Fabric Watch

User's Guide

Supporting Fabric OS v4.4.0

Supporting SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, 24000

Publication Number: 53-0000524-05
Publication Date: 09/15/04

 Publication Number: 53-0000524-05

Brocade Communications Systems, Incorporated

Corporate Headquarters
Brocade Communications Systems, Inc.
1745 Technology Drive
San Jose, CA 95110
Tel: 1-408-333-8000
Fax: 1-408-333-8101
E-mail: info@brocade.com

Latin America Headquarters
Brocade Communications System, Inc.
5201 Blue Lagoon Drive
Miami, FL 33126
Tel: 1-305-716-4165
E-mail: latinam-sales@brocade.com

European Headquarters
Brocade Communications Switzerland Sàrl
Centre Swissair
Tour A - 2ème étage
29, Route de l'Aéroport
Case Postale 105
CH-1215 Genève 15
Switzerland
Tel: +41 22 799 56 40
Fax: +41 22 799 56 41
E-mail: emea-info@brocade.com

Asia-Pacific Headquarters
Brocade Communications Systems K.K.
Shiroyama JT Trust Tower 36th FL.
4-3-1 Toranomon, Minato-ku
Tokyo, Japan 105-6036
Tel: +81-3-5402-5300
Fax: +81-3-5402-5399
E-mail: japan-info@brocade.com

Document History

The following table lists all versions of the *Brocade Fabric Watch User's Guide*.

Document Title	Publication Number	Summary of Changes	Publication Date
Fabric Watch User's Guide	53-0001559-02	n.a.	May 2000
Fabric Watch User's Guide	53-0000198-02	n.a.	January 2002
Fabric Watch User's Guide	53-0000186-02	n.a.	March 2002
Fabric Watch User's Guide	53-0000504-02	n.a.	April 2003
Fabric Watch User's Guide	53-0000524-02	n.a.	April 2003
Fabric Watch User's Guide	53-0000524-03	Updated default values and restructured the document.	December 2003
Fabric Watch User's Guide	53-0000524-04	Rewrote the document completely and added new features. Reorganized procedures into steps, rewrote many sections to improve clarity. Added technical and editorial changes.	April 2004
Fabric Watch User's Guide	53-0000524-05	Updates to support Fabric OS v4.4.0 features and SilkWorm 3016 and 4100 switches. Rewrote Chapter 4, "Configuring Fabric Watch."	September 2004

Contents

About This Document

This document is a user's guide to help you use the Fabric Watch product to monitor and improve fabric health.

"About This Document" contains the following sections:

How This Document Is Organized

This document contains:

- Chapter 1, "An Introduction to Fabric Watch," provides an introduction to Fabric Watch and the benefits of its use.
- Chapter 2, "Fabric Watch Concepts," includes definition of all concepts useful in Fabric Watch configuration and all terms used in this guide.
- Chapter 3, "Activating and Accessing Fabric Watch,"describes the Fabric Watch requirements, provides an overview of the interfaces and explains the methods of accessing Fabric Watch through each interface.
- Chapter 4, "Configuring Fabric Watch," describes all of the methods of performing Fabric Watch configuration.
- Chapter 5, "Generating Fabric Watch Reports," describes the reports available through Fabric Watch and the methods of accessing each.
- Appendix A, "Default Threshold Values," describes the Fabric Watch default threshold values for all classes.
- Appendix B, "Basic Fabric Watch Configuration Guidelines," describes some of the changes Fabric Watch users should consider when configuring their implemention.
- Appendix C, "Using Fabric Watch with Configuration Files," describes the two methods of using configuration files.
- The glossary defines both terms specific to Brocade technology and common industry terms with uses specific to Brocade technology.
- The index points you to the exact pages on which specific information is located.

Supported Hardware and Software

This document has been updated to include information specific to the Fabric OS v4.4.0 release, including:

- Additional functionality or support in the software from Fabric OS v4.4.0
- SilkWorm 3016 support
- SilkWorm 4100 support

Although many different software and hardware configurations are tested and supported by Brocade Communications Systems, Inc. for the Brocade Fabric OS v4.4.0 release, documenting all possible configurations and scenarios is beyond the scope of this document.

This document does not support all 4.x Fabric OS versions. This document is specific to the Brocade Fabric OS v4.4.0 release. To obtain information about an OS version other than v4.4.0, refer to the documentation specific to your OS version.

What's New in This Document

The following changes have been made since this document was last released:

- Information that was added:
  - Disable/Enable/View Port Thresholds
  - Configuring Switch Status Policy
  - In the Port Detail Report there is a new column, Buffer Limited Port (BLP)
  - SilkWorm 3016 and 4100 support
- Information that was changed:
  - Terminology changes in the default threshold values
  - Error log message formats
  - Chapter 4, "Configuring Fabric Watch," has been rewritten to improve usability. Information in the following sections has been changed:
    - "Configuring Fabric Watch Thresholds"
    - "Configuring FRUs"
- Information that was deleted:
  - Within the default threshold values, the exceeded state removed
  - SilkWorm 3200 and 3800 support is no longer included in this document
  - CRC counters are not supported on the SilkWorm 4100 platform

For further information, refer to the Fabric OS v4.4.0 Release Notes.

Document Conventions

This section describes text formatting conventions and important notices formats.

Text Formatting

The narrative-text formatting conventions that are used in this document are as follows:

bold text	Identifies command names Identifies GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles and cross-references
`code` text	Identifies CLI output Identifies syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, **switchShow**. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, Cautions, and Warnings

The following notices appear in this document.

Note

A note provides a tip, emphasizes important information, or provides a reference to related information.

Caution

A caution alerts you to potential damage to hardware, firmware, software, or data.

Warning

A warning alerts you to potential danger to personnel.

Additional Information

This section lists additional Brocade and industry-specific documentation that you might find helpful.

Brocade Resources

The following related documentation is provided on the Brocade Documentation CD-ROM and on the Brocade Web site, through Brocade Connect.

Note

Go to *http://www.brocade.com* and click **Brocade Connect** to register at no cost for a user ID and password.

- Fabric OS documentation
  - *Fabric OS System Error Message Reference Manual*
  - *Fabric OS Procedures Guide*
  - *Fabric OS Command Reference Manual*
  - *Fabric OS MIB Reference Manual*
- Fabric OS optional features documentation
  - *Fabric OS Features Guide*
  - *Advanced Web Tools Administrator's Guide*
  - *Secure Fabric OS User's Guide*
  - *Secure Fabric OS QuickStart Guide*
- Brocade Hardware documentation
  - *SilkWorm 24000 Hardware Reference Manual*
  - *SilkWorm 12000 Hardware Reference Manual*
  - *SilkWorm 3900 Hardware Reference Manual*
  - *SilkWorm 3250/3850 Hardware Reference Manual*
  - *SilkWorm 3016 Hardware Reference Manual*
  - *SilkWorm 4100 Hardware Reference Manual*

For practical discussions about SAN design, implementation, and maintenance, you can obtain *Building SANs with Brocade Fabric Switches* through:

http://www.amazon.com

For additional Brocade documentation, visit the Brocade SAN Info Center and click the Resource Library location:

http://www.brocade.com

Release notes are available on the Brocade Connect Web site and are also bundled with the Fabric OS firmware.

Other Industry Resources

For additional resource information, visit the Technical Committee T11 Web site. This Web site provides interface standards for high-performance and mass storage applications for Fibre Channel, storage management, as well as other applications:

http://www.t11.org

For information about the Fibre Channel industry, visit the Fibre Channel Industry Association Web site:

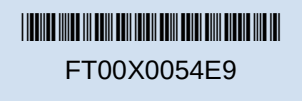
http://www.fibrechannel.org

Getting Technical Help

Contact your switch support supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. **General Information**
   - Technical Support contract number, if applicable
   - Switch model
   - Switch operating system version
   - Error messages received
   - **supportShow** command output
   - Detailed description of the problem and specific questions
   - Description of any troubleshooting steps already performed and results
   - Provide custom configuration (if used)
2. **Switch Serial Number**

   The switch serial number and corresponding bar code are provided on the serial number label, as shown here:

   The serial number label is located as follows:

   - *SilkWorm 3016 switch:* Side of chassis
   - *SilkWorm 3250, 3850, and 3900 switches:* Bottom of chassis.
   - *SilkWorm 4100 switches*: On the switch ID pull-out tab located on the port side and on the inside of the chassis, near power supply 1 (on the right when looking at the nonport side).
   - *SilkWorm 12000 and 24000 directors:* Inside the front of the chassis, on the wall to the left of the ports.

3. **World Wide Name (WWN)**
    - *SilkWorm 3016, 3250, 3850, 3900, and 4100 switches* and *SilkWorm 12000 and 24000 directors:* Provide the license ID. Use the **licenseIDshow** command to display the license ID.
    - *All other SilkWorm switches:* Provide the switch WWN. Use the **wwn** command to display the switch WWN.

Document Feedback

Because quality is our first concern at Brocade, we have made every effort to ensure the accuracy and completeness of this document. However, if you find an error or an omission, or you think that a topic needs further development, we want to hear from you. Forward your feedback to *documentation@brocade.com*. Provide the title and version number and as much detail as possible about your issue, including the topic heading and page number and your suggestions for improvement.

An Introduction to Fabric Watch

Chapter 1

This chapter contains the following sections:

Fabric Watch Overview

Fabric Watch is an optional storage area network (SAN) health monitor software for Brocade SilkWorm switches running Fabric OS 2.2 or higher. It enables each switch to constantly watch its SAN fabric for potential faults and to automatically alert you to problems long before they become costly failures.

Fabric Watch tracks a variety of SAN fabric elements, events, and counters. Monitoring fabric-wide events, ports, GBICs, and environmental parameters enables early fault detection and isolation as well as performance measurement. You can select custom fabric elements and alert thresholds or choose from a selection of preconfigured settings. You can also easily integrate Fabric Watch with enterprise systems management solutions.

By implementing Fabric Watch, you can rapidly improve SAN availability and performance without installing new software or system administration tools.

For a growing number of organizations, SAN fabrics are a mission-critical part of their systems architecture. These fabrics can include hundreds of elements, such as hosts, storage devices, switches, and inter-switch links (ISLs). An instrumentation solution for SANs delivers optimal value by tracking a wide spectrum of fabric events. For instance, Fabric Watch monitors:

- Fabric resources, including fabric reconfigurations, zoning changes, and new logins.
- Switch environmental functions such as temperature, power supply, and fan status, along with security violations.
- Port state transitions, errors, and traffic information for multiple port classes as well as operational values for supported models of "Smart" GBICs/SFPs.
- Performance information for AL_PA, end-to-end, and SCSI command metrics.

Fabric Watch lets you define how often to measure each switch and fabric element and to specify notification thresholds. Whenever fabric elements exceed these thresholds, Fabric Watch automatically provides notification using several methods, including email messages, SNMP traps, and log entries.

Fabric Watch provides the following two types of automatic notifications:

- A continuous alarm provides a warning message whenever a threshold is breached; it continues to send alerts until the condition is corrected. For example, if a switch exceeds its temperature threshold, Fabric Watch activates an alarm at every measurement interval until the temperature returns to an acceptable level.
- A triggered alarm generates the first warning when a threshold condition is reached and a second alarm when the threshold condition is cleared.
- Fabric Watch provides event notifications in several different formats to ensure that event details are accessible from all platforms and operating systems. In response to an event, Fabric Watch can record event data as any (or all) of the following:
- Simple network management protocol (SNMP) trap

  Following an event, Fabric Watch transmits critical event data as an SNMP trap. Support for SNMP makes Fabric Watch readily compatible with both network and enterprise management solutions.

- Event log entry

  Following an event, Fabric Watch adds an entry to the internal Event Log for an individual switch, which stores up to 1024 error messages.

- Lock port log

  Following an event, Fabric Watch adds an entry to the internal port log for an individual switch and freezes the log to ensure that detail-level information is available.

- RapiTrap

  Following an event, Fabric Watch forwards event information to a proxy switch, which then forwards the information to a server to notify you.

- Email notification

  Following an event, Fabric Watch creates and sends an Informational email to a designated recipient.

Fabric Watch is designed for rapid deployment. Simply enabling Fabric Watch permits immediate fabric monitoring. Fabric Watch is also designed for rapid custom configuration. You can easily create and modify configuration files using a text editor and then distribute configurations to all the switches in the SAN through the Fabric OS configuration management utility. Fabric Watch also comes with preconfigured profiles for rapid implementation.

See Also: For information on configuring and managing your SAN, refer to the *Fabric Manager User's Guide*.

Introduction to Fabric Health

Fabric health refers to the capability of the fabric to support data to be routed through it. A healthy fabric enables effective data transmission between networked devices.

Although the concept of fabric health initially seems fairly simple, it can be a deep and complex topic due to the number of factors that are involved. One of the more obvious criteria for fabric health is the condition of the network hardware. A switch or port failure could easily prevent data packets from reaching their destination. Network traffic can also influence fabric health.

If the number of packets routed through a port exceeds the port bandwidth, it causes network delays and packet losses. Even environmental factors can become issues, as network hardware can fail to function properly when stored in locations that do not meet the environmental conditions for the device. For example, switches can fail when stored in rooms that are too hot.

Because of the varied and complex factors in determining fabric health, you need fabric monitoring software such as Fabric Watch to help you to quickly detect, identify, and resolve fabric health issues by continuously monitoring possible issues and reporting any potential concerns. Fabric Watch automatically provides detailed reports on detected issues and helps you correct failures.

Fabric Watch provides customizable monitoring thresholds. You can configure Fabric Watch to provide notification before problems arise, such as reporting when network traffic through a port is approaching the bandwidth limit. This information enables you to perform preemptive network maintenance such as trunking or zoning and avoid potential network failures.

1

Fabric Watch Concepts

Chapter 2

This chapter contains the following sections:

Fabric Watch Components

Fabric Watch uses a hierarchical organization to track the network device information it monitors. There is a class, area, and element associated with every monitored behavior. Classes are the highest level in the system, subdivided into one or more areas. Areas contain one or more elements.

The following sections explain this hierarchy and its application within Fabric Watch.

Classes

Classes are high-level categories of elements. Classes are intentionally wide groupings of similar fabric devices or fabric data.

Examples of classes include Port (which includes all physical ports on a switch), Security (which includes information related to unauthorized login attempts), and Environment (which contains information related to the room temperature, supplied power and fan assemblies).

In some cases, classes are divided into subclasses. This additional level in the hierarchy increases the flexibility of setting monitoring thresholds. You can use subclasses to add additional event monitoring to fabric objects that meet the requirements of a subclass.

For example, ports connected to another switch can be monitored using both the Port class and E_Port subclass. You can configure general port monitoring using the Port class and monitoring specific to a type of port using the E_Port class. Ports connected to another switch can trigger events based on either of these configurations. Ports that are not connected to another switch are not affected by the additional monitoring configured into the E_Port class.

Table 2-1 describes the classes into which Fabric Watch groups all switch and fabric elements.

Table 2-1 Fabric Watch Classes

Class	Description
Environment	Includes information about the physical environment in which the switch resides and the internal environment of the switch. For example, an Environment-class alarm alerts you to problems or potential problems with temperature and power.
Fabric	Groups areas of potential problems arising between devices, including interswitch link (ISL) details, zoning, and traffic. A Fabric-class alarm alerts you to problems or potential problems with interconnectivity.
Field Replaceable Unit (FRU)	Monitors the status of FRUs and provides an alert when a part replacement is needed. This class monitors states, not thresholds.
Performance Monitor	Serves as a tuning tool. Performance Monitor classes group areas that track the source and destination of traffic. Use the Performance Monitor class thresholds and alarms to determine traffic load and flow and to reallocate resources appropriately. The Performance Monitor class is divided into the areas AL_PA Performance Monitor, EE (end-to-end) Performance Monitor, and Filter Performance Monitor.
Port	Enables you to set additional thresholds, specific to different types of ports. The Port class is divided into separate classes: E_Port class—Represents ports connected to another switch. F/FL_Port class —Represents fabric or fabric loop ports that are made of copper or optical fiber.
Resource	Monitors flash memory. It calculates the amount of flash space consumed and compares it to a defined threshold.
Security	Monitors all attempts to breach your SAN security, helping you fine-tune your security measures.
SFP	Groups areas that monitor the physical aspects of SFPs. An SFP class alarm alerts you to a SFP malfunction fault.

Areas

While classes represent large groupings of information, areas represent the information that Fabric Watch monitors. For example, switch temperature, one of the values tracked by Fabric Watch, is an area within the class Environment.

The tables in this section describe all of the areas monitored by Fabric Watch, organized by their associated classes.

Environment Class Areas

Table 2-2 lists and describes the Fabric Watch areas in the Environment class.

Table 2-2 Environment Class Areas

Area	Description
Fan	Refers to the speed of the fans inside the switch, in revolutions per minute. It is important that the fans spin quickly enough to keep the ambient temperature from rising to levels at which switch damage might occur.
Power Supply	Monitors whether power supplies within the switch are on, off, present, or absent. Fabric Watch monitors power supplies to be sure that power is always available to a switch.
Temperature	Refers to the ambient temperature inside the switch, in degrees Celsius. Temperature sensors monitor the switch in case the temperature rises to levels at which damage to the switch might occur.

Note

The SilkWorm 3016 only supports the temperature environment class area because it has no fan or power supply associated with it.

Fabric Class Areas

Table 2-3 lists Fabric Watch areas in the Fabric class and describes each area.

Table 2-3 Fabric Class Areas

Area	Description
Domain ID Changes	Monitors forcible domain ID changes. Forcible domain ID changes occur when there is a conflict of domain IDs in a single fabric and the principal switch has to assign another domain ID to a switch.
Fabric Logins	Occurs when ports and devices initialize with the fabric.
Fabric Reconfiguration	Tracks the number of reconfigurations of the fabric. Fabric reconfiguration occurs when: • Two fabrics with the same domain ID are connected. • Two fabrics are joined. • An E_Port has gone offline. • A principal link has segmented from the fabric.

Table 2-3 Fabric Class Areas (Continued)

Area	Description
Loss of E_Port	Tracks the number of times that an E_Port goes down. E_Ports go down each time you remove a cable or an SFP (where there are SFP failures or transient errors).
Segmentation Changes	Tracks the cumulative number of segmentation changes. Segmentation changes occur due to: • Zone conflicts. • Incompatible link parameters. During E_Port initialization, ports exchange link parameters, and incompatible parameters result in segmentation. This is a rare event. • Domain conflicts. • Segmentation of the principal link between two switches.
SFP State Changes	Indicates whether the state of the SFP is normal or faulty, on or off. A faulty or off state means that you must reinsert, turn on, or replace the SFP. Fabric Watch monitors only Digital Diagnostic SFP.
Zoning Changes	Tracks the number of zone changes. Because zoning is a security provision, frequent zone changes might indicate a security breach or weakness. Zone change messages occur whenever there is a change in zone configurations.

FRU Class Areas

Table 2-4 lists Fabric Watch areas in the FRU class and describes each area. Possible states for all FRU-class areas are absent, faulty, inserted, on, off, ready, and up.

Table 2-4 FRU Class Areas

Area	Indicates
Slot	State of a slot has changed.
Power Supply	State of a power supply has changed.
Fan	State of a fan has changed.
WWN	State of a WWN card has changed.

Supported FRU areas depend on the types of Brocade switches. For nonmodular switches such as 3250, 3850, 3900, and the 4100, the Slot and WWN areas are not supported. The SilkWorm 3016 does not support any of the FRU class areas.

Performance Monitor Class Areas

Table 2-5 lists Fabric Watch areas in the Performance Monitor class and describes each area.

Table 2-5 Performance Monitor Class Areas

Area	Indicates
Customer Define	Relies on performance monitor telnet commands. For more information on this area, refer to the *Fabric OS Command Reference Manual*.
Invalid CRC	Errors have been detected in the Fibre Channel frame. Invalid CRC messages occur when the number of CRC errors in Fibre Channel frames for specific source ID (S_ID) and destination ID (D_ID) pairs change. These messages can also be caused by dirty or aging equipment and temperature fluctuations.
Receive Performance	The percentage of word frames traveling from the configured S_ID to the D_ID exceeds the configured thresholds.
Transmit Performance	The percentage of word frames traveling from the configured S_ID to the D_ID; user configuration triggers these messages, so you can use the Transmit Performance area to tune your network.

Port Class Areas

Table 2-6 lists and describes the Fabric Watch areas in the port class.

Table 2-6 Port Class Areas

Area	Indicates
Invalid Cyclic Redundancy Checks (CRCs)	A frame is invalid and cannot be transmitted. Invalid CRCs can represent noise on the network. Such frames are recoverable by retransmission. Invalid CRCs indicate a potential hardware problem. These errors occur mostly in aging fabrics.
Invalid Transmission Word	A word did not transmit successfully. Invalid word messages usually indicate a hardware problem.
Link Failure Count	A link loses signal. Both physical and hardware problems can cause link failures. Link failures frequently occur due to a loss of synchronization. Check for concurrent loss of synchronization errors and, if applicable, troubleshoot those errors. Link failures also occur due to hardware failures.
Loss of Signal Count	The number of times that a signal loss occurs in a port. Signal loss indicates that no data is moving through the port. A loss of signal usually indicates a hardware problem.
Loss of Synchronization (Sync) Count	Two devices failed to communicate at the same speed. Synchronization losses are always accompanied by link failure. Loss of synchronization errors frequently occur due to a faulty SFP or cable.

Table 2-6 Port Class Areas (Continued)

Area	Indicates
Primitive Sequence Protocol Error	A CRC sum disparity. Occasionally, these errors occur due to software glitches. Persistent errors occur due to hardware problems.
Receive (RX) Performance	The percentage of maximum bandwidth consumed in packet receipts.
State Changes	The state of the port has changed for one of the following reasons: • The port has gone offline. • The port has come online. • The port is testing. • The port is faulty. • The port has become an E_Port. • The port has become an F/FL_Port. • The port has segmented. • The port has become a trunk port.
Transmit (TX) Performance	The percentage of maximum bandwidth consumed in packet transmissions.

Resource Class Area

Table 2-7 describes the Fabric Watch resource class area.

Table 2-7 Resource Class Area

Area	Description
Flash Monitor	Monitors the compact flash space available by calculating the percentage of flash space consumed and comparing it with the configured high threshold value.

Security Class Areas

Table 2-8 lists Fabric Watch areas in the security class and describes what each area indicates. For details on each area, refer to the *Secure Fabric OS User's Guide*.

Table 2-8 Security Class Areas

Area	Indicates
API Violation	An API access request reaches a secure switch from an unauthorized IP address.
DCC Violation	An unauthorized device attempts to log in to a secure fabric.
Front Panel Violation	A secure switch detects unauthorized front panel access.
HTTP Violation	A browser access request reaches a secure switch from an unauthorized IP address.

Table 2-8 Security Class Areas (Continued)

Area	Indicates
Illegal Command	Commands permitted only to the primary Fibre Channel Switch (FCS) are executed on another switch.
Incompatible DB	Secure switches with different version stamps have been detected.
Invalid Certificates	The primary FCS sends a certificate to all switches in the secure fabric before it sends configuration data. Receiving switches accept only packets with the correct certificate; any other certificates are invalid and represent an attempted security breach.
Invalid Signatures	If a switch cannot verify the signature of a packet, the switch rejects the packet and the signature becomes invalid.
Invalid Timestamps	If a time interval becomes too great from the time a packet is sent to the time it is received, the timestamp of the packet becomes invalid and the switch rejects it.
Login Violation	A login violation occurs when a secure fabric detects a login failure.
MS Violation	An MS (Management Server) violation occurs when an access request reaches a secure switch from an unauthorized WWN (World Wide Name). The WWN appears in the ERRLOG.
No FCS	The switch has lost contact with the primary FCS.
RSNMP Violation	An RSNMP (remote simple network management protocol) violation occurs when an SNMP (simple network management protocol) **get** operation reaches a secure switch from an unauthorized IP address.
SCC Violation	An SCC violation occurs when an unauthorized switch tries to join a secure fabric. The WWN of the unauthorized switch appears in the ERRLOG.
Serial Violation	A serial violation occurs when a secure switch detects an unauthorized serial port connection request.
SES Violation	An SES violation occurs when an SES (SCSI Enclosed Services) request reaches a secure switch from an unauthorized WWN.
SLAP Bad Packets	A SLAP (Switch Link Authentication Protocol) bad packets failure occurs when the switch receives a bad SLAP packet. Bad SLAP packets include unexpected packets and packets with incorrect transmission IDs.
SLAP Failures	A SLAP failure occurs when packets try to pass from a nonsecure switch to a secure fabric.
Telnet Violation	A telnet violation occurs when a telnet connection request reaches a secure switch from an unauthorized IP address.
TS Out of Sync	A TS (Time Server) Out of Synchronization error has been detected.
WSNMP Violation	A WSNMP violation occurs when an SNMP **set** operation reaches a secure switch from an unauthorized IP address.

SFP Class Areas

Table 2-9 lists Fabric Watch areas in the SFP class and describes each area.

Table 2-9 SFP Class Areas

Area	Description
Temperature	The temperature area measures the physical temperature of the SFP, in degrees Celsius. A high temperature indicates that the SFP might be in danger of damage.
Receive Power	The receive power area measures the amount of incoming laser, in µwatts, to help determine if the SFP is in good working condition. If the counter often exceeds the threshold, the SFP is deteriorating.
Transmit Power	The transmit power area measures the amount of outgoing laser, in µwatts. Use this to determine the condition of the SFP. If the counter often exceeds the threshold, the SFP is deteriorating.
Current	The current area measures the amount of supplied current to the SFP transceiver. Current area events indicate hardware failures.
Supply Voltage	The supply voltage area measures the amount of voltage supplied to the SFP. If this value exceeds the threshold, the SFP is deteriorating.

Elements

Fabric Watch defines an *element* as any fabric or switch component that the software monitors. Within each area, there are a number of elements equivalent to the number of components being monitored. For instance, on a 64-port switch, each area of the Port class will include 64 elements.

Each element contains information pertaining to the description suggested by the area. To continue the Ports example, each element in the Invalid word area of Ports would contain exactly 64 ports, each of which would contain the number of times invalid words had been received by the port over the last time interval. Each of these elements maps to an index number, so that all elements can be identified in terms of class, area, and index number. As an example, the monitoring of the temperature sensor with an index of one may be viewed by accessing the first temperature sensor within the temperature area of the environment class.

Subclasses are a minor exception to the above rule. Subclasses, such as E_Ports, contain areas with elements equivalent to the number of valid entries. Within the same example used thus far in this section, in a 64-port switch in which eight ports are connected to another switch, each area within the E_Port class would contain eight elements.

Each area of a subclass with defined thresholds will act in addition to the settings applied to the element through the parent class. Assignment of elements to subclasses does not need to be performed by a network administrator. These assignments are seamlessly made through automated detection algorithms.

Configuring Events

The following area attributes are used to define and detect events in Fabric Watch:

- "Event Behavior Types" next
- "Data Values," on page 2-9
- "Threshold Values," on page 2-10
- "Time Bases," on page 2-11
- "Event Settings," on page 2-14

You can customize the information reported by Fabric Watch by configuring event behavior types, threshold values, time bases, and event settings. You cannot change data values; these represent switch behavior that is updated by the software.

Event Behavior Types

Based on the number of notifications delivered for events there are two categories of event behavior types:

- "Continuous Event Behavior"
- "Triggered Event Behavior"

Continuous Event Behavior

Areas with event behavior types set to *continuous* trigger events in every sample period until the fabric no longer meets the criteria defined for the event.

For example, you can configure Fabric Watch to notify you during every sample period that a port is at full utilization. This information can help you plan network upgrades.

Triggered Event Behavior

If you do not want notification during each sample period from the port hardware failure to the time of its repair, you can define the event behavior as *triggered*.

When an event behavior is defined as triggered, Fabric Watch sends only one event notification when the fabric meets the criteria for the event. It does not send out any more notifications.

For example, when a port fails, Fabric Watch sends you a notification of the failure. After you repair the port, Fabric Watch detects the repair. At this time, Fabric Watch determines that the fabric no longer meets the event criteria, and watches for the error again. The next time the port fails, it sends you another notification.

Data Values

A data value represents an aspect of a fabric in three ways: counter value, measured value or state value. Data values are updated by Fabric Watch approximately every six seconds. You cannot change them.

Counter value is the total number of times that a given event has occurred. For each monitored event during the time period, the value is incremented.

Measured value is the current, measurable value of a fabric or fabric element, such as environmental temperature or fan speed.

State value, which is the only qualitative data value, provides information on the overall state of a fabric component, such as the physical health of a fan. Instead of numerical data, state values contain information on whether components are faulty, active, or in another state.

Fabric Watch compares counter values and measured values to a set of configurable limits to determine whether fabric monitoring has occurred and whether to notify you. You must set appropriate threshold boundaries to trigger an event.

State values are handled differently, as Fabric Watch monitors state values for certain states, which you can select. When a state value transitions to one of the monitored states, an event is triggered.

Threshold Values

Threshold values are of the following types:

- "High and Low Thresholds"
- "Buffer Values"

High and Low Thresholds

High and low threshold values are the values at which potential problems might occur. For example, in configuring a temperature threshold, you can select the temperatures at which a potential problem can occur due to both overheating and freezing.

You can compare high and low thresholds with a data value. The units of measurement are the same as that of the associated data.

Buffer Values

You can use buffer values to reduce the occurrence of events due to data fluctuation. When you assign a buffer value, it is used to create a zone in which events cannot occur both above the high threshold and below the low threshold.

Figure 2-1 shows an example in which each time a signal crosses the high limit, an event occurs. The blue arrows indicate the area where the event criteria is met. In this case, there is a great deal of fluctuation. Even when the monitor is set to triggered, a number of messages are sent.

Figure 2-1 Threshold Monitoring

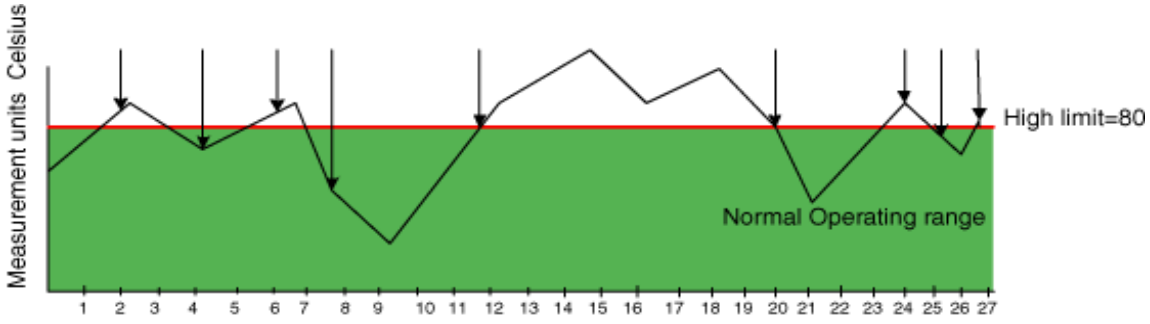
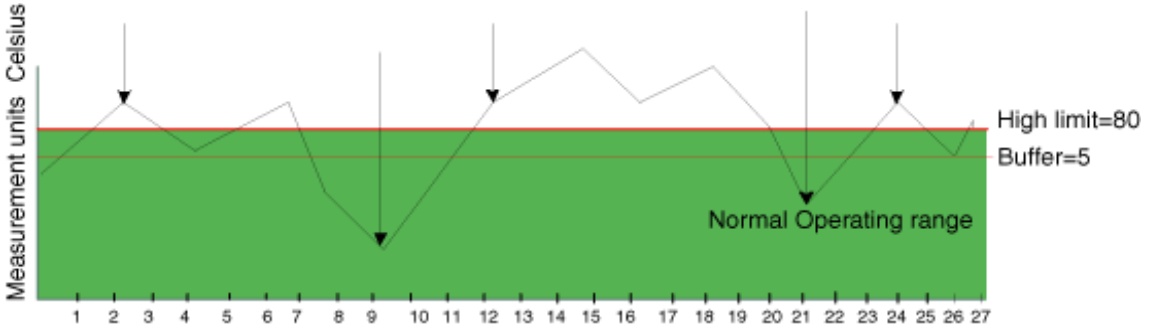


Figure 2-2 shows how to limit the number of event notifications using a buffer. When you specify a buffer, events cannot occur both above the high threshold and below the low threshold. Event notification occurs only where the arrow indicates. The event criteria is continued to be met until the data sensed falls below the high threshold value.

Figure 2-2 A Buffered Data Region



Time Bases

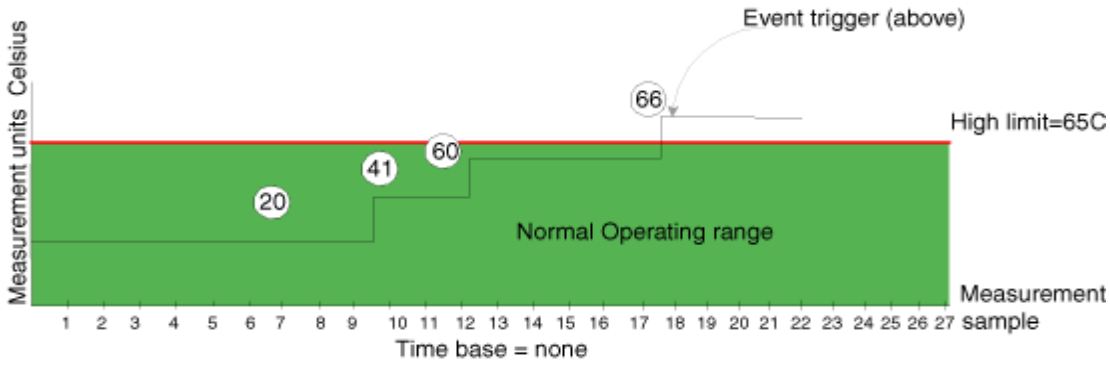
Time bases are time periods within Fabric Watch. This configurable field impacts the comparison of sensor-based data with user-defined threshold values.

Setting Time Base to None

If you set a time base to **none**, Fabric Watch compares a data value against a threshold boundary level. When the absolute value of the measuring counter exceeds the threshold boundary, an event is triggered.

Figure 2-3 shows a high limit of 65 degrees Celsius placed on a counter measuring temperature. During each sample period, Fabric Watch measures the temperature is measured and compares it against the high threshold. If the measured temperature exceeds the high threshold, it triggers an event.

Figure 2-3 Time Base Set to None



Specifying a Time Base

If you specify a time base value other than **none** (**seconds**, **minute**, **hour**, or **day**), Fabric Watch does not use the current data value. Instead, it calculates the difference between the current data value and the data value as it existed one time base ago. It compares this difference to the threshold boundary limit.

For example, if you specify the time base *minute*, Fabric Watch calculates the counter value difference between two samples a minute apart. It then compares the difference (current data value – data value one minute ago) against the preset threshold boundary.

When you set a time base to a value other than **none**, there are two main points to remember when configuring events:

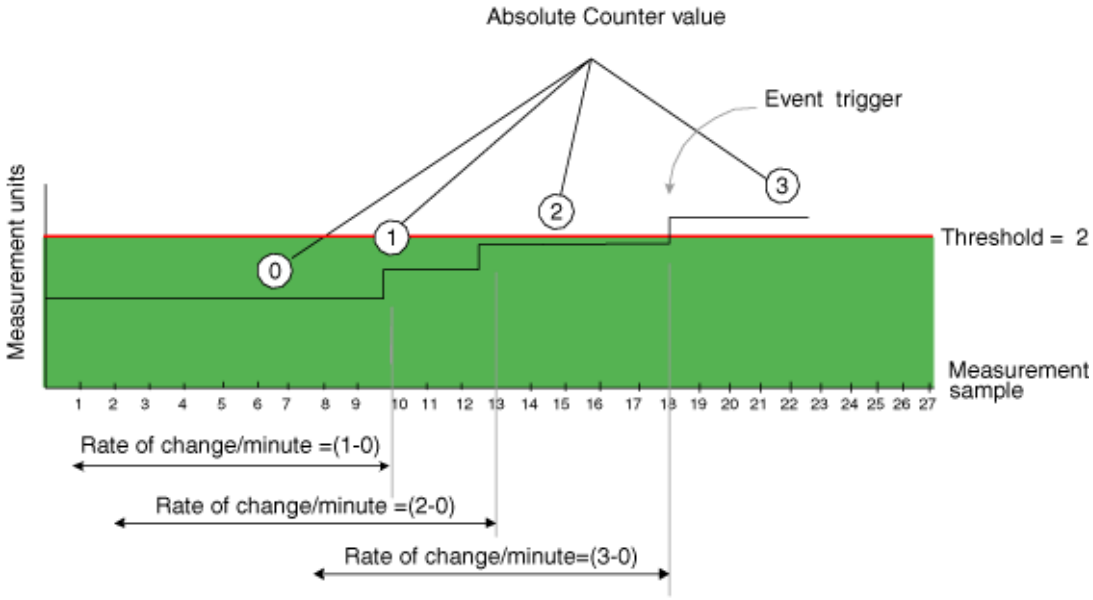
- Fabric Watch triggers an event only if the difference in the data value exceeds the preset threshold boundary limit.
- Even if the current data value exceeds the threshold, Fabric Watch does not trigger an event if the rate of change is below the threshold limit.

The following examples illustrate each point.

Example1: Triggering an Event

Figure 2-4 shows a sample graph of data obtained by Fabric Watch (the type of data is irrelevant to the example). A high threshold of 2 is specified to trigger an event. A time base of *minute* is defined. An event occurs only if the rate of change in the specific interval (one minute in this example) is across the threshold boundary. It should be either higher than the high threshold limit or lower than the low threshold limit. As illustrated on the tenth sample, the counter value changes from 0 to 1; hence calculated rate of change is 1 per minute. At the thirteenth sample, the rate of change is 2 per minute. The rate of change must be at least 3 per minute to exceed the event-triggering requirement of 2, which is met on the eighteenth sample.

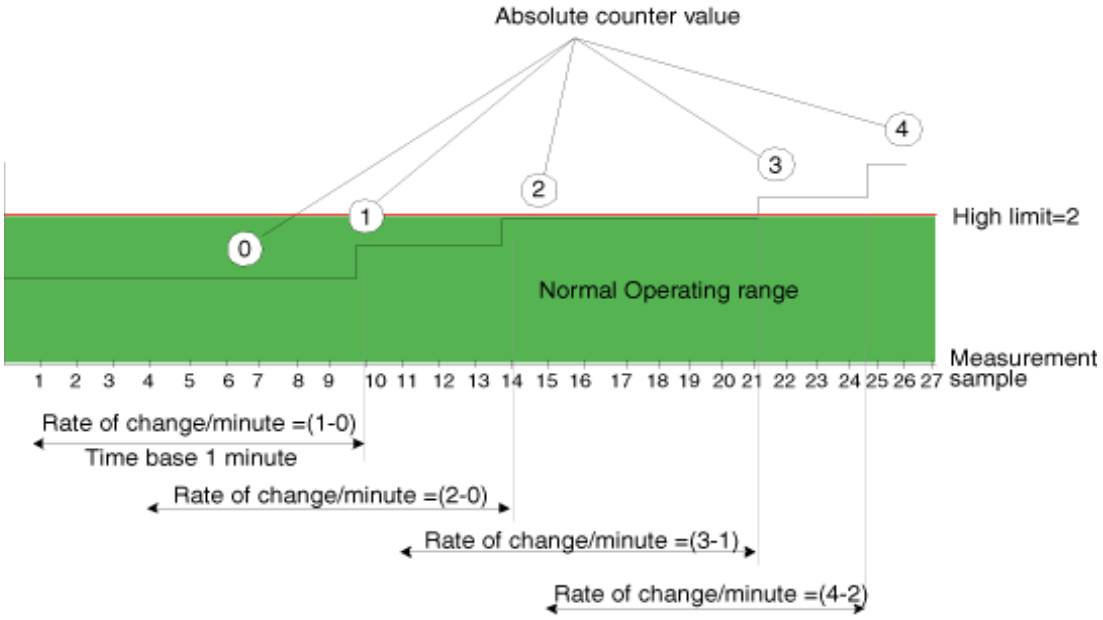
Figure 2-4 Event Trigger



Example 2: Not Triggering an Event

Figure 2-5 uses the same data to illustrate a case in which a threshold is exceeded without triggering an event. In this case, the calculated rate of change in the data value is always less than or equal to the high threshold of 2. At the tenth sample, the rate of change is one per minute. At the fourteenth, twenty-first, and twenty-fifth sample, the rate of change remains equal to the high threshold of 2. In this case, Fabric Watch does not trigger an event even though the absolute value of the counter reaches 4, which is well above the high threshold.

Figure 2-5 Example Without an Event



Event Settings

This section describes how Fabric Watch compares a fabric element's data value against a threshold value to determine whether or not to trigger an event. It describes how a specified buffer zone impacts event triggering.

Fabric Watch monitors data values for one of the following conditions:

- "Above Event Triggers" next
- "Below Event Trigger," on page 2-14
- "Changed Event Trigger," on page 2-14
- "In-Between Triggers," on page 2-15

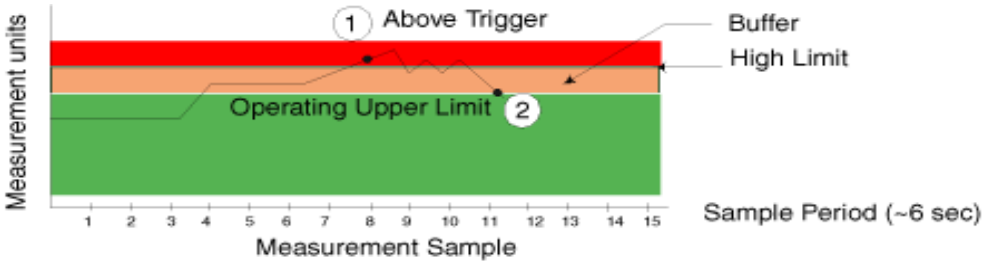
For Fabric Watch to monitor these conditions, the alarm setting must be set to a non-zero value.

Above Event Triggers

Use the Above event trigger for an element that requires only high threshold monitoring. In the Above event trigger, Fabric Watch triggers an event immediately after the data value becomes greater than the high threshold.

Define a buffer zone within the operational limit of an area to suppress multiple events when the counter value fluctuates above the high threshold and buffer zone. Figure 2-6 shows an Above event trigger with a buffer zone.When a buffer is used, the data value must be greater than the sum of the high threshold and the buffer value (event 1 in Figure 2-6). When the data value becomes less than the high threshold again, Fabric Watch triggers a second event (event 2) to indicate that it has returned to normal operation.

Figure 2-6 Above Event Trigger with Buffer Zone



Below Event Trigger

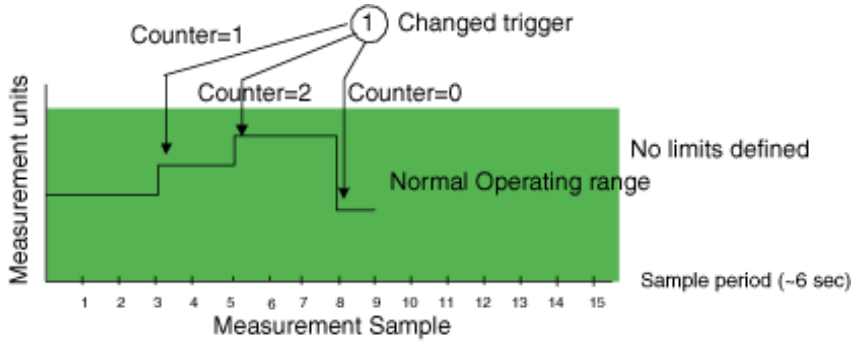
The Below event trigger generates an event when a data value becomes less than the low threshold boundary.

When a buffer is defined, the data value must be below the buffer value and the low threshold.

Changed Event Trigger

Use the Changed event trigger for an element that requires "rate of change" monitoring. When Fabric Watch detects a change in the counter value between two sample periods (defined by the time base), it triggers an event regardless of high or low threshold settings. Figure 2-7 shows events generated when the data value changes. Each arrow in the figure indicates a generated event.

Figure 2-7 Changed Threshold



Use Changed event triggers with discretion. They are most useful when a change in value is expected to be rare. Monitoring a fabric element that is subject to frequent change generates so many events that it can render it virtually useless. For example, this trigger type is appropriate for FRU failures. It is not appropriate for temperature monitoring.

In-Between Triggers

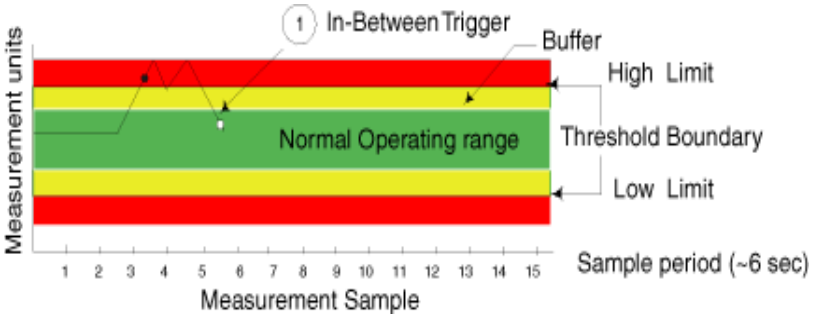
Fabric Watch event triggers are usually set to notify the user of a warning or failure condition, but there is an exception. You can define the In-Between trigger to receive a notification of fault recovery. For example, when measuring port performance, crossing the high threshold triggers an Above threshold event, which displays a warning message. The threshold might be crossed for a period so brief that is not a true cause for an alarm. An In-Between trigger indicates that the port performance has returned to the acceptable range.

Use the In-Between trigger to:

- Verify a successful recovery from a faulty condition.
- Reset the counter value for the next event.
- Identify an element that is consistently operating under marginal condition.

Figure 2-8 illustrates event notification using an In-Between trigger. The arrow marked with one indicates the point at which event notification occurs.

Figure 2-8 In-Between Trigger



Port Persistence

In the case of port monitoring, there is an additional factor to consider. The data collected in port monitoring can vary a lot over short time periods. Therefore, the port can become a source of frequent event messages (the data can exceed the threshold range and return to a value within the threshold range).

Fabric Watch uses port persistence for a port event that requires the transition of the port into a marginal status. Fabric Watch does not record any event until the event persists for a length of time equal to the port persistence time. If the port returns to normal boundaries before the port persistence time elapses, Fabric Watch does not record any event.

The port persistence time is measured in seconds, and can be configured. Configuring the port persistence time to zero disables this feature.

Notification Methods

There are five notification methods available through Fabric Watch, but not all notification methods can be applied to all of the classes. Valid notification methods are represented through the valid alarm matrix.

Fabric Watch provides the following notification methods:

- "Switch Event (Error) Log Entry" next
- "SNMP Trap," on page 2-17
- "RAPITrap," on page 2-17
- "Port Log Lock," on page 2-17
- "Email Alert," on page 2-17

To enable event settings, you must set the associated attribute to a nonzero value between one and thirty one. The exact value you specify determines which event notification method Fabric Watch uses if the event setting criteria is met.

See Also: For details about valid notification methods in the alarm matrix, see "Assigning Notification Methods," on page 2-18.

Switch Event (Error) Log Entry

The switch event (error) log holds up to 1024 entries. This error log stores event information but does not actively send alerts. Use the **ErrShow** command to view the log.

Log entries can also trigger SNMP traps if the SNMP agent is configured. When the SNMP agent is configured to a specific error message level, then error messages at that level triggers SNMP traps. For information on configuring the SNMP agent using the **agtCfgSet** command, see the *Fabric OS Command Reference Manual*.

SNMP Trap

The Simple Network Management Protocol (SNMP) performs an operation called a *trap* that notifies a management station (a workstation that runs network management applications using SNMP protocol) when events occur.

You must configure the software to receive trap information from the network device. You must also configure the SNMP agent on the switch to send the trap to the management station using the **agtCfgSet** command. For more information on this command, refer to the *Fabric OS Command Reference Manual.*

An SNMP trap forwards the following information to an SNMP management station:

- Name of the element whose counter registered an event
- Class, area, and index number of the threshold that the counter crossed
- Event type
- Value of the counter that exceeded the threshold
- State of the element that triggered the alarm
- Source of the trap

The trap stores event information but does not actively send alerts. Port changes do not generate SNMP traps.

RAPITrap

RAPITrap is a Fabric Watch alarm that actively alerts you to events. After you enable RAPITrap, Fabric Watch forwards all event information to a designated proxy switch. The host API automatically configures the proxy switch, based on firmware version. The switch forwards the information to a server and alerts the SAN manager to event activity.

Third-party applications that use the Brocade API determine the manner that RAPITrap presents alarms to the user.

Port Log Lock

The port log locks to retain detailed information about an event preventing the information from being overwritten as the log becomes full. This alarm stores event information but does not actively send alerts, which is done automatically when some thresholds are exceeded and an alert is triggered.

See Also: For more information about locking, unlocking, and clearing the port log, refer to the *Fabric OS Command Reference Manual*.

Email Alert

Email alert sends information about a switch event to a specified email address. Email alert can send information about any error from any element, area, and class.

The email specifies the threshold and describes the event, much like an error message. Use the **fwMailCfg** command to configure email alerts.

Note

To send email alerts, the switch must be connected to a DNS server.

Assigning Notification Methods

Specify the particular notification method that you want Fabric Watch to use by assigning it a value. Table 2-10 shows the numerical values for each notification method.

Table 2-10 Numerical Values of Notification Methods

Notification Method	Assigned Value
Error Log Entry	1
SNMP Trap	2
RapiTrap	4
Port Log Lock	8
E-mail Notification	16

To determine the value for the event setting attribute that enables all desired notification methods, add the values assigned to each method. For example, to enable SNMP trap, RapiTrap and email notification, use the value 22, which is equal to the sum of 2, 4, and 16.

Not all notification methods are valid for all areas. Every area has an associated valid alarm matrix, which is the sum of all valid notification methods for that area. For example, an area with a valid alarm matrix of 25 allows the error log entry (1), port log lock (8) and e-mail notification (16) methods, but does not allow the SNMP trap (2) or RapiTrap (4) methods.

An area with a valid alarm matrix of 31 allows all of the notification types.

Switch Policies

Switch policies are a series of rules that define specific states for the overall switch. Fabric OS interacts with Fabric Watch using these policies. Each rule defines the number of types of errors that transitions the overall switch state into a state that is not healthy. For example, you can specify a switch policy so that if a switch has two port failures, it is considered to be in a marginal state; if it has four failures, it is in a down state.

You can define these rules for a number of classes and field replaceable units, including ports, power supplies, flash memory and fans.

See Also: See Chapter 5, “Generating Fabric Watch Reports” to view the current switch policies using the switch policy report.

Interpreting Event Messages

For information on specific error messages generated by Fabric Watch, refer to the *Fabric OS System Error Message Reference Manual.*

Activating and Accessing Fabric Watch

Chapter 3

This chapter contains the following sections:

Activating Fabric Watch

Fabric Watch must be activated on each switch individually before use. Use telnet or Brocade Advanced Web Tools to activate Fabric Watch, as described next. Web Tools offers a user-friendly graphical interface that most users find convenient.

After it is activated, configure Fabric Watch to monitor your system and its health, as described later in this document.

Activating with Telnet

To activate Fabric Watch using telnet commands:

1. Log in as admin.
2. Enter **licenseShow** at the prompt to view a list of activated licenses.

```
swd21:admin> licenseshow
SedQyzdQbdTfeRzZ:
    Web license
    Zoning license
bedR9dyyzzcfeSAW:
    Fabric license
Scy9SbRQd9VdzATb:
    Fabric Watch license
```

   If the Fabric Watch license does not appear in the list, continue to step 3; otherwise, you are ready to use Fabric Watch.

3. Type **licenseAdd "***key***"**, where *key* is the Fabric Watch license key. License keys are case-sensitive, so type the license key exactly as it appears.

```
switch:admin> licenseadd "R9cQ9RcbddUAdRAX"
```

4. To verify successful activation, enter **licenseShow**. If the license does not appear, verify that you typed the key correctly; if you did not, then repeat step 3.

If you still do not see the license, verify that the entered key is valid, and that the license key is correct before repeating step 3.

5. Enter **fwClassinit** to initialize the Fabric Watch classes.

Activating with Advanced Web Tools

To activate Fabric Watch using Web Tools:

1. Launch your Web browser, enter the switch name or the IP address of the switch in the **Address** field (for example, *http://111.222.33.1*), and press **Enter**.

   This launches Web Tools and displays the **Fabric** view.

2. Click the **Admin View** button on the relevant switch panel. The login window appears.
3. Log in as admin.
4. Click the **License Admin** tab.
5. Enter the license key in the **License Key:** field and click **Add License**. This activates Fabric Watch.

Accessing Fabric Watch

This section provides a brief overview of the available user interfaces. Further details about Fabric Watch operations for each interface are provided later in this guide. User interfaces include:

- "Telnet"
- "Advanced Web Tools"
- "SNMP-Based Enterprise Managers"
- "Configuration File"

Telnet

Use a telnet session to:

- Observe the current monitors on a switch with the **fwShow** command.
- Query and modify threshold and alarm configurations (whether default or customized) with the **fwConfigure** command.
- View and configure the FRU module with the **fwFruCfg** command.
- View and configure the e-mail addresses to which event messages are sent with the **fwMailCfg** command.

To establish a telnet session, use the following command, where *switch* represents the name or IP address of the switch:

```
telnet switch
```

When this command is executed, you are prompted for a username and password. To use Fabric Watch, connect using an account with administrative privileges.

Advanced Web Tools

Use Web Tools to:

- View fabric and switch events.
- View and modify threshold and alarm configurations with the Fabric Watch View.
- Upload and download the configuration file with the **Config Admin** tab.
- View and configure the FRU module.
- View and configure the e-mail addresses to which event messages are sent.

To create a connection to Fabric Watch using Web Tools:

1. Open a Web browser.
2. Enter the IP address of the switch into the address field of the Web browser.

   The Web browser should display a screen that includes a window similar to the following:

3. To access Fabric Watch View, click the **Watch** button in this portion of the screen, which appears as follows:

4. When the login window appears, log in as admin.

SNMP-Based Enterprise Managers

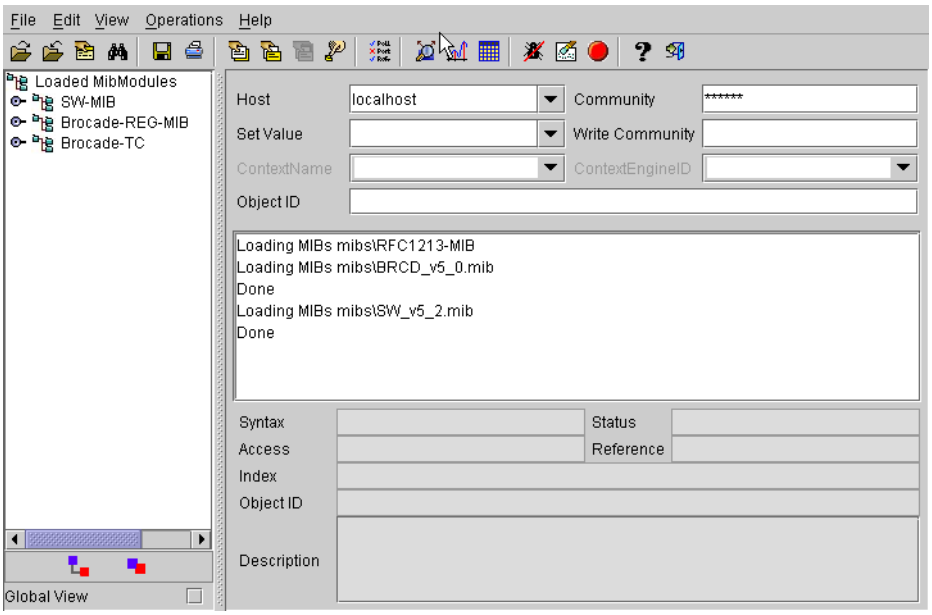
Use SNMP-based enterprise managers to:

- Query the MIB variable for individual fabric and switch elements.
- Query and modify threshold and alarm configurations.
- Receive alarm notification via SNMP traps.
- View and configure the mail database.

Note: The following instructions apply to the AdvantNet MIB browser. There may be some variation in the procedures when other MIB browsers are used.

To configure Fabric Watch with an SNMP-based enterprise manager, begin by connecting to the switch using a MIB browser:

1. Open a MIB browser.
2. If not already done, load the appropriate MIB files. First load the Brocade common MIB file, followed by the Brocade software MIB file. The system should respond with a screen similar to the following:



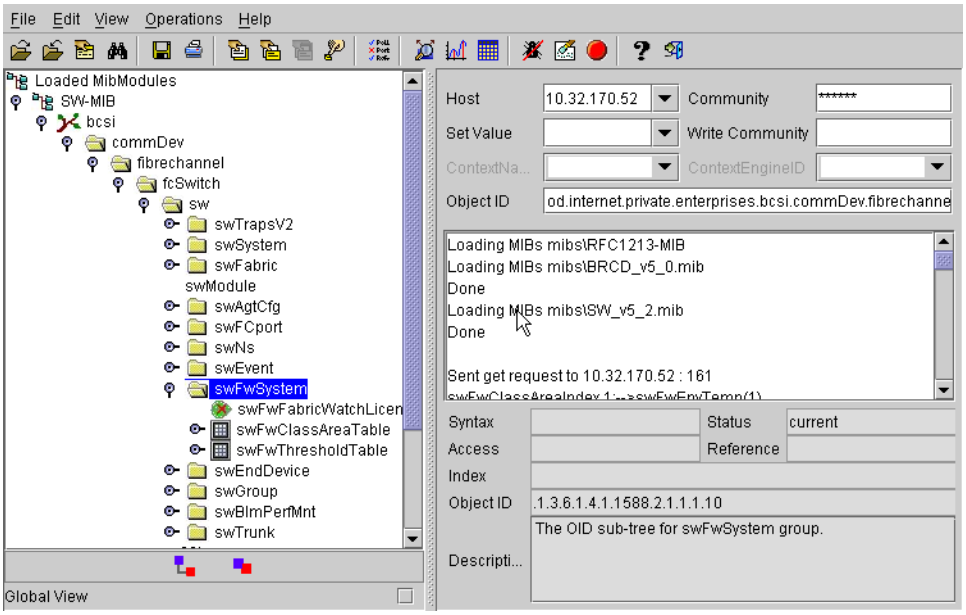
   The MIB browser has populated the left side of the screen with a MIB tree that you can navigate.

3. Begin a telnet session with the switch and issue the **agtCfgSet** command.

   Information on the **agtCfgSet** command may be found in the *Fabric OS Command Reference*.

4. Enter the IP address for the switch into the **Host** field. Enter the community into the **Community** field. Enter the write community into the **Write Community** field, if you want to perform set operations.

5. Drill down through the tree on the left until you find the Fabric Watch OID information:.



Configuration File

Use a configuration file to:

- Upload a configuration file, make changes in a text editor, and download the file to all switches.
- Upload and download the configuration file through a telnet session or with Web Tools. Uploading and downloading a configuration file to multiple switches efficiently populates your SAN with consistent Fabric Watch settings.

See Also: For details about configuration file usage, see Appendix C, “Using Fabric Watch with Configuration Files”.

Configuring Fabric Watch

Chapter 4

This chapter describes the procedures used to configure Fabric Watch and contains the following sections:

See Also: This chapter does not explain Fabric Watch terminology and concepts; refer to Chapter 2, "Fabric Watch Concepts" for these.

Configuring Fabric Watch Thresholds

After it is activated, Fabric Watch starts using a set of default factory settings that might vary from system to system, depending on the software version and the switch hardware. You can create custom threshold configurations to suit to your unique environment.

Both the factory default and user-customized Fabric Watch settings are individually maintained. You cannot change the default values. During Fabric Watch configuration, you can select whether Fabric Watch should use the default or custom settings for monitoring.

Configuring Fabric Watch thresholds enables you to define your own unique event conditions (such as threshold traits, alarms, and email configuration). For example, it is unlikely that you would need to change the default values for Environment class because the hardware has been tested so extensively. However, if you anticipate a need for additional notifications, or you need to better gauge performance because of noticeable congestion on certain ports, you might want to configure the values for some thresholds.

The steps to configure Fabric Watch Thresholds are:

Step 1: Select the Class and Area to Configure

During your planning activities, you should determine exactly what elements or monitors you want to configure, and in which class they reside. After you have made this decision, you need to identify the classes.

To navigate to a specific class and area, use the **fwConfigure** command from a telnet prompt:

1. Log in to the switch as the administrator.
2. Enter **fwConfigure** at the command prompt.
3. The fwConfigure menu, shown in Figure 4-1, appears.

Figure 4-1 fwConfigure Menu

```
swd77:admin> fwconfigure

1  : Environment class
2  : SFP class
3  : Port class
4  : Fabric class
5  : E-Port class
6  : F/FL Port (Optical) class
7  : Alpa Performance Monitor class
8  : EE Performance Monitor class
9  : Filter Performance Monitor class
10 : Security class
11 : Resource class
12 : Quit
Select a class => : (1..12) [12] 5
```

The fwConfigure menu contains 12 menu items. The first 11 items correspond to the classes available for configuration. Item 12, which is the default, exits the fwConfigure application.

4. From the list displayed, enter the number corresponding to the class that you want to configure. For example, if you enter 5, the menu corresponding to the E-Port class (shown in Figure 4-2) appears.

Figure 4-2 E-Port Class Menu

```
1  : Link loss
2  : Sync loss
3  : Signal loss
4  : Protocol error
5  : Invalid words
6  : Invalid CRCS
7  : RXPerformance
8  : TXPerformance
9  : State Changes
10 : return to previous page
Select an area => : (1..10) [10] 7
```

For each class that you select, Fabric Watch provides a list of the areas of the class available for configuration. The final item in the list, which is always the default, returns you to the previous selection screen.

5. Enter the number corresponding to the area that you want to configure, such as **7** for RXPerformance. Fabric Watch displays a list of monitored elements in this area. Figure 4-3 shows the monitored elements in the RXPerformance area menu.

Figure 4-3 RXPerformance Area Menu

```
Index ThresholdName   Port                          CurVal                 Status
          LastEvent   LasteventTime                 LastVal                LastState
================================================================================
8  eportRXPerf008                                8   0 Percentage(%)/min      enabled
  inBetween           Wed Aug 25 01:01:05 2004    0 Percentage(%)/min      Informative
17 eportRXPerf017                               17   0 Percentage(%)/min      enabled
  inBetween           Wed Aug 25 01:01:05 2004    0 Percentage(%)/min      Informative
26 eportRXPerf026                               26   0 Percentage(%)/min      enabled
  inBetween           Wed Aug 25 01:01:11 2004    0 Percentage(%)/min      Informative
27 eportRXPerf027                               27   0 Percentage(%)/min      enabled
  inBetween           Wed Aug 25 01:01:11 2004    0 Percentage(%)/min      Informative
28 eportRXPerf028                               28   0 Percentage(%)/min      enabled
  inBetween           Wed Aug 25 01:01:11 2004    0 Percentage(%)/min      Informative
29 eportRXPerf029                               29   0 Percentage(%)/min      enabled
  inBetween           Wed Aug 25 01:01:11 2004    0 Percentage(%)/min      Informative

1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
Select choice => : (1..5) [5]
```

Table 4-1 describes the column headers in the RXPerformance menu (shown in Figure 4-3).

Table 4-1 Element Listing Information - RXPerformance Area Menu

Heading	Meaning
Index	A numeric identifier assigned to the element
ThresholdName	A string identifier assigned to the element
Port	The user port number
CurVal	The current data value contained by the element
Status	Monitoring status, either enabled or disabled
LastEvent	The last event setting that triggered an event.
LasteventTime	The timestamp of the last triggered event for the element
LastVal	The data value of the element at the time of the last event
LastState	The last detected state of the element

See Also: See Chapter 2, “Fabric Watch Concepts” for more details about classes and areas.

Step 2: Configure Thresholds

After you've identified and selected the appropriate class and areas, you can configure thresholds for those classes and areas. If you want a basic configuration, accept the default configuration settings. Unless you want to accept the basic (default) configuration, or first disable, enable, or refresh all existing thresholds, proceed to option 4, advanced configuration.

Note

There are a variety of reasons. For example, you might have 10 E-Ports to monitor, but you want to monitor only 8 of them because the remaining 2 are experiencing performance problems. If you disable monitoring for an element, Fabric Watch does not display this information for it.

The RXPerformance area menu (Figure 4-3) displays the following five options, which are described in the following sections:

```
1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
```

1. refresh

The **refresh** option redraws the screen with the most recently updated monitoring information. After the screen refreshes, the same five options appear.

2. disable a threshold

To stop monitoring a selected option, use the **disable a threshold** option, as follows:

1. Enter **2** at the command prompt.

   The system generates output similar to that in Figure 4-4, but the output you see varies based on the class and area you selected.

```
1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
Select choice => : (1..5) [5] 2
```

   In Figure 4-4, the numerical values shown in between the brackets (in this case, 8-29) correspond to the index numbers of the elements within the area. The first element is always selected by default.

2. Enter the index number of the element for which Fabric Watch should disable monitoring.

   Fabric Watch redraws the element table with the selected element disabled. The second row of information about the selected element does not appear any more, and the status of the element is set to **disabled** (see Figure 4-4**)**.

Figure 4-4 Disabling a Threshold

```
Select threshold index => : (8..29) [8] 8

Index ThresholdName    Port                          CurVal                  Status
          LastEvent    LasteventTime                 LastVal                 LastState
================================================================================
8 eportRXPerf008       8                           0 Percentage(%)/min     disabled
        inBetween      Wed Aug 25 01:01:05 2004    0 Percentage(%)/min     Informative
17 eportRXPerf017      17                          0 Percentage(%)/min     enabled
        inBetween      Wed Aug 25 01:01:05 2004    0 Percentage(%)/min     Informative
26 eportRXPerf026      26                          0 Percentage(%)/min     enabled
        inBetween      Wed Aug 25 01:01:11 2004    0 Percentage(%)/min     Informative
27 eportRXPerf027      27                          0 Percentage(%)/min     enabled
       inBetween       Wed Aug 25 01:01:11 2004     0 Percentage(%)/min    Informative
28 eportRXPerf028      28                          0 Percentage(%)/min     enabled
       inBetween       Wed Aug 25 01:01:11 2004     0 Percentage(%)/min    Informative
29 eportRXPerf029      29                          0 Percentage(%)/min     enabled
       inBetween       Wed Aug 25 01:01:11 2004     0 Percentage(%)/min    Informative
```

3. enable a threshold

To start monitoring a selected element, use the **enable a threshold** option as follows:

1. Enter **3** at the command prompt.

   The system generates output similar to that in Figure 4-5, but the output you see varies based on the class and area you selected.

   ```
   1 : refresh
   2 : disable a threshold
   3 : enable a threshold
   4 : advanced configuration
   5 : return to previous page
   Select choice => : (1..5) 3
   ```

   The numerical values shown in between the brackets (in this case, 8-29) correspond to the index numbers of the elements within the area. The first element is always selected by default.

2. Enter the index number of the element for which Fabric Watch should enable monitoring.

   Fabric Watch redraws the element table with the selected element enabled. A second row of information about the selected element appears, and the status of the element is set to **enabled**.

Figure 4-5 Enabling a Threshold

```
Select threshold index => : (8..29) [8] 8

Index ThresholdName    Port                          CurVal            Status
          LastEvent    LasteventTime                 LastVal           LastState
================================================================================
8     eportRXPerf008   8                          0 Percentage(%)/min     enabled
          inBetween    Wed Aug 25 01:01:05 2004   0 Percentage(%)/min     Informative
17    eportRXPerf017   7                          0 Percentage(%)/min     enabled
          inBetween    Wed Aug 25 01:01:05 2004   0 Percentage(%)/min     Informative
26    eportRXPerf026   26                         0 Percentage(%)/min     enabled
          inBetween    Wed Aug 25 01:01:11 2004   0 Percentage(%)/min     Informative
27    eportRXPerf027   27                         0 Percentage(%)/min     enabled
          inBetween    Wed Aug 25 01:01:11 2004   0 Percentage(%)/min     Informative
28    eportRXPerf028   28                         0 Percentage(%)/min     enabled
          inBetween    Wed Aug 25 01:01:11 2004   0 Percentage(%)/min     Informative
29    eportRXPerf029   29                         0 Percentage(%)/min     enabled
          inBetween    Wed Aug 25 01:01:11 2004   0 Percentage(%)/min     Informative
```

4. advanced configuration

To customize Fabric Watch monitoring to suit to your environment, use the **advanced configuration** option as follows:

1. Enter **4** at the command prompt.

   The system generates output similar to Figure 4-6. The output you see varies based on the class and area you select. In the Advanced Configuration menu shown here, the output is based on the E-Port class and RXPerformance area.

See Also: See Chapter 2, “Fabric Watch Concepts” for more details about threshold and buffer values.

Figure 4-6 Advanced Configuration Menu

```
1 : refresh
2 : disable a threshold
3 : enable a threshold
4 : advanced configuration
5 : return to previous page
Select choice => : (1..5) [5] 4

Index ThresholdName    BehaviorType    BehaviorInt
    8 eportRXPerf008       Triggered              1
   17 eportRXPerf017       Triggered              1
   26 eportRXPerf026       Triggered              1
   27 eportRXPerf027       Triggered              1
   28 eportRXPerf028       Triggered              1
   29 eportRXPerf029       Triggered              1

Threshold boundary level is set at : Default

                Default        Custom
      Unit    Percentage(%)    Percentage(%)
 Time base        minute        minute
       Low             0             0
      High           100             0
   BufSize             0             0

Threshold alarm level is set at : Default

Errlog-1, SnmpTrap-2, PortLogLock-4
RapiTrap-8, EmailAlert-16

Valid alarm matrix is 31

                Default        Custom
   Changed             0             0
     Below             0             0
     Above             0             0
 InBetween             0             0

1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18]
```

Note

To ensure that your threshold setting configuration takes effect, remember to change the threshold boundary level to Custom using option 3, and then apply the threshold boundary level settings using option 16.

Table 4-2 describes the event behavior of each element in the Advanced Configuration menu.

Table 4-2 Element Listing Information - Advanced Configuration Menu

Heading	Meaning
Index	A numeric identifier assigned to the element
ThresholdName	A string identifier assigned to the element
BehaviorType	Frequency of alarm notifications
BehaviorInt	The element behavior interval, in seconds

The threshold boundary section of the Advanced Configuration menu includes the threshold information for the selected area. It contains two columns, Default (the default settings column) and Custom (the custom settings column), and indicates the current setting.

Fabric Watch displays the units of measurement (Unit), time base (Time base), low threshold (Low), high threshold (High) and buffer size (BufSize) for each column (see Figure 4-7).

In Figure 4-7 a value of 80% is chosen as the custom high value for RXPerformance. The default value is 100%.

Figure 4-7 Customizing High Threshold Boundary for RXPerformance

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 7
Enter high threshold => : (0..100) [0] 80

Index ThresholdName    BehaviorType    BehaviorInt
    8 eportRXPerf008       Triggered             1
   17 eportRXPerf017       Triggered             1
   26 eportRXPerf026       Triggered             1
   27 eportRXPerf027       Triggered             1
   28 eportRXPerf028       Triggered             1
   29 eportRXPerf029       Triggered             1

Threshold boundary level is set at : Default

                Default        Custom
      Unit    Percentage(%)    Percentage(%)
 Time base        minute         minute
       Low             0              0
      High           100             80
   BufSize             0              0

.
.
.
```

Figure 4-8 shows how to change the threshold boundary level to custom so that the new custom value of 80 is the new trigger point. Figure 4-9 shows how to apply the custom value; unless you apply the value, it does not take effect.

Figure 4-8 Changing the Threshold Boundary Level

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 3
1  : Default
2  : custom
Enter boundary level type => : (1..2) [1] 2

Index ThresholdName    BehaviorType    BehaviorInt
    8 eportRXPerf008       Triggered             1
   17 eportRXPerf017       Triggered             1
   26 eportRXPerf026       Triggered             1
   27 eportRXPerf027       Triggered             1
   28 eportRXPerf028       Triggered             1
   29 eportRXPerf029       Triggered             1

Threshold boundary level is set at : Custom
.
.
.
```

Figure 4-9 Applying Threshold Boundary Changes

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 9
.
.
.
```

Table 4-3 describes the event behavior of each element in the Threshold Boundary menu.

Table 4-3 Element Listing Information - Threshold Boundary Menu

Heading	Meaning
Default	The Fabric OS default settings
Custom	User-defined settings

See Also: See Chapter 2, “Fabric Watch Concepts” for details about the event setting table and notification methods for each of the possible event settings.

For details about advanced configuration menu options, see Table 4-4 on page 4-13.

Step 3: Configure Alarms

Alarms act as a signal or alert that notifies you when a threshold has been crossed. You can configure the following types of notification settings for Fabric Watch:

- Triggered
  A triggered behavior type signals you once, after a threshold has been crossed. Triggered is the default behavior type signal for all class areas.
- Continuous
  A continuous behavior type signals you continuously after a threshold has been crossed.

To set an alarm, choose the type of event about which you want to receive notifications:

- Changed
  Triggers an alarm every time the value of what you are monitoring is changed.
- Below
  Triggers an alarm every time the value of what you are monitoring goes below the low boundary.
- Above
  Triggers an alarm every time the value of what you are monitoring goes above the high boundary.
- In-Between
  Triggers an alarm every time the value of what you are monitoring goes in between your low and high threshold boundary.

Figure 4-10 shows how to change the above alarm for the RXPerformance class. Here, a value of 19 is specified. The value is the sum of the alarm matrix values: in this case EmailAlert-16, SnmpTrap-2, and Errlog-1 (16+2+1=19).

To calculate the values to specify in your alarms:

1. Add the numbers beside each state (for the states you want to include). The values for the states are:
   - Errlog - 1
   - SnmpTrap - 2
   - PortLogLock - 4
   - RapiTrap - 8
   - EmailAlert - 16
2. Enter the total at the prompt.

Figure 4-10 Change Above Alarm

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 14

Errlog-1, SnmpTrap-2, PortLogLock-4
RapiTrap-8, EmailAlert-16

Valid alarm matrix is 31
Enter above alarm matrix => : (0..31) [0] 19

Index ThresholdName    BehaviorType    BehaviorInt
    8 eportRXPerf008       Triggered              1
   17 eportRXPerf017       Triggered              1
   26 eportRXPerf026       Triggered              1
   27 eportRXPerf027       Triggered              1
   28 eportRXPerf028       Triggered              1
   29 eportRXPerf029       Triggered              1

Threshold boundary level is set at : Custom

                Default        Custom
      Unit    Percentage(%)    Percentage(%)
 Time base        minute         minute
       Low             0              0
      High           100             80
   BufSize             0              0

Threshold alarm level is set at : Default

Errlog-1, SnmpTrap-2, PortLogLock-4
RapiTrap-8, EmailAlert-16

Valid alarm matrix is 31

                Default        Custom
   Changed            0              0
     Below            0              0
     Above            0             19
```

Figure 4-11 shows how to select the custom settings for the threshold alarm level for the RXPerformance area. The options are either to accept the default settings or provide custom settings.

Figure 4-11 Changing the Threshold Alarm level

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 11
1  : Default
2  : custom
Enter alarm level type => : (1..2) [1] 2

Index ThresholdName    BehaviorType    BehaviorInt
    8 eportRXPerf008       Triggered             1
   17 eportRXPerf017       Triggered             1
   26 eportRXPerf026       Triggered             1
   27 eportRXPerf027       Triggered             1
   28 eportRXPerf028       Triggered             1
   29 eportRXPerf029       Triggered             1

Threshold boundary level is set at : Custom

                 Default        Custom
      Unit    Percentage(%)    Percentage(%)
 Time base        minute         minute
       Low             0              0
      High           100             80
   BufSize             0              0

Threshold alarm level is set at : Custom
.
.
.
```

Figure 4-12 shows how to apply the custom value for the threshold alarm changes; unless you apply the value, it does not take effect.

Figure 4-12 Applying Threshold Alarm Changes.

```
1  : change behavior type             11 : change threshold alarm level
2  : change behavior interval         12 : change changed alarm
3  : change threshold boundary level  13 : change below alarm
4  : change custom unit               14 : change above alarm
5  : change custom time base          15 : change inBetween alarm
6  : change custom low                16 : apply threshold alarm changes
7  : change custom high               17 : cancel threshold alarm changes
8  : change custom buffer             18 : return to previous page
9  : apply threshold boundary changes
10 : cancel threshold boundary changes
Select choice => : (1..18) [18] 16
.
.
.
```

Note

To ensure that your alarm setting configuration is in effect, remember to change the alarm level to Custom and then apply the alarm settings.

Table 4-4 describes the 18 customization options displayed at the end of the Advanced Configuration menu. With the exception of the last option, which exits advanced configuration mode, each option has similar behavior. For each option, one or two lines will appear, prompting you to accept the new setting information, and, after the information has been provided, the entire screen will refresh to display the updated information.

Table 4-4 Advanced Configuration Options

Option	Effect	Input Information
change behavior type	Changes the behavior type of a single element to either Triggered or Continuous. The change is volatile because this option is not saved to flash memory. Every time the switch is rebooted, this option is reset.	The element index and the required behavior type
change behavior interval	Changes the behavior interval for a single element. The change is volatile because this option is not saved to flash memory. Every time the switch is rebooted, this option is reset.	The element index and the required behavior interval, in seconds
change threshold boundary level	Changes between the factory default and custom threshold information.	The required threshold column
change custom unit	Changes the measurement unit assigned to the monitored data values, but only affects the custom column.	The required measurement unit, as a string
change custom time base	Changes the time base for the area, but only affects the custom column.	The required time base

Table 4-4 Advanced Configuration Options (Continued)

Option	Effect	Input Information
change custom low	Changes the low setting for the threshold, but only affects the custom column.	The required low threshold, in the units defined by the area
change custom high	Changes the high setting for the threshold, but only affects the custom column.	The required high threshold, in the units defined by the area
change custom buffer	Changes the buffer size for the threshold, but only affects the custom column.	The required buffer size, in the units defined by the area
apply threshold boundary changes	Confirms the changes made to the threshold information. This must be done to retain the changes made.	None
cancel threshold boundary changes	Returns the boundary information to the last confirmed state.	None
change threshold alarm level	Changes between the factory default and custom event settings for the area.	The required event setting column
change changed alarm	Changes the notification method for changed event occurrences for this method, but only affects the custom column.	The required notification methods
change above alarm	Changes the notification method for above event occurrences for this method, but only affects the custom column.	The required notification methods
change below alarm	Changes the notification method for below event occurrences for this method, but only affects the custom column.	The required notification methods
change inBetween alarm	Changes the notification method for inBetween event occurrences for this method, but only affects the custom column.	The required notification methods
apply threshold alarm changes	Confirms the changes made to the event setting information. This must be done to retain the changes made.	None
cancel threshold alarm changes	Returns the event setting information to the last confirmed state.	None

Note

Not all areas allow for the customization of all fields. If you attempt an illegal modification, Fabric Watch displays an error message. Ensure that all changes to the threshold and event setting areas of the screen are confirmed before leaving advanced configuration, or the changes are lost.

Step 4: Disable and Enable Thresholds by Port (Optional)

On certain occasions, you might want to disable all port thresholds at once. For example, during an event such as an upgrade of a device or server, you might elect not to receive error messages for particular ports. When the upgrade is complete, you can show and enable disabled port thresholds.

To disable all the thresholds for a port, at the command prompt enter:

```
swd77:admin> fwConfigure --disable --port 9
```

When you are ready to enable the disabled port thresholds, you can first view all previously disabled ports using the following command:

```
swd77:admin> fwshow --disable --port

Port     Threshold Status
=========================
 9           disabled
```

A port is not considered disabled if one of the port thresholds is still enabled.

To enable all the thresholds for a port, at the command prompt enter:

```
swd77:admin> fwconfigure --enable --port 9
```

Configuring Notifications

You can be notified of an alarm condition through a notification. The tasks for configuring notifications using Fabric Watch are:

Configuring Alarm Notifications

When you use alarm notifications, error messages are sent to designated locations such as an error log, SNMP trap view, or email. With an error log, you can log in to a particular switch to view the error messages that have been captured for that particular switch. You can parse the log file to make error message searches quicker and easier.

To ensure that notifications appear in the error log, use the following command:

```
swd77:admin> fwAlarmsFilterSet 1
```

The option **1** turns on the alarm notification.

If you decide not to have notifications sent, use the following command:

```
swd77:admin> fwAlarmsFilterSet 0
```

The option **0** turns the alarm notification off.

All alarms are suppressed when alarm notifications are turned off, except for the Environment class and Resource class.

To verify or view your current alarm notifications, use the **fwAlarmsFilterShow** command.

```
swd77:admin> fwalarmsfiltershow
FW: Alarms are enabled
```

Configuring SNMP Notifications

In environments in which you have a high number of messages (for example, hundreds per day) coming from a variety of switches, you might want to receive them in a single location and view them using a graphical user interface (GUI). In this type of scenario, SNMP notifications might be the most efficient notification method. You can avoid having to log on to each switch individually as you would have to do for error log notifications.

SNMP notifications are configured using **snmpMibCapSet**, and within Fabric Watch, using alarms.

See Also: See “Step 3: Configure Alarms” on page 4-10 for details about setting alarms.

For details about SNMP configuration, including traps, see the **agtCfgSet** cand **snmpConFig** ommands in the *Fabric OS Command Reference Manual* and the *Fabric OS Procedures Guide*.

Configuring API Notifications

In the Brocade Fabric OS API, notifications are triggered programatically.

The Brocade Fabric OS API is an application programming interface (API) that provides the method for any application to access critical information about a Brocade SAN. Using Fabric OS API, an application can query or control individual switches or the entire fabric. You can also configure API notifications using the Brocade Fabric OS API.

Configuring Port Log Lock Actions

Port Log Lock freezes in time the port log dump output if an event is triggered. See "Step 3: Configure Alarms" on page 4-10 for details about configuring port log lock actions.

See Also: See Chapter 2, "Fabric Watch Concepts" for more details about port log lock.

Configuring Email Notifications

In environments where it is critical that you are notified about errors quickly, you might want to use email notifications. With email notifications, you can be notified of serious errors via email or a pager, so you can react quickly.

To configure email notifications in a telnet session, enter the **fwMailcCg** command at the prompt. The fwMailcfg menu, shown in Figure 4-13, appears.

Figure 4-13 fwMailcfg Menu

```
1  : Show Mail Configuration Information
2  : Disable Email Alert
3  : Enable Email Alert
4  : Send Test Mail
5  : Set Recipient Mail Address for Email Alert
6  : Quit
Select an item  => : (1..6) [6]
```

The following sections describe how to use the fwMailCfg menu options.

1: Show Mail Configuration Information

1. Enter **1** in the fwMailCfg menu (shown in Figure 4-13) to view the current email configuration classes.

   The config show menu (shown in Figure 4-14) appears.

Figure 4-14 Config Show Menu

```
            Config Show Menu
        ____________________________
        1  : Environment class
        2  : SFP class
        3  : Port class
        4  : Fabric class
        5  : E-Port class
        6  : F/FL Port (Optical) class
        7  : Alpa Performance Monitor class
        8  : End-to-End Performance Monitor class
        9  : Filter Performance Monitor class
        10 : Security class
        11 : Resource class
        12 : FRU class
        13 : Quit
Select an item  => : (1..13) [13]
```

   The Config Show menu lists each class for which you can provide a separate email address.

2. Enter the number corresponding to the class for which the email configuration should be displayed.

Fabric Watch displays information such as:

```
        Mail Recipient Information
       ____________________________________
        Email Alert       = enabled
        Mail Recipient    = sysadmin@mycompany.com
```

The system returns to the main fwMailCfg menu.

2: Disable Email Alert

1. Enter **2** in the fwMailCfg menu (shown in Figure 4-13) to disable email alerts for a specific class.

   The Config Show menu (shown in Figure 4-14) appears.

2. Select a class for which Fabric Watch should disable email alerts.

   The following confirmation message appears:

```
Email Alert is disabled!
```

   The system returns to the main fwMailCfg menu.

3: Enable Email Alert

1. Enter **3** in the fwMailCfg menu (shown in Figure 4-13) to enable email alert for a specific class.

   The Config Show menu (shown in Figure 4-14) appears.

2. Select a class for which Fabric Watch should enable email alerts.

   The following confirmation message appears:

```
Email Alert is enabled!
```

   If the class does not have an email configuration (there is no email address assigned to the class), the following error message appears:

```
Mail configuration for class Environment is not done.
Email Alert is not enabled!
```

   The system returns to the main fwMailCfg menu.

Note

To ensure that the mail server address and domain name are configured correctly, use the **dnsConfig** command. For more details, see the *Fabric OS Command Reference Manual*.

4: Send Test Mail

1. Enter **4** in the fwMailCfg menu (shown in Figure 4-13) to test the mail configuration for a specific class.

   The Config Show menu (shown in Figure 4-14) appears.

2. Select a class to test.

   If the email configuration for the class is complete, the following confirmation message appears:

```
Email has been sent
```

If the email configuration for the class is not complete, the following error message appears:

```
Email has not been sent.
Check Mail configuration for Environment class!
```

The email address specified in the mail configuration receives a test email message.

The system returns to the main fwMailCfg menu.

5: Set Recipient Mail Address for Email Alert

1. Enter **5** in the fwMailCfg menu (shown in Figure 4-13) to specify the recipient to whom Fabric Watch should send the email alert for a class.

   The Config Show menu (shown in Figure 4-14) appears.

2. Select a class.

   The following prompt appears:

   ```
   Mail To: [NONE]
   ```

   Enter the email address of the person responsible for the specific class of alerts.

   Fabric Watch uses the default value, located between the brackets in the prompt, as the current email address for the class. A value of NONE indicates that no email address has been provided.

Note
Email addresses must not exceed 128 characters.

The system displays a confirmation message and returns to the main fwMailCfg menu.

6: Quit

Enter **6** in the fwMailCfg menu (shown in Figure 4-13) to exit the menu.

Configuring Switch Status Policy

The tasks for configuring a switch status policy are:

"Step 1: Plan and Define Your Switch Status Policy" on page 4-20

"Step 2: Implement Your Switch Status Policy" on page 4-21

"Step 3: View Your Switch Status Policy" on page 4-21

Your switch status policy monitors the overall status of a switch based on several contributing parameters. The policy parameter values determine how many failed or faulty units of each contributor are allowed before triggering a status change in the switch from Healthy to Marginal or Down. While some users find that the default settings suit their needs, others need to configure a switch status policy due to unpredictable power outages, temperature changes, or redundancy requirements, among other conditions.

You can configure your switch status policy to define the health of your switch. Generally speaking, Fabric Watch defines the health of your switch using the following terms:

- Healthy
  Every contributor is working and therefore healthy.
- Marginal
  One or more components are triggering a Warning alarm.
- Down
  One or more contributors have failed.

Status events are integrated into Brocade Web Tools and Fabric Manager so that if the overall status of your switch is Healthy, the switch color is green. If the overall switch status is Marginal, then the switch color is yellow. Finally, if the overall switch status is Down, the switch color is red. The overall status is calculated based on the most severe status of all contributors.

See Also: See the *Advanced Web Tools Administrator's Guide* for more details about configuring status events using Web Tools.

Step 1: Plan and Define Your Switch Status Policy

Before entering the **switchStatusPolicySet** command, plan your switch status policy. How many fans must fail before you consider a switch Marginal? Look at the needs of your system along with the factors that affect its monitors. Table 4-5 lists the monitors in a switch and identifies the factors that affect their health. Note that note all switch use the monitors listed in Table 4-5.

Table 4-5 Switch Status Policy Monitor Health Factors

Monitor	Health Factors
Power Supplies	Power supply thresholds, absent or failed power supply. For SilkWorm 24000, can also occur when Power Supplies are not in the correct slot for redundancy.
Temperatures	Temperature thresholds, faulty temperature sensors.
Fans	Fan thresholds, faulty fans.
WWN	Faulty WWN card (applies to modular switches).
CP	Switch does not have a redundant CP (applies to modular switches).
Blade	Faulty blades (applies to modular switches).
Flash	Flash thresholds.
Marginal Ports	Port, E-Port, optical port, and copper port thresholds. Whenever these thresholds are persistently high, the port is Marginal.
Faulty Ports	Hardware-related port faults.
Missing SFPs	Ports that are missing SFP media.

Step 2: Implement Your Switch Status Policy

After planning and defining your switch status policy, enter the **switchStatusPolicySet** command to configure each policy. Each policy has two parameters that can be configured: Marginal and Down. Set the number of units Marginal or Down based on your system requirements for each policy/parameter. The following example shows a switch status policy for Temperature:

```
Bad Temperatures contributing to DOWN status: (0..10) [0] 3
Bad Temperatures contributing to MARGINAL status: (0..10) [0] 1
```

The following example shows a switch status policy for Fans:

```
Bad Fans contributing to DOWN status: (0..3) [0] 2
Bad Fans contributing to MARGINAL status: (0..3) [0] 1
```

Switch status policies are saved in a non volatile memory, and therefore are persistent until changed.

Step 3: View Your Switch Status Policy

After defining and configuring your switch status policy, you can view them using the **switchStatusPolicyShow** command. Note that the policy you defined here determines the output in the Switch Status Policy Report.

See Also: See Chapter 5, “Generating Fabric Watch Reports” for more details about the Switch Status Policy Report.

Configuring FRUs

The configuration of FRUs is an exception to the procedures described thus far in this chapter. FRUs are monitored using state values, as opposed to the quantitative values used to monitor the rest of the fabric. As a result of the qualitative nature of this monitoring, the concept of thresholds does not apply.

To configure FRUs:

1. Establish a telnet connection with a switch.
2. Log in using administrative privileges.
3. Enter the **fwFruCfg** command at the command prompt.

The **fwFruCfg** command displays your current FRU configuration, as shown in Figure 4-15. The types of FRUs are different for the various platforms. In the prompt that follows your current FRU configuration, you are asked to provide values for each FRU alarm state and alarm action. To accept the default value for each FRU (as shown in Figure 4-15), press Return. After you have configured a FRU alarm state and alarm action, the values apply to all FRUs of that type. For example, the values specified for a slot FRU will apply to all slots in the enclosure.

Note

The **fwFruCfg** command does not configure any elements on the SilkWorm 3016.

Figure 4-15 fwFruCfg Configuration

```
swd123:admin> fwfrucfg

The current FRU configuration:
                  Alarm State         Alarm Action
-----------------------------------------------------
           Slot           31                   1
   Power Supply            0                   0
            Fan            0                   0
            WWN            0                   0
Note that the value 0 for a parameter means that it is NOT used
in the calculation

Configurable Alarm States are:
Absent-1, Inserted-2, On-4, Off-8, Faulty-16

Configurable Alarm Actions are:
Errlog-1, E-mail-16
Slot Alarm State: (0..31) [31]
Slot Alarm Action: (0..17) [1]
Power Supply Alarm State: (0..31) [0]
Power Supply Alarm Action: (0..17) [0]
Fan Alarm State: (0..31) [0]
Fan Alarm Action: (0..17) [0]
WWN Alarm State: (0..31) [0]
WWN Alarm Action: (0..17) [0]
Fru configuration left unchanged
```

You can specify triggers for any number of alarm states or alarm actions. The first prompt enables you to select which FRU states trigger events.

To select a group of FRU states:

1. Add the numbers beside each state (for the states you want to include).
2. Enter the total at the prompt

For example, to trigger events using the Absent, Off, and Faulty states, add the assigned values and enter that value at the prompt. In this case, the values are 1, 8, and 16, respectively, and the total is 25.

Configuring Fabric Watch Using Web Tools

To configure Fabric Watch using Advanced Web Tools, see the *Advanced Web Tools Administrator's Guide*.

Configuring Fabric Watch Using SNMP

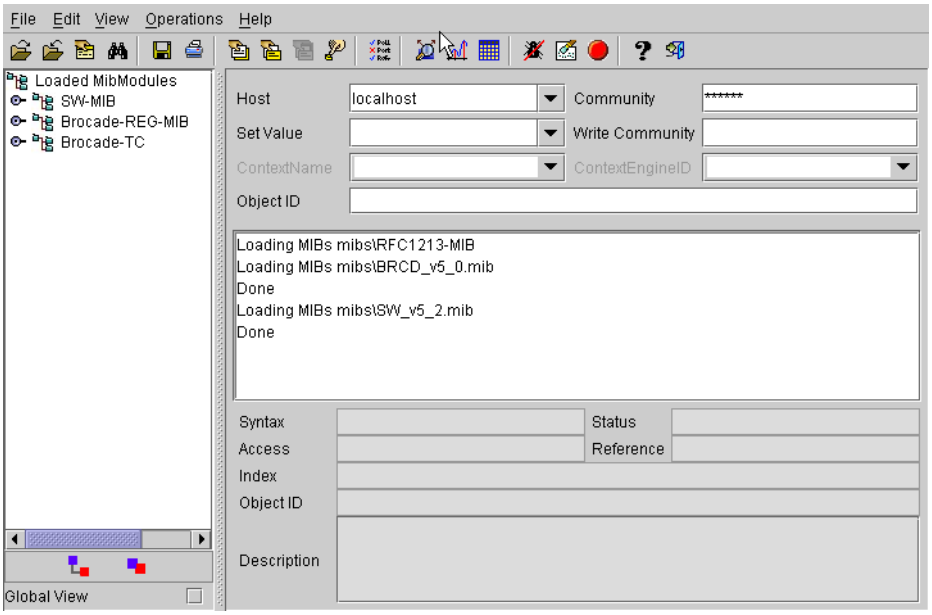
Note

The instructions given in this procedure apply to the AdvantNet MIB browser. The procedure might vary if you use other MIB browsers.

To configure Fabric Watch using SNMP:

1. Open a MIB browser.
2. Load the appropriate MIB files. First, load the Brocade common MIB file (BRCD_v5_0.mib), followed by the Brocade software MIB file (SW_v5_2.mib). If this is successful, the system displays a screen similar to Figure 4-16.

Figure 4-16 Configuring Fabric Watch Using SNMP



In Figure 4-16, the MIB browser has populated the left side of the screen with a MIB tree that can be navigated.

3. Start a telnet session with the switch, and enter the **snmpMibCapSet** command at the prompt; this enables you to send Fabric Watch traps to an SNMP management station (see Figure 4-17). Then enter the **agtCfgSet** command to configure the SNMP management host IP address (see Figure 4-18).

Figure 4-17 Enabling Fabric Watch Traps in SNMP

```
swd77:admin> snmpmibcapset
The SNMP Mib/Trap Capability has been set to support
FE-MIB
SW-MIB
FA-MIB
SW-TRAP
FA-TRAP
FA-MIB (yes, y, no, n): [yes]
FICON-MIB (yes, y, no, n): [no]
HA-MIB (yes, y, no, n): [no]
SW-TRAP (yes, y, no, n): [yes] yes
   swFCPortScn (yes, y, no, n): [no]
   swEventTrap (yes, y, no, n): [no]
   swFabricWatchTrap (yes, y, no, n): [no] yes
   swTrackChangesTrap (yes, y, no, n): [no]
FA-TRAP (yes, y, no, n): [yes]
   connUnitStatusChange (yes, y, no, n): [no]
   connUnitEventTrap (yes, y, no, n): [no]
   connUnitSensorStatusChange (yes, y, no, n): [no]
   connUnitPortStatusChange (yes, y, no, n): [no]
SW-EXTTRAP (yes, y, no, n): [no]
swd77:admin>
```

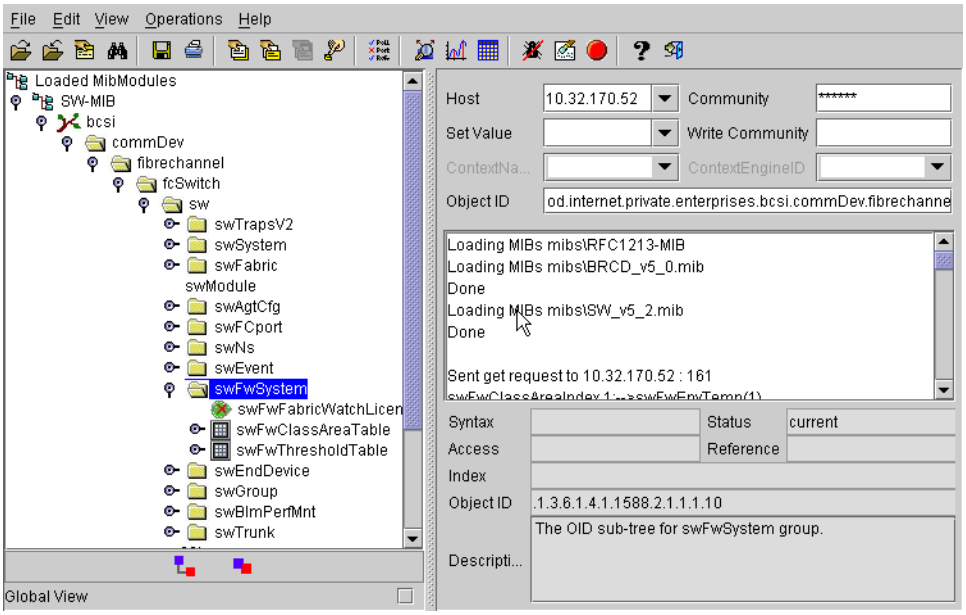
Figure 4-18 Configuring SNMP Management Host IP Address

```
swd77:admin> agtcfgset

Customizing MIB-II system variables ...

At each prompt, do one of the following:
  o <Return> to accept current value,
  o enter the appropriate new value,
  o <Control-D> to skip the rest of configuration, or
  o <Control-C> to cancel any change.

To correct any input mistake:
<Backspace> erases the previous character,
<Control-U> erases the whole line,
sysDescr: [Fibre Channel Switch.]
sysLocation: [End User Premise.]
sysContact: [Field Support.]
authTrapsEnabled (true, t, false, f): [false]

SNMP community and trap recipient configuration:
Community (rw): [Secret C0de]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (rw): [private]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (ro): [public]
Trap Recipient's IP address in dot notation: [0.0.0.0] 192.168.2.2
Trap recipient Severity level : (0..5) [0]
Community (ro): [common]
Trap Recipient's IP address in dot notation: [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address in dot notation: [0.0.0.0]

SNMP access list configuration:
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
Access host subnet area in dot notation: [0.0.0.0]
Read/Write? (true, t, false, f): [true]
.
.
.
Committing configuration...done.
swd77:admin>
```

4. Enter the IP address for the switch in the Host field. Enter the community string in the Community field. To perform set operations, enter the write community into the Write Community field.
5. Expand the tree on the left to find the Fabric Watch OID information. To find the OID, use the following hierarchy: SW-MIB, bcsi, commDev, fibrechannel, fcSwitch, sw, swFwSystem.

   Fabric Watch displays a screen similar to the one shown in Figure 4-19.

Figure 4-19 Example OID Tree

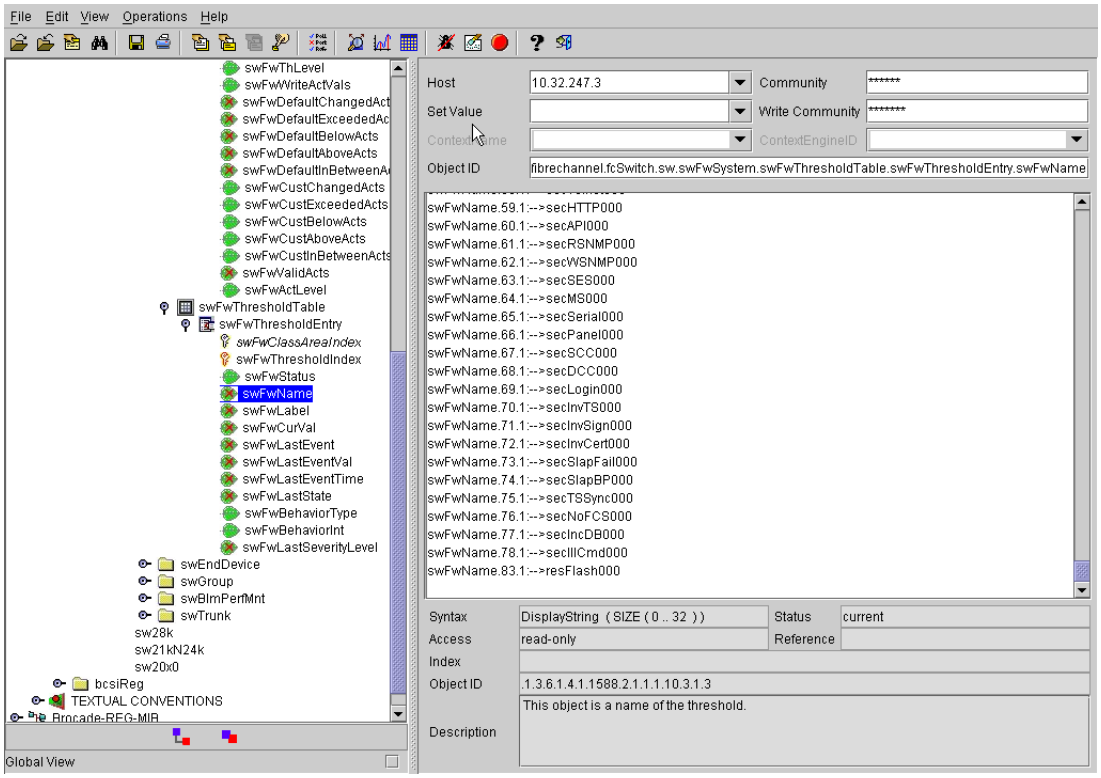


6. Obtain the specific identifier for the element that will be modified. To get the identifier, click the swFwThresholdTable and swFwThresholdEntry directory, and run a get operation on swFwName. A list of elements appears in which each element is preceded by an identifier. Remember the numeric portion of the identifier, which appears before the "==>" symbol. You can scroll through the list to find the numeric identifier for the element in which you are interested.

   Figure 4-19 shows a sample screen.

   See Also: For detailed descriptions of the SNMP fields in both telnet and Web Tools, see the *Fabric OS MIB Reference Manual*.

Figure 4-20 Example swFwName Screen



In this example, 83.1 is numeric identifier for the element referenced as resFlash000.

7. Traverse the fields beneath swFwClassAreaTable and swFwThresholdTable, appending the numeric identifier from the previous step to each field before performing a get or write operation. For example, to get and modify information specific to the resFlash000 element, select one of the fields and append “83.1” in the Object ID field on the right side of the screen.

   To modify information, you must define a write community. To modify an entry:

   a. Select a field.

   b. Append the numeric identifier to the Object ID.

   c. Enter the new value into the Set Value field.

   d. Select **Set** from the Operations menu.

Generating Fabric Watch Reports

Chapter 5

This chapter describes the basic Fabric Watch reports that you can generate through a telnet connection or by using Advanced Web Tools. This chapter contains the following sections:

Types of Fabric Watch Reports

You can run reporting commands in Fabric Watch to get instant access to switch information. Although the **switchShow** command provides basic switch information, the Fabric Watch reports provide detailed information and enable you to track marginal or faulty ports that can affect throughput or the switch performance.

You can run reports on the command line using a telnet session, or by using Advanced Web Tools (if you have installed a Web Tools license). Both tools generate reports that contain the same information, but is presented differently.

The examples in this chapter use the command line interface.

You can generate the following types of reports using Fabric Watch:

SAM Report

The switch availability monitor (SAM) report lets you see the uptime and downtime for each port. It also enables you to check if a particular port is failing more often than the others. The following is an example of a SAM report.

Example: SAM Report

```
                              Total       Total       Down        Total
Port#                 Type    Up Time     Down Time   Occurrence  Offline T
                              (Percent)   (Percent)   (Times)     (Percent)
=========================================================================
  0                 E_PORT      99          0           0           0
  1                 L_PORT     100          0           0           0
  2                 U_PORT       0          0           0         100
  3                 U_PORT       0          0           0         100
  4                 U_PORT       0          0           0         100
  5                 U_PORT       0          0           0         100
  6                 U_PORT       0          0           0         100
  7                 U_PORT       0          0           0         100
  8                 U_PORT       0          0           0         100
  9                 U_PORT       0          0           0         100
 10                 U_PORT       0          0           0         100
 11                 U_PORT       0          0           0         100
 12                 U_PORT       0          0           0         100
 13                 U_PORT       0          0           0         100
 14                 U_PORT       0          0           0         100
 15                 U_PORT       0          0           0         100
 16                 U_PORT       0          0           0         100
```

Table 5-1 describes the fields in the SAM report.

Table 5-1 SAM Report Information

Heading	Meaning
Total Up Time (Percent)	The percentage of time that the port is active
Total Down Time (Percent)	The percentage of time that the port experiences faults
Down Occurrence (Count)	The number of faults experienced on the port
Total Offline Time (Percent)	The percentage of time that the port is inactive for reasons other than a fault.

Switch Health Report

The switch health report lists

- Current health of each port, based on the currently configured policy settings.
- High-level state of the switch as well as power supplies, fans, and temperatures.
- All ports that are in an abnormal state and indicates the current health state of each port.

The switch health report is available even without Fabric Watch, but for licensed Fabric Watch users, the marginal and faulty ports are included in the report. The following is an example of a switch health report.

Example: Switch Health Report

```
Switch Health Report                          Report time: 01/16/2004 10:53:55 AM
Switch Name:    swd21
IP address:     10.32.243.21
SwitchState:    HEALTHY
Duration:       23:14

Power supplies monitor  HEALTHY
Temperatures monitor    HEALTHY
Fans monitor            HEALTHY
Flash monitor           HEALTHY
Marginal ports monitor  HEALTHY
Faulty ports monitor    HEALTHY
Missing SFPs monitor    HEALTHY


All ports are healthy
```

The final portion of the report, detailing port health, is not available without a Fabric Watch license.

Switch Status Policy Report

The switch status policy report lets you see the current policy parameters. Run the **switchStatusPolicyShow** command to generate a switch status policy report.

The following is an example of the **switchStatusPolicyShow** command for nonmodular switches such as the Brocade SilkWorm 3250, 3850, 3900, and 4100. The SilkWorm 3016 output is similar to that of other non-modular switches, except it does not show data for the power supplies or fan (since it doesn't have either).

For modular switches such as the Brocade SilkWorm 12000 and 24000, the switch status policy report also contains information on the WWN, Blade, and CP.

Example: Switch Status Policy Report

```
The current overall switch status policy parameters:
                  Down    Marginal
 ---------------------------------
     PowerSupplies  2         2
      Temperatures  2         1
              Fans  2         1
             Flash  0         1
     MarginalPorts  2         1
       FaultyPorts  2         1
       MissingSFPs  0         0
```

Port Detail Report

If the switch health report shows marginal throughput or decreased performance, use the port detail report to see statistics on each port. The port detail report is a Fabric Watch licensed product.

The following is an example of a port detail report. An "X" in the column for a condition indicates that the condition has exceeded the threshold.

Example: Port Detail Report

```
Port Detail Report                          Report time: 01/16/2004 11:12:28 AM
Switch Name:    swd21
IP address:     10.32.243.21
Port Exception report [by All]

                            --------Port-Errors------------ -----SFP-Errors----
Port# Type  State    Dur(H:M) LFA LSY LSI PER INW CRC PSC BLP STM SRX STX SCU SV0
-------------------------------------------------------------------------------
000    E   HEALTHY   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
001    L   HEALTHY   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
002    U   MARGINAL  062:11   -   -   -   -   -   -   -   -   X   -   -   -   -
003    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
004    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
005    U   MARGINAL  062:11   -   -   -   X   -   -   -   -   -   -   -   -   -
006    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
007    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
008    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
009    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
010    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
011    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
012    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
013    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
014    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
015    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
016    U   OFFLINE   062:11   -   -   -   -   -   -   -   -   -   -   -   -   -
```

Table 5-2 lists and describes each item in the port detail report.

Table 5-2 Port Detail Report Columns

Report Item	Description
LFA	Link Loss: the number of link loss occurrences out of range for time period
LSY	Sync Loss: the number of sync loss occurrences out of range for time period
LSI	Signal Loss: the number of signal loss occurrences out of range for time period
PER	Protocol Error: the number of protocol errors out of range for time period
INW	Invalid word. The number of invalid words out of range for time period
CRC	Invalid CRC: the number of CRC errors out of range for time period
PSC	Port hardware state changed too often due to fabric reconfiguration
BLP	Buffer limited port: the switch status changes when a port is in a buffer limited mode based on the switch status policy.
STM	SFP temperature is out of specifications

Table 5-2 Port Detail Report Columns (Continued)

Report Item	Description
SRX	SFP receive power is out of specifications
STX	SFP transmit power is out of specifications
SCU	SFP current is out of specifications
SVO	SFP voltage is out of specifications

Viewing Fabric Watch Reports

You can view Fabric Watch reports in the following ways:

- "Viewing Fabric Watch Reports Using Telnet" next
- "Viewing Fabric Watch Reports Using Web Tools," on page 5-5

Viewing Fabric Watch Reports Using Telnet

To view Fabric Watch reports using telnet, start a telnet session and enter the command (from Table 5-3) corresponding to the report you want to view.

Table 5-3 Telnet Commands for Viewing Fabric Watch Reports

Use the Command	To View
fwSamShow	Port failure rate report
switchStatusShow	Switch health report
switchStatusPolicyShow	Switch status policy report
fwPortDetailShow	Port detail report

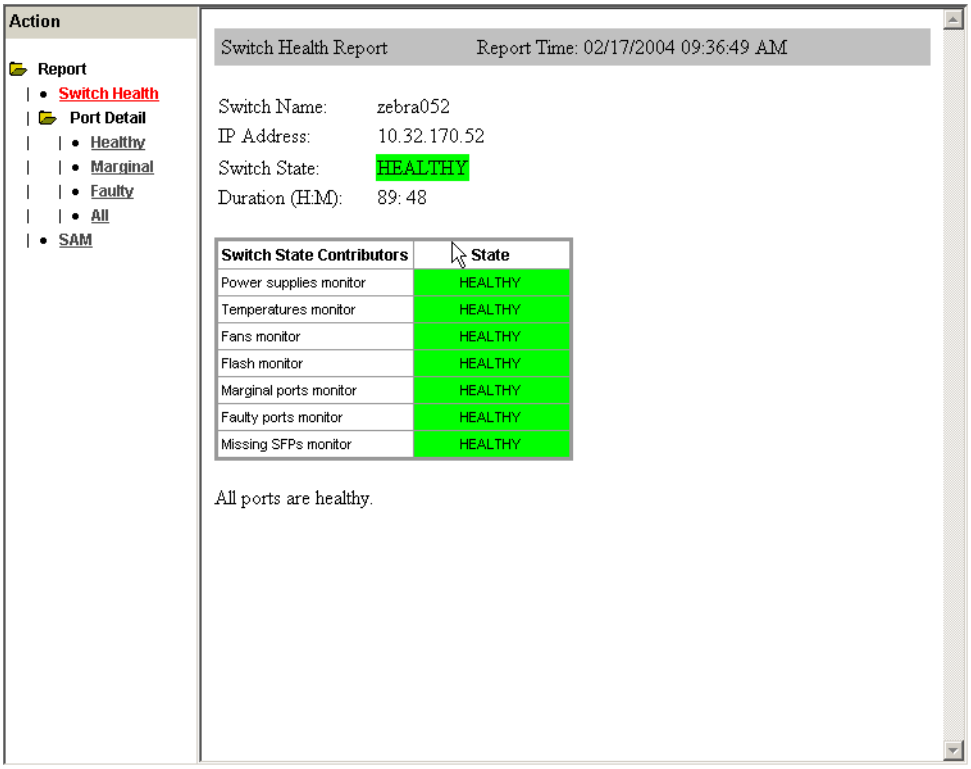
Viewing Fabric Watch Reports Using Web Tools

To view Fabric Watch reports using Advanced Web Tools, connect to a switch using a web browser, and select the report button (shown in Figure 5-1).

Figure 5-1 Report Button

A report view window (shown in Figure 5-2) appears.

Figure 5-2 Report View Window



The Web Tools report view window contains choices to view the switch health, port detail, or SAM report.

Note

The switch status policy report is not available through Web Tools.

Viewing Reports

To view a report, click its name on the left of the report view window.

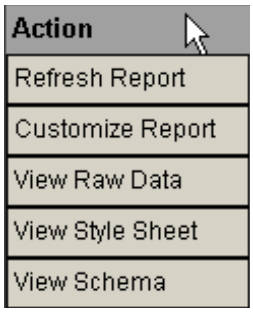
You can use this interface to filter the port detail report based on the current state of the port. You can choose to display the port detail report for all ports or for only the Healthy, Marginal, or Faulty ports.

Customizing Reports

To customize reports, click the Action button above the report tree in the window.

The menu, shown in Figure 5-3, appears.

Figure 5-3 Action Menu



The following section explains the options in the Action menu.

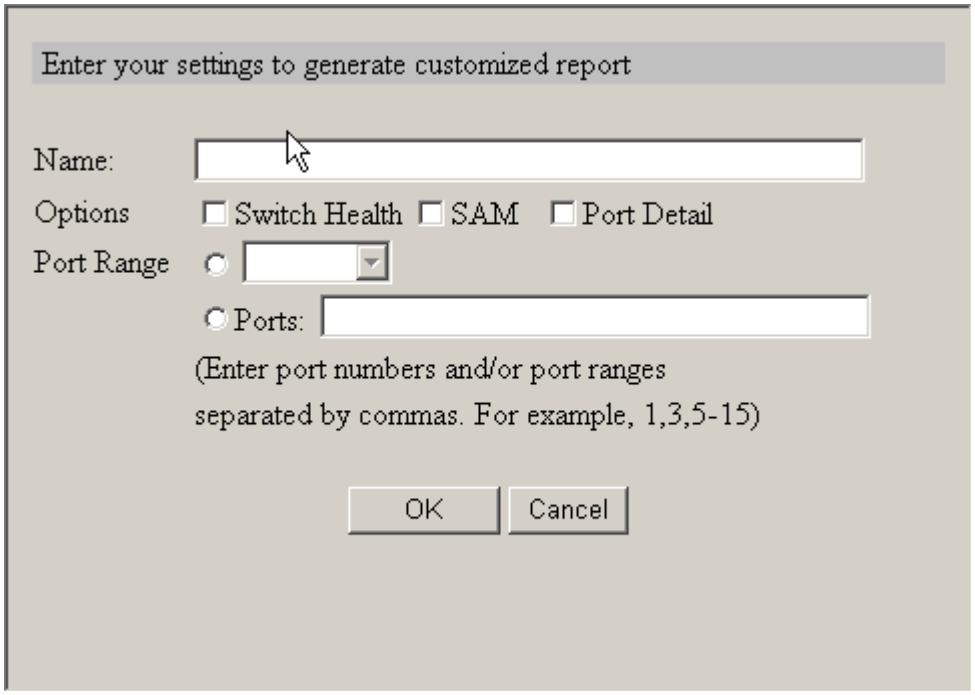
Refresh Report

Use this option to update the current report with the new data.

Customize Report

Use this option to modify the report design. When you select the customize report option, the report customization window (shown in Figure 5-4) appears.

Figure 5-4 Customizing Reports



The report customization window contains the following:

- Name—Enter the report name in this field. The name you enter appears at the top of the report.
- Options—Select the type of report to generate by clicking one of the following options:
  - **Switch Health**
  - **SAM**
  - **Port Detail**

If you select the **Port Detail** option, you can filter the ports for which the report is generated based on port number or port state.

If you filter based on port number, you can enter either the port numbers (separated by commas) or the range of port numbers. To enter a range of ports, enter the first and last ports in the range, separated by a hyphen. Port ranges should be comma-separated from other elements in the list.

If you filter based on port state, Fabric Watch includes only the selected ports in the report.

View Raw Data

Use this option to view the XML source files used to create the report screen.

View Style Sheet

Use this option to view the XML style sheet used to format the report screen.

View Schema

Use this option to view the XML source code.

Appendix

A

Default Threshold Values

This appendix lists Fabric Watch default threshold values for all classes except the FRU class, which has none.

The following tables list all of the default values used for the default Fabric Watch configuration settings when running Fabric OS v4.4.0 on Brocade SilkWorm 3016, 3250, 3850, 3900, 4100, 12000, and 24000 switches. Values for earlier versions may differ. The SilkWorm 3016 does not have fans or power supplies.

Environment Class

Table A-1 provides default settings for areas in the Environment class. These defaults are hardware-dependent. Check the appropriate Hardware Reference Manual for differences in environmental requirements.

Table A-1 Environment Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Fan	Monitors switch fan speed in RPMs	Unit: RPM Time Base: none *SilkWorm 3850 and 3250* Low: 4500 High: 11000 Buffer: 3 *SilkWorm 3900* Low: 2600 High: 10000 Buffer: 3 *SilkWorm 4100* Low: 3000 High: 12000 Buffer: 3 *SilkWorm 12000* Low: 2000 High: 3400 Buffer: 3 *SilkWorm 24000* Low: 1600 High: 3400 Buffer: 3	Changed: 0 Above: 3 Below: 3 In-Between: 1	Informative Out_of_range Out_of_range In_range
Power Supply	Monitors power supply condition	Unit: 1/0 (OK/ FAULTY) Time Base: none The default threshold settings for all platforms are: Low: 1 High: 0 Buffer:0	Changed: 0 Below: 3 Above: 3 In-Between: 0	Informative Out_of_range In_range Informative

Table A-1 Environment Class Threshold Defaults (Continued)

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Temperature	Monitors switch temperature in Celsius	Unit: degrees C Time Base: none *SilkWorm 3016* Low: 0 High: 71 Buffer: 10 *SilkWorm 3850 and 3250* Low: 0 High: 64 Buffer: 10 *SilkWorm 3900* Low: 10 High: 67 Buffer: 10 *SilkWorm 4100* Low:0 High: 60 Buffer: 10 *SilkWorm 12000* Low: 10 High: 75 Buffer: 10 *SilkWorm 24000* Low: 0 High: 75 Buffer: 10	Changed: 0 Below: 3 Above: 3 In-Between: 3	Informative Out_of_range Out_of_range In_range

Fabric Class

Table A-2 provides default settings for areas in the Fabric class. These defaults are hardware-dependent. Check the appropriate Hardware Reference Manual for differences in environmental requirements.

Table A-2 Fabric Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Domain ID Changes	Monitors forcible DOMAIN ID changes	Unit: D_ID Change(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
GBIC Change	Monitors the insertion and removal of GBIC	Unit: change(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Loss of E_Port	Monitors E_Port status	Unit: down(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Fabric Logins	Monitors host device fabric logins	Unit: login(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Fabric to Quick Loop Changes	Monitors changes from Fabric to Quick, Loop, or Quick and Loop to Fabric	Unit: change(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Fabric Reconfiguration	Monitors configuration changes	Unit: reconfig(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Segmentation Changes	Monitors segmentation changes	Unit: segmentation(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
Zoning Changes	Monitors changes to currently enabled zoning configurations	Unit: zone change(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Performance Monitor Class

Table A-3 provides default settings for areas in the AL_PA Performance Monitor class.

Table A-3 AL_PA Performance Monitor Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
AL_PA Invalid CRCs	Monitors the number of arbitrated loop physical address CRC errors	Unit: error(s) Time Base: minute Low: 0 High: 60 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

Note

End-to-end and AL_PA CRC counters are not supported on the Silkworm 4100 platform.

Table A-4 provides default settings for areas in the Customer-Defined Performance Monitor class.

Table A-4 Customer-Defined Performance Monitor Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Customer-Defined Filter	Monitors the number of frames that are filtered out by the port	Unit: frame(s) Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Table A-5 provides default settings for areas in the End-to-End Performance Monitor class.

Table A-5 End-to-End Performance Monitor Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
End-to-End Invalid CRC Count	Monitors the number of CRC errors between a SID_DID pair in a port	Unit: errors Time Base: none Low: 1 High: 10 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
End-to-End Receive Performance	Monitors the receiving traffic between a SID_DID pair in a port	Unit: KB/sec Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
End-to-End Transmit Performance	Monitors the transmit traffic between a SID_DID pair in a port	Unit: KB/sec Time Base: none Low: 0 High: 0 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Port Class

Table A-6 provides default settings for areas in the Port class.

Table A-6 Port Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Invalid CRC Count	Monitors the number of CRC errors	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Transmission Word	Monitors the number of invalid words transmitted	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Signal Count	Monitors the number of signal loss errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

Table A-6 Port Class Threshold Defaults (Continued)

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive Performance	Monitors receive rate, by percentage	Unit: percentage Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: error(s) Time Base: minute Low:0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Transmit Performance	Monitors transmission rate, by percentage	Unit: percentage Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Table A-7 provides default settings for areas in the E-Port class.

Table A-7 E-Port Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Invalid CRC Count	Monitors the number of CRC errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Transmission Word	Monitors the number of invalid words transmitted	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Signal Count	Monitors the number of signal loss errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

Table A-7 E-Port Class Threshold Defaults (Continued)

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive Performance	Monitors the receive rate, by percentage	Unit: percentage Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: error(s) Time Base: minute Low: 0 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Transmit Performance	Monitors the transmit rate, by percentage	Unit: percentage Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative

Table A-8 provides default settings for areas in the F/FL_Port class.

Table A-8 F/FL-Port Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Loss of Synchronization Count	Monitors the number of loss of synchronization errors	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Receive Performance	Monitors the receive rate, by percentage	Unit: percentage Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
State Changes	Monitors state changes	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Transmit Performance	Monitors the transmit rate, by percentage	Unit: percentage Time Base: minute Low: 0 High: 100 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Informative Informative Informative
Invalid CRC Count	Monitors the number of CRC errors	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

Table A-8 F/FL-Port Class Threshold Defaults (Continued)

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Invalid Transmission Word	Monitors the number of invalid words transmitted	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Link Failure Count	Monitors the number of link failures	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Loss of Signal Count	Monitors the number of signal loss errors	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range
Primitive Sequence Protocol Error	Monitors the number of primitive sequence errors	Unit: error(s) Time Base: minute Low: 1 High: 5 Buffer: 0	Changed: 0 Below: 0 Above: 0 In-Between: 0	Informative Informative Out_of_range In_range

Resource Class

Table A-9 provides default settings for areas in the Resource class.

Table A-9 Resource Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Flash	Monitors the percentage of compact flash used	Unit: percentage Time base: none Low: 0 High: 85 Buffer: 0	Changed: 0 Below: 0 Above: 1 In-Between: 0	Informative Informative Out_of_range In_range

Security Class

Table A-10 provides default settings for areas in the Security class.

Table A-10 Security Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
API Violations	Monitors API violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
DCC Violations	Monitors DCC violations	Unit: violation(s) Time Base: minute Low: 1 High: 4 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Front Panel Violations	Monitors front panel violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
HTTP Violations	Monitors HTTP violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Illegal Commands	Monitors illegal commands	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Incompatible Security DB	Monitors incompatible security databases	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Certificates	Monitors invalid certificates	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Invalid Signatures	Monitors invalid signatures	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range

Table A-10 Security Class Threshold Defaults (Continued)

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Invalid Timestamp	Monitors invalid timestamps	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Login Violations	Monitors login violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
MS Violations	Monitors MS violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
No FCS Violations	Monitors No FCS	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
RSNMP Violations	Monitors RSNMP violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
SCC Violations	Monitors SCC violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Serial Violations	Monitors serial violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
SES Violations	Monitors SES violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range

Table A-10 Security Class Threshold Defaults (Continued)

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
SLAP Bad Packets	Monitors SLAP bad packets	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
SLAP Failures	Monitors SLAP failures	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
Telnet Violations	Monitors telnet violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
TS Out of Sync	Monitors instances in which the timestamp is out of sync	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range
WSNMP Violations	Monitors WSNMP violations	Unit: violation(s) Time Base: minute Low: 1 High: 2 Buffer: 0	Changed: 0 Below: 0 Above: 3 In-Between: 0	Informative Informative Out_of_range In_range

SFP Class

Table A-11 provides default settings for areas in the SFP class.

Table A-11 SFP Class Threshold Defaults

Area	Description	Default Threshold Settings	Default Alarm Settings	Threshold State
Current	Monitors SFP current	Unit: mA Time Base: none Low: 0 High: 50 Buffer: 1	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Informative
Receive Power	Monitors receive power in µWatts	Unit: µWatts Time Base: none Low: 0 High: 5000 Buffer: 25	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Informative
Supply Voltage	Monitors SFP electrical force in volt(s)	Unit: mV Time Base: none Low: 3150 High: 3600 Buffer: 10	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Informative
Temperature	Monitors SFP Temperature	Unit: degrees C Time Base: none Low: -10 High: 85 Buffer: 3	Changed: 0 Below: 1 Above: 1 In-Between: 1	Informative Out_of_range Out_of_range Normal
Transmit Power	Monitors transmit power in µWatts	Unit: µWatts Time Base: none Low: 0 High: 5000 Buffer: 25	Changed: 0 Below: 1 Above: 1 In-Between: 0	Informative Out_of_range Out_of_range Normal

A

Appendix

B

Basic Fabric Watch Configuration Guidelines

A default Fabric Watch configuration is available for the purpose of saving setup time. As you gain familiarity with Advanced Fabric Watch features, they can be tailored to suit the fabric environment. The custom settings available in Fabric Watch provide an advanced user much needed flexibility of redefining boundary thresholds and alarm notification methods. The basic concept of Fabric Watch is to monitor the health of an element by sampling the status, comparing the sample data, and if found outside the threshold limits notify the user of the event using one or more selected methods. Since Fabric Watch monitors a variety of *classes* and *class elements*, each element with a unique trait must be evaluated prior to defining custom thresholds to meet a specific objective. This section discusses some of the changes that one should consider implementing to improve the overall efficiency of Fabric Watch.

Customization is recommended to achieve the following objectives.

- Selecting appropriate message delivery method for critical and non–critical events.
- Selecting appropriate thresholds and alarm levels relevant to each class element.
- Defining the appropriate Time Base event triggering based on the class element traits.
- Eliminating message delivery that has little or no practical value to the SAN administrator.
- Consolidating multiple messages, generated from a single event.

When Fabric Watch is improperly configured, a large number of error messages can be sent over a short period of time, making it difficult to find those messages that are actually meaningful. If this happens, there are a few simple ways to improve the configuration.

When a large number of messages are sent that are not of importance, the source of the messages can be identified from the error message. Examining error messages for the source can identify those classes which need to be reconfigured.

When the messages are not desired or not of importance, consider the following options for reconfiguration.

Recheck the threshold settings. If the current thresholds are not realistic for the class and area, messages may be sent frequently without need. For example, a high threshold for temperature monitoring set to less than room temperature is probably incorrectly configured.

If the event setting is continuous, consider switching to triggered. A continuos event setting will cause error messages to be sent repeatedly as long as the event conditions are met. While each message may be meaningful, a high volume of these messages could cause other important messages to be missed.

Examine the notification settings. If you are not interested in receiving messages under certain conditions, ensure that the notification setting for that event is set to zero. For example, you may not be interested in knowing when the sensed temperature is between your high and low temperature settings, so setting the InBetween notification setting to zero for this area will eliminate messages generated in this situation.

B

Appendix

C

Using Fabric Watch with Configuration Files

When you activate Fabric Watch, the software starts, using the default settings described in Appendix B, “Basic Fabric Watch Configuration Guidelines”. You cannot alter these default settings; if the default values do not suit your specific needs, configure Fabric Watch to use more appropriate settings.

When you configure the new settings for Fabric Watch, your switch stores the settings in the configuration file. If you change or add settings directly into the configuration file, those settings become your custom configuration.

This chapter discusses the two methods for configuration file usage:

Configuration Files

You can manually edit the configurations files to ensure that the settings meet your needs.

To custom configure Fabric Watch with the configuration file:

1. Type **configUpload** to upload your configuration file to your host.
2. Use a text editor to edit the Fabric Watch values for the elements you want to change.
3. Type **configDownload** to download the updated configuration to your switch.
4. Type **fwConfigReload** to reload the Fabric Watch configuration.

Note

This process is disruptive, as a switch reboot will be required.

Profiles

Brocade provides partial configuration files, or *profiles*, that help you configure Fabric Watch in a way that is most appropriate to your particular SAN needs.

To configure Fabric Watch with a profile:

1. Upload the configuration file to the host by typing **configUpload**.
2. Open one of the profiles that appears on the Brocade Web site at

   http://www.brocade.com/support/mibs_rsh/index.jsp

3. Open your configuration file in a text editor.
4. Copy the contents of the profile and append that information to the **[Configuration]** section of the configuration file.

   The contents of the profile overwrite any duplicate information earlier in the configuration.
5. To download your updated configuration to your switch, enter the **configDownload** command.

Glossary

A

API Application programming interface. A defined protocol that allows applications to interface with a set of services.

B

bandwidth The total transmission capacity of a cable, link, or system. Usually measured in bps (bits per second). May also refer to the range of transmission frequencies available to a link or system. *See also throughput.*

C

CLI Command line interface. Interface that depends entirely on the use of commands, such as through telnet or SNMP, and does not involve a GUI.

compact flash Flash (temporary) memory that is used in a manner similar to hard disk storage. It is connected to a bridging component which connects to the PCI bus of the processor. Not visible within the processor's memory space.

Configuration The way in which a system is set up. May refer to hardware or software.

- **Hardware**: The number, type, and arrangement of components that make up a system or network.
- **Software**: The set of parameters that guide switch operation. May include general system parameters, IP address information, domain ID, and other information. Modifiable by any login with administrative privileges.

May also refer to a set of zones. *See also zone configuration.*

CRC Cyclic redundancy check. A check for transmission errors that is included in every data frame.

D

DLS Dynamic load sharing. Dynamic distribution of traffic over available paths. Allows for recomputing of routes when an Fx_Port or E_Port changes status.

domain ID Unique identifier for all switches in a fabric, used in routing frames. Usually automatically assigned by the principal switch, but can be assigned manually. The domain ID for a SilkWorm switch can be any integer between| 1 and 239. Generally, the default domain ID is 1.

E

E_Port Expansion port. A type of switch port that can be connected to an E_Port on another switch to create an ISL.

error As applies to Fibre Channel, a missing or corrupted frame, time-out, loss of synchronization, or loss of signal (link errors).

exchange The highest level Fibre Channel mechanism used for communication between N_Ports. Composed of one or more related sequences, and can work in either one or both directions.

F

F_Port Fabric port. A port that is able to transmit under fabric protocol and interface over links. Can be used to connect an N_Port to a switch. *See also FL_Port, Fx_Port.*

fabric A Fibre Channel network containing two or more switches in addition to hosts and devices. May also be referred to as a switched fabric. *See also SAN, topology.*

fabric name The unique identifier assigned to a fabric and communicated during login and port discovery.

FCP Fibre channel protocol. Mapping of protocols onto the Fibre Channel standard protocols. For example, SCSI FCP maps SCSI-3 onto Fibre Channel.

FCS switch Fabric Configuration Server Switch. One or more designated SilkWorm switches that store and manage the configuration and security parameters for all switches in the fabric. FCS switches are designated by WWN, and the list of designated switches is communicated fabric-wide. *See also, primary FCS switch.*

FL_Port Fabric loop port. A port that is able to transmit under fabric protocol and also has arbitrated loop capabilities. Can be used to connect an NL_Port to a switch. *See also F_Port, Fx_Port.*

FRU Field-Replaceable Unit. A component that can be replaced on site.

FSPF Fabric shortest path first. Brocade's routing protocol for Fibre Channel switches.

Fx_Port A fabric port that can operate as either an F_Port or FL_Port. *See also F_Port, FL_Port.*

G

G_Port Generic port. A port that can operate as either an E_Port or F_Port. A port is defined as a G_Port when it is not yet connected or has not yet assumed a specific function in the fabric.

I

idle Continuous transmission of an ordered set over a Fibre Channel link when no data is being transmitted, to keep the link active and maintain bit, byte, and word synchronization.

integrated fabric The fabric created by connecting multiple SilkWorm switches with multiple ISL cables, and configuring the switches to handle traffic as a seamless group.

isolated E_Port An E_Port that is online but not operational due to overlapping domain IDs or nonidentical parameters (such as E_D_TOVs). *See also E_Port.*

L

L_Port Loop port. A node port (NL_Port) or fabric port (FL_Port) that has arbitrated loop capabilities. An L_Port can be in one of two modes:

- **Fabric mode**: Connected to a port that is not loop capable, and using fabric protocol.
- **Loop mode**: In an arbitrated loop and using loop protocol. An L_Port in loop mode can also be in participating mode or non-participating mode.

See also non-participating mode, participating mode.

link As applies to Fibre Channel, a physical connection between two ports, consisting of both transmit and receive fibres.

M

.

MIB Management Information Base. An SNMP structure to help with device management, providing configuration and device information.

P

N_Port Node port. A port on a node that can connect to a Fibre Channel port or to another N_Port in a point-to-point connection. *See also NL_Port, Nx_Port.*

name server Frequently used to indicate Simple Name Server. See also *SNS.*

NL_Port Node loop port. A node port that has arbitrated loop capabilities. Used to connect an equipment port to the fabric in a loop configuration through an FL_Port. *See also N_Port, Nx_Port.*

node A Fibre Channel device that contains an N_Port or NL_Port.

non-participating mode A mode in which an L_Port in a loop is inactive and cannot arbitrate or send frames, but can retransmit any received transmissions. This mode is entered if there are more than 127 devices in a loop and an AL_PA cannot be acquired. *See also L_Port, participating mode.*

Nx_Port A node port that can operate as either an N_Port or NL_Port.

P

packet A set of information transmitted across a network.

participating mode A mode in which an L_Port in a loop has a valid AL_PA and can arbitrate, send frames, and retransmit received transmissions. *See also L_Port, non-participating mode.*

PLOGI Port login. The port-to-port login process by which initiators establish sessions with targets.

point-to-point A Fibre Channel topology that employs direct links between each pair of communicating entities. *See also topology.*

primary FCS switch Primary fabric configuration server switch. The switch that actively manages the configuration and security parameters for all switches in the fabric.

R

route As applies to a fabric, the communication path between two switches. May also apply to the specific path taken by an individual frame, from source to destination. *See also FSPF.*

routing The assignment of frames to specific switch ports, according to frame destination.

S

SAN Storage Area Network. A network of systems and storage devices that communicate using Fibre Channel protocols. *See also fabric.*

sequence A group of related frames transmitted in the same direction between two N_Ports.

SilkWorm The brand name for the Brocade family of switches.

SNMP Simple Network Management Protocol. An internet management protocol that uses either IP for network-level functions and UDP for transport-level functions, or TCP/IP for both. Can be made available over other protocols, such as UDP/IP, because it does not rely on the underlying communication protocols.

SNS Simple Name Server. A switch service that stores names, addresses, and attributes for up to 15 minutes, and provides them as required to other devices in the fabric. SNS is defined by Fibre Channel standards and exists at a well-known address. May also be referred to as directory service.

switch Hardware that routes frames according to Fibre Channel protocol and is controlled by software.

switch policies Rules that define specific states for the entire switch.

switch port A port on a switch. Switch ports can be E_Ports, F_Ports, or FL_Ports.

T

throughput The rate of data flow achieved within a cable, link, or system. Usually measured in bps (bits per second). *See also bandwidth.*

topology As applies to Fibre Channel, the configuration of the Fibre Channel network and the resulting communication paths allowed. There are three possible topologies:

- **Point to point**: A direct link between two communication ports.
- **Switched fabric**: Multiple N_Ports linked to a switch by F_Ports.
- **Arbitrated loop**: Multiple NL_Ports connected in a loop.

trap (SNMP) The message sent by an SNMP agent to inform the SNMP management station of a critical error. *See also SNMP*.

U

U_Port Universal port. A switch port that can operate as a G_Port, E_Port, F_Port, or FL_Port. A port is defined as a U_Port when it is not connected or has not yet assumed a specific function in the fabric.

W

well-known address As pertaining to Fibre Channel, a logical address defined by the Fibre Channel standards as assigned to a specific function, and stored on the switch.

workstation A computer used to access and manage the fabric. May also be referred to as a management station or host.

WWN World Wide Name. An identifier that is unique worldwide. Each entity in a fabric has a separate WWN.

Z

zone A set of devices and hosts attached to the same fabric and configured as being in the same zone. Devices and hosts within the same zone have access permission to others in the zone, but are not visible to any outside the zone.

zone configuration A specified set of zones. Enabling a configuration enables all zones in that configuration.

Index