This event is generated for domain id changes on the reporting SAN256N director logical domain.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
34002	DIRECTOR_HAS_BECOME_ISOLATED	E	EV_SEVERITY_ERROR	Director has become isolated due to the last E-port not logging in.	Correct port level isolations previously reported.
34003	SS_OPERATIONAL_STATE_CHANGED	E	EV_SEVERITY_WARNING	This event is reported when the last board in a logical domain is removed, thus effectively putting the logical domain in an offline state. It is also reported when the first board is inserted into any slot of the logical domain.	
34005	ALL_EXTERNAL_PORTS_SET_OFFLINE	E	EV_SEVERITY_INFO	All external ports have been set offline to prepare the system for a graceful power down. NOTE: on SAN256N director platforms with multiple logical domains, each logical domain should be issued the command before powering down. Additional info is valueName2.	
35001	BOARD_OPERATIONAL_STATE_CHANGED	E	EV_SEVERITY_WARNING	This event reported when an administrative state change has taken effect and is reflected in the operational hardware. If board is put offline, then all ports on the board must go offline.	
36001	PORT_OPERATIONAL_STATE_CHANGED	E	EV_SEVERITY_WARNING	Port operational state changed from previousValue to newValue.	
36002	PORT_TYPE_DISCOVERED	E	EV_SEVERITY_INFO	Mode of operation of the SAN256N director Port	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
36003	PORT_HAS_BECOME_ISOLATED	E	EV_SEVERITY_ERROR	Port linked to a Switch/ Director has become isolated. E-Port is operationally offline due to incompatible E-port attachment. Once all E-ports are isolated, the DIRECTOR_HAS_BECOME_ISOLATED event is generated. Isolation cause is valueName1.	Correct cause of isolation.
36004	PORT_OPERATIONAL_SPEED_CHANGED	E	EV_SEVERITY_INFO	Operational speed of port has changed.	
36005	SB_NODE_IDENTIFIER_UPDATE	I	EV_SEVERITY_INFO	Registered node identifier information for Single Byte (SB) format.	
36006	SB_NODE_IDENTIFIER_REGENERATED	I	EV_SEVERITY_BUG	Regenerated Registered node identifier information for Single Byte (SB) format. This event is reported upon request by EM when it is attaching to SAN256N director in order to refresh its connectivity view.	
36007	PORT_PHYSICAL_LOGICAL_ASSIGNMNT	E	EV_SEVERITY_INFO	A logical port has been associated with a physical port. Physical ports may have more than one logical port association. At port swap, a logical port is swapped with another logical port.	
36008	PORT_NAME_SERVER_UPDATE	E	EV_SEVERITY_INFO	Name Server update for a remote port. New NS entry is newValue, with 0 in previous value field; FC address is newValue. Removed NS entry is previousValue, with 0 in new value field.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
36009	INVALID_ATTACHMENT_ STATUS_CHG	E	EV_SEVERITY _ERROR	Invalid attachment detected on switch port. Status of EV_FAIL indicates the invalid attachment in newValue; status of EV_SUCCESS indicates the port no longer has invalid attachment.	Correct cause of invalid attachment.
39001	ZONESET_ACTIVATED_ STATUS	E	EV_SEVERITY _INFO	Status = 'success'=ACTIVATED; 'fail = DEACTIVATED. Zoneset name is valueName1.	
48001	SERVICE_ROLE_ASSIG NMENT_FAILURE	E	EV_SEVERITY _ERROR	Config service is not successful in assigning service role. Name of service is valueName1. logical domain field indicates network or logical domain index.	Retrieve debug backup logs and call technical support.
48002	SERVICE_ROLE_ASSIG NMENT_NOTRCVD	E	EV_SEVERITY _WARNING	Config service determines that role assignment notification is not received by service. Name of service is valueName1. Logical domain indicates network or logical domain index.	
48003	SYSTEM_INIT_COMPLE TE	E	EV_SEVERITY _INFO	System ready state achieved. E ports ready to be placed online. This event is expected to come after the System_Reset_or_Poweru p Event generated when the system initialization begins. This event reported after EM Service is initialized.	.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
48004	SYSTEM_CODE_VERSIONS_INVALID	E	EV_SEVERITY_CRITICAL	Code set is not valid. TCM firmware reports that not all the files mentioned in info.bin file have been downloaded successfully. Verification against security header has failed. Code set is identified in valueName1. First mismatched file is valueName2.	Issue 1-button code load from EM in order to properly load the system.
48005	CODE_VERSION_MISMATCH	E	EV_SEVERITY_WARNING	Code version mismatch on a board has been detected. First mismatched filename in valueName1 System will automatically load the proper code to the board.	
48006	SECONDARY_SYNC_FAILED	E	EV_SEVERITY_WARNING	Failure to update secondary server. Name of service is valueName1. Logical domain indicates network or logical domain index.	
48007	SYSTEM_RESET_OR_POWER_UP	E	EV_SEVERITY_WARNING	Event generated by primary process on TCM to indicate system restart has begun.	.
48008	SYSTEM_DATE_AND_TIME_NOT_SET	E	EV_SEVERITY_CRITICAL	System Time Not Set. RTC set to default time.	Set system time from EM.
48009	CLONE_SYNC_FAILED	E	EV_SEVERITY_WARNING	Failure to sync cloned process during NDCL activation. Name of process is valueName1. logical domain indicates network or logical domain index.	
48010	MEMORY_UTILIZATION_HIGH_STATUS	I	EV_SEVERITY_WARNING	Memory utilization status reported when available memory low, indicated by status of EV_FAIL. Return to good level indicated by status of EV_SUCCESS. Board slot number specified in slotOrFruNum field.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
48011	SYSTEM_HARD_RESET_REQUESTED	E	EV_SEVERITY_ERROR	System hard reset requested by management user.	.Wait for system to restart before issuing further commands.
48012	SYSTEM_SOFT_RESET_REQUESTED	E	EV_SEVERITY_WARNING	System soft reset requested by management user.	.
48013	TMI_INITIALIZATION_FAILED	I	EV_SEVERITY_ERROR	SAN256N director Management Interfaces initialization has failed. The reporting TCM is indicated in slotOrFruNum field.	Call technical support.
48014	LOCK_GRANTED	I	EV_SEVERITY_INFO	Lock granted for a subsequent database change. Lock type is identified in the failedValue enumeration. In the case of logical domain lock, the logical domain contains logical domain index.	
48015	LOCK_RELEASED	I	EV_SEVERITY_INFO	Lock released. Lock type is identified in the failedValue enumeration. In the case of logical domain lock, the logical domain contains logical domain index.	
48016	TMI_READY_STATE	I	EV_SEVERITY_INFO	I event to record SAN256N director Management Interfaces ready state.	.
48017	NDCL_OVERALL_COMPLETION_STATUS	E	EV_SEVERITY_INFO	Overall NDCL completion status reported by the NDCL controlling board. The controlling board is reported in FRU and the controlling process is valueName1. Bitmap of overall NDCL process status is failedValue.	
48018	NDCL_ABORTED	E	EV_SEVERITY_ERROR	NDCL has been aborted. The offending board is reported in FRU and the offending process is valueName1. Abort cause is valueName2.	Retry Activation from EM.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
48019	NDCL_SPAWN_TIMEOUT	I	EV_SEVERITY_ERROR	NDCL has failed due to spawn timeout. The offending board is reported in FRU and the offending process is valueName1.	Retry Activation from EM.
48020	NDCL_SUSPEND_TIMEOUT	I	EV_SEVERITY_ERROR	NDCL has failed due to suspend timeout. The offending board is reported in FRU and the offending process is valueName1.	Retry Activation from EM.
48021	NDCL_RESUME_TIMEOUT	I	EV_SEVERITY_ERROR	NDCL has failed due to resume timeout. The offending board is reported in FRU and the offending process is valueName1.	Retry Activation from EM.
48022	NDCL_END_TIMEOUT	I	EV_SEVERITY_ERROR	NDCL has failed due to completion timeout. The offending board is reported in FRU and the offending process is valueName1.	Retry Activation from EM.
48023	CODE_LOAD_COMPLETION_STATUS	E	EV_SEVERITY_INFO	Event reports the status of code load: success or failure.	
48024	CODE_LOAD_ROLLBACK_STATUS	E	EV_SEVERITY_INFO	Event reports the status of code rollback: success or failure. In case of failure, failure cause is failedValue. Code set in question is valueName1.	
48025	CODE_ACTIVATION_STATUS	E	EV_SEVERITY_INFO	Event reports the status of code activation: success or failure. In case of failure, failure cause is failedValue.	
48026	TCM_PRIMARY_CLOCK_ASSIGNED	I	EV_SEVERITY_INFO	This TCM board has taken the Primary clock role.	
48027	PRIMARY_CLOCK_ACCEPTED	I	EV_SEVERITY_INFO	Board has accepted the primary clock assignment	
48028	TCM_SECONDARY_CLOCK_ASSIGNED	I	EV_SEVERITY_INFO	This TCM board has taken the Secondary clock role	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
48029	SECONDARY_CLOCK_ACCEPTED	I	EV_SEVERITY_INFO	Board has accepted the Secondary clock assignment [0/1] and is now in the ARM state. Or, a board has been sent a message to disarm.	
48030	BOARD_SWITCHED_TCM_CLOCKS	I	EV_SEVERITY_INFO	Board has switched from Primary TCM clock source to Secondary TCM clock source. This requires that the board had previously been assigned a secondary clock and is in the ARM state.	
48031	BOARD_LOSS_OF_TCM_CLOCK	I	EV_SEVERITY_INFO	The TSW/TFIO board has lost its lock on the Primary clock source. This event will not be generated if a BOARD_SWITCHED_TCM_CLOCKS event is generated. This event should only occur when a board switched to its internal oscillator.	
48032	LOG_RETRIEVAL_DONE	I	EV_SEVERITY_INFO	Log retrieval status update.	
48033	BOARD_EVENT_LOG_FULL	E	EV_SEVERITY_CRITICAL	Board's event log is full. This event is generated by the event clients on each board when they have not been able to report their events to the system event server. The recurrence count in this event indicates how long this condition has persisted.	Retrieve debug backup logs and call technical support.
48034	COMMIT_STARTED	I	EV_SEVERITY_INFO	Database commit started. Server name is valueName1, If logical domain or network specific, logical domain has info.	
48035	COMMIT_COMPLETED_STATUS	I	EV_SEVERITY_WARNING	Database commit completed or timeout. Server name is valueName1. If failure status, failure is failedValue.	.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
48036	SERVICE_REASSIGNMENT_COMPLETE	I	EV_SEVERITY_INFO	Event reports that services have been reassigned to give positive indication of when it is safe to remove board.	
48037	SNMP_AGENT_STATUS	I	EV_SEVERITY_INFO	SNMP Agent status event. SNMP is a platform status.	
48038	SYSTEM_TIME_SYNC	I	EV_SEVERITY_INFO	Periodic system time synchronization has occurred. Time stamp is valueName1.	.
48039	LOCK_UNAVAILABLE	I	EV_SEVERITY_WARNING	Lock unavailable for a subsequent database change. Lock type is identified in the failedValue enumeration. In the case of logical domain lock, the logical domain contains logical domain index. Failure code is valueName2.	.
48040	DIAG_FC_PING_PERIODIC_UPDATE	I	EV_SEVERITY_INFO	Fault Isolation sends this event to EM periodically when there has been a change to the ongoing FC Ping tests in the system. The number of ongoing tests is failedValue.	
48041	EM_CONNECTION_LOST	E	EV_SEVERITY_ERROR	Connection to EM has failed 3 PING cycles. Sockets have been closed for the EM connection. EM address is valueName1.	Check Ethernet connection and PC hosting EM server.
50001	CUP_ENABLE_PASSWORD_FAILED	E	EV_SEVERITY_ERROR	Invalid password for CUP activation.	Call technical support for CUP enablement code.
50002	RESTRICTED_LOGGING_IN_EFFECT	E	EV_SEVERITY_ERROR	Only events of Critical and Error severity being logged Status is 'fail' when logging restricted; 'success' when restriction lifted.	Retrieve debug backup logs and call technical support.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
50003	CUP_FILE_FUNCTION_COMPLETE	I	EV_SEVERITY_INFO	CUP file function has completed. The filename is valueName1. The function is failedValue.	
51001	BOARD_WARNING_STATE	E	EV_SEVERITY_CRITICAL	Board has been declared in 'warning' state. This condition indicates that the board is operating with a deficiency that could result in subsequent system error.	Retrieve debug backup logs and call technical support.
51002	RAM_BUFFER_RETRIEVAL_REQUEST	I	EV_SEVERITY_INFO	RAM Buffer needs to be retrieved. Either it has reached its threshold or the periodic retrieval is needed. has reached its threshold. This event triggers Em to automatically retrieve the file. Board is slotOrFruNum.	
51004	NVRAM_BLOCK_CORRUPT	E	EV_SEVERITY_ERROR	NVRAM block corruption. Corrupted bock id is failedValue. The corrupted values have been restored to factory defaults.	Retrieve debug backup logs and call technical support.
51007	COMPACT_FLASH_MOUNT_FAILURE	E	EV_SEVERITY_CRITICAL	IDE disk mount failed. Failure indicates a missing disk or other problem with the medium. Specify failure code in failedValue field.	Call technical support.
51008	FW_TRACE_START_EVENT	E	EV_SEVERITY_INFO	Firmware trace has been armed on board slotOrFruNum.	.
51009	FW_TRACE_TRIGGER_1_HIT	E	EV_SEVERITY_INFO	First firmware trace trigger has occurred. If there is a single trigger enabled, trace data will be collected on the board.Trace data collection will stop once trace buffer is full or user issues 'Stop Trace' command.	.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
51010	FW_TRACE_TRIGGER_2_HIT	E	EV_SEVERITY_INFO	Second firmware trace trigger has occurred. Trace data will be collected on the board.Trace data collection will stop once trace buffer is full or user issues 'Stop Trace' command.	.
51011	FW_TRACE_BUFFER_FULL	E	EV_SEVERITY_INFO	Firmware trace buffer is full. The buffer data will now be automatically saved to a file. Trace is disarmed and data collection is stopped. valueName1 contains filename.	Retrieve trace file.
51017	RTC_FAILURE	E	EV_SEVERITY_ERROR	Can't READ OR WRITE system realtime clock.	Retrieve debug backup logs and call technical support.
51024	TIME_SYNC_WITH_TIME_SERVER	I	EV_SEVERITY_INFO	Board's Time synchronized with Time Server	
51025	TIME_SYNC_FAILED	E	EV_SEVERITY_WARNING	Time Synchronizer did not receive response from Time Server.	
51026	BOARD_HARD_RESET_REQUESTED	E	EV_SEVERITY_WARNING	Board hard reset requested by management user.	.
51027	BOARD_SOFT_RESET_REQUESTED	E	EV_SEVERITY_WARNING	System soft reset requested by management user.	
51028	WATCHDOG_TIMER_EXPIRED	E	EV_SEVERITY_ERROR	Reported at resumption of execution after reset has occurred.	Retrieve debug backup logs and call technical support.
51029	BOARD_INITIALIZED	E	EV_SEVERITY_INFO	Board has been initialized. This event reported when board's external ports are ready to be put in the admin state, online or offline.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
52001	FABRIC_LOGIN_FAILED	E	EV_SEVERITY_WARNING	Unsuccessful FLOGI by device. Failure condition is valueName1.	
52002	PORT_LOGIN	E	EV_SEVERITY_WARNING	Unsuccessful PLOGI by device. Failure condition is valueName1.	
52003	PORT_FAILED_POST	E	EV_SEVERITY_ERROR	Port has failed POST3 test.	Attempt placing port offline, then online to fix the failure. If unsuccessful, retrieve debug backup logs and call technical support.
52005	CRC_ERROR_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	CRC error threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of CRC errors is failedValue.	No user action required. I fault isolation and recovery monitors this event to take corrective action.
52006	SYNC_LOSS_ERR_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	Sync loss error threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of Sync loss errors is failedValue.	No user action required. I fault isolation and recovery monitors this event to take corrective action.
52007	DECODE_ERR_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	Decode error threshold status event. The number of decode errors is failedValue. Status of EV_FAIL indicates threshold exceeded; EV_SUCCESS indicates error has reached falling threshold.	No user action required. I fault isolation and recovery monitors this event to take corrective action.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
52008	FRAMING_ERR_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	Framing error threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of framing errors is failedValue.	No user action required. I fault isolation and recovery monitors this event to take corrective action.
52009	FRAME_DISCARD_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	Frame discard threshold status event. The number of framing errors is failedValue.	No user action required. I fault isolation and recovery monitors this event to take corrective action.
52010	FL_PORT_LIP_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	FL port LIP attempt threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of LIP attempts is failedValue.	No user action required. I fault isolation and recovery monitors this event to take corrective action.
52011	FL_PORT_LIP_FAIL_THRESHLD_STAT	E	EV_SEVERITY_ERROR	FL port LIP failure threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of LIP failures is failedValue.	No user action required. I fault isolation and recovery monitors this event to take corrective action.
52014	LINK_INCIDENT	E	EV_SEVERITY_WARNING	Link incident. LinkIncidentCode is failedValue. Link incident timestamp #of seconds/ #of microseconds is valueName1. Link incident transaction id (0 not valid). Is valueName2.	
52015	TRACE_START_EVENT	E	EV_SEVERITY_INFO	Trace of port specified in the physical platform port number has been armed.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
52016	TRACE_TRIGGER_1_HIT	E	EV_SEVERITY_INFO	First trace trigger of port specified in the physical platform port number has occurred. If there is a single trigger enabled, trace data will be collected on the board.Trace data collection will stop once FIFO is full or user issues 'Stop Trace' command.	.
52017	TRACE_TRIGGER_2_HIT	E	EV_SEVERITY_INFO	Second trace trigger of port specified in the physical platform port number has occurred. Trace data will now be collected on the board. Trace data collection will stop once FIFO is full or user issues 'Stop Trace' command.	
52019	DIAG_FC_PING_COMPLETION_STATUS	E	EV_SEVERITY_WARNING	Event issued by Fault Isolation when ELS ECHO test completes or times out. If test successful, status is EV_SUCCESS. If test fails, status is EV_FAIL, link service reason code for LS_RJT is failedValue, Description of failure is valueName2.	
52020	E_PORT_LOGIN_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	E-Port login attempts threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of login attempts is failedValue.	Take action to correct login problem.
52021	N_PORT_LOGIN_THRESHOLD_STATUS	E	EV_SEVERITY_ERROR	N-Port login attempts threshold status event. Status of EV_FAIL indicates threshold exceeded' EV_SUCCESS indicates error has reached falling threshold. The number of login attempts is failedValue.	Take action to correct login problem.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
52022	LINK_RESET	I	EV_SEVERITY _INFO	Link reset detected. Link reset initiator is failedValue. Additional details are valueName1 valueName2.	
53001	USER_LOGON	E	EV_SEVERITY _INFO	User logon from EM or Telnet. If failed attempt then failedValue indicates failure code. ValueName1 = user name. ValueName2 = failure description.	
53002	USER_LOGOFF	E	EV_SEVERITY _INFO	User logoff from EM or Telnet. If failed attempt then failedValue indicates failure code. ValueName1 = user name. ValueName2 = failure description.	
53003	EV_USER_AUTO_LOGO FF	E	EV_SEVERITY _INFO	User has been automatically logged off. valueName1 = user name.	
54001	PROCESS_UNRESPONS IVE	I	EV_SEVERITY _ERROR	Process monitoring has detected unresponsive process. Process name is valueName1.	
54002	FAILED_SOCKET_CREA TION	I	EV_SEVERITY _ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54003	FAILED_SET_SOCKET_ OPTION	I	EV_SEVERITY _ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54004	FAILED_BINDING_SOCK ET	I	EV_SEVERITY _ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54005	FAILED_LISTENING_ON _SOCKET	I	EV_SEVERITY _ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54006	FAILED_ACCEPTING_ON _SOCKET	I	EV_SEVERITY _ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
54007	FAILED_SHARING_SOCK_WITH_NW_TSK	I	EV_SEVERITY_ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54008	FAILED_SENDING_DATA_ON_SOCKET	I	EV_SEVERITY_ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54009	FAILED_RECEIVING_DATA_ON_SOCK	I	EV_SEVERITY_ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54010	FAILED_SETTING_SOCK_TO_NON_BLK	I	EV_SEVERITY_ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54011	FAILED_SETTING_SOCKET_TO_BLOCK	I	EV_SEVERITY_ERROR	failedValue contains failure code. valueName1 contains ASCII socket type: EM, Telnet, etc.	
54012	PROCESS_RAN_TOO_LONG	I	EV_SEVERITY_ERROR	Self monitored event to indicate that a process is not playing fair. Process name is valueName1. Signal Id is failedValue.	
54013	PROCESS_RAN_TOO_OFTEN	I	EV_SEVERITY_ERROR	Self monitored event to indicate that a process is not playing fair. Process name is valueName1.	
54014	ETHERNET_CONGESTION	I	EV_SEVERITY_CRITICAL	Process monitoring has detected congestion on the Ethernet bus. valueName1 and valueName2 identifies the two endpoints in the congested frame.	Retrieve debug backup logs and call technical support.
54015	LOSS_OF_PRIMARY_ETHERNET_PATH	I	EV_SEVERITY_ERROR	Process monitoring has detected first MAC has failed. failedValue identifies the failed MACA or MACB.	
54016	LOSS_OF_SECONDARY_ETHERNET_PATH	I	EV_SEVERITY_CRITICAL	Process monitoring has detected second MAC has failed. failedValue identifies the failed MACA or MACB.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
54025	QUEUE_SEND_FAILURE	I	EV_SEVERITY _ERROR	Queue Send Error. valueName1 identifies from endpoint process id. valueName2 identifies destination endpoint process id.	Retrieve debug backup logs and call technical support.
54026	REQUEST_TIMEOUT	I	EV_SEVERITY _ERROR	This event generated when a request from one process to another times out. EndPt is the reporting process. valueName1 specifies name of the request message that has timed out. failedValue contains signal number. FRU number is the slot of reporting board.	Retrieve debug backup logs and call technical support.
54027	Q_READ_INVALID_SIGN AL_HANDLE	I	EV_SEVERITY _ERROR	Invalid handle in signal. failedValue contains signal id.	Retrieve debug backup logs and call technical support.
54028	FILE_OPEN_FAILED	E	EV_SEVERITY _ERROR	File Management Server failed to open a file. Filename is valueName1.	Retrieve debug backup logs and call technical support.
54029	FILE_READ_FAIL	I	EV_SEVERITY _WARNING	File Management Server failed to read a file. Filename is valueName1.	Retrieve debug backup logs and call technical support.
54030	FILE_WRITE_FAIL	I	EV_SEVERITY _INFO	File Management Server failed to write a file. Filename is valueName1.	Retrieve debug backup logs and call technical support.
54031	FILE_CREATION_STATU S	I	EV_SEVERITY _ERROR	File creation status: EV_SUCCESS or EV_FAIL status. Filename is valueName1.	If failure, retrieve debug backup logs and call technical support.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
54032	FILE_DELETED_STATUS	I	EV_SEVERITY_WARNING	File deletion status: EV_SUCCESS or EV_FAIL status. Filename is valueName1.	If failure, retrieve debug backup logs and call technical support.
54033	FILE_RENAME_STATUS	E	EV_SEVERITY_WARNING	File renamed status: EV_SUCCESS or EV_FAIL status. Old filename is valueName1; new filename is valueName2.	
54034	FILE_COPY_STATUS	I	EV_SEVERITY_WARNING	File copied status: EV_SUCCESS or EV_FAIL status. Filename is valueName1.	
54035	GET_FILE_FAILED	E	EV_SEVERITY_ERROR	GET file operation is terminated due to error. Failure code is failedValue. Filename is valueName1.	Retrieve debug backup logs and call technical support.
54036	PUT_FILE_FAILED	E	EV_SEVERITY_ERROR	PUT file operation is terminated due to failedValue. Filename is valueName1.	Retrieve debug backup logs and call technical support.
54037	DISK_USAGE_WARNING	E	EV_SEVERITY_WARNING	IDE disk utilization warning. Status of EV_FAIL indicates too full condition; EV_SUCCESS indicates return to safe margin. Current utilization size is failedValue.	
54038	GET_FILE_REQ_RECEIVED	I	EV_SEVERITY_INFO	GET file request is received. Filename is valueName1.	
54039	PUT_FILE_REQ_RECEIVED	I	EV_SEVERITY_INFO	PUT file request is received. Filename is valueName1.	
54040	IDE_FILE_MOVE_COMPLETION_STATUS	I	EV_SEVERITY_INFO	IDE file move completion with EV_SUCCESS or EV_FAIL status. Filename is valueName1. Failure code is failedValue, in failure case.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
54041	RAM_FILE_MOVE_COMPLETION_STATUS	I	EV_SEVERITY_INFO	RAM file move completion with EV_SUCCESS or EV_FAIL status. Filename is valueName1. Failure code is failedValue, in failure case.	
54042	CODE_FILE_DISTRIBUTION_STATUS	I	EV_SEVERITY_INFO	Code file distribution status. Filename is valueName1. Status id failedValue.	
55003	ZONE_CHG_FAIL_INVALID_ZSET_NAME	E	EV_SEVERITY_WARNING	Zone change has failed due to invalid zoneset name. Invalid name is binary data: valueName2.	
55004	ZONE_CHG_FAIL_INVALID_ZN_NAME	E	EV_SEVERITY_WARNING	Zone change has failed due to invalid zone name. Zoneset name is valueName1. Invalid name is binary data: valueName2.	
55005	ZONE_CHG_FAIL_INVALID_MEMBER	E	EV_SEVERITY_WARNING	Zone change has failed due to invalid zone member. Failure cause is failedValue. Zoneset name is valueName1.	
55023	ZONESET_ACTIVATION_FAILED	E	EV_SEVERITY_WARNING	Zoneset activation has failed. Zone server reports this failure when a GS-request fails. Zoneset name is valueName1.	
55024	ZONESET_DEACTIVATION_FAILED	I	EV_SEVERITY_WARNING	Zoneset deactivation has failed. Zone server reports this failure when a GS-request fails. Failure cause is failedValue.	
56001	DB_RECOVERY_STARTED	I	EV_SEVERITY_INFO	Database recovery started.	
56002	DB_RECOVERY_ENDED	I	EV_SEVERITY_INFO	Database recovery completed.	
56003	DB_SYNC_FAILED	E	EV_SEVERITY_WARNING	The secondary failed to execute the last write command.	
56004	DB_LOGIC_ERROR	I	EV_SEVERITY_WARNING	A logic error occurred during a database operation.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
56005	SESSION_START	E	EV_SEVERITY_INFO	User session establishment status. Status of 'fail' indicates unable to create new session; 'success' indicates new session created.	
56006	SESSION_END	E	EV_SEVERITY_INFO	User session removal status. Status of 'fail' indicates unable to remove session; 'success' indicates nsession removed.	
56007	MAX_TELNET_SESSIONS_EXCEEDED	E	EV_SEVERITY_WARNING	Max. TELNET sessions limit is reached.	
56008	ENDING_TELNET_SESSION	I	EV_SEVERITY_INFO	Telnet session is ended	
56009	TELNET_LOGON	I	EV_SEVERITY_INFO	User log-in to TELNET	
56010	TELNET_LOGOFF	I	EV_SEVERITY_INFO	User log-out to TELNET	
56011	DB_SYNC_COMPLETE	I	EV_SEVERITY_INFO	Secondary DB sync complete. Reporting Service is valueName1.	
58001	LRT_STARTED	E	EV_SEVERITY_INFO	LRT started using the parameters specified in LRT setup.	
58002	LRT_STATUS	E	EV_SEVERITY_INFO	LRT status. This event is generated during execution of the LRT. It is generated once per iteration. It summarizes the test progress. If an error is detected in this iteration, then status is failed; if no error this iteration, status is good.	.
58003	LRT_STOPPED_SUMMARY	E	EV_SEVERITY_INFO	LRT stopped. This is issued when the test criteria has been met or upon stop command execution from EM. If an error is detected in any iteration, then status is failed; if no error in any iteration, status is good.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
58004	PROM_EVENT_FAILURE	E	EV_SEVERITY _CRITICAL	Boot PROM diagnostic failure. Failure code is specified in failedValue field. A textual description of the failure is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Call technical support.
58005	PROM_EVENT_WARNIN G	I	EV_SEVERITY _WARNING	Boot PROM diagnostic warning. Failure code is specified in failedValue field. A textual description of the failure is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Retrieve debug backup logs and call technical support.
58006	BOARD_BOOT_FAILURE	E	EV_SEVERITY _CRITICAL	Failure to boot board. Diagnostic specific to board type. Failure code is specified in failedValue field. A textual description of the failure is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Call technical support.
58007	BOARD_BOOT_WARNIN G	I	EV_SEVERITY _WARNING	Board Boot error in diagnostic specific to board type. Error code is specified in failedValue field. A textual description of the error is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Retrieve debug backup logs and call technical support.
58008	OSE_STARTUP_FAILUR E	E	EV_SEVERITY _CRITICAL	Failure to start application Failure code is specified in failedValue field. A textual description of the failure is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Retrieve debug backup logs and call technical support.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
58009	OSE_STARTUP_WARNING	I	EV_SEVERITY_WARNING	Recoverable error occurred on application start. Error code is specified in failedValue field. A textual description of the error is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Retrieve debug backup logs and call technical support.
58010	OSE_RUNTIME_FAILURE	E	EV_SEVERITY_CRITICAL	OSE runtime failure. Failure code is specified in failedValue field. A textual description of the failure is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Retrieve debug backup logs and call technical support.
58011	OSE_RUNTIME_WARNING	I	EV_SEVERITY_WARNING	Transient system error indicative of system resource issue. Error code is specified in failedValue field. A textual description of the error is contained in valueName1. The binary data (up to 7 long words) for the failure is specified in valueName2.	Retrieve debug backup logs and call technical support.
58012	FI_ISOLATION_STATE_CHANGE	E	EV_SEVERITY_INFO	Event records the enabling or disabling of fault isolation where EV_SUCCESS = enabled and EV_FAIL = disabled.	.
58013	FI_RECOVERY_STATE_CHANGE	E	EV_SEVERITY_INFO	Event records the enabling or disabling of fault recovery where EV_SUCCESS = enabled and EV_FAIL = disabled.	.
58014	FI_MESSAGE_FAILURE	I	EV_SEVERITY_ERROR	Fault isolation message failure.	
58015	FI_OVER_QUEUE_LIMIT	E	EV_SEVERITY_ERROR	Fault isolation analysis over queue limit. Fault isolation process reporting the queue overflow is running on the TCM slot identified in slotOrFruNum field.	Retrieve debug backup logs and call technical support.

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
58016	FI_WARNING_FC_PORT	E	EV_SEVERITY _ERROR	Fault Isolation has identified a port problem due to either HW failure on IO board or external device.	No user action. Fault isolation may place port offline if condition persists.
58017	FI_SYSTEM_EXPOSURE _CONDITION	E	EV_SEVERITY _ERROR	Fault Isolation has detected that control links for a particular TIO board have been placed offline and the loss of any more control links would result in a loss of credit upload or credit download granularity.	Call technical support and schedule a replacement of the board FRU indicated.
58018	LRT_ERROR_EVENT	E	EV_SEVERITY _WARNING	LRT has detected an error. Transmitting port is platformPortNum. Failure is failedValue. Error is valueName1.	.
58019	LRT_SETUP	E	EV_SEVERITY _INFO	LRT has been setup. Ports involved are in diagnostic state.LRT will begin once the start command is issued.	.
58020	LRT_CMD_TO_INFRAST RUCT_ERR	I	EV_SEVERITY _WARNING	LRT command to infrastructure has timed out. This is caused by a time-out while waiting for an expected LRT response. This is usually caused by a board that has stopped responding due to a hang or reset.	
58021	LRT_CMD_INFRASTUCT _ERR_ALL_GRPS	I	EV_SEVERITY _WARNING	LRT command to all groups has timed out. This may happen if the all boards that are supposed to be running the LRT stop responding, or an Ethernet problem that is common to all boards. If only one board is to run the LRT, it is probably hung or has reset.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
58022	LRT_STACK_IURSP_RCV_WRONG_STATE	I	EV_SEVERITY_BUG	LRT has received IU response in the wrong state. This may be attributable to a duplicate or delayed response from FC Stack. System busy or timeout too short (firmware error?).	
58023	LRT_INVALID_SETUP_ERR	I	EV_SEVERITY_WARNING	LRT setup is invalid. Run request received before set-up was complete. There may have been a problem with a previous setup or the termination of an LRT.	
58024	LRT_RCVD_IU_WAIT_TO_ERR	I	EV_SEVERITY_WARNING	LRT time out occurred while waiting for a test frame to be received. This may indicate that an erroneous frame was received and absorbed by FC Stack. First port of the failed group is identified.	
58025	LRT_ABORTED_EVT	E	EV_SEVERITY_INFO	User has aborted LRT.	
58026	LRT_TSDS_FCCFG_PORT_RELEASE_REQ	I	EV_SEVERITY_WARNING	SAN256N director System Diag Server unable to send request to release port, most likely due to board failure in system.	
58027	LRT_TSDS_FCCFG_PORT_RELEASE	I	EV_SEVERITY_WARNING	SAN256N director System Diag Server failure to release a port due to abort, FC Config internal error, or a board failure.	
58028	LRT_STATE_TRANS_REQ_INVALID	I	EV_SEVERITY_WARNING	LRT group in an unexpected state, mostly likely due to lost message or slow response.	
58029	LRT_STACK_REG_FAILED_ERR	I	EV_SEVERITY_WARNING	LRT unable to register port with FC stack. Firmware error in FC stack. Group number is valueName1. First port of the failed group is platformPortNum.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
58030	LRT_STACK_LOGI_REQ_FAILED_ERR	I	EV_SEVERITY_WARNING	LRT unable to register port parameters with FC stack. Most likely due to failed board or FC stack error. Group number is valueName1. Tx port for the group is platformPortNum	
58031	LRT_ROUTING_FAILED_ERR	I	EV_SEVERITY_WARNING	LRT unable to setup routing for a port. Group number is valueName1. Failed port is platformPortNum.	
58032	LRT_GROUP_WRONG_STATE_FOR_SETUP	I	EV_SEVERITY_WARNING	LRT found group in wrong state for setup command. Group number is valueName1.	
58033	LRT_SEND_IU_FAILED_ERR	I	EV_SEVERITY_WARNING	LRT unable to send test frame to FC stack for transmission. First port of the failed group is identified.	
58034	LRT_SND_IU_RSP_RCVD_WRONG_STATE	I	EV_SEVERITY_WARNING	LRT response to Send IU not expected in this state.	
58035	LRT_SETUP_STACK_UNEXPECT_RSPERR	I	EV_SEVERITY_BUG	LRT response to setup send IU not expected in this state.	
58036	LRT_PROCESSOR_ROUTING_RSP_ERR	I	EV_SEVERITY_WARNING	LRT reports that routing service has returned an error. Error is failedValue. Failed port is identified.	
58037	LRT_STATUS_EARLY_REQ_ERR	I	EV_SEVERITY_WARNING	LRT response to status request not expected yet.	
58038	LRT_STATS_COLL_NO_BOARDS_ONLINE	E	EV_SEVERITY_INFO	LRT cannot be run because there are no boards in the system. LRT has been setup to run, but no boards are currently in the system.	
58039	FI_FC_PORT_FORCED_OFFLINE	E	EV_SEVERITY_ERROR	Fault Isolation has forced a port offline.	Retrieve debug backup logs and call technical support.
59001	XBAR_UNEXPECTED_CYCLONE_ERROR	I	EV_SEVERITY_ERROR	Unexpected Cyclone Error	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59002	XBAR_MSG_STORE_FULL	I	EV_SEVERITY_ERROR	XBAR message store full.	
59003	XBAR_WRN_TOKEN_WRITE_FAILURE	I	EV_SEVERITY_WARNING	XBAR warning token write failure	
59004	XBAR_WRN_TOKEN_READ_FAILURE	I	EV_SEVERITY_WARNING	XBAR warning token read failure.	
59005	XBAR_ERR_TOKEN_READ_FAILURE	I	EV_SEVERITY_ERROR	XBAR error token read failure.	
59006	XBAR_ERR_TOKEN_WRITE_FAILURE	I	EV_SEVERITY_ERROR	XBAR error token write failure.	
59007	XBAR_ERR_XBAR_TOKEN_PARITY	I	EV_SEVERITY_WARNING	XBAR error crossbar token parity failure.	
59008	XBAR_XBAR_TOKEN_FIFO_FULL_RCV1	I	EV_SEVERITY_WARNING	XBAR crossbar token FIFO full error.	
59009	XBAR_XBAR_TOKEN_FIFO_FULL_XMT_L	I	EV_SEVERITY_WARNING	XBAR error crossbar token FIFO full local transmit error.	
59010	XBAR_XBAR_TOKEN_FIFO_FULL_XMIT1	I	EV_SEVERITY_WARNING	XBAR error crossbar token FIFO full.	
59011	XBAR_ERR_MISSING_TOKEN_RESPONSE	I	EV_SEVERITY_WARNING	XBAR error missing token response: software induced error. FailedValue field identifies the source file; valueName1 contains the line number where the error originated. ValueName2 contains the original error code value.	
59012	XBAR_WRN_UPIF_UNSOLICITED_TOKEN	I	EV_SEVERITY_WARNING	XBAR warning UPIF unsolicited token.	
59013	XBAR_WRN_UPIF_TOKEN_PARITY	I	EV_SEVERITY_WARNING	XBAR warning UPIF token parity.	
59014	XBAR_ERR_ARB_TOKEN_PARITY	I	EV_SEVERITY_WARNING	XBAR error arbitration token parity.	
59015	XBAR_ERR_ARB_TOKEN_TAG	I	EV_SEVERITY_WARNING	XBAR error arbitration token tag.	
59016	XBAR_ARB_TOKEN_FIFO_FULL_RCV1	I	EV_SEVERITY_WARNING	XBAR error arbitration token FIFO full Receiver1.	
59017	XBAR_ARB_TOKEN_FIFO_FULL_RCV0	I	EV_SEVERITY_WARNING	XBAR error arbitration token FIFO full Receiver0.	
59018	XBAR_ARB_TOKEN_FIFO_FULL_XMT_L	I	EV_SEVERITY_WARNING	XBAR error arbitration token FIFO full Transmit Local.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59019	XBAR_ARB_TOKEN_FIFO_FULL_XMIT1	I	EV_SEVERITY_WARNING	XBAR error arbitration token FIFO full Transmitter 1.	
59020	XBAR_ARB_TOKEN_FIFO_FULL_XMIT0	I	EV_SEVERITY_WARNING	XBAR error arbitration token FIFO full transmitter 0.	
59021	XBAR_ERR_TOKENRING_TIMEOUT	I	EV_SEVERITY_WARNING	XBAR errorTOKEN RING timeout.	
59022	XBAR_WRN_PQ_TOKEN_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning PQ token FIFO full.:	
59023	XBAR_ERR_PQ_TOKEN_PARITY	I	EV_SEVERITY_WARNING	XBAR error PQ token parity.	
59024	XBAR_WRN_MS_TOKEN_TX_FULL	I	EV_SEVERITY_WARNING	XBAR warning MS token TRANSMIT full.	
59025	XBAR_WRN_MS_TOKEN_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning MS token FIFO full.	
59026	XBAR_WRN_MS_UP_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning MS UP FIFO full.	
59027	XBAR_WRN_MS_POLL_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning MS FIFO full.	
59028	XBAR_ERR_MS_TOKEN_PARITY	I	EV_SEVERITY_WARNING	XBAR error MS token parity.	
59029	XBAR_ERR_MS_INBAND_TX_FULL	I	EV_SEVERITY_WARNING	XBAR error inband transmit full.	
59030	XBAR_ERR_MS_INBAND_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR error MS inband FIFO full.	
59031	XBAR_WRN_MS_UP_RX_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning MS UP Receive FIFO full.	
59032	XBAR_WRN_FIFO_SEND_REGS	I	EV_SEVERITY_WARNING	XBAR warning FIFO send registers.	
59033	XBAR_WRN_FIFO_RECV_REGS	I	EV_SEVERITY_WARNING	XBAR warning FIFO receive registers.	
59034	XBAR_WRN_FLUSH_FIFO_REGS	I	EV_SEVERITY_WARNING	XBAR warning flush FIFO registers.	
59035	XBAR_WRN_PQ_INBAND_RX_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning PQ inband receive FIFO full.	
59036	XBAR_WRN_PQ_POLL_FIFO_FULL	I	EV_SEVERITY_WARNING	XBAR warning PQ poll FIFO full.	
59037	XBAR_ERR_SEQUENCE_SYSCFG	I	EV_SEVERITY_ERROR	XBAR error sequence system config.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59038	XBAR_ERR_HALTED_SYSCFG	I	EV_SEVERITY_ERROR	XBAR error halted system config: software induced error. FailedValue field identifies the source file; valueName1 contains the line number where the error originated. ValueName2 contains the original error code value.	
59039	XBAR_ERR_EMPTY_SYSCFG	I	EV_SEVERITY_ERROR	XBAR errors empty system config.	
59040	XBAR_ERR_DISABLED_CARDID	I	EV_SEVERITY_ERROR	XBAR error disabled card ID.	
59041	XBAR_ERR_CFGCTRLMSG_STATE	I	EV_SEVERITY_WARNING	XBAR error config control message state.	
59042	XBAR_ERR_ACCESS_SLOTID	I	EV_SEVERITY_ERROR	XBAR error accessing board slot id.	
59043	XBAR_ERR_PORTCARD_TASK_FAILED	I	EV_SEVERITY_CRITICAL	XBAR error portcard task has failed.	
59044	XBAR_ERR_PORTCARD_TASK_MISSING	I	EV_SEVERITY_BUG	XBAR error portcard task not allocated.	
59045	XBAR_WRN_POLLTIME_EXCEEDS_RATE	I	EV_SEVERITY_BUG	XBAR warning poll time exceeds poll rate.	
59046	XBAR_WRN_POLL_RATE	I	EV_SEVERITY_BUG	XBAR warning poll rate.	
59047	XBAR_ERR_PQ_CE8	I	EV_SEVERITY_WARNING	XBAR PQ chip error: ce_8 err indicates that the 8ns clock between chips has been invalid for at least 1 cycle.	
59048	XBAR_ERR_MS_CE8	I	EV_SEVERITY_WARNING	XBAR MS chip error: ce_8 err indicates that the 8ns clock between chips has been invalid for at least 1 cycle. FailedValue field identifies the source file; valueName1 contains descriptive text. ValueName2 contains the original error code value.	
59049	XBAR_ERR_ARB_CE8	I	EV_SEVERITY_WARNING	XBAR ARB chip err: ce_8 err indicates that the 8ns clock between chips has been invalid for at least 1 cycle.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59050	XBAR_ERR_XBAR_CE8	I	EV_SEVERITY_WARNING	XBAR chip err: ce_8 err indicates that the 8ns clock between chips has been invalid for at least 1 cycle.	
59051	XBAR_WRN_PQ_CSU_PLL_STATUS	I	EV_SEVERITY_CRITICAL	XBAR PQ Clock Synthesis Unit Phase-Locked Loop Status Register. PLL loss of lock status for the group of eight transmit links and receive links.	
59052	XBAR_WRN_MS_CSU_PLL_STATUS	I	EV_SEVERITY_CRITICAL	XBAR MS Clock Synthesis Unit Phase-Locked Loop Status Register. PLL loss of lock status for the group of eight transmit links and receive links. Current PLL status is returned in extra bytes 5 and 6; prev PLL in bytes 7 and 8. (reg = 245, bits 0-7)	
59053	XBAR_WRN_ARB_CSU_PLL_STATUS	I	EV_SEVERITY_CRITICAL	XBAR ARB Clock Synthesis Unit Phase-Locked Loop Status Register. PLL loss of lock status for the group of eight transmit links and receive links. Current PLL status is returned in extra bytes 5 and 6; prev PLL in bytes 7 and 8. (reg = 245, bits 0-7)	
59054	XBAR_WRN_XBAR_CSU_PLL_STATUS	I	EV_SEVERITY_CRITICAL	XBAR Clock Synthesis Unit Phase-Locked Loop Status Register. PLL loss of lock status for the group of eight transmit links and receive links. Current PLL status is returned in extra bytes 5 and 6; prev PLL in bytes 7 and 8. (reg = 245, bits 0-7)	
59055	XBAR_ERR_PLL_LOCK_STATUS	I	EV_SEVERITY_CRITICAL	XBAR PLL Clock Loss of Lock encountered during startup. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=PLL status reg 246; 6=PLL status reg 245	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59056	XBAR_MS_LINK_STATUS	I	EV_SEVERITY_WARNING	XBAR MS link status. Status = EV_FAIL indicates error rates have exceeded threshold for a data link; EV_SUCCESS = MS link cleared.	
59057	XBAR_MS_CHANNEL_EXOFF_Q2MS_STAT	I	EV_SEVERITY_WARNING	XBAR Q2MS Emergency XOFF per channel. EV_FAIL =error condition; EV_SUCCESS = error cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel	
59058	XBAR_MS_CHAN_EXOFF_CTL_PID_FIFO	I	EV_SEVERITY_WARNING	XBAR CTL Pid FIFO Emergency XOFF per channel as indicated when operating as fMS. EV_FAIL=error condition; EV_SUCCESS = error cleared.Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel	
59059	XBAR_MS_CHANNEL_EXOFF_IC_IS	I	EV_SEVERITY_WARNING	XBAR Emergency XOFF in one of the IC_IS cell counters. EV_FAIL=error condition; EV_SUCCESS = error cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type	
59060	XBAR_MS_XOFF_IC_IS_STATUS	I	EV_SEVERITY_WARNING	XBAR chip stat. For iMS, level 1 XOFF stat bit is set for indicated channel/ subchannel. IC_IS XOFF results in NOT RDY for the indicated input chan/ subchan. EV_FAIL=error;EV_SUCCESS=cleared.Info: 1=slot; 2=card; 3=chip id; 4=chip type; 5=channel; 6=subchan	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59061	XBAR_MS_XOFF_COS_ STATUS	I	EV_SEVERITY _WARNING	XBAR chip stat. For eMS, COS flow control status bit set for indicated channel/ COS. EV_FAIL=error;EV_SUCC ESS=cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel; 6=COS	
59062	XBAR_WRN_MS_COUNT ER_XOFF_STATUS	I	EV_SEVERITY _WARNING	XBAR chip stat. XOFF status bit set for counter XON/XOFF flow control. EV_FAIL=error;EV_SUCC ESS=cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=counter (0-31)	
59063	XBAR_ERR_ARB_LINK	I	EV_SEVERITY _WARNING	XBAR chip stat. Error rates have exceeded threshold for control link. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=link #; 6=0:persistent, 6=1:transient; 7=high reg 253; 8=low reg 252	
59064	XBAR_ERR_ARB_PERM ANENT_LINK_STA	I	EV_SEVERITY _WARNING	XBAR chip stat. Link failure exists on a (accept stream) link from an Arbiter to a PQ. EV_FAIL=error; EV_SUCCESS= cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=link #; 6=0:persistent, 6=1:transient; 7=high reg 253; 8=low reg 252	
59065	XBAR_ERR_XBAR_LINK _STATUS	I	EV_SEVERITY _WARNING	XBAR chip stat. Error rates have exceeded threshold for data link. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=link #; 6=0:persistent, 6=1:transient; 7=high reg 253; 8=low reg 252	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59066	XBAR_ERR_PQ_PORT_ XOFF_STATUS	I	EV_SEVERITY _WARNING	XBAR chip stat. A second level port XOFF was generated from one or more channels. EV_FAIL=error; EV_SUCCESS= cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=lphysical channel flags (0,1,2,3)	
59067	XBAR_ERR_PQ_EMERG ENCY_XOFF_STAT	I	EV_SEVERITY _WARNING	XBAR chip stat. A third level emergency XOFF was generated from one or more channels. EV_FAIL=error; EV_SUCCESS= cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=lphysical channel flags (0,1,2,3)	
59068	XBAR_ERR_PQ_CHANN EL_XOFF_STATUS	I	EV_SEVERITY _WARNING	XBAR chip stat.A first level channel XOFF was generated from one or more channels. EV_FAIL=error; EV_SUCCESS= cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=lphysical channel flags (0,1,2,3)	
59069	XBAR_ERR_PQ_LINK_S TATUS	I	EV_SEVERITY _WARNING	XBAR chip stat.Error rates have exceeded threshold for control link. EV_FAIL=error; EV_SUCCESS= cleared. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=link #; 6=0:persistent, 6=1:transient; 7=high reg 253; 8=low reg 252	
59070	XBAR_ERR_INCORREC T_STATE	I	EV_SEVERITY _ERROR	XBAR error: Operation cannot be executed due to incorrect state.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59071	XBAR_ERR_BAD_PARAMETER	I	EV_SEVERITY_WARNING	XBAR error: Function was passed with bad parameter. This will be categorized as 'internal' after development completes.	
59072	XBAR_WRN_LOAD_REBALANCED	I	EV_SEVERITY_INFO	XBAR event. System diagnostic message sent when the system load balance is recalculated. Returns the previous and new primary Arbiter and primary PQ card IDs. Used for informational purposes only.	
59073	XBAR_WRN_PORTCARDS_ASSIGNED	I	EV_SEVERITY_INFO	System diagnostic message sent when the system load balance is recalculated. Sent for every configured switch card on the system returning the port card assignments for each switch card. Used for informational purposes only.	
59074	XBAR_ERR_DELAY_XBAR_DATALINK	I	EV_SEVERITY_ERROR	XBAR chip error. Delay value not found or out of range for Crossbar chip link. Delay set to 0. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=link id; 6=computed delay value; 7=best link delay range start	
59075	XBAR_WRN_PQ_GPIO_READ	I	EV_SEVERITY_WARNING	XBAR event: Reflects the state of the gpio[7:0] pins whether they are configured for input or output.Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=GPIO Read register [7:0]	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59076	XBAR_ERR_PQ_DISABLED_QUEUE	I	EV_SEVERITY_WARNING	XBAR chip event. Chip reports that an attempt was made to queue a PID to a disabled queue; the PID was diverted to the lowest numbered enabled queue. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel (0,1,2,3)	
59077	XBAR_ERR_PQ_QUEUE_OVERFLOW_CELL	I	EV_SEVERITY_WARNING	XBAR event. chip reports that an attempt was made to queue a PID to a full queue; the packet record was dropped causing the packet to be lost in the MS. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel (0,1,2,3)	
59078	XBAR_ERR_PQ_UNCORRECTABLE_BIT	I	EV_SEVERITY_WARNING	XBAR chip event. An uncorrected bit error was detected; the packet record was dropped causing the packet to be lost in the MS.Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel (0,1,2,3)	
59079	XBAR_ERR_PQ_CORRECTED_BIT_ERROR	I	EV_SEVERITY_WARNING	XBAR chip event. A single bit in the COSQ SRAM was corrected.nfo bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=physical channel (0,1,2,3)	
59080	XBAR_ERR_PQ_CONTROL_LINK_PARITY	I	EV_SEVERITY_WARNING	XBAR chip event. Indicates a parity error was detected on a control link. Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5=control link.	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59081	XBAR_ERR_PQ_CRDT_ CNTR_SYNCH_INC	I	EV_SEVERITY _ERROR	XBAR chip error: PQ credit controller sync incomplete. Credit counter synchronization did not complete within expected number of retries.Info bytes: 1=slot; 2=card; 3=chip id; 4=chip type; 5&6=credit counter resynch address	
59082	XBAR_ERR_PQ_BYTE_S LIP_DETECT	I	EV_SEVERITY _WARNING	XBAR chip error: PQ byte slip detected on the primary arbiter link. Indicates that the PQ and MS may be out of sync causing packets to be lost and misdelivered. The new sync offset written to reg 6 bits 1-3 for the link.	
59083	XBAR_ERR_PQ_CHIP_N OT_OPERATIONL	I	EV_SEVERITY _CRITICAL	XBAR chip error: PQ chip not operational.	
59084	XBAR_ERR_PQ_COUNT ER_TIMEOUT	I	EV_SEVERITY _WARNING	XBAR chip error: PQ credit counter watchdog timer expired. At least one counter has 0 credits and 0 credits were received within watchdog interval configured in regs 0xA9-0xA8.	
59085	XBAR_WRN_PQ_RESYN C_TIMEOUT_CNTR	I	EV_SEVERITY _WARNING	XBAR chip error: PS counter resynch due to credit counter timeout state reported by PQ High Priority Message register 0xFE bit[2]	
59086	XBAR_ERR_MS_INVALID _OUT_SUBCHAN	I	EV_SEVERITY _WARNING	XBAR MS chip error: Number of packets that were dropped because of a invalid output sub-channels. Accumulated count stored in OPTERRORINFO.dwOptAccValue. (reg 180, bits 0-7)	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59087	XBAR_ERR_INVALID_OUTPUT_CHANELS	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of packets that were dropped because of a invalid output channels. Accumulated count stored in OPTERRORINFO.dwOptAccValue. (reg 179, bits 0-7)	
59088	XBAR_ERR_MS_INVALID_OUT_PORTS	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of packets that were dropped because of a invalid output ports. Accumulated count stored in OPTERRORINFO.dwOptAccValue. (reg 178, bits 0-7)	
59089	XBAR_WRN_MS_SHORT_PACKET	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of short packets received. Accumulated count stored in OPTERRORINFO.dwOptAccValue. (reg 152, bits 0-7)	
59090	XBAR_WRN_MS_IMT_UCAST_PKT_DROP	I	EV_SEVERITY_ERROR	XBAR MS chip error: Number of unicast packets dropped by the ISM. Accumulated count stored in OPTERRORINFO.dwOptAccValue. (reg 150, bits 0-7)	
59091	XBAR_ERR_MS_MULT_INVALID_PID	I	EV_SEVERITY_ERROR	XBAR MS chip error: Multiple PID request. (reg 146, bit 2)	
59092	XBAR_ERR_MS_INVALID_PID_REQUEST	I	EV_SEVERITY_ERROR	XBAR MS chip error: Invalid PID request; PID request received while a packet is being sent. (reg 146, bit 1)	
59093	XBAR_ERR_MS_INVALID_PID	I	EV_SEVERITY_ERROR	XBAR MS chip error: Invalid PID; received a PID with a value of 0. (reg 146, bit 0)	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59094	XBAR_ERR_MS_OMT_SINGLEBIT	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of single bit errors which occurred on a read from the OMT.Accumulated count stored in OPTERRORINFO.dwOptAccValue. (reg 145, bits 0-7)	
59095	XBAR_ERR_MS_OMT_DOUBLEBIT	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of double bit errors which occurred on a read from the OMT. Accumulated count stored in OPTERRORINFO.dwOptAccValue. ERR_MS_OMT_DOUBLEBIT(reg 144, bits 0-7)	
59096	XBAR_WRN_MS_NO_SOP	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of times start of packet not received.Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 137, bits 0-7)	
59097	XBAR_WRN_MS_NO_EOP	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of times end of packet not received.Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 136, bits 0-7)	
59098	XBAR_WRN_MS_IMT_MCAST_PKT_DROP	I	EV_SEVERITY_BUG	XBAR MS chip error: Number of multicast packets dropped by the ISM.Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 135, bits 0-7)	
59099	XBAR_ERR_MS_IMT_SINGLEBIT	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of single bit errors which occurred on a read from the IMT Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 132, bits 0-7)	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59100	XBAR_ERR_MS_IMT_DOUBLEBIT	I	EV_SEVERITY_WARNING	XBAR MS chip error: Number of double bit errors which occurred on a read from the IMT. Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 131, bits 0-7)	
59101	XBAR_ERR_MS_FIFO_PARITY_CELL	I	EV_SEVERITY_ERROR	XBAR MS chip error: Number of parity errors which occurred on PIDs read from the FIFO Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 130, bits 0-7)	
59102	XBAR_ERR_MS_CELL_LIST_PARITY	I	EV_SEVERITY_ERROR	XBAR MS chip error: Number of parity errors which occurred on a cell list read Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 129, bits 0-7)	
59103	XBAR_ERR_MS_CELL_FREELIST_PARIT	I	EV_SEVERITY_ERROR	XBAR MS chip error: Number of parity errors which occurred on a cell free list read Accumulated count stored in OPTERRORINFO.dwOptAccValue.(reg 128, bits 0-7)	
59104	XBAR_ERR_MS_CHIP_NOT_OPERATIONL	I	EV_SEVERITY_CRITICAL	XBAR MS chip error: MS chip not operational error.	
59105	XBAR_WRN_ARB_STEADYSTATE_RESYNC	I	EV_SEVERITY_ERROR	XBAR MS chip error: Steady-State Resync - an arbiter in secondary mode has resynchronized to a primary PQ while in steady-state operation (reg 200, bit 3)	
59106	XBAR_ERR_ARB_LINK_TRANSITION	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: A control link has transitioned from bad to good. The link has actually been determined to be bad by the firmware and is treated as such. (reg 247-250 0xF7-0xFA, bits 0-7)	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59107	XBAR_ERR_ARB_CHIP_NOT_OPERATION	I	EV_SEVERITY_CRITICAL	XBAR arbiter chip error: Arbiter chip not operational error.(reg 255 0xff, bit 7)	
59108	XBAR_ERR_ARB_LINK_SYNC	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: A corresponding iPQ link has failed to synchronize with the primary Arbiter.(reg 224-227 0xE0-0xE3, bits 0-7)	
59109	XBAR_ERR_NOSYNC_ENABLED_CARDID	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: Arbiter did not synchronize the configured and enabled port card.	
59110	XBAR_ERR_PRIM_PORTSEL_CTRLLINK	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: No common (error-free) arbiter control link is available for primary port selection.	
59111	XBAR_ERR_PRIMARBSEL	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: No suitable arbiter found to select as system primary arbiter.	
59112	XBAR_ERR_PQ_I_DRAIN_UNAVAIL_PRT	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: Data was detected queued to an unavailable port; iPQ port/channel drained.	
59113	XBAR_ERR_VALUE_CHIPREG	I	EV_SEVERITY_ERROR	XBAR arbiter chip error: Unexpected value retrieved from indicated chip register.	
59114	XBAR_ERR_AVAIL_CTRLLINK	I	EV_SEVERITY_ERROR	XBAR chip error: No available (error-free) control links in arbiter.	
59115	XBAR_ERR_RESPONSE_TIMEOUT	I	EV_SEVERITY_ERROR	XBAR error: An operation did not complete within the expected time.	
59116	XBAR_WRN_CBFC_CONFIG_UPDATED	I	EV_SEVERITY_INFO	XBAR config was modified: iPQ credits for encoder/decoder, eMS credit encoder, and ARB link select updated.	
59117	XBAR_WRN_MS_EMPTY_TIMEOUT	I	EV_SEVERITY_WARNING	XBAR error: During shutdown, a MS did not empty its cells within the expected time	

Table 24. Event codes (Continued)

EC	Name	Type	Severity	Description	Action
59118	XBAR_ERR_PQ_I_FAILED_TO_DRAIN	I	EV_SEVERITY_ERROR	XBAR error: A queue failed to drain completely during an iPQ drain operation.	
59119	XBAR_ERR_MS_FAILED_COSXOFF_CTRS	I	EV_SEVERITY_ERROR	XBAR error: Failed to reset the MS COSXOFF counters most likely due to the inability to empty the MS of existing cells.	
59120	XBAR_WRN_MS_RESET_COSXOFF_CNTRS	I	EV_SEVERITY_INFO	XBAR error: Successfully reset the MS COSXOFF counters.	
59121	XBAR_ERR_CFGCTRLMSG_INPROGRESS	I	EV_SEVERITY_INFO	XBAR error: Previous configuration or switch fabric control message is still in progress	
59122	XBAR_WRN_SLOT_EVENT_CONNECT	I	EV_SEVERITY_ERROR	XBAR error: Connectivity to slot re-established.	
59123	XBAR_WRN_SLOT_EVENT_DISCONNECT	I	EV_SEVERITY_CRITICAL	XBAR error: Lost connectivity to slot.	
59124	XBAR_ERR_UNKNOWN_STATE_CARDID	I	EV_SEVERITY_ERROR	XBAR error: Configured card placed in unknown state because it is not accessible.	
59125	XBAR_UNDECODED_CYCLONE_ERROR	I	EV_SEVERITY_ERROR	XBAR error yet to be decoded.	
59126	XBAR_CYCLONE_FW_RSP_ERROR	I	EV_SEVERITY_ERROR	XBAR cyclone firmware error response received. Command is specified in the failedValue enumeration.	

Glossary

A

ACC. Accept Link Service reply. Accept is the normal reply to an Extended Link Service request (such as FLOGI) and indicates that the request has been completed.

ACK. Acknowledgement Frame. An ACK is used for end-to-end flow control. An ACK is sent to verify receipt of one or more frames in Class 1 and Class 2 Services.

Address Identifier. A 3-byte value typically assigned by the Fabric used to address an N_Port. Used in frames in the S_ID (source identifier) and D_ID (destination identifier) fields.

AL_PA. Arbitrated Loop Physical Address. A 1-byte value used in the Arbitrated Loop topology used to identify L_Ports. This value will then also become the last byte of the address identifier for each public L_Port on the loop.

AL_TIME. Arbitrated Loop Time-out value. Twice the amount of time it would take for a Transmission Word to propagate around a worst-case Loop, i.e. a Loop with 134 L_Ports and 10 km links between each L_Port, with a 6 Transmission Word delay through each L_Port. This value is set at 15 ms.

ARB. Arbitrate Primitive Signal. This Primitive Signal applies only to the Arbitrated Loop topology. It is transmitted as the Fill Word by an L_Port to indicate that the L_Port is arbitrating to access to the Loop.

B

BB_Credit. Buffer-to-buffer credit value. Used for buffer-to-buffer flow control, this determines the number of frame buffers available in the port it is attached to, i.e., the maximum number of frames it may transmit without receiving an R_RDY.

BP. FCM Boot Prom Program.

C

Class 1 Service. A method of communicating between N_Ports in which a dedicated connection is established between them. The ports are guaranteed the full bandwidth of the connection and frames from other N_Ports may be blocked while the connection exists. In-order delivery of frames is guaranteed. Uses end-to-end flow control only.

Class 2 Service. A method of communicating between N_Ports in which no connection is established. Frames are acknowledged by the receiver. Frames are routed through the Fabric, and each frame may take a different route. In-order delivery of frames is not guaranteed. Uses both buffer-to-buffer flow and end-to-end flow control.

Class 3 Service.A method of communicating between N_Ports similar to Class 2 service, except there is no acknowledgment of received frames. Frames are routed through the Fabric as in Class 2, and in-order delivery is not guaranteed. Uses only buffer-to-buffer flow control.

CLS. Close Primitive Signal. This Primitive Signal applies only to the Arbitrated Loop topology. It is Primitive Signal is sent by an L_Port which is currently communicating on the Loop (i.e., it has won access to the loop or was opened by another L_Port which had won access to the Loop) to close communication with the other L_Port.

D

D_ID. Destination identifier. A 3-byte field in the frame header used to indicate the address identifier of the N_Port the frame is to be delivered to.

Disparity. The difference between the number of 1's and 0's in a Transmission Character. A Transmission Character with more 1's than 0's is said to have positive running disparity. A Transmission Character with more 0's than 1's is said to have negative running disparity. A Transmission Character with an equal number of 1's and 0's is said to have neutral disparity.

E

E_D_TOV. Error Detect Time-out value. A timer used to represent the longest possible time for a frame to make a round trip through the Fabric. This value is negotiated at N_Port Login and will typically be on the order of a few seconds. E_D_TOV is used to decide when some particular error recovery action must be taken.

EE_Credit. End-to-end credit value. Used for end-to-end flow control, determines the maximum number of frames that may remain unacknowledged.

EOF. End of Frame delimiter. This Ordered Set is always the last Transmission Word of a Frame. It is used to indicate that a Frame has ended and indicates whether the Frame is valid or invalid.

Exchange. The highest level Fibre Channel mechanism used for communication between N_Ports. Exchanges are composed of one or more related sequences. Exchanges may be bidirectional or unidirectional.

F

Fabric. One of the three Fibre Channel topologies. In the Fabric topology, N_Ports are connected to F_Ports on a switch. Depending on vendor support, fabric switches may be interconnected to support up to 16 million+ N_Ports on a single network.

© Copyright IBM Corp. 2004

FB. FCM Flash Boot program.

F_BSY. Fabric Port Busy Frame. This Frame is issued by the Fabric to indicate that a particular cannot be delivered because the Fabric or the destination N_Port is too busy.

FC_AL. Fibre Channel Arbitrated Loop. Refers to the ANSI FC-AL document which specifies operation of the Arbitrated Loop topology.

FC_PH. Fibre Channel Physical and Signaling Interface. Refers to the ANSI FC-PH document which specifies the FC-0, FC-1, and FC-2 layers of the Fibre Channel protocol. FC-0 Fibre Channel layer 0. Specifies the physical signalling used in Fibre Channel, as well as cable plants, media types, and transmission speeds.

FC-1. Fibre Channel layer 1. Specifies the IBM patented 8B/10B data encoding used in Fibre Channel.

FC-2. Fibre Channel layer 2. Specifies the frame format, Sequence/Exchange management, and Ordered Set usage in Fibre Channel.

FC-3. Fibre Channel layer 3. Specifies services provided for multiple N_Ports in a single node.

FC-4. Fibre Channel layer 4. Specifies mapping of Upper Level Protocols such as SCSI and IP onto the Fibre Channel Protocol.

FICON Mode. The purpose of FICON mode is to enable FC-SB-2 specific formatting for some of the ELS's. FICON mode requires PIM to be enabled. Currently, with FICON mode enabled, RNID responses are formatted as per SB-2 which varies from open systems versions of fibre channel.

Fill Word. The Primitive Signal is used by L_Ports to be transmitted in between Frames. This may be Idle or ARBx, depending on which, if any, L_Ports are Arbitrating for Loop access, and will not necessarily be the same for all L_Ports on the Loop at any given time.

F/NL_Port. An NL_Port which is capable of providing certain Fabric services to other NL_Ports on a Loop in the absence of a Fabric. This NL_Port will respond to requests to open communication with AL_PA hex'00', even though it may actually have another value for its AL_PA.

F_Port. Fabric port. A port on a fabric switch to which N_Ports may be directly connected. An F_Port is uses the address identifier hex'FFFFFE'.

Frame. The basic unit of communication between two N_Ports. Frames are composed of a starting delimiter (SOF), a header, the payload, the Cyclic Redundancy Check (CRC), and an ending delimiter (EOF). The SOF and EOF contain the Special Character and are used to indicate where the frame begins and ends. The 24-byte header contains information about the frame, including the S_ID, D_ID, routing information, the type of data contained in the payload, and sequence/exchange management information. The payload contains the actual data to be transmitted, and may be 0-2112 bytes in length. The CRC is a 4-byte field used for detecting bit errors in the received frame.

F_RJT. Fabric Port Reject Frame. This Frame is issued by the Fabric to indicate that delivery of a particular frame is being denied. Some reasons for issuing an F_RJT include: Class not supported; invalid header field(s); and N_Port unavailable.

H

HSSDC. High Speed Serial Data Connector cable is a duplex cable assembly where both the transmit and receive contacts are part of the same keyed plug assembly.

I

Idle. An Ordered Set transmitted continuously over a link when no data are being transmitted. Idle is transmitted to maintain an active link over a fibre and lets the receiver and transmitted maintain bit, byte, and word synchronization.

Intermix. A service in which Class 2 and Class 3 frames may be delivered to an N_Port which has a Class 1 dedicated connection open. The Class 2 and 3 frames are delivered during times which no Class 1 frames are being delivered on the connection.

L

Link Service. Link Services are facilities used between an N_Port and a Fabric or between two N_Ports and are used to for such purposes as Login, Sequence and Exchange management, and maintaining connections.

LIP. Loop Initialization Primitive Sequence. This Primitive Sequence applies only to the Arbitrated Loop topology. It is transmitted by an L_Port to (re)initialize the Loop.

LIFA. Loop Initialization Fabric Assigned Frame. This is the first Frame transmitted in the Loop initialization process after a temporary Loop master has been selected. L_Ports which have been assigned their AL_PA by the Fabric will select their AL_PA's in this frame as it makes its way around the Loop.

LIHA. Loop Initialization Hard Assigned Frame. This is the third Frame transmitted in the Loop initialization process after a temporary Loop master has been selected. L_Ports which have been programmed to select a particular AL_PA (if available) by the manufacturer will select their AL_PA's in this frame as it makes its way around the Loop.

LILP. Loop Initialization Loop Position Frame. This is the second Frame transmitted in the Loop initialization process after all L_Ports have selected an AL_PA (after LISA has been around the loop). This Frame is transmitted around the Loop so that all L_Ports may know the relative position of all other L_Ports around the Loop. Support for this Frame by an L_Port is optional.

LIPA. Loop Initialization Previously Assigned Frame. This is the second Frame transmitted in the Loop initialization process after a temporary Loop master has been selected. L_Ports which had an AL_PA prior to the Loop initialization will select their AL_PA's in this frame as it makes its way around the Loop.

LIRP. Loop Initialization Report Position Frame. This is the first Frame transmitted in the Loop initialization process after all L_Ports have selected an AL_PA (after LISA has been around the loop). This Frame is transmitted around the Loop so that all L_Ports report their relative physical position on the loop. Support for this Frame by an L_Port is optional.

LISA. Loop Initialization Soft Assigned Frame. This is the fourth Frame transmitted in the Loop initialization process after a temporary Loop master has been selected. L_Ports which did not select an AL_PA in any of the previous Loop Initialization Frames (LIFA, LIPA, or LIHA) will select their AL_PA's in this frame as it makes its way around the Loop.

LISM. Loop Initialization Select Master Frame. This Frame applies only to the Arbitrated Loop topology. It is the first frame transmitted in the initialization process in which L_Ports select an AL_PA. It is used to select a temporary Loop master, or the L_Port that will subsequently initiate transmission of the remaining initialization frames (LIFA, LIPA, LIHA, LISA, LIRP, and LILP).

LPB. Loop Port Bypass Primitive Sequence. This Primitive Sequence applies only to the Arbitrated Loop topology. It is transmitted by an L_Port to bypass the L_Port it is directed to. For example, if Port A suspects that Port B is malfunctioning, Port A can send an LPB to Port B so that Port B will only retransmit everything it receives, and will not be active on the Loop.

LPE. Loop Port Enable Primitive Sequence. This Primitive Sequence applies only to the Arbitrated Loop topology. It is transmitted by an L_Port to enable an L_Port which has been bypassed with the LPB Primitive Sequence.

LPSM. Loop Port State Machine. This is a state machine maintained by an L_Port to track its behavior through different phases of Loop operation, i.e., how it behaves when it is arbitrating for Loop access, how it behaves when it has control of the Loop, etc.

LR. Link Reset Primitive Sequence. This Primitive Sequence is used during link initialization between two N_Ports in the Point-to-point topology or an N_Port and an F_Port in the Fabric topology. The expected response to a port sending LR is the LRR Primitive Sequence.

LRR. Link Reset Response Primitive Sequence. This Primitive Sequence is used during link initialization between two N_Ports in the Point-to-point topology or an N_Port and an F_Port in the Fabric topology. It is sent in response to the LR Primitive Sequence. The expected response to a port sending LRR is Idle.

LRT. Link Rate Test.

M

MRK. Mark Primitive Signal. This Primitive Signal applies only to the Arbitrated Loop topology. It is transmitted by an L_Port for synchronization purposes and its use is vendor specific.

N

NL_Port. Node-Loop port. An N_Port which can operate on the Arbitrated Loop topology.

Nonparticipating Mode. An L_Port will enter the nonparticipating mode if there are more than 127 devices on a Loop, and it thus cannot acquire an AL_PA. An L_Port may also voluntarily enter the nonparticipating mode if it is still physically connected to the Loop, but wishes not to participate. An L_Port in the nonparticipating mode is not capable of generating Transmission Words on the Loop and may only retransmit words received on its inbound fibre.

NOS. Not Operational Primitive Sequence. This Primitive Sequence is used during link initialization between two N_Ports in the Point-to-point topology or an N_Port and an F_Port in the Fabric topology. It is sent to indicate that the transmitting port has detected a link failure or is offline. The expected response to a port sending NOS is the OLS Primitive Sequence.

N_Port. Node port. A port on a computer, disk drive, etc. through which the device does its Fibre Channel communication.

N_Port Name. An 8-byte manufacturer-assigned value which uniquely identifies the N_Port throughout the world.

O

OLS. Offline Primitive Sequence. This Primitive Sequence is used during link initialization between two N_Ports in the Point-to-point topology or an N_Port and an F_Port in the Fabric topology. It is sent to indicate that the transmitting port is attempting to initialize the link, has recognized the NOS Primitive Sequence, or is going offline. The expected response to a port sending OLS is the LR Primitive Sequence.

OPN. Open Primitive Signal. This Primitive Signal applies only to the Arbitrated Loop topology. The OPN Primitive Signal is sent by an L_Port that has won the arbitration process to open communication with one or more other ports on the Loop.

Ordered Set. A 4-byte Transmission Word which has the Special Character as its first Transmission Character. An

Ordered Set may be a Frame Delimiter, a Primitive Signal, or a Primitive Sequence. Ordered Sets are used to distinguish Fibre Channel control information from data.

Originator. The N_Port which originated an Exchange.

OX_ID. Originator Exchange Identifier. A 2-byte field in the frame header used by the originator of an Exchange to identify frames as being part of a particular Exchange.

P

Participating Mode. The normal operating mode for an L_Port on a Loop. An L_Port in this mode has acquired an AL_PA and is capable of communicating on the Loop.

PB. Port Block is a single chassis containing 64 ports.

PIM. Protocol Intermix Mode: Note that PIM is always enabled when in E_Port mode. The intent of PIM is to allow the coexistence of both FICON and open systems traffic. Although the FC/9000 will allow open systems traffic with PIM either enabled or disabled, you should be aware that when it is enabled you are limited to single director configurations only (i.e., no cascading, single stage only). At the moment, FICON doesn't support cascading yet. We expect this restriction to be removed from the FC/9000 in a future release at least for open systems.

When PIM is enabled, the chassis ID numbering scheme does change. With PIM disabled, each board (FIO and FSW) takes up one chassis ID so a 64 port system would use a total of twelve chassis IDs. Once you enable PIM, a single FC/9000-64 chassis uses only ONE chassis ID (two for a 128 port director).

It's important to note that since PIM does affect the addressing scheme within the director, it is disruptive to any traffic passing through the box when it is enabled/ disabled. You would typically set this mode during installation and then leave it alone. This is why all these settings are intended to be changed only by trained service personnel in maintenance mode.

POST. Power On Self Test

Primitive Sequence. An Ordered Set transmitted repeatedly and used to establish and maintain a link. LR, LRR, NOS, and OLS are Primitive Sequences used to establish an active link in a connection between two N_Ports or an N_Port and an F_Port. LIP, LPB, and LPE are Primitive Sequences used in the Arbitrated Loop topology for initializing the Loop and enabling or disabling an L_Port.

Primitive Signal. An Ordered Set used to indicate an event. Idle and R_RDY are used in all three topologies. ARB, OPN, CLS, and MRK are used only in the Arbitrated Loop topology.

Private Loop. An Arbitrated Loop which stands on its own, i.e., it is not connected to a Fabric.

Private NL_Port. An NL_Port which only communicates with other ports on the loop, not with the Fabric. Note that a Private NL_Port may exist on either a Private Loop or a Public Loop.

Public Loop. An Arbitrated Loop which is connected to a Fabric.

Public NL_Port. An NL_Port which may communicate with other ports on the Loop.

Responder. The N_Port to with which an Exchange originator wishes to communicate.

RX_ID. Responder Exchange Identifier. A 2-byte field in the frame header used by the responder of the Exchange to identify frames as being part of a particular Exchange.

S

Sequence. A group of related frames transmitted unidirectionally from one N_Port to another.

SEQ_ID. Sequence Identifier. A 1-byte field in the frame header used to identify which Sequence of an Exchange a particular frame belongs to.

Sequence Initiator. The N_Port which began a new Sequence and transmits frames to another N_Port.

Sequence Recipient. The N_Port to which a particular Sequence of data frames is directed.

S_ID. Source Identifier. A 3-byte field in the frame header used to indicate the address identifier of the N_Port the frame was sent from.

SOF. Start of Frame delimiter. This Ordered Set is always the first Transmission Word of a Frame. It is used to indicate that a Frame will immediately follow and indicates which class of service the Frame will use.

Special Character. A special 10-bit Transmission Character which does mot have a corresponding 8-bit value, but is still considered valid. The Special Character is used to indicate that a particular Transmission Word is an Ordered Set. The Special Character is the only Transmission Character to have 5 1's or 0's in a row. The Special Character is also referred to as K28.5 when using K/D format.

T

Transmission Character. A (valid or invalid) 10-bit character transmitted serially over the fibre. Valid Transmission Characters are determined by the 8B/10B encoding specification.

Transmission Word. A string of four consecutive Transmission Characters.

U

ULP. Upper Level Protocol. The protocol which runs on top of Fibre Channel through the FC-4 layer. Typical ULPs running over Fibre Channel are Small Computer System Interface (SCSI), Internet Protocol (IP), High Performance Parallel Interface (HIPPI), and Intelligent Peripheral Interface (IPI).

8B/10B. The IBM patented encoding method used for encoding 8-bit data bytes to 10-bit Transmission Characters. Data bytes are converted to Transmission Characters to improve the physical signal such that the following benefits are achieved: bit synchronization is more easily achieved, design of receivers and transmitters is simplified, error detection is improved, and control characters (i.e., the Special Character) can be distinguished from data characters.

V

VCC. *See* Virtual Circuit Connection

VCI. *See* Virtual Circuit Identifier

Virtual Circuit Connection (VCC). A concatenation of virtual channel links between to endpoints where higher-layer protocols are accessed.

Virtual Circuit Identifier (VCI). A connection-identifying value found in the header of each ATM connection cell.

Index

© Copyright IBM Corp. 2004

Readers' Comments — We'd Like to Hear from You

IBM TotalStorage SAN n–type Director Family
Enterprise Manager Installation and Operation Guide

Publication No. GC26-7720-00

Overall, how satisfied are you with the information in this book?

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Overall satisfaction	□	□	□	□	□

How satisfied are you that the information in this book is:

	Very Satisfied	Satisfied	Neutral	Dissatisfied	Very Dissatisfied
Accurate	□	□	□	□	□
Complete	□	□	□	□	□
Easy to find	□	□	□	□	□
Easy to understand	□	□	□	□	□
Well organized	□	□	□	□	□
Applicable to your tasks	□	□	□	□	□

Please tell us how we can improve this book:

Thank you for your responses. May we contact you? □ Yes □ No

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Name

Address

Company or Organization

Phone No.

Readers' Comments — We'd Like to Hear from You

GC26-7720-00

Cut or Fold
Along Line

Fold and Tape **Please do not staple** Fold and Tape

NO POSTAGE
NECESSARY
IF MAILED IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST-CLASS MAIL PERMIT NO. 40 ARMONK, NEW YORK

POSTAGE WILL BE PAID BY ADDRESSEE

International Business Machines Corporation
Information Development
Department GZW
9000 South Rita Road
Tucson, Arizona U.S.A. 85775-4401

Fold and Tape **Please do not staple** Fold and Tape

Cut or Fold
Along Line

Printed in USA