HP BLc QLogic 4X QDR InfiniBand Managed Switch and InfiniBand Switch Management Module User Guide

for the HP c-Class BladeSystems

HP Part number: QL-CSWUG-1B
Published: June 2010
Edition: 1.1

invent

© Copyright 2010 Hewlett-Packard Development Company, L.P.
The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

InfiniBand™ is a trademark of the InfiniBand® Trade Association.

QLogic®, the QLogic logo, FastFabric®, and vFabric® are registered trademarks of QLogic®, Inc.

Document Revision History	
Revision B, June 2010	
Changes	**Sections Affected**
Added information for using IPv6.	"OOB LAN IP" on page 1-32

Contents

Operations and Administration . . . 5

Introduction . . . 5
Chassis Viewer Home Page . . . 6
Component Details Area . . . 6
  Details Header . . . 7
    Logout . . . 7
    Reboot . . . 8
    View Field Replaceable Unit (FRU) . . . 8
    View Log . . . 9
  Information Area . . . 10
Menu . . . 10
  Logging . . . 11
    Set Level . . . 11
    Reset Levels . . . 15
  Maintenance . . . 16
    Firmware Update . . . 16
    LDAP Configuration . . . 17
    HTTP/CLI Session Configuration . . . 17
    Subnet Manager Config File . . . 19
  SNMP . . . 20
    Target Configuration . . . 20
    Filter Status . . . 23
    Set Community Strings . . . 23
  Port Stats . . . 24
    IB Port Stats . . . 24
    Set Field Thresholds . . . 27
    Port Beacon . . . 29
Time Service . . . 30
  OOB LAN IP . . . 32
    Set OOB LAN IPv6 . . . 32
  Subnet Manager . . . 33
    Configuration . . . 33
License Keys . . . 34
    Key Administration . . . 34

Troubleshooting and Technical Reference . . . 35

Hardware Checks . . . 35
  Switch . . . 35
  InfiniBand Ports . . . 35
Troubleshooting Scenarios . . . 35
  InfiniBand . . . 35
    Invalid IP Address set on the Switch . . . 35
    Nodes cannot be seen in QLogic Fabric Viewer . . . 35

Figures

1 User Authentication . . . 5
2 Chassis Viewer Home Page . . . 6
3 Help Button . . . 6
4 Component Details Area . . . 6
5 Details Header . . . 7
6 Logout Question Screen . . . 7
7 Session Logout Screen . . . 7

8 Close Window Screen 8
9 Reboot Window 8
10 FRU Information Window 8
11 Log Messages Window 9
12 Menu 11
13 Logging Submenu 11
14 Log System Configurator (Device Tab) 11
15 Log System Configurator: Device Tab 12
16 Log System Configurator: Preset Tab 14
17 Log System Configurator: Syslog Host Tab 15
18 Reset Log Levels Window 15
19 Maintenance Menu 16
20 Firmware Update Screen 16
21 LDAP Authentication Screen 17
22 HTTP/CLI Session Configuration Screen 18
23 User Authentication Dropdown List 18
24 Http Mode Dropdown List 18
25 Https Mode Dropdown List 19
26 Upload/Download Esm Config File Screen 19
27 SNMP Submenu 20
28 SNMP Target Configuration Window 20
29 SNMP Filter Status Screen 23
30 Set Community Strings Window 24
31 Port Statistics Menu 24
32 Chassis IB Port Statistics 25
33 Set Field Thresholds Screen 27
34 Port Beacon Screen 29
35 Switch Time Service Menu 30
36 System Time Information Screen 30
37 Time Service - NTP Setup 31
38 Time Service - Manual Setup 31
39 Time Service - Time Zone/Daylight Saving Time Setup 32
40 OOB LAN IP Menu 32
41 Set OOB LAN IPv6 Window 33
42 Subnet Manager Menu 33
43 Subnet Manager Configuration 33
44 License Keys Menu 34
45 License Key Management Information Window 34
46 License Key Management Information Add Key Window 34

1 Operations and Administration

Introduction

Chassis Viewer is QLogic browser-based device management software. Chassis Viewer provides the primary management interface for the QLogic switches, allowing you to perform management, configuration, and monitoring tasks related to InfiniBand networks.

- Chassis Viewer runs on the Switch Management Module of the switch.
- The browser must be on a workstation that has connectivity to the subnet as the switch.
- Management Workstation requires Internet Explorer 6.0 or later, or Mozilla 1.6.x or later

To access Chassis Viewer, point a browser to the IP address of the switch. If user authentication is enabled, the User Authentication dialog box (Figure 1) is displayed:

Figure 1 User Authentication

Enter the default user name and password:

- Username: `admin`
- Password: `adminpass`

The Chassis Viewer home page (Figure 2) is displayed.

The Chassis Viewer manages:

- Chassis configuration
- Logging and monitoring functionality

Chassis Viewer Home Page

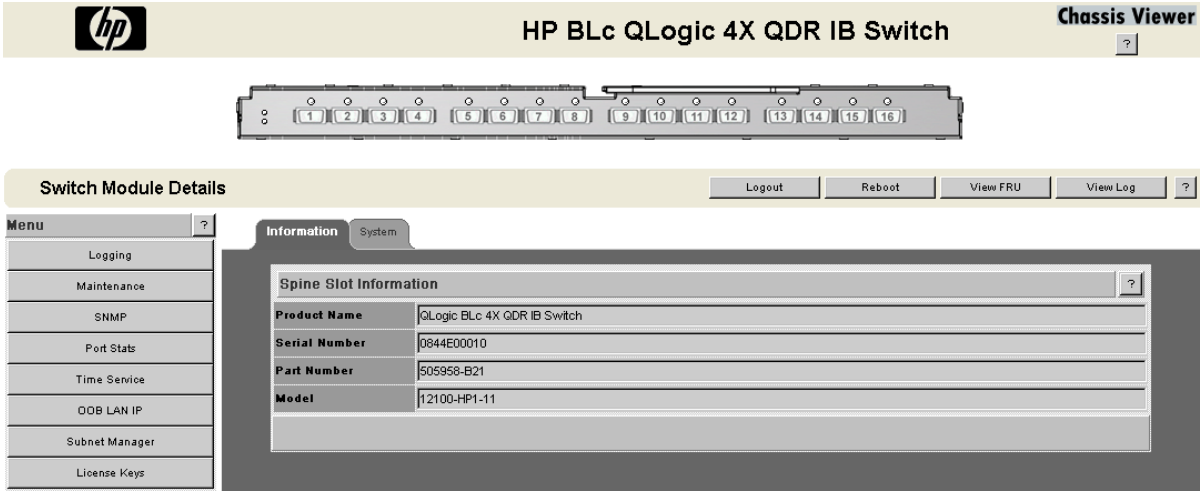


Figure 2 Chassis Viewer Home Page

Chassis Viewer's home page provides a high-level overview of the switch. The selected component provides hyperlinks to related menus and information where you can perform configuration and monitoring tasks. The buttons at the top right of the Chassis Viewer home page have the following functions:

- ? (Help) Button

Figure 3 Help Button

The **? (HELP)** button displays online help. Each help screen provides a high-level, topic-specific description.

Component Details Area

The **Component Details Area** for the switch has three areas as shown in Figure 4.

- Details Header (callout 1 in Figure 4)
- Information area (callout 2 in Figure 4)
- Menu (callout 3 in Figure 4)

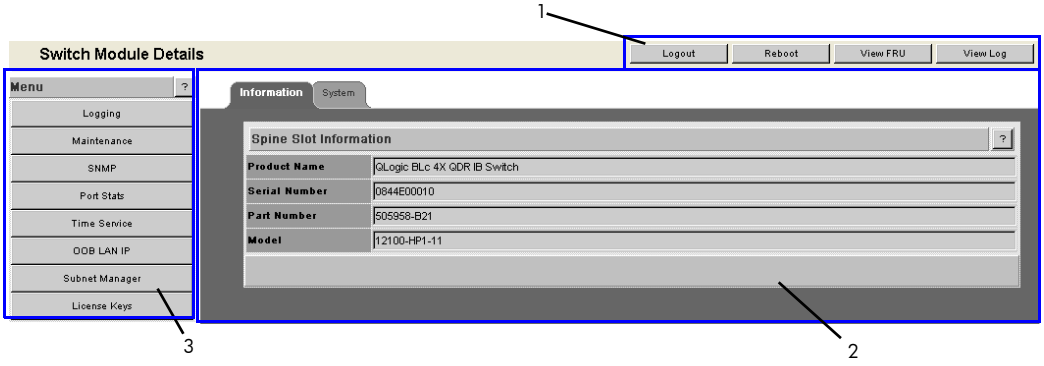


Figure 4 Component Details Area

Details Header

The Details Header lets you quickly access and execute the commands typically most used and/or immediately needed (see Figure 5).

Figure 5 Details Header

All component Details Headers contain the following buttons:

- **Logout**

NOTE: The **Logout** button is only displayed if you have set the User Authentication parameter to **Login Enabled** through the HTTP Session Configuration submenu. See "HTTP/CLI Session Configuration" on page 17 for more information.

- **Reboot**
- **View FRU** (Field Replaceable Unit)
- **View Log**

Logout

To log out from the Chassis Viewer session, follow these steps:

1. From the Details Header, click **Logout**. The Logout window displays (Figure 6).

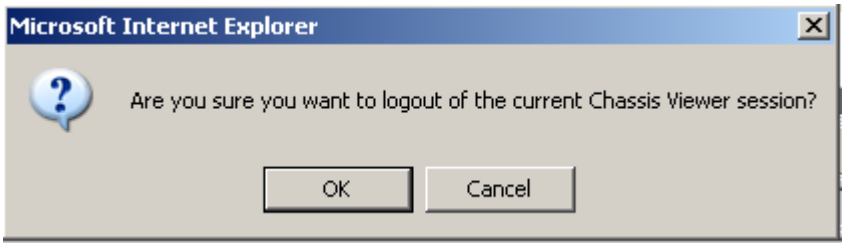


Figure 6 Logout Question Screen.

2. Click **OK**. This changes the viewer window to Session Logout (Figure 7).

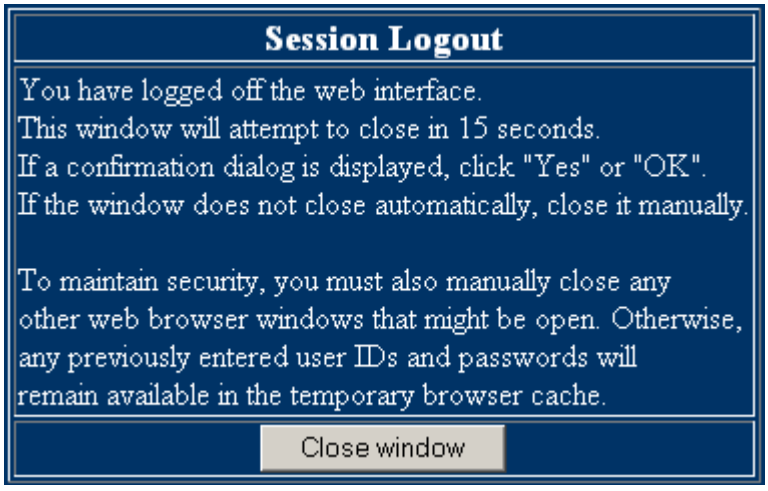


Figure 7 Session Logout Screen

3. Click **Close window**. The "Do you want to close this window" window displays (Figure 8).

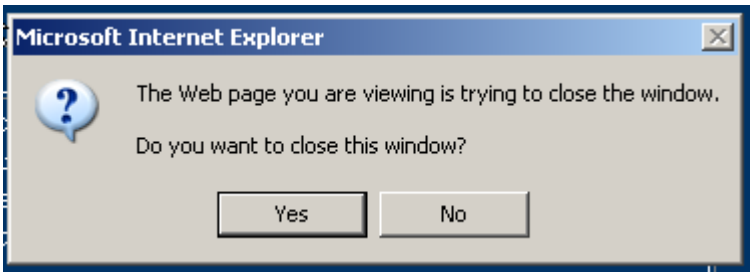


Figure 8 Close Window Screen

4. Click **Yes**. This closes the Internet Explorer window.

Reboot

To reboot the switch, follow these steps:

1. From the Details Header, click **Reboot**. The Reboot window is displayed (Figure 9).

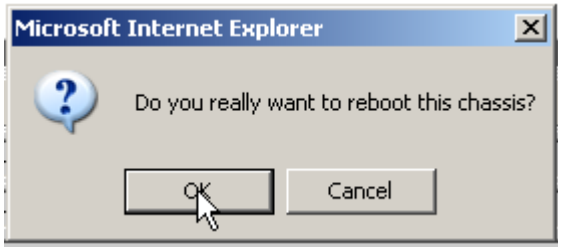
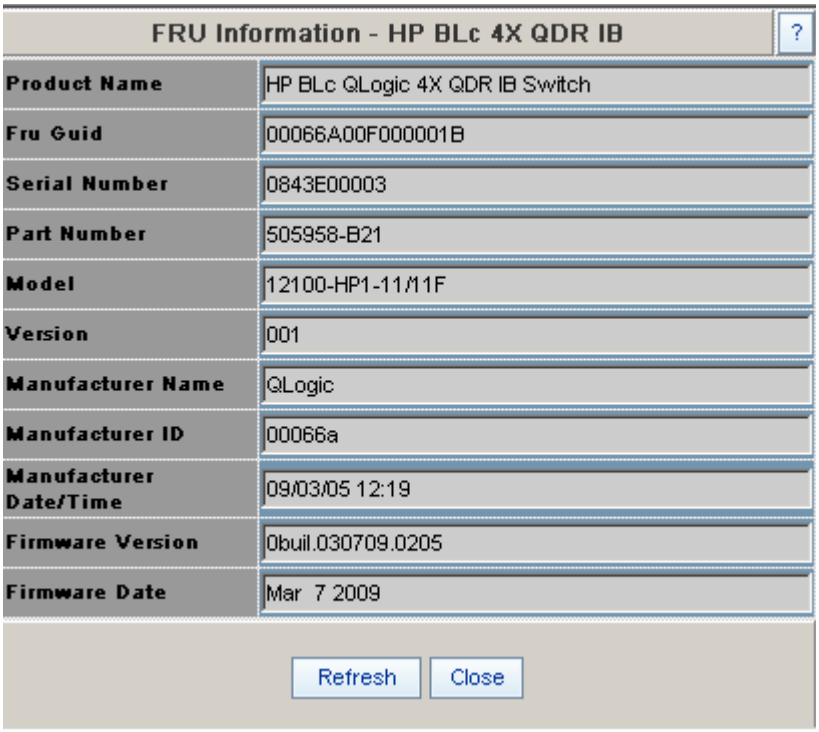


Figure 9 Reboot Window

2. Click **OK** button. The switch reboots.

View Field Replaceable Unit (FRU)

To view the FRU information, from the Details Header, click **View FRU**. The FRU Information window is displayed (Figure 10).



FRU Information - HP BLc 4X QDR IB

Product Name	HP BLc QLogic 4X QDR IB Switch
Fru Guid	00066A00F000001B
Serial Number	0843E00003
Part Number	505958-B21
Model	12100-HP1-11/11F
Version	001
Manufacturer Name	QLogic
Manufacturer ID	00066a
Manufacturer Date/Time	09/03/05 12:19
Firmware Version	0buil.030709.0205
Firmware Date	Mar 7 2009

Refresh Close

Figure 10 FRU Information Window

The FRU Information window includes the following items specific to the chassis:

`Product Name`
: The name of the component, from the tracked data.

`FRU Guid`
: GUID (Global User ID) for this FRU.

`Serial Number`
: Component serial number.

`Part Number`
: Component part number.

`Model`
: Model number of the component.

`Version`
: Hardware version of the component.

`Manufacturer Name`
: Name of the manufacturer.

`Manufacturer ID`
: Official InfiniBand Identification number for the manufacturer.

`Manufacturer Date/Time`
: Date/Time the hardware was manufactured.

`Firmware Version`
: Component firmware version that is currently loaded and running.

`Firmware Date`
: Date that the Firmware, which is currently loaded and running, was created.

`Refresh` Button
: Refreshes all fields in the Chassis FRU tab.

`Close` Button
: Closes the FRU Information window.

View Log

1. To view log messages, from the Details Header, click **View Log**. The **Log Information** window is displayed (Figure 11).

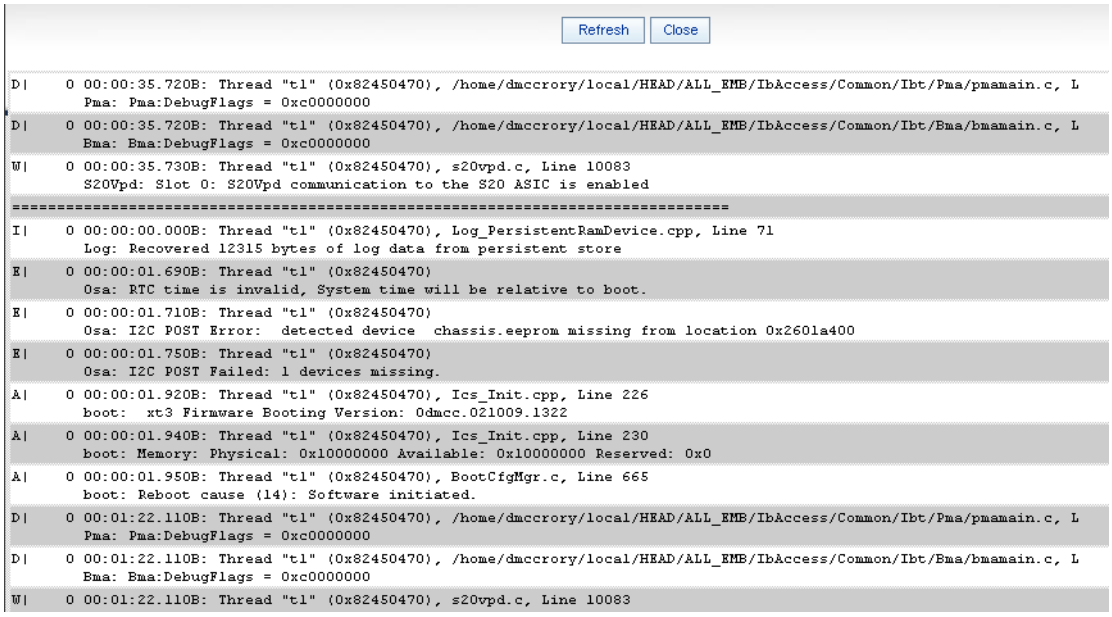


Figure 11 Log Messages Window

The Log Messages window includes the following items:

Refresh Button

Refreshes the log messages in the Log Messages window.

Close Button

Closes the Log Messages window.

Information Area

The Information area (callout 2, in Figure 4 on page 6) displays two tabs, Information and System, at the top of the area. The Information tab shows the following details, which are a subset of the FRUs information that is typically the most frequently needed for quick reference:

- Product Name
- Serial Number
- Part Number
- Model

The System tab shows the following details:

- Out of Band LAN IP
- Net Mask
- System Description
- IB Node Description
- System Uptime
- System Contact
- System Name
- System Location

Menu

The Menu section (Figure 12) of the Details area includes the following selections:

- Logging
- Maintenance
- SNMP
- Port Stats
- Time Service
- OOB LAN IP
- Subnet Manager
- License Keys

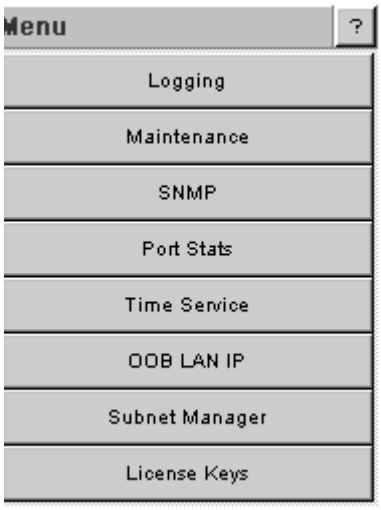


Figure 12 Menu

Logging

The Logging menu lets you set and reset levels for log message files. Click **Logging**. The submenus display (Figure 13).

Figure 13 Logging Submenu

Set Level

Set Level lets you set log level configuration parameters for all software modules.

To set log levels:

1. From the menu, select **Logging.**
2. From **Logging**, select **Set Level**. The Log System Configurator (**Device** tab) window is displayed (Figure 14)

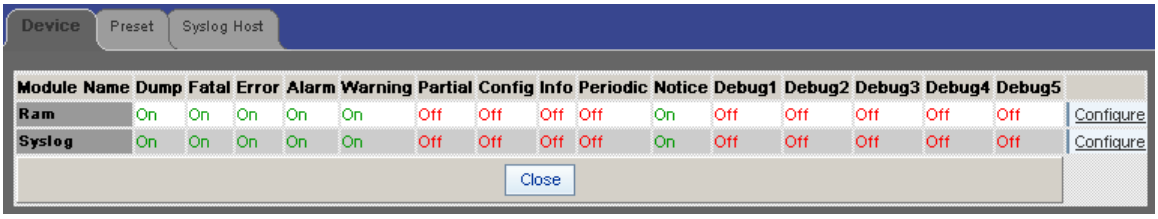


Figure 14 Log System Configurator (Device Tab)

Device Tab

The **Device** tab presents current log level configuration settings for the following software modules:

RAM

The circular log buffer contained in memory. To access the contents of this buffer, select the Chassis Viewer **View Log** button.

Syslog

Messages that are sent to the syslog host specified on the Syslog tab.

From this screen, you can change any of the log level settings for a specific software module by clicking on **Configure**, which displays a configuration screen (Figure 15). Both **Ram** and **Syslog** contain the same information.

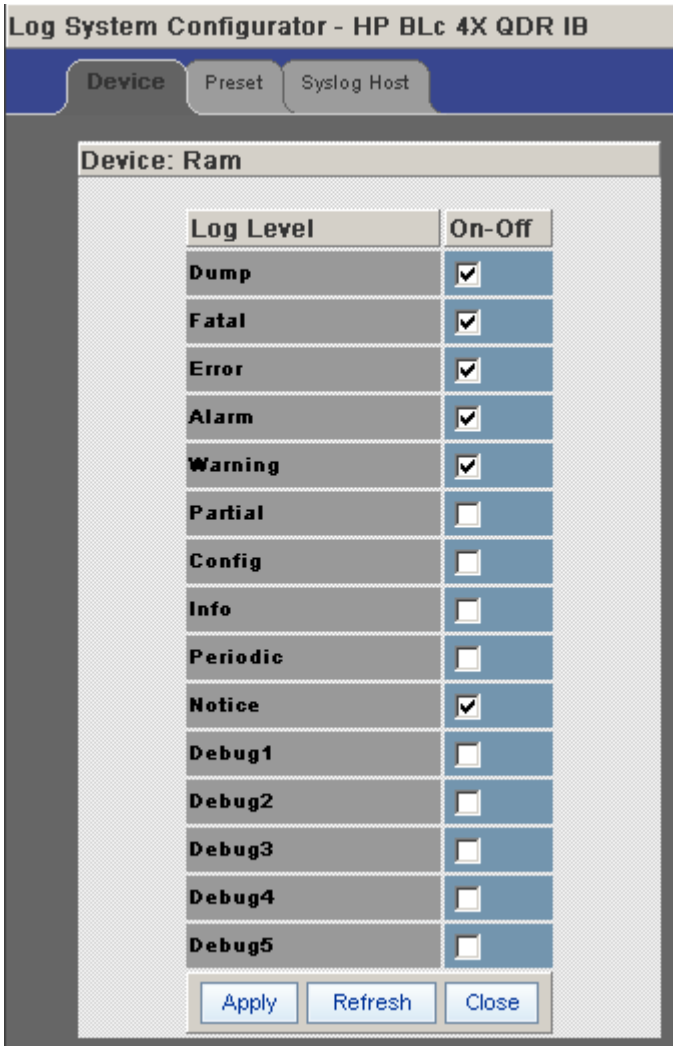


Figure 15 Log System Configurator: Device Tab

To change any **Log Level** settings:

1. Click the **On-Off** checkbox to the right of the setting.
2. Click **Apply** to save any changes.

The following list describes each of the Log Level configuration parameters.

Dump

Indicates that a problem has caused the system to produce a system dump file. In most circumstances, HP recommends that you retrieve the dump that was produced. Support engineers may require the information contained in the dump file to diagnose the cause of the problem.

Fatal

Indicates that a nonrecoverable system problem has occurred. Reboot the system or component and verify that the subsystem is fully functional to determine whether the fault has been corrected. If the problem persists, contact the supplier.

Error

Indicates that a serious system error has occurred that might be recoverable. If the system exhibits any instability, reboot the system or component. If errors persist, immediately contact the supplier's technical support.

`Alarm`

Indicates that a serious problem has occurred that degrades capacity or service. If the error is recoverable, correct the failure. If the alarm/failure persists, reboot the system at a convenient time. If the problem is still not cleared, contact the supplier.

`Warning`

Indicates that a recoverable problem has occurred. You do not need to take any action.

`Partial`

When more information is available, Partial causes additional message-related details to be displayed.

`Config`

An informational message indicating changes that were made to the system configuration. You do not need to take any action.

`Info`

Informational messages that occur during a system or component boot. You do not need to take any action.

`Periodic`

An informational message containing periodic statistics. You do not need to take any action.

`Notice`

Notice is used for failures that could be a result of "frequent" user actions, such as a server reboot.

`Debug message levels 1 through 5`

Debug messages are for supplier and/or QLogic Engineering use and are not necessarily indicative of actions that an end user may need to take.

`Debug1`

Messages that describe the states of connections and links.

`Debug2`

Messages that describe major configuration changes or operations.

`Debug3`

Messages that describe the I/O flow.

`Debug4`

Messages that contain the packet dumps within an I/O flow. I/O flows contain multiple packets.

`Debug5`

Messages that contain the packet dumps within an I/O flow. I/O flows contain multiple packets.

IMPORTANT: When configuring the log levels to display debug messages, be careful to ensure that system performance issues are weighed against troubleshooting requirements. Generally, the higher the debug number the more information is written to the log. Specifically, debug 3-5 have the most effect on system performance.

Refresh Button

Refreshes the **On-Off** checkboxes in the Log System Configurator window.

Close Button

Closes the Log System Configurator window.

Preset Tab

The **Preset** tab lets you quickly change log level settings for all software modules on the switch (Figure 16).

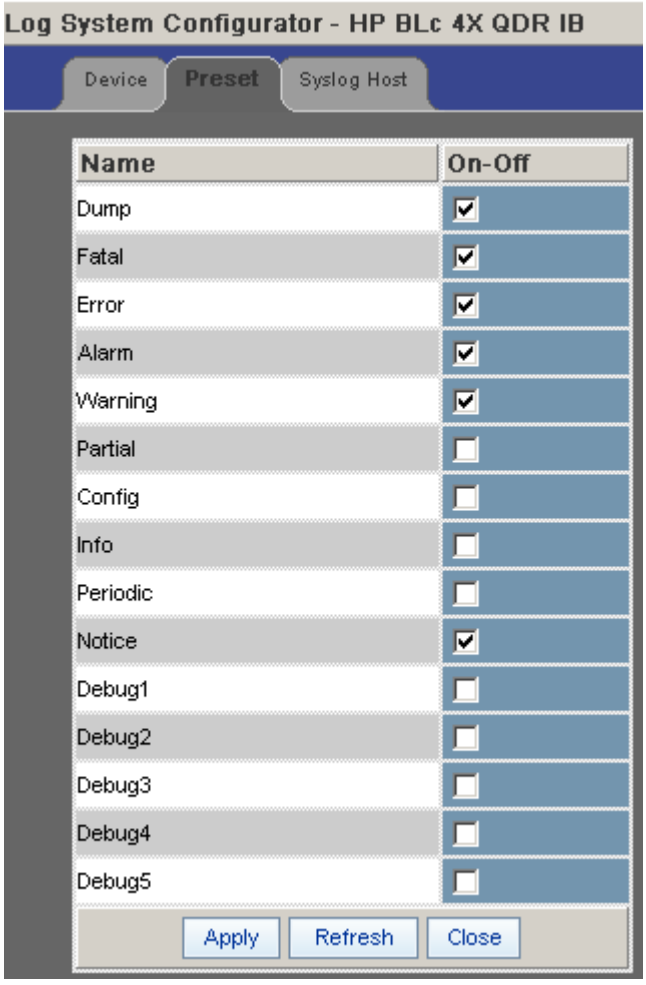


Figure 16 Log System Configurator: Preset Tab

To change the log level settings:

1. Click the **On-Off** checkbox to the right of the setting(s).
2. Click **Apply** to save any changes.

The following list describes the selections of the Preset tab.

On-Off checkbox
: Selects the preset condition.

Apply Button
: Applies the changes made to the Preset tab.

Refresh Button
: Refreshes the **On-Off** checkboxes in the Log System Configurator window.

Close Button
: Closes the Log System Configurator window.

Syslog Host Tab

The **Syslog Host** tab lets you configure logging messages to be sent to a syslog host (Figure 17). If the Host IP address is 0.0.0.0, no syslog host is configured, otherwise log messages are sent to the syslog server at a specified IP address and port.

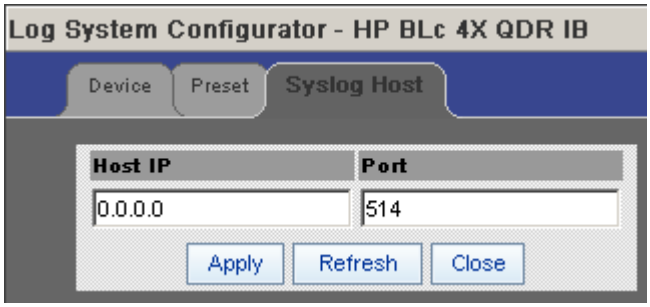


Figure 17 Log System Configurator: Syslog Host Tab

To set up the syslog host:

1. In the **Host IP** text box, enter the IP address of the syslog host where the log files are to be saved.
2. Click **Apply** to save the IP address.

NOTE: To use this feature a syslog server must be configured, running, and ready to accept input. To set up a syslog server, see your company specific procedures for Syslog Server setup.

NOTE: To centralize logging for all switches in an InfiniBand fabric, you can configure each switch to point to the same syslog server, which has the syslog daemon (`syslogd`) running.

Reset Levels

Reset Levels resets the logging levels to their factory default values.

To reset the logging levels:

1. From the menu, select **Logging.**
2. Click **Logging**.
3. Click **Reset Levels**. The Reset Levels window is displayed:

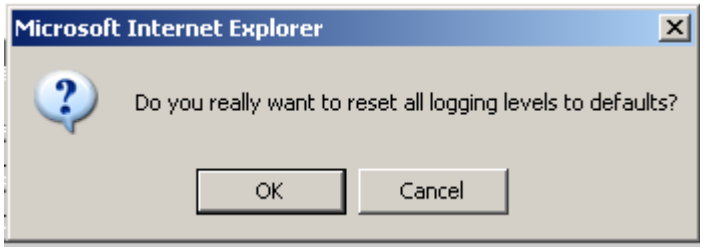


Figure 18 Reset Log Levels Window

4. To reset the logging levels, click **OK**.

Maintenance

The Maintenance menu lets you update the firmware, configure LDAP, and configure the Http/Cli sessions. Clicking **Maintenance** causes the submenus to display (Figure 19).

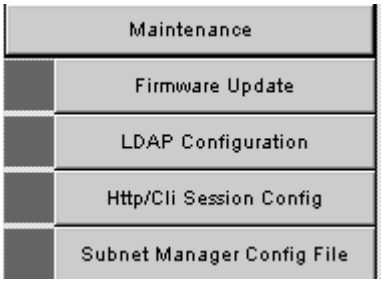


Figure 19 Maintenance Menu

NOTE: For rebooting information, see "Reboot" on page 8.

Firmware Update

The **Firmware Update** lets you select an alternate firmware file for the switch.

To download firmware:

1. Click **Firmware Update** under the **Maintenance** menu. The Firmware Update screen is displayed (Figure 20).

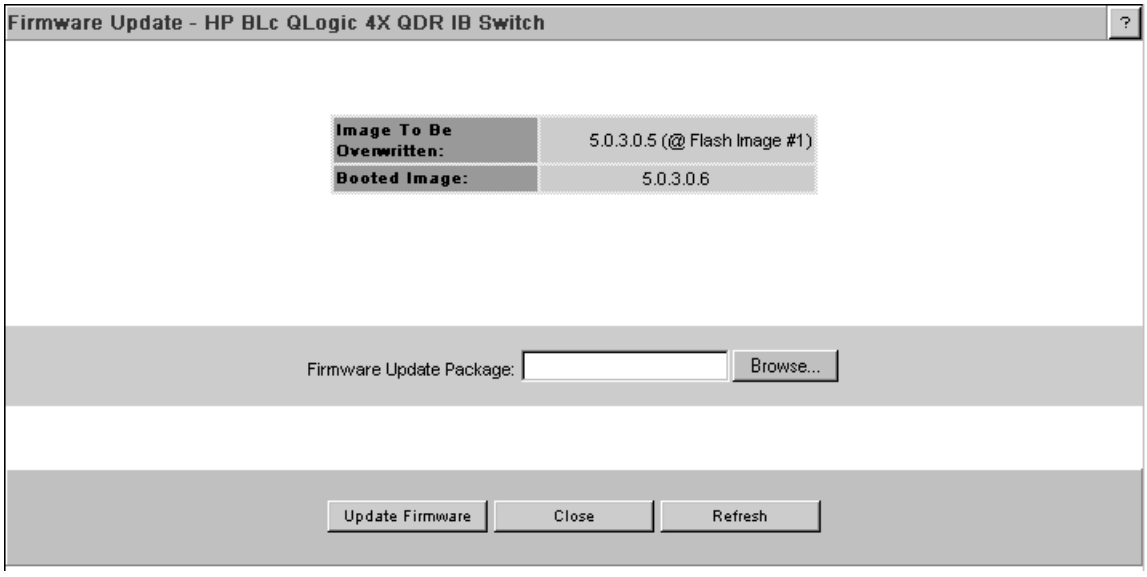


Figure 20 Firmware Update Screen

The information in this window includes:

- **Image to Be Overwritten** field — describes which image of two possible stored within system memory will be overwritten with the newly selected image. For this product, this will always be "the image that is not currently booted."
- **Booted Image:** field — Booted image information
- **Firmware Update Package:** field — New firmware text input field
- **Browse** button — Browse for firmware file
- **Update Firmware** button — Starts firmware update
- **Close** button — Closes Firmware Update window
- **Refresh** button — Refreshes information

2. In the **Firmware Update Package:** text box, enter the path to the alternate firmware file. If the path is not known, the user can use the **Browse...** button to locate it.

NOTE: Before using the **Browse...** button, make certain that the browser is tied to an FTP server where the firmware files reside (i.e., if the file(s) does not reside on a local computer).

---

3. Click **Update Firmware**. This starts updating the firmware.

LDAP Configuration

The lightweight directory access protocol (LDAP) configuration feature lets you set and configure authentications for the switch. The LDAP service resides on a server that has access to a usercode and password database.

On a switch with LDAP enabled, when you attempt to log in to either Chassis Viewer or the CLI, the LDAP client intercepts the login attempt and rather than authenticating internally, encrypts and packages the information in an LDAP packet and sends it to a pre-configured LDAP server over TCP/IP (i.e., the out of band LAN). The LDAP server receives the request, passes it on to the authentication services, and responds to the client with a yes or no, either allowing or denying the user access to the switch.

When LDAP is disabled internal authentication becomes the default.

To set up LDAP authentication:

1. Click **LDAP Configuration** under the **Maintenance** menu. The LDAP Authentication screen is displayed (Figure 21).

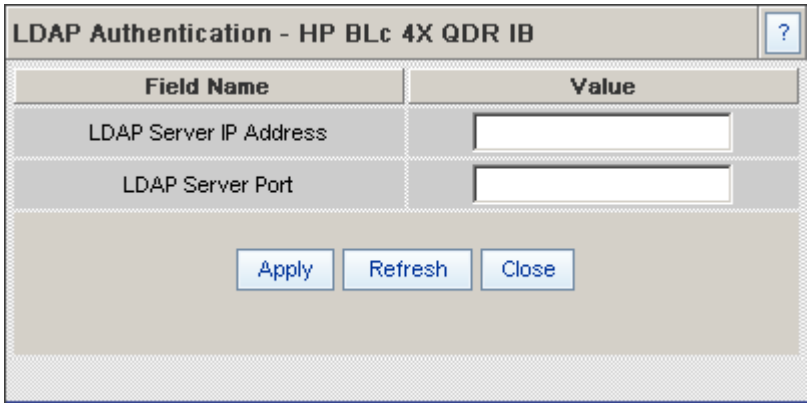


Figure 21 LDAP Authentication Screen

The information in this window includes:

- **LDAP Server IP Address** field — LDAP server IP address entry field
- **LDAP Server Port** filed — LDAP server port number entry field
- **Firmware Update Package:** field — New firmware text input field
- **Apply** button — Applies the information entered
- **Refresh** button — Refreshes information
- **Close** button — Closes Firmware Update window

2. In the **LDAP Server IP Address** field, enter the address of the applicable LDAP server.
3. In the **LDAP Server Port** filed, enter the applicable server port number (the default is 389).
4. When finished, click **Apply**.

HTTP/CLI Session Configuration

The hyper text transfer protocol (HTTP) and command line interface (CLI) session configuration feature lets you to set HTTP and CLI session timeout parameters, as well as set security requirements for the switch.

The session timeout duration is the length of time that a session remains active if there is no GUI activity. If a session is inactive for a time exceeding the timeout duration, the user will be logged out.

To modify the HTTP and CLI configurations:

1. Click **HTTP/CLI Session Config** under the **Maintenance** menu. The HTTP/CLI Session Configuration screen is displayed.(Figure 22)

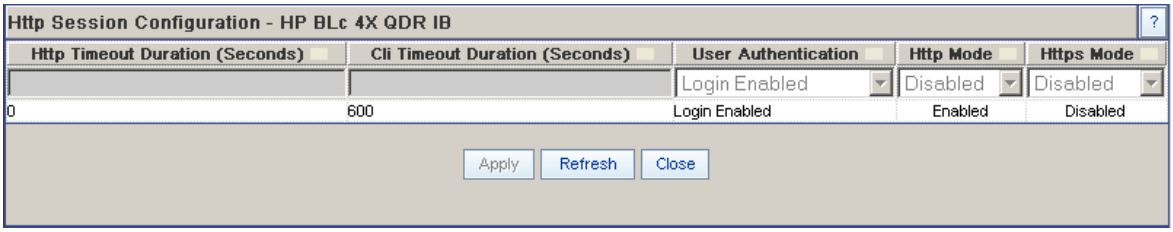


Figure 22 HTTP/CLI Session Configuration Screen

2. To modify the session timeout duration (in seconds), click on the existing configuration. The row changes to orange.
3. In the **Http Timeout Duration** field, enter the new timeout duration (in seconds). The default is 0 seconds (i.e., no timeout).
4. In the **Cli Timeout Duration** field, enter the new timeout duration (in seconds). The default is 600 seconds.
5. To change the **User Authentication** parameter, click on the drop-down list. The following options are displayed (Figure 23):

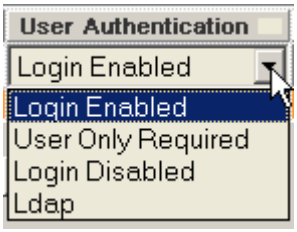


Figure 23 User Authentication Dropdown List

6. Select the preferred user authentication method. These are:
   - **`Login Enabled`** — UserName and Password must be entered, and must match what is in the database of the local switch.
   - **`User Only Required`** — According to the local switch database, a valid username must be entered. A password is not required.
   - **`Login Disabled`** — Does not require a username or password.
   - **`LDAP`** — Use an LDAP server. If the username/password validation fails to complete successfully, check in the database of the local switch.
7. To change the **HTTP Mode** parameter, click on the dropdown list. The following options are displayed (Figure 24):

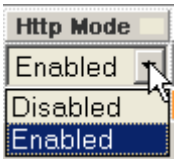


Figure 24 Http Mode Dropdown List

8. Select **Enabled** or **Disabled**.

9. To change the **Https Mode** parameter, click on the dropdown list. The following options are displayed (Figure 25):

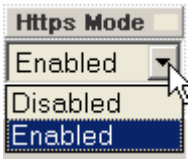


Figure 25 Https Mode Dropdown List

10. Select Enabled or Disabled.
11. When finished, click **Apply**.

Subnet Manager Config File

The Subnet Manager Config File menu lets you view the current configuration file and upload a new configuration file. It also states the time that the switch has been running, its status and what state the switch is in.

To modify the Subnet Manager Config File:

1. Click **Subnet Manager Config File** under the **Maintenance** menu. The Upload/Download Esm config file screen is displayed.(Figure 26)

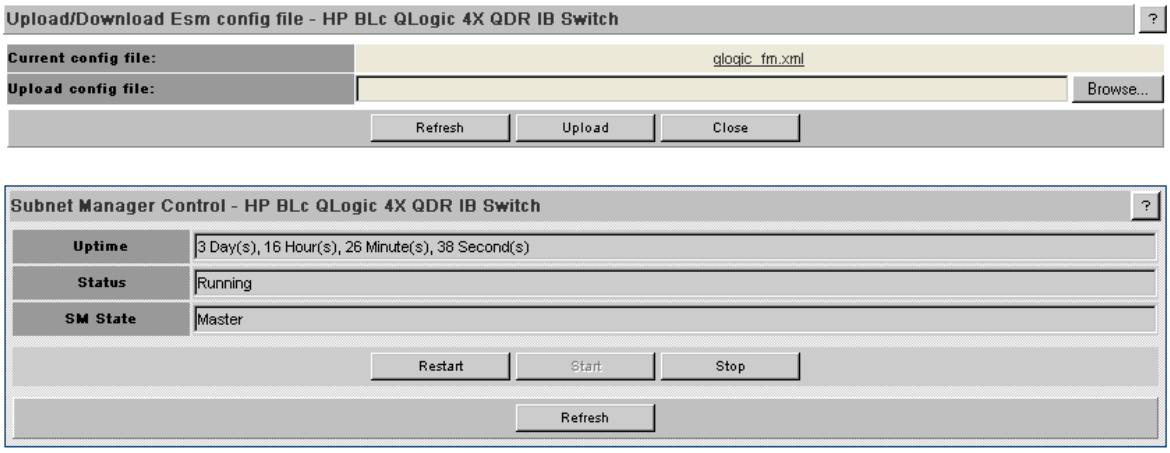


Figure 26 Upload/Download Esm Config File Screen

The information in this window includes:

- **Current config file** — Name of the current configuration file
- **Upload config file** — Name of the configuration file to be uploaded
- **Browse...** button — Select to browse for the file to upload
- **Refresh** button — Select to browse for the file to upload
- **Upload** button — Select to upload the file selected
- **Close** button — Select to close the window
- **Uptime** — The time the Subnet Manager has been running
- **Status** — Status of the Subnet Manager
- **SM State** — State of the Subnet Manager
- **Restart** button — Select to restart the Subnet Manger
- **Start** button — Select to start the Subnet Manager
- **Stop** button — Select to stop the Subnet Manger
- **Refresh** button — Select to refresh this screen

2. To upload a new config file select **Browse...** .
3. Find and select the new or updated config file you want to upload and select **Open**.
4. Select Upload to upload the file you have selected to replace the existing configuration file.

SNMP

The SNMP submenu lets you view and modify SNMP trap configuration information. Clicking **SNMP** causes the submenus to display (Figure 27).

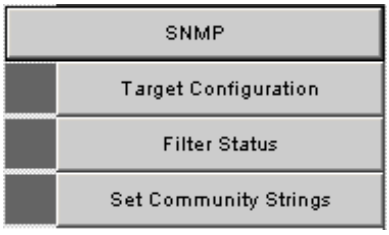


Figure 27 SNMP Submenu

Target Configuration

The **Target Configuration** button displays the SNMP Target Configuration window, allowing you to view and edit existing SNMP trap destinations (Figure 28).

To display the SNMP Target Configuration window:

1. Select **Target Configuration** under the **SNMP** menu. The SNMP Target Configuration window is displayed:

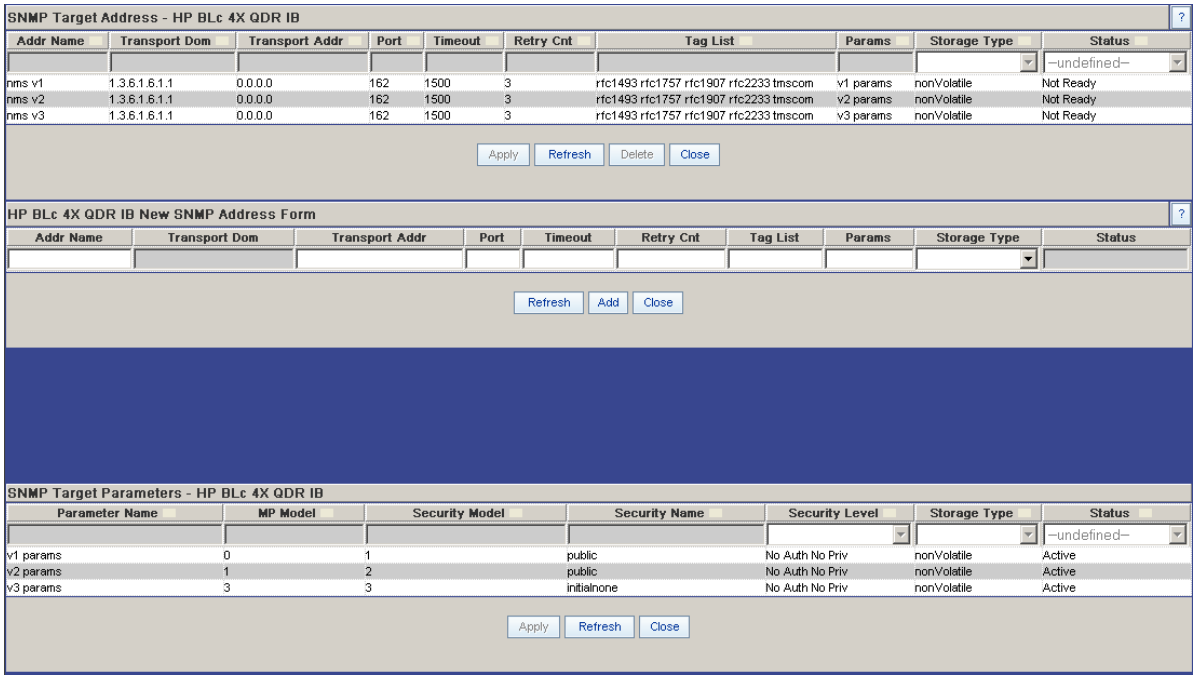


Figure 28 SNMP Target Configuration Window

The **SNMP Target Configuration** window is divided into three sections. The top section of the window, **SNMP Target Address**, lets you determine what type of SNMP traps are sent, and where they are sent. The rows provide an area for specifying multiple trap destinations. The center section of the window, **SNMP Address Form**, lets you add target addresses to the list. The bottom section of the window, **SNMP Target Parameters**, lets you configure each trap destination with version, optional security information, and filtering mechanisms.

The **Apply** button applies the current settings to either the SNMP Target Addresses or SNMP Target Parameters section.

NOTE: The Target Configuration window is used for viewing and modifying existing SNMP target entries. It is not used to create new target entries.

To create a new target entry, use the following CLI command:

```
snmpTargetAddr add -n name -a addr [-p port] [-t timeout] [-r retry_count] [-l
tag_list] [-v parameters] [-s storage_type]
```

For example, to add a trap target with the IP address 192.168.0.123 that accepts SNMP v2c style traps, you would use the following CLI command:

```
snmpTargetAddr add -n traphost1 -a 192.168.0.123 -v "v2 params"
```

Or, to add the same target, except using SNMP v1traps, you would, use the following CLI command:

```
snmpTargetAddr add -n traphost1 -a 192.168.0.123 -v "v1 params"
```

Target Configuration Window Field Descriptions

The following are descriptions for each field in the Target Configuration window:

SNMP Target Address and New SNMP Address Form

- **Addr**(ess) **Name**

  Specifies a unique, administrator-defined name the system uses to identify a row.
- **Transport Dom**(ain)

  Specifies the transport type of the address contained in the snmpTargetAddrTAddress object (e.g., 1.3.6.1.6.1.1 = udp, 1.3.6.1.4.1.1977.200.1 = tcp).
- **Transport Addr**(ess)

  Specifies the IP address in dotted decimal format.

  NOTE: The combination of the Transport Domain and the Transport Address fields determines the trap destination.

- **Port**

  Specifies the TCP or UDP port that the SNMP trap is sent.
- **Timeout**

  Specifies the time (in milliseconds) that the trap sender waits on a response before resending the trap.
- **Retry C(**ou)**nt**

  Specifies the number of attempts to be made to send the trap after a timeout condition occurs.

  NOTE: Timeout and Retry Count apply to SNMP v2.c and later versions, and are not applicable for v1 traps.

- **Tag List**

  Specifies which traps should be sent to this particular destination.

  NOTE: RFC2233 specifies the link up/down traps. Including RFC2233 in the Tag List specifies that the trap receiver will get link up/down traps.

- **Param**(eter)**s**

  Specifies a mapping to an entry in the SNMP Target Parameters table, determining the version of SNMP to use.
- **Storage Type**

  This field determines whether or not the entry is saved for each reboot of the switch using the following options:
  - *Nonvolatile* means that the value is saved, and remains with each subsequent reboot.
  - *Volatile* or *Other* indicates it will not be saved.

- **Status**

  Indicates the current status of the row. The row may be in one of three states:

  - Active
  - Not in service
  - Not Ready

  NOTE: A status of **not in service** indicates that the current row will not be used in the event a trap is generated by the system. Toggling a trap to not in service, which temporarily suspends trap forwarding, may be useful to keep values intact.

- **Apply** Button

  Applies changes made to the **SNMP Target Address** section.
- **Refresh** button

  Refreshes information
- **Delete** button

  Deletes the selected row
- **Add** button

  Adds the new SNMP Target Address to the list
- **Close** button

  Closes SNMP Target Configuration window

SNMP Target Parameters

NOTE: Changes can only be made to rows that have a status of **not in service**.

- **Parameter Name**

  Specifies a mapping to an entry in the SNMP Target Parameters table, determining the version of SNMP to use.
- **MP Model**

  The Message Processing Model to be used when generating SNMP messages for entry. Values for this field are 0 for SNMP v1, 1 for SNMP v2, or 3 for SNMP v3.
- **Security Model**

  The Security Model to be used when generating SNMP messages using this entry. Values for this field are 1 for SNMP v1, 2 for SNMP v2, or 3 for SNMP v3
- **Security Name**

  Security name identifies the entity for whom SNMP messages will be generated.

  NOTE: This is equivalent to the community string in an SNMP get.

- **Security Level**

  One of three options:

  - *NoAuthNoPriv*: No Authentication, no privacy.
  - *AuthNoPriv*: Authentication, no privacy.
  - *AuthPriv*: Authentication and privacy
- **Storage Type**

  This field determines whether or not the entry is saved for each reboot of the switch using the following options:

  - *Nonvolatile* means that the value is saved, and remains with each subsequent reboot.

- *Volatile* or *Other* indicates it will not be saved.

- **Status**

  Indicates the current status of the row. The row may be in one of three states:

  - Active
  - Not in service
  - Not Ready

  NOTE: A status of **not in service** indicates that the current row will not be used in the event a trap is generated by the system. Toggling a trap to not in service, which temporarily suspends trap forwarding, may be useful to keep values intact.

- **Apply** Button

  Applies changes made to the **SNMP Target Parameters** section.

- **Refresh** button

  Refreshes information

- **Close** button

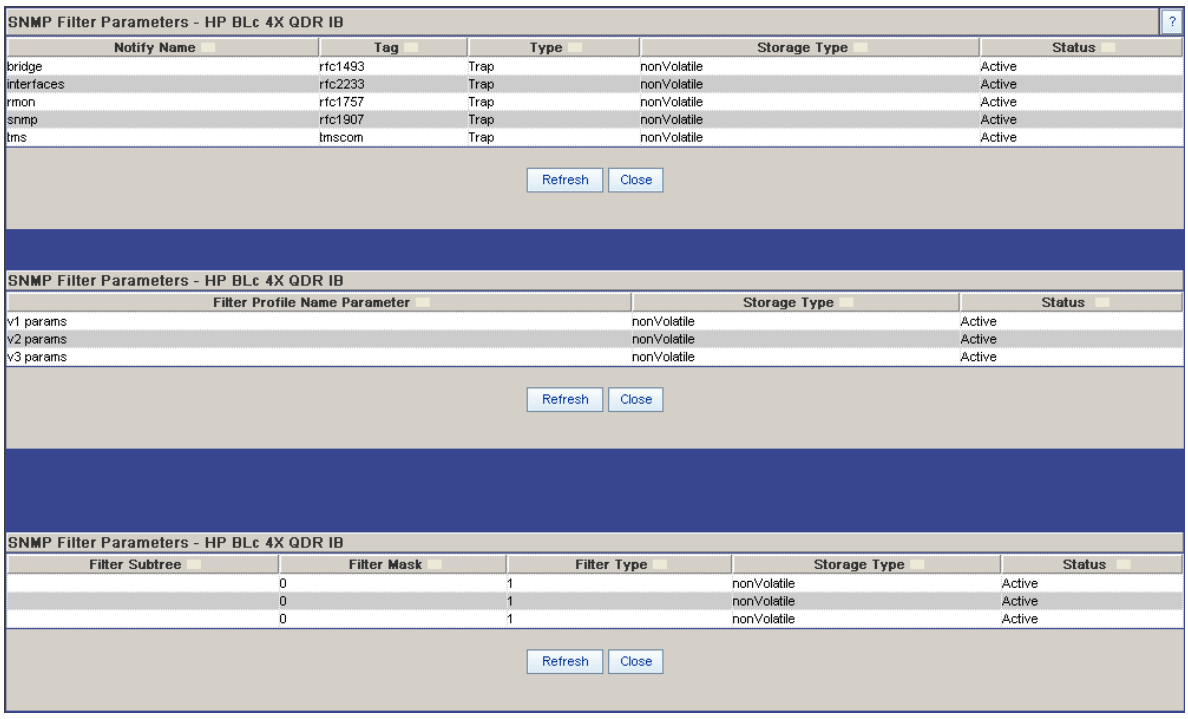
  Closes SNMP Target Configuration window

Filter Status

The SNMP Filter Status screen lets you view parameters for rfc2273 (SNMP-NOTIFICATION-MIB).

To view the SNMP filter status:

1. Click **Filter Status** under the **SNMP** menu. The **SNMP Filter Status** screen is displayed (Figure 29).



SNMP Filter Parameters - HP BLc 4X QDR IB

Notify Name	Tag	Type	Storage Type	Status
bridge	rfc1493	Trap	nonVolatile	Active
interfaces	rfc2233	Trap	nonVolatile	Active
rmon	rfc1757	Trap	nonVolatile	Active
snmp	rfc1907	Trap	nonVolatile	Active
tms	tmscom	Trap	nonVolatile	Active

Refresh Close

SNMP Filter Parameters - HP BLc 4X QDR IB

Filter Profile Name Parameter	Storage Type	Status
v1 params	nonVolatile	Active
v2 params	nonVolatile	Active
v3 params	nonVolatile	Active

Refresh Close

SNMP Filter Parameters - HP BLc 4X QDR IB

Filter Subtree	Filter Mask	Filter Type	Storage Type	Status
	0	1	nonVolatile	Active
	0	1	nonVolatile	Active
	0	1	nonVolatile	Active

Refresh Close

Figure 29 SNMP Filter Status Screen

Set Community Strings

The Set Community Strings screen lets you set two SNMP community names:

- Read Only Community Name
- Read/Write Community Name

To set the Community Strings:

1. Click **Set Community Strings** under the **SNMP** menu. The **Set Community Strings** screen is displayed (Figure 30).

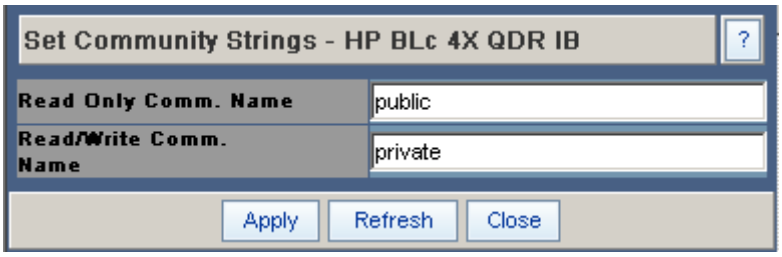


Figure 30 Set Community Strings Window

The first field, **Read Only Comm. Name**, is the community string that when specified in an SNMP client, allows read only access to SNMP fields exported by the SNMP server.

The second field, **Read/Write Comm. Name**, is the community string that when specified in an SNMP client, allows read and write access to SNMP fields exported by the SNMP server.

2. In each field, enter a meaningful name (such as **public** and **private** shown above), and click on **Apply**.

Port Stats

The Port Statistics menu provides InfiniBand port information for all of the external and internal ports of the switch. Clicking **Port Stats** causes the submenus to display (Figure 31).

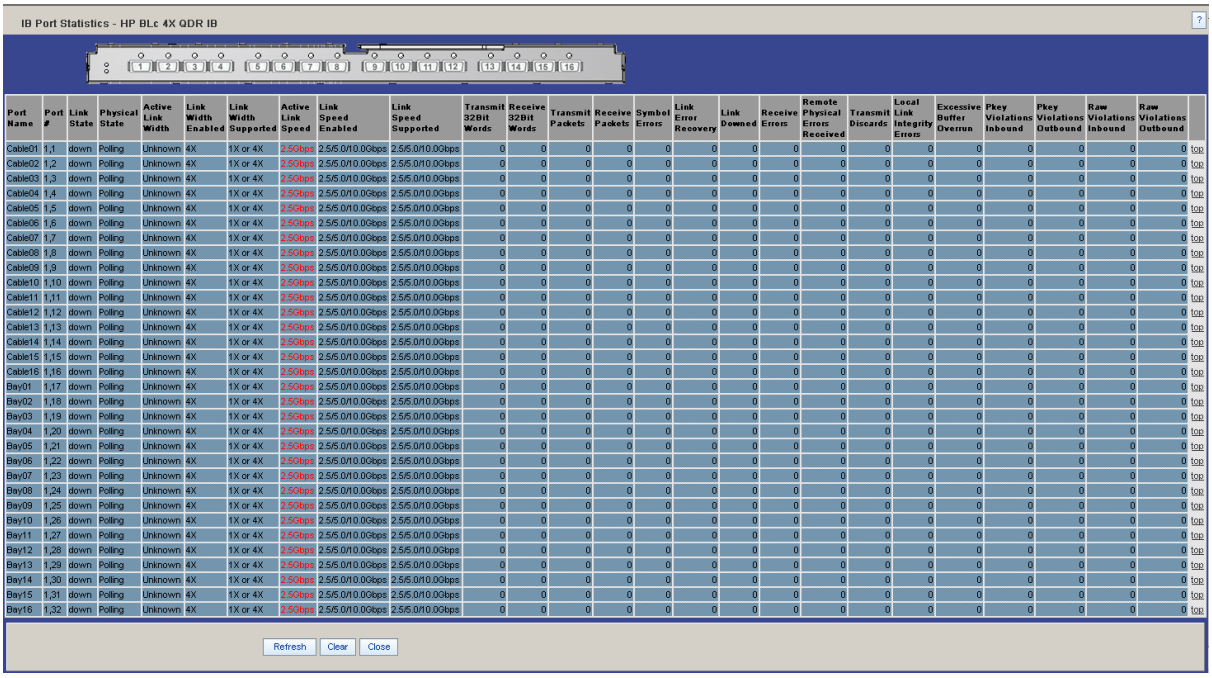
Figure 31 Port Statistics Menu

IB Port Stats

The IB Port Statistics screen lets you see all of the information on every port in the switch.

To view port statistical information:

1. Click **IB Port Stats** under the **Port Stats** menu. The **IB Port Statistics** window is displayed (Figure 32):



Port Name	Port #	Link State	Physical State	Active Link Width	Link Width Enabled	Link Width Supported	Active Link Speed	Link Speed Enabled	Link Speed Supported	Transmit 32Bit Words	Receive 32Bit Words	Transmit Packets	Receive Packets	Symbol Errors	Link Error Recovery	Link Downed	Receive Errors	Remote Physical Errors Received	Transmit Discards	Local Link Integrity Errors	Excessive Buffer Overrun	Pkey Violations Inbound	Pkey Violations Outbound	Raw Violations Inbound	Raw Violations Outbound	
Cable01	1,1	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable02	1,2	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable03	1,3	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable04	1,4	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable05	1,5	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable06	1,6	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable07	1,7	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable08	1,8	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable09	1,9	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable10	1,10	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable11	1,11	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable12	1,12	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable13	1,13	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable14	1,14	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable15	1,15	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Cable16	1,16	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay01	1,17	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay02	1,18	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay03	1,19	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay04	1,20	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay05	1,21	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay06	1,22	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay07	1,23	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay08	1,24	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay09	1,25	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay10	1,26	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay11	1,27	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay12	1,28	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay13	1,29	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay14	1,30	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay15	1,31	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top
Bay16	1,32	down	Polling	Unknown	4X	1X or 4X	2.5Gbps	2.5/5.0/10.0Gbps	2.5/5.0/10.0Gbps	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	top

Figure 32 Chassis IB Port Statistics

Understanding Port Naming Conventions

The conventions used in the **Port Name** column are as follows.

Cable01 through **16** — External ports that ISLs or external servers can be attached.

Bay01 through **16** — Internal server bay connections that correspond to labeling on an HP c-Class chassis.

The following are descriptions for each field in the **IB Port Statistics** window broken down into groups:

Port Statistics Field Descriptions

- **Port #**

  Indicates the switch number and port number.
- **Link State**

  Indicates whether the InfiniBand link associated with the physical port is up or down. Possible values are **no state change**, **down**, **init**, **armed**, **active**, and **unknown**.
- **Physical State**

  Indicates whether the internal connection to the InfiniBand port is up or down. Possible values are **No State Change**, **Sleep**, **Polling**, **Disabled**, **Training, Up**, and **Error Recovery**.
- **Active Link Width**

  Indicates the number of full duplex serial links that are currently being used on a port. The current bandwidth capability of a port is determined by multiplying this value by the Active Link Speed of this port. For instance a 4X QDR link has a bandwidth capability of 40Gb/s.

  NOTE: Values of 1X are possible in this field with 4X InfiniBand cables if poor cable connections or defective 4X InfiniBand cables are used.

- **Link Width Enabled**

  Link Width Enabled is the allowed link width(s) that a port can arbitrate to. Normally, this defaults to the Link Width Supported value, but can be overridden by the subnet manager.

- **Link Width Supported**

  Indicates the link width in terms of multipliers of 2.5 Gbit/sec full duplex serial links supported by the port.
- **Active Link Speed**

  Indicates the speed of the full duplex serial link. This is either 2.5Gbps (single data rate, or SDR), 5.0Gbps (double data rate, or DDR), or 10.0Gbps (quadruple data rate, or QDR).
- **Link Speed Enabled**

  Link Speed Enabled is the allowed link speed(s) that a port can arbitrate to. Normally this defaults to the Link Speed Supported value, but can be overridden by the subnet manager.
- **Link Speed Supported**

  The supported link speed of the port. This could be 2.5Gbps (SDR), 5.0Gbps (DDR), 10.0Gbps (QDR) or any two or all three.

InfiniBand Statistics

- **Transmit 32 Bit Words**

  The number of 32-bit data words transmitted by the port, not including flow control and VCRC data.
- **Receive 32 Bit Words**

  The number of 32-bit data words received by the port, not including flow control and VCRC data.
- **Transmit Packets**

  The number of data packets transmitted by the port, not including flow control packets.
- **Receive Packets**

  The number of data packets received by the port, not including flow control packets.
- **Symbol Errors**

  The number of times a 8B10B encoding violation, or a disparity violation was detected. If multiple errors are detected simultaneously (in more than one lane), the counter only increments by one. The value of the counter is not incremented past 65535. The Performance Manager may reset and/or consolidate the results of this counter.
- **Link Error Recovery**

  Indicates the number of times the link error recovery process happened successfully. The value of the counter is not incremented past 65535. The Performance Manager may reset and/or consolidate the results of this counter.
- **Link Downed**

  The number of times the link error recovery process failed. The value of the counter is not incremented past 65535. The Performance Manager may reset and/or consolidate the results of this counter.
- **Receive Errors**

  Number of errors received on the port.
- **Remote Physical Errors Received**

  Indicates bit errors on a link other than the physically attached link.
- **Transmit Discards**

  Number of port transmit discards.
- **Local Link Integrity Errors**

  An error caused by a marginal link. Depending upon the number of code violations, physical switch problems are detected at the physical layer. These errors are based on a count of local physical errors.
- **Excessive Buffer Overrun**

  This error is detected when the Overrun Errors threshold is exceeded by the number of consecutive flow control update periods with at least one overrun error in each period given in the PortInfo attribute.
- **Pkey Violations Inbound**

  Indicates the number of times an invalid partition key (PKey) was received. PKeys support an advanced InfiniBand feature for logically partitioning a physical subnet into logical access domains.

- **Pkey Violations Outbound**

  Indicates the number of times an invalid PKey was sent. PKeys support an advanced InfiniBand feature for logically partitioning a physical subnet into logical access domains.
- **Raw Violations Inbound**

  Number of times a raw inbound packet was discarded.
- **Raw Violations Outbound**

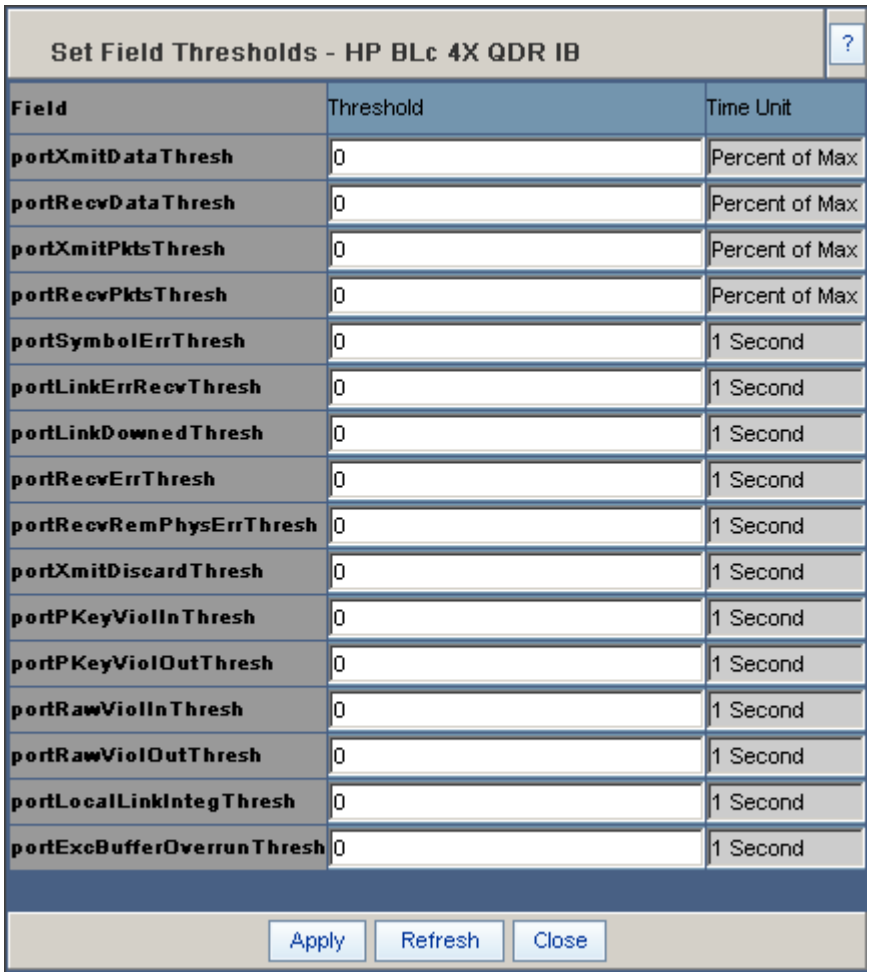
  Number of times a raw outbound packet was discarded.

Set Field Thresholds

The Set Field Thresholds screen lets you set, for a specific parameter(s), an error message threshold for the cable ports on the switch.

To change error reporting thresholds:

1. Click on **Set Field Thresholds** under the **Port Stats** menu. The **Set Field Thresholds** screen is displayed (Figure 33):



Set Field Thresholds - HP BLc 4X QDR IB

Field	Threshold	Time Unit
portXmitDataThresh	0	Percent of Max
portRecvDataThresh	0	Percent of Max
portXmitPktsThresh	0	Percent of Max
portRecvPktsThresh	0	Percent of Max
portSymbolErrThresh	0	1 Second
portLinkErrRecvThresh	0	1 Second
portLinkDownedThresh	0	1 Second
portRecvErrThresh	0	1 Second
portRecvRemPhysErrThresh	0	1 Second
portXmitDiscardThresh	0	1 Second
portPKeyViolInThresh	0	1 Second
portPKeyViolOutThresh	0	1 Second
portRawViolInThresh	0	1 Second
portRawViolOutThresh	0	1 Second
portLocalLinkIntegThresh	0	1 Second
portExcBufferOverrunThresh	0	1 Second

Apply Refresh Close

Figure 33 Set Field Thresholds Screen

2. To change a threshold value for any field:
   a. Click in the **Threshold** field.
   b. Enter a new threshold value.

NOTE: For those fields with a **Percent of Max** time unit, the user may enter a number from 0 to 100. For those fields with a **1 Second** time unit, you can enter a number from 1 to 65,535.

c. Click **Apply**.

NOTE: If any threshold is exceeded on any port, the port will be displayed as red on the switch map and a warning message will be logged.

The following are descriptions for each field in the Set Field Thresholds area:

NOTE: The thresholds for the following four fields are set as a percentage of maximum; that is, the percentage of maximum port capacity, which depending upon InfiniBand fabric configuration can be:

- 4X (10/20/40Gbps)
- 1X (2.5Gbps)

- **portXmitDataThresh**
  The threshold for the number of 32-bit data words transmitted by the port.
- **portRecvDataThresh**
  The threshold for the number of 32-bit data words received by the port.
- **portXmitPktsThresh**
  The threshold for the number of data packets transmitted by the port.
- **portRecvPktsThresh**
  The threshold for the number of data packets received by the port.

NOTE: The thresholds for the following fields are set based upon the number of error messages that can occur in one second. The value can be from 1 to 65,535.

- **portSymbolErrThresh**
  The threshold for the number of times a 8B10B encoding violation, or a disparity violation, was detected on the port.
- **portLinkErrRecvThresh**
  The threshold for the number of times the link error recovery process happened successfully on the port.
- **portLinkDownedThresh**
  The threshold for the number of times the link error recovery process failed on the port.
- **portRecvErrThresh**
  The threshold for the number of errors received on the port.
- **portRecvRemPhysErrThresh**
  The threshold for the number of remote physical errors received on the port.
- **portXmitDiscardThresh**
  The threshold for the number of transmit discards received on the port.
- **portPKeyViolInThresh**
  The threshold for the number of times a PKey inbound was invalid on the port.
- **portPKeyViolOutThresh**
  The threshold for the number of times a PKey outbound was invalid on the port.
- **portRawViolInThresh**
  The threshold for the number of times a raw inbound packet was discarded by the port.
- **portRawViolOutThresh**
  The threshold for the number of times a raw outbound packet was discarded by the port.
- **portLocalLinkIntegThresh**

The threshold for the number of local link integrity errors on the port.

- **portExcBufferOverrunThresh**
  The threshold for the number of excessive buffer overrun errors on the port.
- **Apply** Button
  Applies changes made to the **Set Field Thresholds** screen.
- **Refresh** button
  Refreshes information
- **Close** button
  Closes **Set Field Thresholds** screen

Port Beacon

The Port Beacon screen lets you enable or disable the Beacon for the cable ports on the switch. The Port Beacon feature allows the user to enable IB port(s) LED to flash, assisting a user in locating a port

To enable/disable the Port Beacons:

1. Click on **Port Beacon** under the **Port Stats** menu. The Port Beacon screen is displayed (Figure 34):

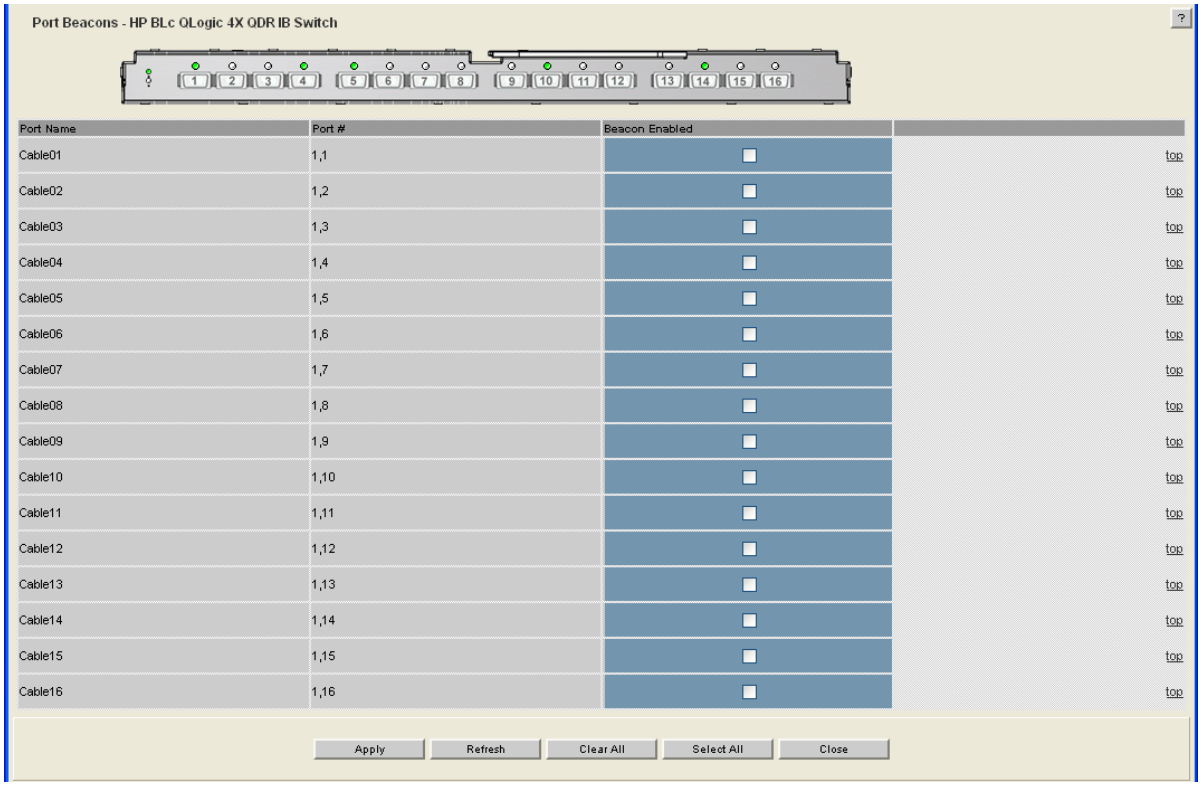


Figure 34 Port Beacon Screen

2. Click **Beacon Enabled** checkbox to the right of the Port Name and Port # Columns.
3. Click **Apply**. The physical port will blink. In Chassis Viewer, the IB Link Status LED for the port is outlined.

Time Service

The **Time Service** menu lets you set the system time using either network time protocol (NTP) or manual overrides. Clicking **Time Service** causes the submenus to display (Figure 35).

Figure 35 Switch Time Service Menu

To set the system time:

1. Click **Set System Time** under the **Time Service** menu. The **System Time Information** screen is displayed (Figure 36):

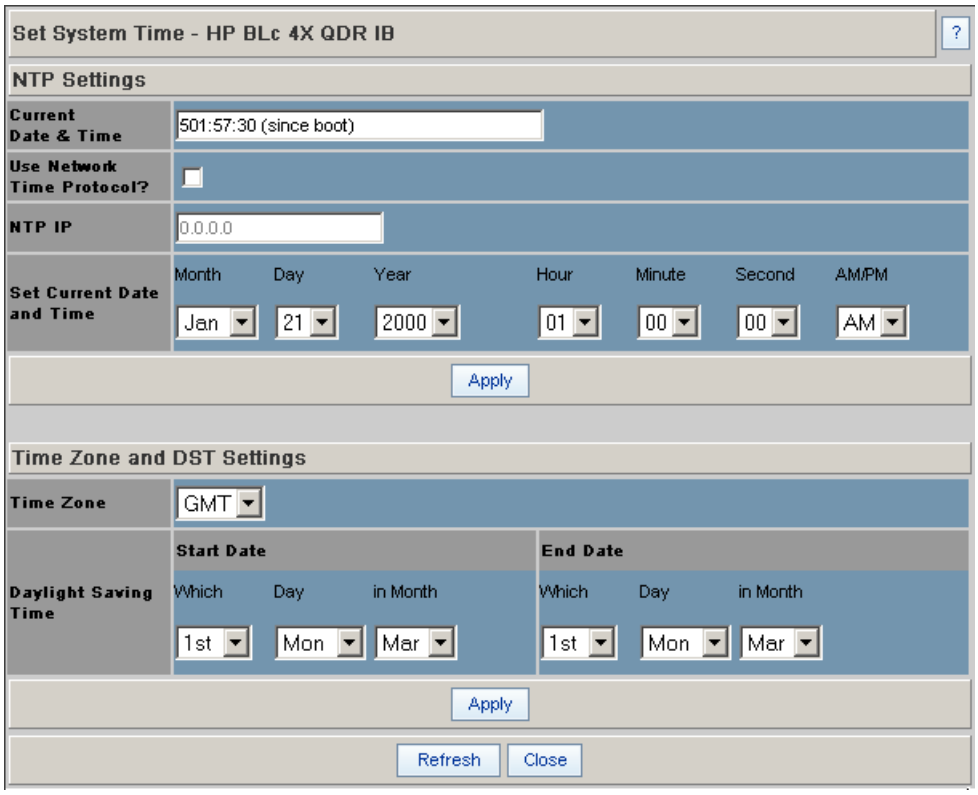


Figure 36 System Time Information Screen

To set up the system time to use NTP:

1. Click the **Use Network Time Protocol?** checkbox (callout 1, Figure 37).
2. Enter the IP address for the NTP server (callout 2, Figure 37).

3. To save, click **Apply** (callout 3, Figure 37).

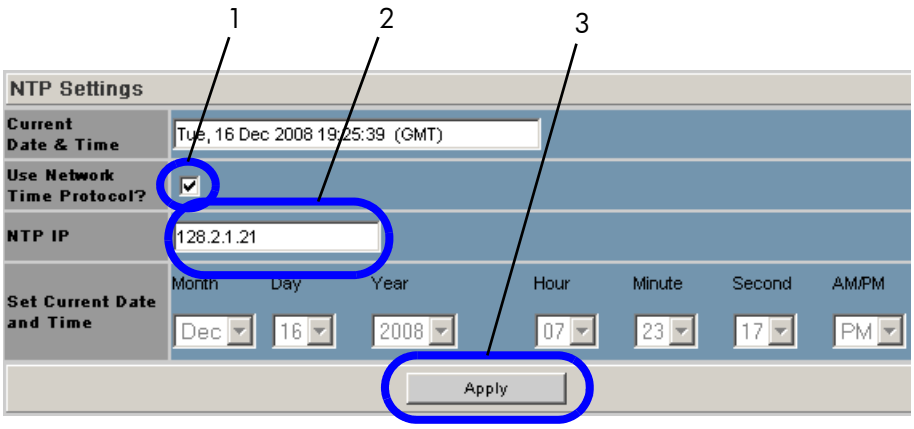


Figure 37 Time Service - NTP Setup

To manually set the system time:

1. Make sure the **Use Network Time Protocol?** checkbox is unchecked (callout 1, Figure 38).
2. Set the current date and time using the drop-downs for **Month**, **Day**, and **Year** as well as **Hour**, **Minute**, **Seconds**, and **AM/PM** (callout 2, Figure 38).
3. To save, click on **Apply** (callout 3, Figure 38).

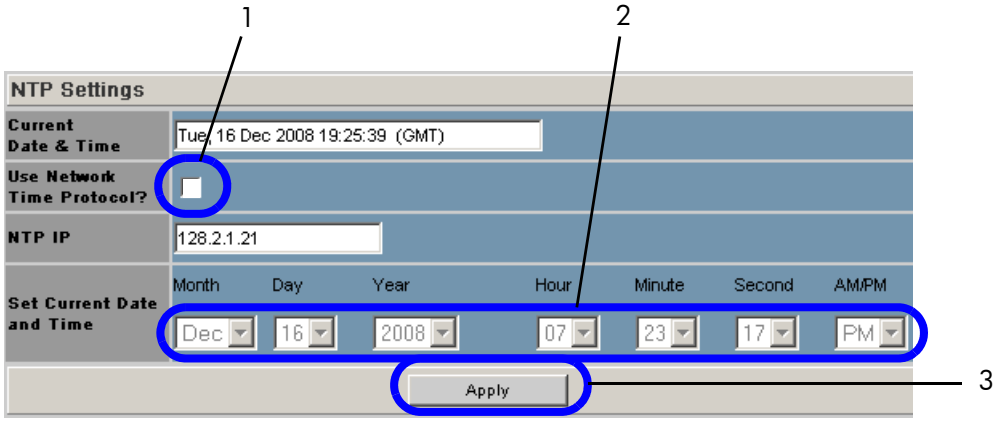


Figure 38 Time Service - Manual Setup

To set the time zone and Daylight Saving Time (DST) settings:

1. In the **Time Zone** drop-down, select the correct time zone based upon Greenwich Mean Time (GMT) (callout 1, Figure 39).
2. Using the **Which**, **Day**, and **in Month** drop-downs, set the start and end dates for Daylight Saving Time (callout 2, Figure 39).

3. To save, click **Apply** (callout 3, Figure 39).

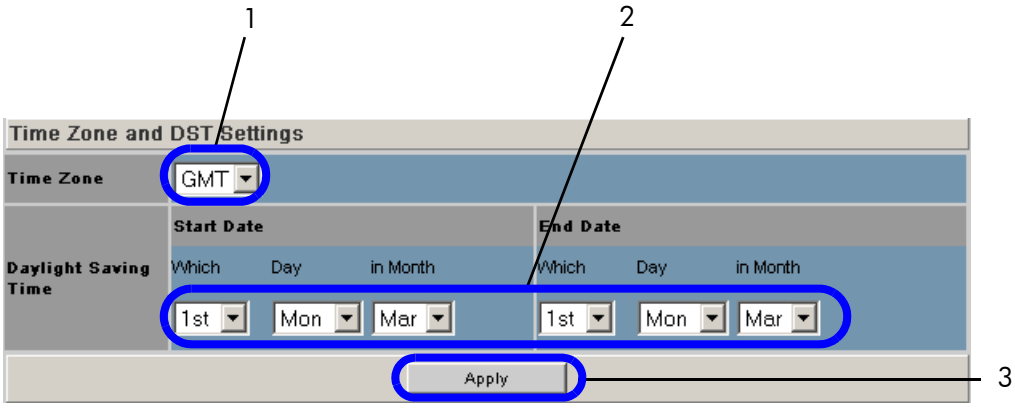


Figure 39 Time Service - Time Zone/Daylight Saving Time Setup

---

TIP: Time Zone:

In the US the following time zones are in effect:

- Eastern Standard Time = GMT –5
- Central Standard Time = GMT –6
- Mountain Standard Time = GMT –7
- Pacific Standard Time = GMT -8

TIP: Daylight Saving Time:

For most of the United States, Daylight Saving Time in the United States begins at 2 a.m. on the second Sunday of March, and ends at 2 a.m. on the first Sunday in November.

Additionally, for those US regions that do not observe DST, the start and end dates in the **Which**, **Day**, and **in Month** settings should be set to the **exact same date**.

OOB LAN IP

The **OOB LAN IP** menu lets you set the OOB LAN IPv6 address. Clicking **OOB LAN IP** causes the submenu to display (Figure 40).

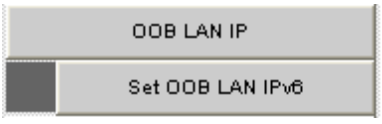


Figure 40 OOB LAN IP Menu

Set OOB LAN IPv6

To configure the switch IPv6 address:

1. Click **Set OOB LAN IPv6** under the **OOB LAN IP** menu. The **Set OOB LAN IPv6** screen is displayed (Figure 41):

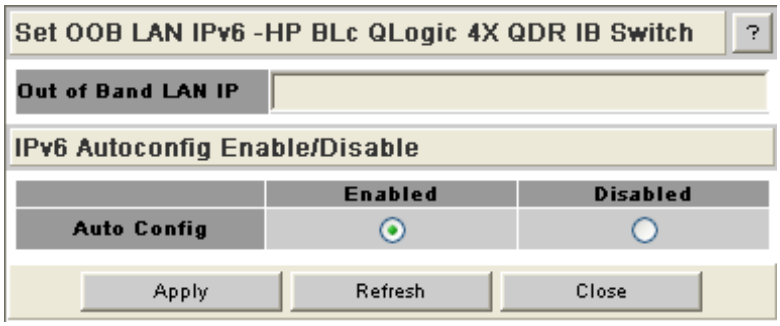


Figure 41 Set OOB LAN IPv6 Window

2. Enter an applicable static IPv6 address (in hexadecimal format address/prefix) in the **Out of Band LAN IP** text box.
3. To automatically assign addresses from an IPv6 router, click the **Enabled** radio button for automatic configuration.

> **NOTE:** The IPv6 router must be configured to assign addresses using stateless address auto configuration.

4. Click **Apply**.

Subnet Manager

The **Subnet Manager** menu lets you enable or disable the Subnet Manager at boot. Clicking **Subnet Manager** causes the submenus to display (Figure 42).

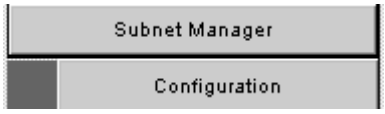


Figure 42 Subnet Manager Menu

Configuration

To enable or disable start-at-boot:

1. Click **Configuration** The **Subnet Manager Configuration** screen is displayed (Figure 43).

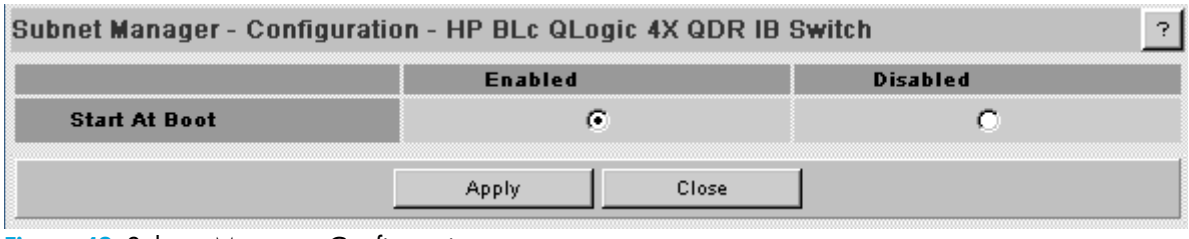


Figure 43 Subnet Manager Configuration

2. Select **Enable** or **Disable**.
3. Select **Apply**.

License Keys

The License Keys menu lets you manage the License Keys. Clicking **License Keys** causes the submenus to display (Figure 44).

Figure 44 License Keys Menu

Key Administration

To add License Keys:

1. Select **Key Administration** under the **License Keys** menu.The **License Key Management Information** screen is displayed (Figure 45).

Figure 45 License Key Management Information Window

2. Select **Add Key**. The **License Key Management Information** New Key entry screen is displayed (Figure 46).

Figure 46 License Key Management Information Add Key Window

3. Type in the new License Key information.
4. Click **Apply**.

2 Troubleshooting and Technical Reference

This section describes troubleshooting scenarios and technical reference information for the QLogic BLc 4X QDR IB Managed Switch and IB Switch Management Module. The section is organized in the following manner:

Hardware Checks

Troubleshooting Scenarios

Hardware Checks

Switch

Problem	Fix
The Switch has no power	Ensure that the switch is seated properly.

InfiniBand Ports

Problem	Fix
No LED	Make sure the InfiniBand cable is properly connected to both the switch port and to the destination device. Make sure the other end of the connection is plugged into a functioning HCA or switch. Make sure the cable does not exceed maximum distances.
Bad InfiniBand Cable	Test with a known good InfiniBand cable.

Troubleshooting Scenarios

InfiniBand

This section documents common problems seen with InfiniBand switches.

Invalid IP Address set on the Switch

Symptoms

Cannot access the Chassis Viewer browser window. The browser window times out and Chassis Viewer will not come up.

Resolution / Workaround

1. Invalid IP Address entered for the switch. Access the C7000 Onboard Administrator (OA) And Check the Enclosure Bay IP Addressing section. Check the Interconnect Bays tab to be sure that the address has been set correctly.
2. If attempting to access the switch from a remote LAN, ensure that the default gateway/default route addresses are set correctly in the OA on the Device bays and the Interconnect Bays. Also check that the system used has it's default gateway/default route configured correctly.

Nodes cannot be seen in QLogic Fabric Viewer

Symptoms

When viewing the InfiniBand fabric with the QLogic Fabric Viewer, no nodes are seen.

Resolution / Workaround

1. Possibly a bad InfiniBand cable(s). Ensure the port LED is illuminated on InfiniBand ports of the HP BLc QLogic 4X QDR IB Switch. Make sure that all devices (nodes) can be seen in the Fabric Viewer window.
2. Check the cables and connections subnet manager and the rest of the fabric.
3. The subnet manager may not be running on the IP address specified in Fabric Viewer. Check the IP address and make sure the subnet manager is in the Active state on that node. Depending on the configuration of that node, following a reboot the subnet manager may or may not restart.